Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones

SECRETARÍA DE LA FUNCIÓN PÚBLICA

Unidad de Gobierno Digital

Noviembre, 2009

1. ÍNDICE

		Pág.
1	**ÍNDICE**	2
2	**DEFINICIONES Y TÉRMINOS**	9
3	**INTRODUCCIÓN**	25
4	**OBJETIVOS**	26
4.1	General	26
4.2	Específicos	26
5	**ÁMBITO DE APLICACIÓN/ALCANCE**	26
6	**MARCO JURÍDICO**	27
7	**PROCESOS EN MATERIA DE TIC**	28
7.1	**DIRECCIÓN**	30
7.1.1	**Establecimiento de la estructura de gobierno de TIC**	30
7.1.1.1	Objetivos del proceso	30
7.1.1.2	Descripción del proceso	31
7.1.1.2.1	Mapa general del proceso	31
7.1.1.2.2	Descripción de las actividades del proceso	33
7.1.1.2.3	Descripción de roles	35
7.1.1.2.4	Descripción de productos	35
7.1.1.3	Indicadores	36
7.1.1.4	Reglas del proceso	36
7.1.1.5	Documentación soporte del proceso	36
7.1.2	**Planeación estratégica de TIC**	38
7.1.2.1	Objetivos del proceso	38
7.1.2.2	Descripción del proceso	39
7.1.2.2.1	Mapa general del proceso	40
7.1.2.2.2	Descripción de las actividades del proceso	41
7.1.2.2.3	Descripción de roles	45
7.1.2.2.4	Descripción de productos	46
7.1.2.3	Indicadores	47
7.1.2.4	Reglas del proceso	47
7.1.2.5	Documentación soporte del proceso	48
7.1.3	**Determinación de la dirección tecnológica**	48
7.1.3.1	Objetivos del proceso	49
7.1.3.2	Descripción del proceso	50
7.1.3.2.1	Mapa general del proceso	50
7.1.3.2.2	Descripción de las actividades del proceso	52
7.1.3.2.3	Descripción de roles	56
7.1.3.2.4	Descripción de productos	56
7.1.3.3	Indicadores	57
7.1.3.4	Reglas del proceso	57
7.1.3.5	Documentación soporte del proceso	57
7.2.	**CONTROL**	58
7.2.1.	**Administración del desempeño de TIC**	**58**
7.2.1.1	Objetivos del proceso	58
7.2.1.3	Descripción del proceso	59
7.2.1.3.1	Mapa general del proceso	59
7.2.1.3.2	Descripción de las actividades del proceso	61
7.2.1.3.3	Descripción de roles	65
7.2.1.3.4	Descripción de productos	65

7.2.1.3	Indicadores	66
7.2.1.4	Reglas del proceso	66
7.2.1..5	Documentación soporte del proceso	67
7.2.2.	**Cumplimiento regulatorio**	68
7.2.2.1	Objetivos del proceso	68
7.2.2.2	Descripción del proceso	69
7.2.2.2.1	Mapa general del proceso	69
7.2.2.2.2	Descripción de las actividades del proceso	71
7.2.2.2.3	Descripción de roles	73
7.2.2.2.4	Descripción de productos	74
7.2.2.3	Indicadores	74
7.2.2.4	Reglas del proceso	75
7.2.2.5	Documentación soporte del proceso	75
7.2.3	**Administración de riesgos de TIC**	**76**
7.2.3.1	Objetivos del proceso	76
7.2.3.2	Descripción del proceso	77
7.2.3.2.1	Mapa general del proceso	77
7.2.3.2.2	Descripción de las actividades del proceso	79
7.2.3.2.3	Descripción de roles	82
7.2.3.2.4	Descripción de productos	83
7.2.3.3	Indicadores	84
7.2.3.4	Reglas del proceso	85
7.2.3.5	Documentación soporte del proceso	85
7.3	**ADMINISTRACIÓN DE PROYECTOS**	**86**
7.3.1	**Administración de portafolio de proyectos de TIC**	86
7.3.1.1	Objetivos del proceso	86
7.3.1.2	Descripción del proceso	87
7.3.1.2.1	Mapa general del proceso	87
7.3.1.2.2	Descripción de las actividades del proceso	89
7.3.1.2.3	Descripción de roles	95
7.3.1.2.4	Descripción de productos	96
7.3.1.3	Indicadores	97
7.3.1.4	Reglas del proceso	97
7.3.1.5	Documentación soporte del proceso	98
7.3.2.	**Administración de proyectos de TIC**	**99**
7.3.2.1	Objetivo general del proceso	99
7.3.2.2	Descripción del proceso	100
7.3.2.2.1	Mapa general del proceso	100
7.3.2.2.2	Descripción de las actividades del proceso	102
7.3.2.2.3	Descripción de roles	108
7.3.2.2.4	Descripción de productos	108
7.3.2.3	Indicadores	112
7.3.2.4	Reglas del proceso	114
7.3.2.5	Documentación soporte del proceso	114
7.4	**ADMINISTRACIÓN DE PROCESOS**	**115**
7.4.1.	**Establecimiento del sistema de gestión de procesos**	**115**
7.4.1.1	Objetivos del proceso	115
7.4.1.2	Descripción del proceso	116
7.4.1.2.1	Mapa general del proceso	116
7.4.1.2.2	Descripción de las actividades del proceso	118
7.4.1.2.2	Descripción de roles	125
7.4.1.2.4	Descripción de productos	126
7.4.1.3	Indicadores	130
7.4.1.4	Reglas del proceso	130
7.4.1.5	Documentación soporte del proceso	131

7.5.	**ADMINISTRACIÓN DE RECURSOS**	**132**
7.5.1.	**Administración financiera de TIC**	**132**
7.5.1.1.	Objetivos del proceso	132
7.5.1.2.	Descripción del proceso	133
7.5.1.2.1	Mapa general del proceso	133
7.5.1.2.2	Descripción de las actividades del proceso	135
7.5.1.2.3	Descripción de roles	139
7.5.1.2.4	Descripción de productos	139
7.5.1.3.	Indicadores	141
7.5.1.4.	Reglas del proceso	141
7.5.1.5	Documentación soporte del proceso	142
7.5.2	**Administración de proveedores**	**143**
7.5.2.1	Objetivos del proceso	143
7.5.2.2.	Descripción del proceso	144
7.5.2.2.1	Mapa general del proceso	144
7.5.2.2.2	Descripción de las actividades del proceso	146
7.5.2.2.3	Descripción de roles	148
7.5.2.2.4	Descripción de productos	148
7.5.2.3	Indicadores	150
7.5.2.4	Reglas del proceso	151
7.5.2.5	Documentación soporte al proceso	151
7.5.3	**Adquisiciones de TIC**	**152**
7.5.3.1	Objetivo del proceso	152
7.5.3.2.	Descripción del proceso	153
7.5.3.2.1	Mapa general del proceso	153
7.5.3.2.2	Descripción de las actividades del proceso	155
7.5.3.2.3	Descripción de roles	157
7.5.3.2.4	Descripción de productos	158
7.5.3.3	Indicadores	159
7.5.3.4	Reglas del proceso	160
7.5.3.5	Documentación soporte al proceso	160
7.6	**ADMINISTRACIÓN DE SERVICIOS**	**161**
7.6.1	**Administración de portafolio de servicios de TIC**	**161**
7.6.1.1	Objetivos del proceso	161
7.6.1.2	Descripción del proceso	163
7.6.1.2.1	Mapa general del proceso	162
7.6.1.2.2	Descripción de las actividades del proceso	164
7.6.1.2.3	Descripción de roles	167
7.6.1.2.4	Descripción de productos	168
7.6.1.3	Indicadores	169
7.6.1.4	Reglas del proceso	169
7.6.1.5	Documentación soporte al proceso	170
7.6.2	**Diseño de servicios de TIC**	**171**
7.6.2.1	Objetivos del proceso	171
7.6.2.2.	Descripción del proceso	172
7.6.2.2.1	Mapa general del proceso	172
7.6.2.2.2	Descripción de las actividades del proceso	174
7.6.2.2.3	Descripción de roles	180
7.6.2.2.4	Descripción de productos	180
7.6.2.3	Indicadores	183
7.6.2.4	Reglas del proceso	184
7.6.2.5	Documentación soporte al proceso	184
7.7	**DESARROLLO Y ADQUISICIÓN DE SOLUCIONES**	**185**
7.7.1	**Administración técnica de adquisiciones**	**185**
7.7.1.1	Objetivo general del proceso	185

7.7.1.2	Descripción del proceso	186
7.7.1.2.1	Mapa general del proceso	186
7.7.1.2.2	Descripción de las actividades del proceso	188
7.7.1.2.3	Descripción de roles	190
7.7.1.2.4	Descripción de productos	191
7.7.1.3	Indicadores	193
7.7.1.4	Reglas del proceso	193
7.7.1.5	Documentación soporte al proceso	195
7.7.2	**Desarrollo de soluciones tecnológicas**	**196**
7.7.2.1	Objetivos del proceso	196
7.7.2.2	Descripción del proceso	197
7.7.2.2.1	Mapa general del proceso	197
7.7.2.2.2	Descripción de las actividades del proceso	200
7.7.2.2.3	Descripción de roles	208
7.7.2.2.4	Descripción de productos	208
7.7.2.3	Indicadores	212
7.7.2.4	Reglas del proceso	212
7.7.2.5	Documentación soporte al proceso	222
7.7.3	**Calidad de soluciones tecnológicas**	**224**
7.7.3.1	Objetivo general del proceso	224
7.7.3.2	Descripción del proceso	225
7.7.3.2.1	Mapa general del proceso	225
7.7.3.2.2	Descripción de las actividades del proceso	227
7.7.3.2.3	Descripción de roles	232
7.7.3.2.4	Descripción de productos	233
7.7.3.3	Indicadores	234
7.7.3.4	Reglas del proceso	234
7.7.3.5	Documentación soporte al proceso	235
7.8	**TRANSICIÓN Y ENTREGA**	**236**
7.8.1	**Administración de cambios**	**236**
7.8.1.1	Objetivos del proceso	236
7.8.1.2	Descripción del proceso	237
7.8.1.2.1	Mapa general del proceso	237
7.8.1.2.2	Descripción de las actividades del proceso	239
7.8.1.2.3	Descripción de roles	244
7.8.1.2.4	Descripción de productos	244
7.8.1.3	Indicadores	246
7.8.1.4	Reglas del proceso	247
7.8.1.5	Documentación soporte al proceso	247
7.8.2	**Liberación y entrega**	**248**
7.8.2.1	Objetivos del proceso	248
7.8.2.2	Descripción del proceso	249
7.8.2.2.1	Mapa general del proceso	249
7.8.2.2.2	Descripción de las actividades del proceso	251
7.8.2.2.3	Descripción de roles	255
7.8.2.2.4	Descripción de productos	255
7.8.2.3	Indicadores	256
7.8.2.4	Reglas del proceso	257
7.8.2.5	Documentación soporte al proceso	259
7.8.3	**Transición y habilitación de la operación**	**260**
7.8.3.1	Objetivos del proceso	260
7.8.3.2	Descripción del proceso	261
7.8.3.2.1	Mapa general del proceso	261
7.8.3.2.2	Descripción de las actividades del proceso	263
7.8.3.2.3	Descripción de roles	265

7.8.3.2.4	Descripción de productos	265
7.8.3.3	Indicadores	266
7.8.3.4	Reglas del proceso	266
7.8.3.5	Documentación soporte al proceso	267
7.8.4	**Administración de la configuración**	**268**
7.8.4.1	Objetivos del proceso	268
7.8.4.2.	Descripción del proceso	269
7.8.4.2.1	Mapa general del proceso	269
7.8.4.2.2	Descripción de las actividades del proceso	271
7.8.4.2.3	Descripción de roles	275
7.8.4.2.4	Descripción de productos	276
7.8.4.3	Indicadores	278
7.8.4.4	Reglas del proceso	278
7.8.4.5	Documentación soporte al proceso	279
7.9.	**OPERACIÓN DE SERVICIOS**	**280**
7.9.1	**Operación de la mesa de servicios**	**280**
7.9.1.1	Objetivos del proceso	280
7.9.1.2	Descripción del proceso	281
7.9.1.2.1	Mapa general del proceso	281
7.9.1.2.2	Descripción de las actividades del proceso	285
7.9.1.2.3	Descripción de roles	291
7.9.1.2.4	Descripción de productos	292
7.9.1.3	Indicadores	293
7.9.1.4	Reglas del proceso	294
7.9.1.5	Documentación soporte al proceso	298
7.9.2	**Administración de servicios de terceros**	**300**
7.9.2.1	Objetivos del proceso	300
7.9.2.2	Descripción del proceso	301
7.9.2.2.1	Mapa general del proceso	301
7.9.2.2.2	Descripción de las actividades del proceso	303
7.9.2.2.3	Descripción de roles	305
7.9.2.2.4	Descripción de productos	306
7.9.2.3	Indicadores	308
7.9.2.4	Reglas del proceso	308
7.9.2.5	Documentación soporte al proceso	308
7.9.3.	**Administración de niveles de servicio**	**309**
7.9.3.1.	Objetivos del proceso	309
7.9.3.2.	Descripción del proceso	310
7.9.3.2.1	Mapa general del proceso	310
7.9.3.2.2	Descripción de las actividades del proceso	312
7.9.3.2.3	Descripción de roles	313
7.9.3.2.4	Descripción de productos	314
7.9.3.3	Indicadores	315
7.9.3.4	Reglas del proceso	316
7.9.3.5	Documentación soporte al proceso	316
7.9.4	**Administración de la seguridad de la información**	**317**
7.9.4.1	Objetivos del proceso	317
7.9.4.2	Descripción del proceso	318
7.9.4.2.1	Mapa general del proceso	318
7.9.4.2.2	Descripción de las actividades del proceso	320
7.9.4.2.3	Descripción de roles	321
7.9.4.2.4	Descripción de productos	321
7.9.4.3	Indicadores	325
7.9.4.4	Reglas del proceso	325
7.9.4.5	Documentación soporte al proceso	334

7.10	**ADMINISTRACIÓN DE ACTIVOS**	**335**
7.10.1	**Administración de dominios tecnológicos**	**335**
7.10.1.1	Objetivos del proceso	335
7.10.1.2	Descripción del proceso	336
7.10.1.2.1	Mapa general del proceso	336
7.10.1.2.2	Descripción de las actividades del proceso	338
7.10.1.2.3	Descripción de roles	340
7.10.1.2.4	Descripción de productos	340
7.10.1.3	Indicadores	341
7.10.1.4	Reglas del proceso	343
7.10.1.5	Documentación soporte al proceso	344
7.10.2	**Administración del conocimiento**	**345**
7.10.2.1	Objetivos del proceso	345
7.10.2.2	Descripción del proceso	346
7.10.2.2.1	Mapa general del proceso	346
7.10.2.2.2	Descripción de las actividades del proceso	348
7.10.2.2.3	Descripción de roles	351
7.10.2.2.4	Descripción de productos	351
7.10.2.3	Indicadores	352
7.10.2.4	Reglas del proceso	354
7.10.2.5	Documentación soporte al proceso	354
7.10.3	**Integración y desarrollo del personal**	**355**
7.10.3.1.	Objetivos del proceso	355
7.10.3.2.	Descripción del proceso	356
7.10.3.2.1	Mapa general del proceso	356
7.10.3.2.2	Descripción de las actividades del proceso	358
7.10.3.2.3	Descripción de roles	362
7.10.3.2.5.	Descripción de productos	363
7.10.3.3	Indicadores	364
7.10.3.4	Reglas del proceso	365
7.10.3.5	Documentación soporte al proceso	365
7.11	**OPERACIONES**	**366**
7.11.1	**Administración de la operación**	**366**
7.11.1.1	Objetivos del proceso	366
7.11.1.2	Descripción del proceso	367
7.11.1.2.1	Mapa general del proceso	367
7.11.1.2.2	Descripción de las actividades del proceso	369
7.11.1.2.3	Descripción de roles	371
7.11.1.2.4	Descripción de productos	371
7.11.1.3	Indicadores	372
7.11.1.4	Reglas del proceso	373
7.11.1.5	Documentación soporte al proceso	373
7.11.2	**Administración de ambiente físico**	**374**
7.11.2.1	Objetivos del proceso	374
7.11.2.2	Descripción del proceso	375
7.11.2.2.1	Mapa general del proceso	375
7.11.2.2.2	Descripción de las actividades del proceso	377
7.11.2.2.3	Descripción de roles	380
7.11.2.2.4	Descripción de productos	380
7.11.2.3	Indicadores	380
7.11.2.4	Reglas del proceso	381
7.11.2.5	Documentación soporte al proceso	381
7.11.3.	**Mantenimiento de infraestructura**	**382**
7.11.3.1.	Objetivos del proceso	382
7.11.3.2.	Descripción del proceso	383

7.11.3.2.2.	Mapa general del proceso	383
7.11.3.2.3.	Descripción de las actividades del proceso	385
7.11.3.2.4.	Descripción de roles	387
7.11.3.2.5.	Descripción de productos	387
7.11.3.3	Indicadores	388
7.11.3.4	Reglas del proceso	389
7.11.3.5	Documentación soporte al proceso	389
8	**ÓRGANOS COLEGIADOS**	391
9	**ANEXOS/FORMATOS**	392
10	**VIGENCIA**	400
11	**EMISOR, FECHA Y FIRMA**	400

2. DEFINICIONES Y TÉRMINOS

CONCEPTO	DEFINICIÓN / SIGNIFICADO
Activo:	Cualquier elemento que tenga valor tangible o intangible para la organización, entre los cuales se encuentran, en forma no limitativa: información en cualquier tipo de soporte, bases de datos, programas de cómputo, bienes informáticos físicos y sistemas de información;
Activos críticos:	Los recursos que podrían degradar la capacidad de la dependencia o entidad para el desempeño de sus funciones cuando se encuentre comprometida su seguridad -integridad, confidencialidad y disponibilidad;
Administrador:	La persona responsable de efectuar el proceso especifico de administración sobre procesos o recursos;
Adquisición:	La obtención de las soluciones tecnológicas que cubran la totalidad de los requerimientos, cabe mencionar que puede ser por compra directa, tercerización, o cualquier otra práctica;
Alineación:	El enfoque de las acciones comunes ligadas efectiva y eficientemente, hacia la obtención de las metas institucionales, estrategias, objetivos y prioridades;
Ambiente de trabajo:	El conjunto de herramientas, utilerías, programas, aplicaciones e información que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, en relación con los accesos y privilegios que tenga asignados por medio de un nombre de usuario y contraseña;
Amenaza:	La causa potencial de un incidente que puede provocar daños a uno o más activos o a la propia dependencia o entidad; es una condición causada por una mala configuración o instalaciones realizadas con opciones por omisión, que permite explotar vulnerabilidades de una entidad atentando contra las propiedades de confidencialidad, disponibilidad e integridad de la información. Causa potencial de un incidente no deseado que puede provocar daños a uno o más activos o a la propia dependencia o entidad;
Análisis de protocolos:	El software que permite conocer los paquetes que conforman la información durante los procesos de comunicación, procesamiento o manipulación de datos, mediante la separación de estas partes;
Análisis de riesgos:	El método analítico de la gestión de riesgos que permite la identificación de vulnerabilidades y amenazas de seguridad, así como la evaluación de la magnitud o impacto de los daños a efecto de determinar dónde sería necesaria la implementación de controles o salvaguardas y la cantidad máxima razonable de recursos que sería necesario invertir.;
Antivirus:	El software especializado diseñado para detectar, eliminar y prevenir virus informáticos en los dispositivos de la red Institucional y los conectados a ésta;
Área administrativa:	La dirección general, dirección de área; subdirección o jefaturas administrativa u homólogos, de la dependencia o entidad;
Arquitectura empresarial:	El Modelo que ayuda a la dirección de TIC a razonar sobre su organización de manera global. La arquitectura captura una amplia variedad de información y la

	relaciona de manera que los responsables de la organización puedan consultarla para identificar problemas o tomar decisiones sobre posibles cambios.
Auditoría de seguridad de la información:	El análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores. Los resultados reportan a los responsables, quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas. Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad;
Autenticación:	El proceso en virtud del cual se constata que un servidor público de una dependencia o entidad de la Administración Pública Federal es el que dice ser y que tal situación es demostrable ante terceros;
Autenticidad:	El proceso mediante el cual se puede constatar si la clave pública de un mensaje de datos corresponde a la clave privada con la cual se firmó, permitiendo que el mensaje pueda ser interpretado, validando que fue realmente creado por el titular de un certificado digital o que está reconociendo como propio su contenido;
Bases de datos:	Un conjunto estructurado de datos, gestionado bajo el control de un manejador de bases de datos, el cual se encarga de controlar el acceso concurrente, evitar redundancia, cumplimiento de las restricciones y reglas de integridad, usar elementos que aceleren el acceso físico a los datos (índices, agrupamientos, funciones de dispersión, etc.), distribuir los bloques del disco del modo más adecuado para el crecimiento y uso de los datos, controlar el acceso y los privilegios de los usuarios, recuperar ante fallas, entre otros;
Biblioteca de programas:	Una colección o conjunto de archivos que contienen código, desarrollados por un mismo fabricante bajo ciertos criterios, mismos que suelen ser compatibles y tener interoperabilidad entre ellos;
Carta de aceptación de un producto:	El documento donde se confirma que se ha aceptado un producto, después de haber cumplido o sobrepasado con los requerimientos que el usuario;
Catálogo de proveedores de la entidad:	El listado que proporciona información de los proveedores autorizados por la Dirección de Administración y Finanzas a través de la Subdirección de Recursos Materiales o sus equivalentes;
Certificado digital:	El mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada; al conjunto de datos firmados electrónicamente que vincula a un servidor público con una clave pública;
Ciclo de vida del proyecto:	El conjunto de fases administrativas por las que pasa un proyecto desde su inicio hasta su finalización;
Cifrar o cifrado:	El proceso de transformar un mensaje para ocultar su contenido, de tal manera que el receptor sea la única persona que pueda recuperar el mensaje original; a la acción que permite mediante técnicas matemáticas codificar un documento electrónico para proteger su confidencialidad y que garantiza la integridad de un documento o mensaje electrónico;

Clave privada:	Los datos que el firmante genera de manera secreta y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha firma electrónica avanzada y el firmante; documento electrónico que genera el uso del algoritmo asimétrico, con esta llave privada se realiza el firmado digital, mismo que codifica el contenido de un mensaje y que sólo debe ser conocido y resguardado por el propietario del par de llaves (pública/privada);
Clave pública:	Los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante; documento electrónico que genera el uso de algoritmo asimétrico y que se publica junto con el certificado digital para cifrar la información que se desea enviar al propietario de la llave privada;
Comité de seguridad:	El grupo de trabajo de participación, creado para entender y ser consultado sobre la actuación de la dependencia y entidad, que se encarga de establecer las políticas e iniciativas de seguridad de la información. El comité estará formado por servidores públicos de diversas áreas. El número de miembros que integran el comité de seguridad, será definido por la dependencia o entidad;
Compilador:	El programa informático que genera lenguaje máquina a partir de un lenguaje de programación;
Confidencialidad:	El principio de seguridad de la información que consiste en asegurar que el acceso al activo únicamente se realiza por los autorizados y a través de los procedimientos establecidos para ello; es uno de los servicios de seguridad en la información, el cual está encaminado a revelar el nivel y el tipo de información únicamente a las entidades autorizadas para acceder a la misma; aseguramiento de que la información es accesible sólo a aquellos servidores públicos autorizados para tener acceso a la misma;
Configuración de red:	Los valores asignados y las opciones habilitadas para la operación de la tarjeta de red de un equipo de cómputo dentro de la red de la dependencia o entidad;
Contraseña:	La serie de caracteres que en conjunto con una cuenta (nombre de usuario) permiten el acceso a los recursos o servicios institucionales, misma que debe ser difícil de generar por todas las personas a excepción del dueño de la cuenta; a la serie de caracteres generada por el usuario que lo identifican y que junto con la clave de acceso, sirve para acceder a las soluciones tecnológicas;
Contrato o pedido:	El documento jurídico a través del cual se formalizan las adquisiciones, arrendamientos o servicios según corresponda;
Control de cambios:	La herramienta utilizada para identificar, documentar, aprobar o rechazar y controlar cambios;
Convenio modificatorio:	El documento por el cual se formaliza cualquier modificación a un contrato o pedido celebrado con anterioridad, el cuál debe suscribirse por las mismas personas que intervinieron en él o por las que los hayan sustituido;
Correo electrónico:	El grupo de tecnologías encaminadas a dar un servicio que agiliza y facilita el intercambio de mensajes, documentos e información;
Cronograma:	Las fechas planificadas para realizar las actividades del proyecto y las fechas planificadas para cumplir los hitos del mismo;
Cuenta:	El identificador único y personal asociado a un solo usuario, mismo que en

	conjunto con una contraseña permite el acceso a recursos o servicios de TIC de la dependencia o entidad;
Datos personales:	La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;
Dependencias:	Las que integran la Administración Pública Federal centralizada en términos de los artículos 1o. y 2o. de la Ley Orgánica de la Administración Pública Federal incluyendo en su caso a sus órganos administrativos desconcentrados;
Desarrollador:	La persona que tiene acceso a la infraestructura o servicios informáticos institucionales de manera autorizada, misma que cuenta con los conocimientos necesarios para diseñar, construir y probar aplicaciones para automatizar la operación Institucional;
Dictamen técnico:	El documento que suscribe el titular del área usuaria o solicitante de un bien o servicio, que forma parte del dictamen de adquisición en el que se detalla el cumplimiento o incumplimiento de cada uno de los requisitos técnicos establecidos en las bases de licitación o invitación;
Dirección tecnológica	La estrategia de TIC que se define por la UTIC en función de los objetivos estratégicos de la dependencia o entidad y que guía la definición de los elementos y el diseño de la arquitectura tecnológica de la misma.
Disponibilidad:	El principio de seguridad de la información, que estipula que el activo puede ser utilizado por los autorizados cuando éstos lo requieran; es uno de los servicios de seguridad en la información, encaminado a mantener los servicios habilitados y listos para su uso en el momento en que sean requeridos por los usuarios;
Documento electrónico gubernamental:	El instrumento que contiene datos y/o información, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, el cual debe hacer uso de la firma electrónica avanzada, lo cual permite autenticar la información que se intercambia entre los servidores públicos de las dependencias y entidades paraestatales; consistentes en acuerdo, acta, atenta nota, carta, circular, dictamen, informe, invitación, memorando, minuta, nota informativa, oficio, solicitud, volante y otros que se definan en la subcomisión de sistemas automatizados de control de gestión, así como los archivos que en su caso se adjunten a éstos;
e-Gobierno:	Concepto que define el uso de las tecnologías de la información y comunicaciones, particularmente el Internet, como una herramienta para mejorar el funcionamiento del gobierno y su relación con el ciudadano, al desarrollar y ofrecer información y servicios públicos digitales para satisfacer sus necesidades. Ahora también es conocido como gobierno digital;
Entidades:	Los organismos descentralizados, las empresas de participación estatal mayoritaria y los fideicomisos públicos que tengan el carácter de entidad paraestatal, a que se refieren los artículos 1o., 3o., 45, 46 y 47 de la Ley Orgánica de la Administración Pública Federal;

Entregable:	El producto, resultado o capacidad para prestar un servicio único y verificable que debe producirse para terminar un proceso, una fase o un proyecto;
Equipo de trabajo:	El conjunto de personas que trabajan directamente en la realización de un proyecto, pudiendo o no de diferentes áreas dentro de la institución;
Escenario de prueba:	Conjunto de elementos para la simulación del ambiente real de trabajo en donde aplicará una solución tecnológica utilizados para determinar el comportamiento de un producto o servicio;
Especificaciones:	El conjunto de características cuantitativas y cualitativas que debe cumplir un proyecto en su producto final, ya sea un producto o servicio;
Estándar CMM:	El Modelo de Capacidad y Madurez o CMM (Capability Maturity Model, por sus siglas en inglés)
Estándar ITIL:	La Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library, por sus siglas en inglés). Es un marco de trabajo de buenas prácticas destinadas a facilitar la entrega de servicios de tecnología de información y comunicaciones que ayuda a las organizaciones a lograr calidad y eficiencia en las operaciones de las unidades de tecnología de información y comunicaciones;
Estructura:	La que define cómo se dividen, agrupan y coordinan formalmente las tareas de trabajo. El diseño de la estructura enfoca elementos clave como: especialización del trabajo, desagregación por departamentos, cadena de mando, tramo de control, centralización y descentralización y formalización;
Extensión:	El sufijo, o nombre adicional que se le da a un archivo tal como ".XXX", el cual caracteriza el formato por el que se genera, donde ".XXX" representa un numero limitado de caracteres alfanuméricos dependiendo del sistema operativo, normalmente tiene tres caracteres pero esto es susceptible de variación;
Fideicomisos públicos no paraestatales:	Los fideicomisos públicos constituidos por la Secretaría de Hacienda y Crédito Público, en su calidad de fideicomitente única de la Administración Pública Federal Centralizada o alguna entidad de la Administración Pública Paraestatal en términos de las disposiciones legales y administrativas aplicables, y que no son considerados entidades paraestatales;
Firewall:	El dispositivo físico que permite crear una barrera entre la red interna y red externa, permitiendo el acceso entre las redes de acuerdo a las políticas de seguridad definidas en su configuración;
Firma electrónica:	Los datos en forma electrónica consignados en un mensaje de datos o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en éste;
Firmware:	La parte del software de una computadora que no puede modificarse por encontrarse en la memoria de sólo lectura. Es un híbrido entre el hardware y el software, es decir tiene parte física y una parte de programación consistente en programas internos implementados en memorias no volátiles;
Funcionalidad:	Las características de un producto o servicio que hacen que sea funcional y cubra las necesidades o requerimientos de un área o un usuario;

Funciones:	La actividad o conjunto de actividades genéricas, que desempeña uno o varios elementos, de forma complementaria para conseguir un objetivo concreto y definido;
Garantías:	El documento por medio del cual los proveedores, arrendadores y prestadores de servicios de las dependencias o entidades de la Administración Pública Federal establece a favor de éstos un derecho económico exigible, si no se realiza el cumplimiento de sus obligaciones contraídas en los contratos o pedidos;
Generador de contraseñas:	El dispositivo físico que permite fabricar códigos (contraseñas) de referencia secretos en función de parámetros o características deseables en periodos de tiempo definidos;
Gestión de riesgos:	Las actividades coordinadas para dirigir y controlar una organización respecto de los riesgos que afronta. La gestión de riesgos incluye la evaluación de riesgos, su tratamiento, aceptación y comunicación;
Gobernabilidad de TIC:	La relación que existe entre la estrategia y la gestión de tecnología de información y comunicaciones de la dependencia o entidad de la APF. En un modelo de gobernabilidad los funcionarios de alto mando deben tomar las decisiones estratégicas de tecnología de información y comunicaciones para asegurar la aplicación de las mejores prácticas, la eficiencia en el aprovechamiento de los recursos de tecnología de información y comunicaciones y la satisfacción de los usuarios, entre otras;
Gobierno digital:	El uso de las tecnologías de la información y comunicaciones. El Internet por ejemplo, es una herramienta que al desarrollar y ofrecer información y servicios públicos digitales mejora el funcionamiento del gobierno y la relación que existe con el ciudadano para satisfacer sus necesidades;
Hardware:	Los componentes físicos que conforman un equipo de cómputo;
Incidente:	El o los eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información; cualquier situación que ocurre durante un proceso y sucede en repetidas ocasiones;
Infraestructura:	Los componentes que soportan los servicios informáticos institucionales;
Insumo:	Los bienes o servicios que se incorporan a un proceso, y que con el esfuerzo de un equipo de trabajo se transforman en otro bien o servicio con un valor agregado mayor;
Integridad:	El principio de seguridad de la información que consiste en que el activo sólo puede ser modificado por los autorizados. Es una protección contra la modificación de los datos en forma intencional o accidental. Los datos deben ser mantenidos tal y como fueron proporcionados originalmente, sin sufrir ninguna modificación o eliminación;
Interfaces:	Las zonas de contacto o conexión entre dos elementos de hardware, o entre procesos;
Internet:	El conjunto de redes de computadoras y equipos físicamente unidos a través de medios alámbricos o inalámbricos que unen redes o equipos en todo el mundo;

Interoperabilidad:	La capacidad de los equipos, sistemas y/o arquitecturas tecnológicas de interactuar y/o intercambiar datos y servicios de una manera ágil y segura, a través de redes en las que se asegura la confidencialidad y no exposición de los datos. Usualmente se convienen estándares para lograr la interoperabilidad.
Intrusión:	La acción que una o más personas realizan para introducirse, sin derecho, en uno o más sistemas de información a fin de alterar, copiar o sustraer información que forma parte de esos sistemas, también puede ser en datos, información, bases de datos, etc.;
Lista de control de acceso:	La relación donde controlan las asignaciones de permisos de acceso a los archivos y directorios por usuario;
Macros:	Los programas que se ejecutan dentro de otros programas como word o excel para automatizar tareas, su uso elimina la realización de tareas repetitivas, automatizándolas, básicamente, se trata de un grupo de comandos de una aplicación, organizados según un determinado juego de instrucciones y cuya ejecución puede ser solicitada y autorizada para realizar la función que se desea;
Manual o El Manual	Para denominar al Manual Administrativo de Aplicación General en materia de Tecnologías de Información y Comunicaciones.
Matriz de riesgo:	La herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos;
Memoria USB:	El dispositivo de almacenamiento removible que utiliza un puerto USB para conectarse al computador que lo utilizará;
Mensaje de datos:	La información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos; al intercambio de datos o información entre un emisor y un receptor a través de medios de comunicación electrónica;
Mensajería instantánea:	Las aplicaciones o software que permite comunicarse, o enviar mensajes al instante, así como, intercambio de archivos;
Mesa de servicios:	El punto de contacto, único, encargado de recibir todas aquellas solicitudes de de los usuarios de TIC relacionados;
Metodología:	El sistema de prácticas, técnicas, procedimientos y normas utilizado por quienes trabajan en una disciplina;
Modelo de estructuras y funciones:	La implementación de una estructura organizacional en las áreas de TIC, enfocadas a participar activamente en la planeación estratégica institucional con un enfoque al ciudadano;
Modelo de funcionalidad:	La implementación de una estructura organizacional en las unidades de tecnología de información y comunicaciones, con enfoque a operar de manera eficiente sobre los procesos que, por las responsabilidades y atribuciones que se confieran a cada área de la unidad de tecnología de información y comunicaciones, deba gestionar;
Modelo de gobernabilidad de TIC:	Parte integral del gobierno de la dependencia o entidad, está constituido por las estructuras de liderazgo y los procesos que aseguran que la tecnología de información y comunicaciones de la misma, sostienen y extienden la estrategia

	y los objetivos institucionales;
Modelo de gobierno digital:	La interacción y flujo de los elementos que intervienen en el desarrollo del gobierno digital. Ubica al ciudadano como el centro de su estrategia y a partir de esta premisa, los elementos que intervienen se agrupan en seis niveles fundamentales (ver AGD, capítulo VI, Pág. 15);
Modelo de procesos:	El conjunto estructurado de elementos que describen las características de procesos efectivos y de calidad, que indican “qué hacer”, pero no indican “cómo hacer” ni “quién lo debe hacer”;
Nivel OLA:	El contrato escrito entre áreas de la UTIC que define las relaciones técnicas internas de disponibilidad, tiempo de respuesta y servicio que son necesarias, éste se suscribe para consistencia y objetividad a los contratos escritos de niveles de servicio hacia usuarios de la propia dependencia o entidad y/o de otra dependencia o entidad. Constituyen un elemento para definir y dar soporte a los SLA pactados por la UTIC hacia sus usuarios;
Nivel SLA:	El contrato escrito entre un proveedor de un servicio de tecnología de la información y comunicaciones, que puede ser la unidad de tecnologías de información y comunicaciones de la dependencia o entidad, con el propósito de fijar el nivel acordado para la calidad con que entregará el servicio;
Organizaciones e Instituciones:	Los gobiernos de entidades federativas y municipios; los integrantes del Poder Judicial de la Federación y de las comisiones legislativas del H. Congreso de la Unión; los organismos constitucionales autónomos;
Periféricos:	Los dispositivos que están conectados físicamente a una computadora;
Plan de contingencia:	El documento en el que se plantea la estrategia, el personal y el conjunto de actividades que se requieren para recuperar por completo o parcialmente un servicio, localidad o proceso crítico, en caso de que se presente un desastre. Dentro de este documento se establecen de igual manera las actividades, roles y responsabilidades para regresar a la normalidad una vez resuelto el incidente;
Priorización:	El establecimiento de criterios para contar con un esquema para jerarquizar los proyectos de TIC y facilitar la determinación del portafolio final de proyectos;
Problema:	El asunto respecto del cual existe una controversia, o que no ha sido resuelto y se está analizando;
Procedimiento:	La serie de pasos que se sigue en un orden regular definitivo, con un propósito;
Proceso:	El conjunto de medidas y actividades interrelacionadas realizadas para obtener un conjunto específico de productos, resultados o servicios;
Proveedores:	Las personas físicas o morales que celebren contratos de adquisiciones, arrendamientos y servicios con dependencias o entidades de la Administración Pública Federal;
Proyecto estratégico:	El conjunto de actividades que tiene como propósito fundamental, ampliar la capacidad productiva de un sector económico y social determinado, y que en el contexto de las prioridades definidas en el plan nacional de desarrollo, contribuye de una manera particularmente significativa, para el logro de los objetivos y metas institucionales;
Recibo digital:	El sello de recepción o acuse que generan las soluciones tecnológicas de

	control de gestión para el proceso de recepción del documento electrónico gubernamental. Este sello garantiza la integridad de la transacción;
Recurso:	Los servidores públicos y personal externo especializado de la dependencia o entidad, así como la mención genérica de equipo, servicios, suministros, materias primas, materiales, presupuestos o fondos;
Red de comunicaciones:	El sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión., así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;
Red privada de comunicaciones:	La red de comunicaciones destinada a satisfacer necesidades específicas de servicios de comunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red;
Red pública de comunicaciones:	La red de comunicaciones a través de la cual se explotan comercialmente servicios de comunicaciones. La red no comprende los equipos terminales de comunicaciones de los usuarios ni las redes de comunicaciones que se encuentren más allá del punto de conexión terminal;
Repositorio:	La base de datos fundamental para el diseño, no solo guarda datos, si no también algoritmos de diseño, y en general, elementos de software necesarios para el trabajo de programación, así como la documentación generada durante el proceso;
Requerimiento de certificación:	La solicitud electrónica de un certificado digital que contiene la clave pública y los datos de identificación del solicitante;
Requerimientos funcionales:	Característica que debe cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar;
Riesgo:	La probabilidad de que una amenaza aproveche la o las vulnerabilidades de un activo, así como las consecuencias de su impacto en una dependencia o entidad. Corresponde al grupo de trabajo del comité de seguridad determinar los niveles de riesgo máximos aceptables para la dependencia o entidad;
Rol:	La función definida que debe realizar un miembro del equipo del proyecto, como evaluar, archivar, inspeccionar o codificar;
Ruta crítica:	El subconjunto de tareas de un proyecto, que al variar su duración impacta la fecha de finalización;
Seguridad:	Las acciones tendientes a garantizar la confidencialidad, integridad y disponibilidad de los activos;
Seguridad de la información:	El atributo que expresa la protección de la información y de las soluciones tecnológicas de información, del acceso, uso, modificación, divulgación, interrupción o destrucción no autorizada. Se refiere a la confidencialidad, integridad y disponibilidad de la información y datos, independientemente de la forma, los datos pueden ser: electrónicos, impresos, audio u otros formatos;
Sentencias de aplicabilidad o Enunciados de aplicabilidad	Términos también encontrados como SoA por ser abreviación de Statement of applicability, (ISO 27001), utilizado para establecer controles en un ambiente de TIC relacionados con la seguridad de la información.

Servicio electrónico o Servicio digitalizado:	El producto de la actividad de desarrollo de sistemas o aplicativos de una unidad de tecnología de información y comunicaciones en una dependencia o entidad, que a través de la misma se ofrece a la ciudadanía;
Servicios:	Las aplicaciones que están soportadas en la infraestructura institucional y que agilizan y automatizan las actividades diarias de los usuarios;
Sistema automatizado de control de gestión:	El conjunto de elementos, procesos, procedimientos, herramientas e instrumentos informáticos o electrónicos, entre otros, que permiten realizar, identificar, proteger y controlar las comunicaciones, gestiones y trámites del documento electrónico gubernamental, entre los servidores públicos de las dependencias y entidades;
Sistema de datos personales:	El conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización;
Sistema o aplicativo:	El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso de acuerdo a los requerimientos;
Sistema operativo:	El software encargado de ejercer el control y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de hardware del sistema;
Software comercial:	El software o software libre comercializado, con el propósito de que las compañías que lo producen fijen un costo por el uso, distribución y mantenimiento del producto para la obtención de nuevas versiones, así como para el soporte técnico en el uso, configuración, implementación y otros servicios;
Software de código abierto:	El software que puede ser distribuido y desarrollado libremente. Se puede basar en software libre y hacer uso de una mezcla de software comercial o propietario, o estar completamente basado en software comercial o propietario;
Software libre:	El software mediante el cual el usuario tiene la libertad de ejecutarlo, copiarlo, distribuirlo, estudiarlo, modificarlo y mejorarlo. Suele estar disponible gratuitamente, o bien a un determinado precio para hacer uso de él;
Software propietario:	El software en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo (con o sin modificaciones), o cuyo código fuente no está disponible, o el acceso se encuentra restringido;
Software:	El código, programa de código, conjunto de programas de código, procedimientos automatizados y rutinas de código que se asocian con la operación de equipo de cómputo y que tiene el propósito de ejecutar una función o proveer de un servicio. También se denomina así a sistemas operativos, paquetería para automatización de oficinas, paquetes antivirus, paquetes para desarrollo de sistemas o aplicaciones, paquetes para operación, monitoreo y/o control redes de comunicaciones, paquetes de monitoreo de equipos de hardware y del propio código en operación, paquetes manejadores de bases de datos, navegadores para Internet, paquetes para monitoreo y seguridad de TIC, entre otros;
Solicitud de cambio:	Las solicitudes para ampliar o reducir el alcance de un proyecto, modificar políticas, procesos, planes o procedimientos, modificar costes o presupuestos,

	o revisar cronogramas. Las solicitudes de cambio pueden hacerse directa o indirectamente, pueden iniciarse en forma externa o interna y pueden tener carácter obligatorio u opcional, ya sea desde el punto de vista legal o contractual. Únicamente se procesan las solicitudes de cambio formalmente documentadas, y solo se implementan las solicitudes aprobadas;
Soporte técnico local:	La ayuda técnica que pueden tener los usuarios dentro de su área de trabajo en relación con la distribución geográfica;
Subcomisión:	La Subcomisión de firma electrónica avanzada, integrada por la Secretaría de la Función Pública, la Secretaría de Economía y el Servicio de administración tributaria, en términos del artículo vigésimo del Acuerdo por el cual se crea la Comisión intersecretarial para el desarrollo del gobierno electrónico;
Tarjeta inteligente:	El módulo de memoria del tamaño de una tarjeta de crédito en el cual es posible almacenar información para autenticación de usuarios;
Titular de un certificado digital:	La persona que crea sus claves privada y pública, genera su requerimiento de certificación y obtiene un certificado digital de firma electrónica avanzada ante una autoridad o agencia certificadora;
Trámite electrónico:	La solicitud o entrega de información que las personas físicas o morales realicen por medios electrónicos ante una dependencia o entidad, ya sea para cumplir una obligación, obtener un beneficio o servicio, a fin de que se emita una resolución, así como cualquier documento que dichas personas estén obligadas a conservar, no comprendiéndose aquella documentación o información que sólo tenga que presentarse en caso de un requerimiento de una dependencia o entidad;
Trazabilidad:	Los procedimientos preestablecidos y autosuficientes que permiten conocer el histórico, trayectoria de un producto o proceso a lo largo de la cadena de suministros en un momento dado, a través de una herramienta determinada;
Usuarios:	Las personas que tienen acceso a los servicios institucionales de TIC de manera autorizada;
Validación:	La acción de comprobar que los requerimientos de el área usuaria fueron cubiertos satisfactoriamente por la solución tecnológica adoptada;
Valor público:	El valor creado por el Estado a través de servicios, leyes, regulaciones y otras acciones que benefician a la ciudadanía;
Verificación:	La acción de comprobar o examinar la certeza de la información de los requerimientos entregados por el usuario;
Virus informático:	El programa informático que se ejecuta en la computadora sin previo aviso y que puede corromper el resto de los programas, directorios de datos e, incluso el mismo sistema operativo;
Vulnerabilidad:	La debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas, comprometiendo en consecuencia la confiabilidad, disponibilidad y/o integridad de la información;
Webservices:	Aplicación de software que permite el intercambio de datos mediante un conjunto de estándares y protocolos para ser expuesta y consumida por otras aplicaciones del mismo tipo;

ACRÓNIMO	DEFINICIÓN / SIGNIFICADO
AF:	Administración Financiera. El proceso de administración financiera del marco rector de procesos de este manual;
AC:	Autoridad certificadora: Se denomina así a aquellas dependencias, entidades, organizaciones, instituciones y proveedores que cuentan con la infraestructura tecnológica para la emisión y registro de certificados digitales de firma electrónica avanzada;
ADTI:	Adquisiciones de TIC. El proceso de adquisiciones de TIC del marco rector de procesos de este manual;
AGD:	Agenda de Gobierno Digital. Documento que establece las estrategias de desarrollo que deberá seguir el gobierno federal mediante el uso de las TIC, así como fomentar la participación ciudadana, a través de las dependencias y entidades de la APF, en colaboración con los poderes legislativo y judicial, los gobiernos estatales y municipales, la industria, la academia y la sociedad en general;
ANS:	Administración de Niveles de Servicio. El proceso de administración de niveles de servicio del marco rector de procesos de este manual;
AO:	Administración de la Operación. El proceso de administración de la operación del marco rector de procesos de este manual;
AP:	Administración de proceso. El grupo de procesos de administración de procesos del marco rector de procesos de este manual;
APP:	Administración del Portafolio de Proyectos de TIC. El proceso de administración del portafolio de proyectos de TIC del marco rector de procesos de este manual;
APS:	Administración del Portafolio de Servicios de TIC. El proceso de administración de proyectos de TIC del marco rector de procesos de este manual;
APTI:	Administración de Proyectos de TIC. El proceso de administración de proyectos de TIC del marco rector de procesos del presente manual;
APV:	Administración de Proveedores. El proceso de administración de proveedores del marco rector de procesos de este manual;
AR:	Administración de Recursos. El grupo de procesos de administración de recursos del marco rector de procesos de este manual;
ARTI:	Administración de Riesgos de TIC. El proceso de administración de riesgos del marco rector de procesos de este manual;
AS:	Administración de Servicio. El grupo de procesos de administración de servicios del marco rector de procesos del manual;
ASI:	Administración de la Seguridad de la información. El proceso de administración de la seguridad de la información del marco rector de procesos de este manual;
AST:	Administración de Servicios de Terceros. El proceso de administración de

	servicios de terceros del marco rector de procesos de este manual;
CD:	Compact disc, CD por sus siglas en inglés. El dispositivo de almacenamiento óptico que requiere de un dispositivo de lectura y/o escritura, en el caso de escritura requiere de un láser para imprimir puntos sobre la superficie brillante del CD, para su lectura se requiere de un láser de menor intensidad, estos puntos son representados como cadenas de bits;
CIDGE:	La Comisión intersecretarial para el desarrollo del gobierno electrónico, creada con el objetivo de promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones en la Administración Pública Federal;
CMM:	Capability Maturity Model, CMM por sus siglas en inglés. Modelo de evaluación de los procesos en una organización de TIC;
CN:	Control. El grupo de procesos de control del marco rector de procesos de este manual;
COBIT:	Control Objectives for Information and related Technology, COBIT por sus siglas en inglés.
CR:	Cumplimiento Regulatorio. El proceso de cumplimiento regulatorio del marco rector de procesos de este manual;
CST:	Calidad de Soluciones Tecnológicas. El proceso de calidad de soluciones tecnológicas del marco rector de procesos de este manual;
DA:	Desarrollo y adquisición de soluciones. Grupo de procesos de desarrollo y adquisición de soluciones del marco rector de procesos de este manual;
DDT:	Determinar la dirección de tecnológica. El proceso de determinar la dirección tecnológica del marco rector de procesos de este manual;
DR:	Dirección. El grupo de procesos de dirección del marco rector de procesos de este manual
DSTI:	Diseño de Servicios de TIC. El proceso de diseño de servicios del marco rector de procesos de este manual;
EEG:	Establecimiento de la Estructura de Gobierno de TI. El proceso de establecimiento de la estructura de gobierno de TI del marco rector de procesos de este manual;
ERST:	Especificación de Requerimientos de Soluciones Tecnológicas. El documento en donde se estipulan las necesidades, se incluyen especificaciones y descripciones de las necesidades a detalle, las cuales serán mitigadas con las respectivas soluciones tecnológicas disponibles en el mercado y/o a desarrollar por el área correspondiente;
ESGP:	Establecimiento del Sistema de Gestión de Procesos. El proceso de establecimiento del sistema de gestión de procesos del marco rector de procesos de este manual;
FEA/FIEL:	Firma electrónica avanzada. El medio de identificación electrónica definida en los lineamientos emitidos por la Subcomisión de firma electrónica avanzada, de la Comisión intersecretarial para el desarrollo del gobierno electrónico,

	publicado en Diario Oficial de la Federación del 9 de diciembre de 2005;
HTTPS:	Secure HyperText Transfer Protocol, HTTPS por sus siglas en inglés. Es el protocolo seguro de transferencia de hipertexto. La aplicación utilizada para garantizar la seguridad de las comunicaciones entre el usuario y el servidor web al que dicho usuario se conecta;
IDP:	Integración y Desarrollo de Personal. El proceso de integración y desarrollo de personal del marco rector de procesos de este manual;
ISO/IEC27000:	International Organization for Standardization e IEC International Electro technical Commission, ISO e IEC por sus siglas en inglés. El conjunto de estándares desarrollados o en fase de desarrollo por la ISO que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización de TIC, ya sea pública o privada, independientemente de su tamaño;
ITFEA:	Infraestructura tecnológica de firma electrónica avanzada. Permite la interoperabilidad y el reconocimiento de certificados digitales de firma electrónica avanzada entre las autoridades o agencias certificadoras que la integran;
ITIL:	Information Technology Infrastructure Library, ITIL por sus siglas en inglés. La Biblioteca de Infraestructura de Tecnologías de Información, es un marco de trabajo de mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información y comunicaciones;
LDAP:	Lightweight Directory Access Protocol, LDAP por sus siglas en inglés. El directorio de usuarios que se utiliza principalmente para asociar nombres direcciones de correo electrónico y otros atributos de identificación y de privilegios de acceso a servicios. Es un estándar abierto para servicios en una red local y/o en Internet.;
LE:	Liberación y Entrega. El proceso de liberación y entrega del marco rector de procesos de este manual;
MI:	Mantenimiento de Infraestructura. El proceso de mantenimiento de infraestructura del marco rector de procesos de este manual;
OLA:	Operating Level Agreement, OLA por sus siglas en inglés. Acuerdo de nivel operativo que se suscribe entre áreas internas de una entidad responsable de TIC en una organización;
OMS:	Operación de la Mesa de Servicios. El proceso de operación de la mesa de servicios del marco rector de procesos de este manual.
OS:	Operación de Servicios. El grupo de procesos de operación de servicios del marco rector de procesos de este manual;
PE:	Planeación Estratégica. El proceso de planeación estratégica de TIC del marco rector de procesos de este manual;
PEPSU:	Proveedor, Entrada, Proceso, Salida y Usuario. El esquema metodológico que permite conocer, para un proceso, el proveedor, la entrada, el proceso que los utiliza, las salidas que produce el proceso y el usuario de la salida.
PETIC:	Plan Estratégico de Tecnologías de la Información y Comunicaciones. El plan

	estratégico de tecnologías de la información que anualmente elaboran las dependencias y entidades de la APF a través de sus UTIC.;
PMG:	El Programa especial de Mejora de la Gestión 2007-2012. Es el instrumento del ejecutivo federal, de carácter obligatorio, que se enfoca a realizar mejoras que orienten sistemáticamente la gestión de las instituciones públicas y del gobierno federal al logro de mejores resultados;
PR:	Proyectos. El grupo de procesos de administración de proyectos del marco rector de procesos de este manual;
PSC:	El Prestador de Servicios de Certificación. El proveedor que cuenta con los elementos humanos, materiales, económicos y tecnológicos para la emisión, registro y administración de certificados digitales de firma electrónica avanzada y que se encuentra acreditado por la Secretaría de Economía;
RCD:	El Registro de Certificados Digitales. El registro que contiene los certificados digitales de firma electrónica avanzada emitidos por una autoridad o agencia certificadora, indicando su estado;
RUP:	Rational Unified Process, RUP por sus siglas en inglés: Uno de los procesos internacionalmente adoptados para el desarrollo de soluciones tecnológicas o aplicativos;
SAT:	Servicio de Administración Tributaria;
SE:	Secretaría de Economía;
SFP:	Secretaría de la Función Pública;
SGSI:	SGSI, Sistema de Gestión de Seguridad de la Información. El concepto es utilizado principalmente por la ISO/IEC 27001, en inglés "Information Security Management System" (ISMS). Es el sistema que articula el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno;
SLA:	Service Level Agreement, SLA por sus siglas en inglés. El acuerdo o acuerdos de nivel de servicio;
SLR:	Service level Requirement, SLR por sus siglas en inglés. Los requerimientos de niveles de un Servicio;
SOA:	Statement of applicability, SoA por sus siglas en inglés. Enunciados o sentencias de aplicabilidad. Elementos de control de seguridad de la información utilizado para el establecimiento del SGSI en el marco rector de este manual.
TCP/IP:	Transfer Control Protocol/Internet Protocol por sus siglas en inglés. El protocolo estándar de comunicaciones en red utilizado para conectar sistemas informáticos a través de Internet;
TE:	Transición y entrega. Grupo de procesos de transición y entrega del marco rector de procesos de este manual;

TIC:	Siglas empleadas convencionalmente para denominar a las Tecnologías de Información y Comunicaciones;
THO:	Transición y Habilitación de la Operación. Proceso de transición y habilitación de la operación del marco rector de procesos de este manual;
UTIC:	La unidad administrativa responsable de los servicios de tecnologías de la información y comunicaciones en una dependencia o entidad;
UC:	Contratos de soporte en el que se definen los objetivos a cumplir, al respecto de los objetivos de nivel de servicio, en un SLA;
UGD:	Unidad de Gobierno Digital, en la Subsecretaría de la Función Pública de la Secretaría de la Función Pública;
USB:	Universal Serial Bus, USB por sus siglas en inglés. El puerto que sirve para conectar periféricos con conexión serial comúnmente a una computadora o a cualquier otro dispositivo de TIC;
WAN:	Wide area network, WAN por sus siglas en inglés. La red de cómputo que se encuentra distribuida en un área geográfica determinada como una ciudad o un estado, su finalidad está encaminada a enlazar los diferentes edificios de una organización;
WWW:	World Wide Web, WWW por sus siglas en inglés. El sistema de documentos interconectados por enlaces de hypertexto, que se ejecutan en Internet;
XML:	eXtensible Markup Language, XML por sus siglas en inglés. El metalenguaje destinado a la creación de lenguaje de definición de datos, que permiten la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre redes.

3. INTRODUCCIÓN

En el mes de septiembre de 2009, el presidente de los Estados Unidos Mexicanos, Felipe Calderón Hinojosa, instruyó a la Secretaría de la Función Pública profundizar las acciones en materia de reforma regulatoria y derogar todos aquellos acuerdos, oficios, decretos o reglamentos cuya necesidad no quedara plenamente justificada, con el propósito de mejorar la eficiencia institucional y la calidad de los servicios que brindan las diversas dependencias y entidades de la Administración Pública Federal.

El trabajo consistió en la simplificación de la normatividad que enmarca la operación de adquisiciones, arrendamientos y servicios; auditoría, control, obra pública, recursos financieros, recursos humanos / servicios personales, recursos materiales y servicios generales, tecnologías de la información y transparencia. Para cada una de las temáticas mencionadas se especificaron también procesos y subprocesos eficientes y eficaces, definiendo responsables de sus actividades y los documentos necesarios para realizarlas.

Las definiciones surgieron de un trabajo en equipo en que participaron las unidades normativas, líderes técnicos de las materias tratadas, áreas de auditoría y desarrollo de la mejora de la gestión pública de algunos órganos internos de vigilancia y control, quienes fungieron como líderes de los grupos de trabajo, instituciones federales de distinta índole, que validaron el contenido de los manuales y la Unidad de Políticas de Mejora de la Gestión Pública, quien coordinó los trabajos.

La publicación de nueve instrumentos generales sobre los temas mencionados constituye un importante esfuerzo por eliminar la sobrerregulación de los procesos de apoyo, imprescindibles para el buen funcionamiento de las instituciones públicas. El perfeccionamiento de los manuales será posible incorporando paulatinamente mejores prácticas derivadas de la mejora de la gestión de las dependencias y entidades federales.

Los cambios vertiginosos originados durante los últimos años por el uso de las tecnologías de la información y las comunicaciones han tenido un impacto en diversos aspectos de nuestra sociedad, reflejados en importantes esfuerzos y logros. En el ámbito de la Administración Pública Federal, las tecnologías de la información y comunicaciones han venido a transformar los esquemas tradicionales del quehacer público directamente para eficientar los procesos internos y mejorar la entrega de los servicios proporcionados a la ciudadanía, para brindarle una mejor calidad de vida.

La estrategia de desarrollo del gobierno digital en nuestro país, coordinada por la Secretaría de la Función Pública, a través de la Unidad de Gobierno Digital, impulsa la utilización óptima de las tecnologías de información y de comunicaciones para hacer más eficiente la gestión gubernamental, proporcionar servicios de mayor calidad y oportunidad a la sociedad, transparentar la función pública en todos los ámbitos de gobierno y combatir las prácticas de corrupción al interior de las oficinas gubernamentales.

El presente manual administrativo en materia de TIC forma parte del proyecto de Regulación Base Cero, que tiene como fin eliminar toda aquella regulación o normatividad que limita o impide brindar un proceso o servicio de forma ágil y oportuna por la Administración Pública Federal a sus ciudadanos.

Con relación a los procesos que integran este manual administrativo, se ha diseñado un marco rector de procesos fundamentado en las mejores prácticas, de manera que se tenga una cobertura total de la gestión de las unidades administrativas de tecnologías de la información y comunicaciones así como de los servicios que estas áreas proporcionan a sus usuarios, tanto al interior del gobierno, como a los ciudadanos y sus organizaciones.

4. OBJETIVOS

Objetivos

General.-

El presente documento forma parte de un conjunto de manuales de aplicación obligatoria para todas las dependencias y entidades de la administración pública federal y tienen por objetivo establecer los procesos, procedimientos, disposiciones normativas, responsables, indicadores y estándares que, respetando el marco legal, eliminen la sobrerregulación y las actividades que no agregan valor. De este modo la operación institucional de apoyo puede ser más eficiente, oportuna y transparente.

Específicos.-

1. Proporcionar a las dependencias y entidades de la Administración Pública Federal un marco de referencia general unificado que estandarice la operación en materia de tecnologías de la información y comunicaciones.
2. Simplificar y homologar el marco normativo de los procesos internos relacionados con las tecnologías de la información y comunicaciones.
3. Ofrecer al personal del sector público una guía descriptiva de las actividades secuenciales para simplificar, homologar y hacer eficientes los procesos en materia de tecnologías de la información y comunicaciones.
4. Establecer indicadores comunes que permitan medir los resultados, productos, avance o impacto de los procesos de tecnologías de la información y comunicaciones, con el fin de brindar recomendaciones e información útil para la toma de decisiones, la rendición de cuentas y fomentar el aprendizaje institucional.
5. Contribuir mediante el uso de las TIC a alcanzar una mayor eficiencia en las actividades y procesos institucionales e interinstitucionales, así como mejorar la entrega de servicios a la sociedad, a partir de una orientación al ciudadano, de una arquitectura orientada a servicios, de la conformación de infraestructuras comunes a las diferentes dependencias y entidades, de la interoperabilidad, de la integración de servicios, de la búsqueda de sinergias, así como de la utilización de economías de escala.

5. ÁMBITO DE APLICACIÓN / ALCANCE

El presente manual, es de observancia obligatoria para las dependencias y entidades de la Administración Pública Federal, la Procuraduría General de la República y las unidades de la Presidencia de la República, salvo las excepciones o regímenes especiales que se señalen de manera expresa en este documento.

El presente manual se actualizará de acuerdo a las necesidades de los servicios digitales que la ciudadanía requiera, a las de las dependencias y entidades de la Administración Pública Federal así como a las del avance tecnológico, de mejores prácticas y de metodologías de Tecnologías de Información y Comunicaciones.

La Secretaría de la Función Pública, a través de la Unidad de Gobierno Digital, informará sobre las actualizaciones que se efectúen a este manual mediante publicación en el Diario Oficial de la Federación y en la página electrónica http://www.cidge.gob.mx.

6. MARCO JURÍDICO

1. La Constitución Política de los Estados Unidos Mexicanos
2. Ley Orgánica de la Administración Pública Federal.
3. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento.
4. Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.
5. Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental y su Reglamento.
6. Ley del Servicio Profesional de Carrera y su Reglamento.
7. Plan Nacional de Desarrollo.
8. Reglamento Interior de la Secretaría de la Función Pública.
9. Decreto que establece las medidas de austeridad y disciplina del gasto de la Administración Pública Federal.
10. Lineamientos específicos para la aplicación y seguimiento de las medidas de austeridad y disciplina del gasto de la Administración Pública Federal.
11. Lineamientos generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal
12. Lineamientos generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal
13. Lineamientos de Protección de Datos Personales y las Recomendaciones sobre medidas de Seguridad aplicables a los Sistemas de Datos Personales emitidos por el Instituto Federal de Acceso a la Información

7. PROCESOS EN MATERIA DE TIC

El presente manual administrativo en materia de TIC tiene un enfoque a procesos, por lo que se ha efectuado el diseño de 31 procesos rectores agrupados en 11 macroprocesos que, integrados, forman el marco rector de procesos de tecnologías de información y comunicaciones.

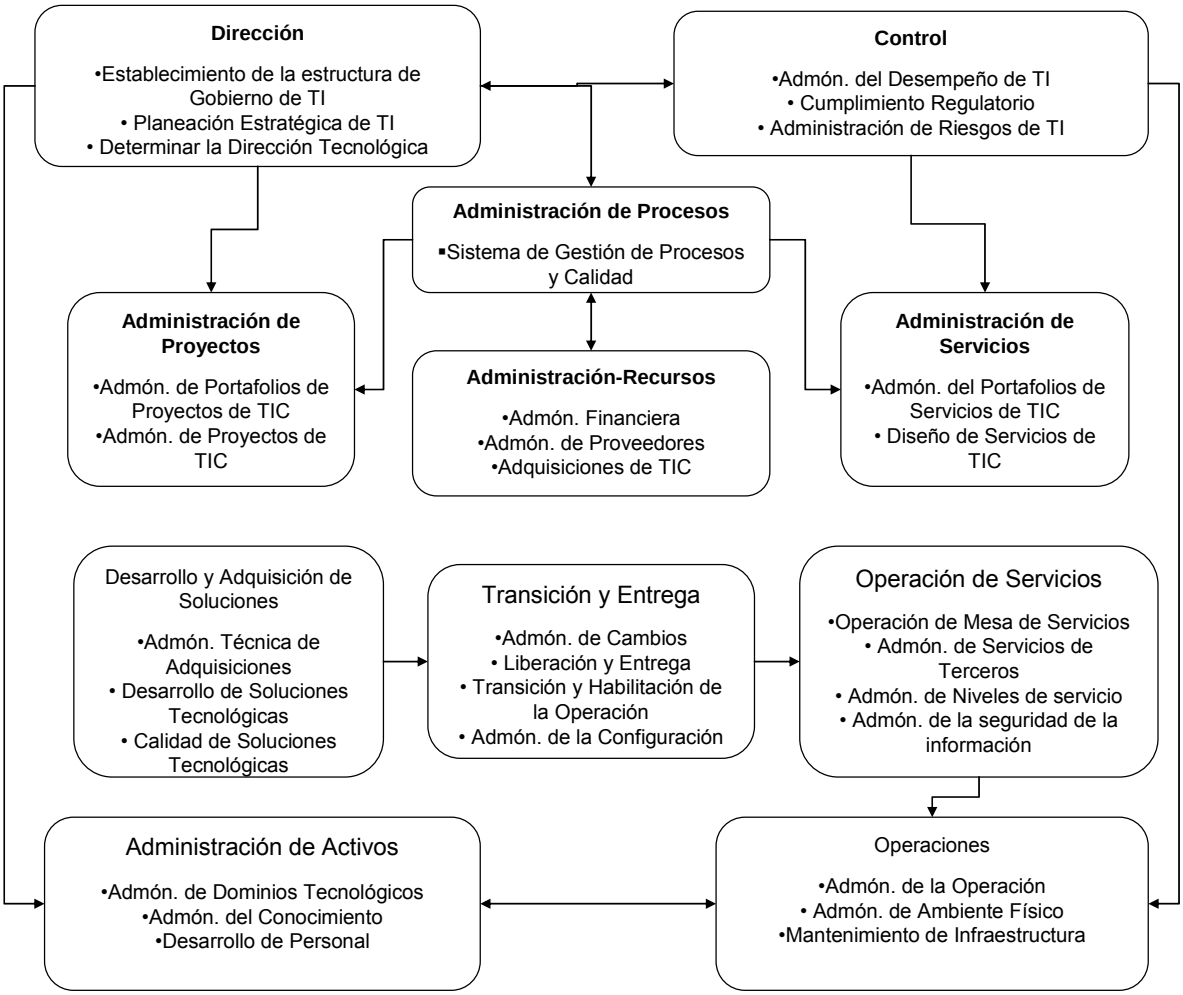
El marco rector se muestra de manera general en la siguiente figura:

Figura: marco rector de macroprocesos de tecnologías de información y comunicaciones y sus relaciones relevantes.

El marco rector de los procesos de tecnologías de información y comunicaciones basa su diseño, y el de los procesos que lo conforman en las mejores prácticas de tecnologías de información y comunicaciones nacionales e internacionales, vigentes a la fecha de elaboración del presente manual.

El marco rector de los procesos de tecnologías de información y comunicaciones tiene como objetivo fundamental lograr la cobertura total de la gestión, de punta a fin, de las unidades administrativas de tecnologías de información y comunicaciones UTIC, de manera que independientemente de la estructura organizacional con que cuentan actualmente y que llegaran a adoptar, las funciones se acoplen a los procesos y se logre la cohesión total para una mejor gestión y el logro de la aplicación de las mejores prácticas.

En la siguiente figura se muestran los 31 procesos del marco rector:



Cada uno de los procesos dentro de los macroprocesos se relaciona con diversos procesos de los 31 procesos del marco rector, de acuerdo a las necesidades propias de cada proceso y de la gestión integral de la UTIC.

7.1 DIRECCIÓN

7.1.1. Establecimiento de la estructura de gobierno de TIC

7.1.1.1. Objetivos del proceso

General.-

Crear un marco de responsabilidad destinado a apoyar la toma de decisiones de la dependencia o entidad, basada en el análisis de las oportunidades de aprovechamiento de las TIC y de sus riesgos, así como a promover el uso adecuado de las TIC para contribuir a la mejora de la organización.

Específicos.-

1. Establecer una estructura para el gobierno y dirección del aprovechamiento de las TIC, que determine las prioridades de inversión en TIC, alineadas a las necesidades de la dependencia o entidad.
2. Establecer y mantener una estructura organizacional adecuada de la UTIC para desempeñar las funciones inherentes a las tecnologías de la información y comunicaciones, que considere los procesos, y los requerimientos de personal necesarios para ejecutar los procesos correspondientes.
3. Asegurar la transparencia, el control y el compromiso de los mandos medios y de los titulares de las unidades administrativas de la dependencia o entidad en la dirección y control de la inversión y entrega efectiva y eficiente de servicios de TIC.
4. Cohesionar procesos y estructura en la toma de decisiones, para minimizar la evasión de toma de decisiones y su rechazo.

7.1.1.2 Descripción del proceso

7.1.1.2.1 Mapa general del proceso

Diagrama de flujo de información

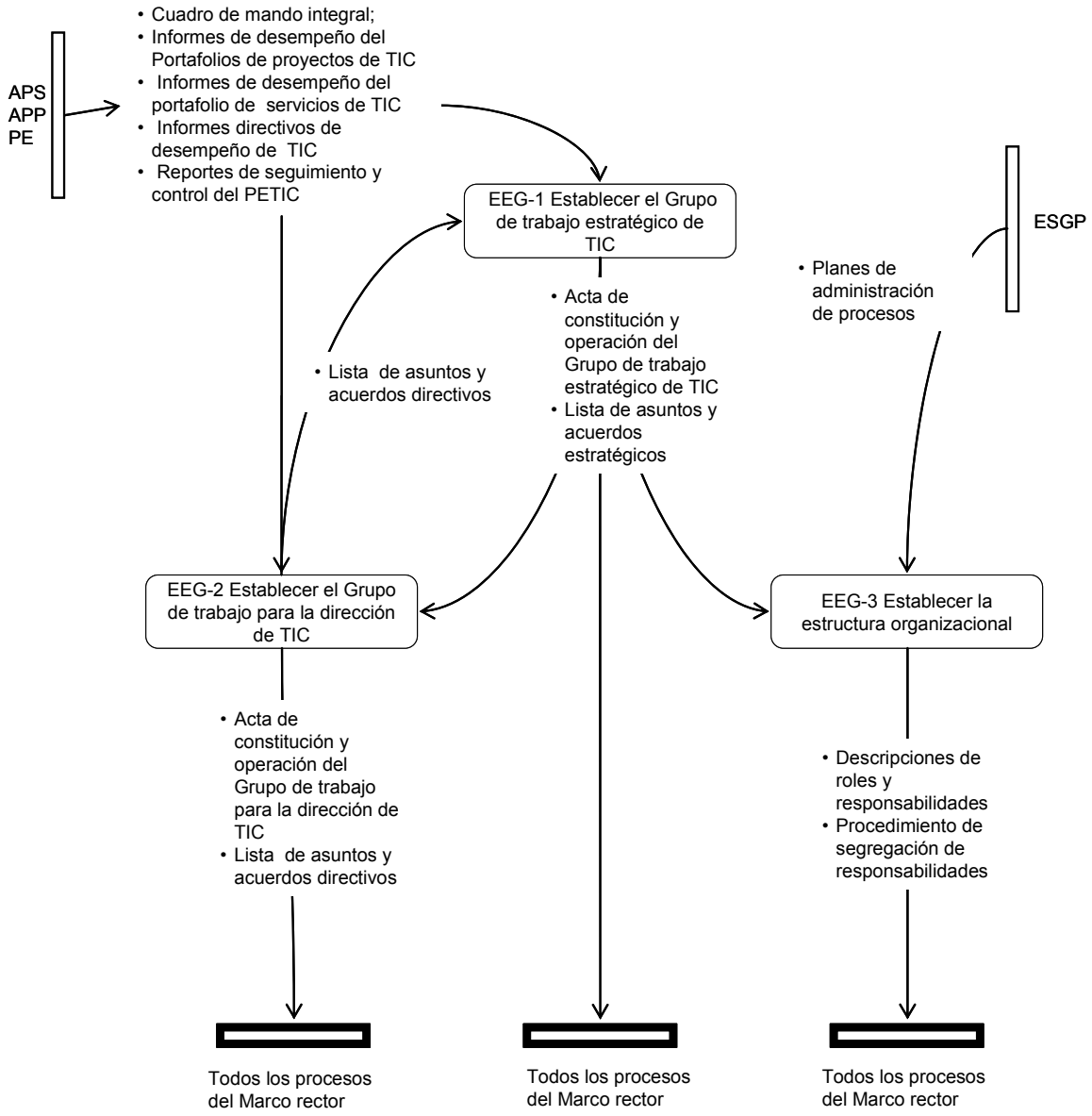
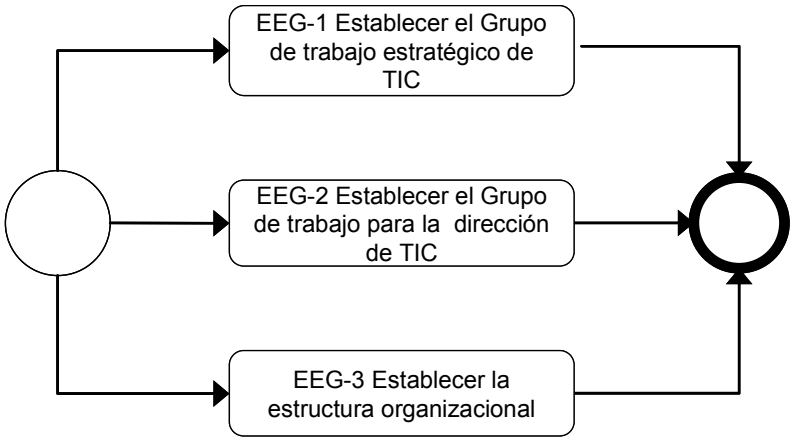


Diagrama de flujo de actividades



7.1.1.2.2 Descripción de actividades del proceso

EEG-1 Establecer el grupo de trabajo estratégico de TIC

Descripción	Establecer un grupo de trabajo estratégico de TIC (o su equivalente) a nivel de Director General o equivalente. Este grupo deberá asegurar que el gobierno de las TIC, como parte del gobierno de la dependencia o entidad, se maneje de forma integral, asesore sobre la dirección estratégica de la institución y dar seguimiento a las inversiones principales en esta materia, para asegurar que éstas se encuentran alineadas a los objetivos estratégicos de la dependencia o entidad y generar los beneficios esperados.
Factores Críticos	1. Definir y comunicar el alcance, objetivos, participantes, roles y responsabilidades del grupo de trabajo estratégico de TIC. 2. Establecer el grupo de trabajo estratégico de TIC integrado por titulares de las unidades responsables de la dependencia o entidad con el conocimiento y la experiencia para valorar la contribución de éstas en el funcionamiento de la misma, y será coordinado por el titular de la UTIC, con la finalidad de determinar las oportunidades y los riesgos que genera a la institución el uso de dichas tecnologías. 3. Ejecutar sesiones del grupo de trabajo estratégico de TIC. El grupo de trabajo estratégico de TIC deberá reunirse periódicamente para atender asuntos estratégicos, incluyendo la revisión ejecutiva del estado de las inversiones y avance de los proyectos prioritarios de TIC. 4. Asegurar que el grupo de trabajo estratégico de TIC reporte directamente al titular de la dependencia o entidad.
Relación de Productos	• Acta de constitución y operación del grupo de trabajo estratégico de TIC • Lista de asuntos y acuerdos estratégicos

EEG-2 Establecer el grupo de trabajo directivo de TIC

Descripción	Establecer el grupo de trabajo para la dirección de las TIC (o su equivalente), integrado por los titulares de las áreas responsables y de la UTIC. El grupo de trabajo para la dirección de las TIC puede estar constituido a su vez por varios subgrupos de trabajo de acuerdo a las necesidades y estructura de la dependencia o entidad.
Factores Críticos	1. El grupo de trabajo para la dirección de las TIC deberá: • Determinar las prioridades de las iniciativas de inversión de TIC alineadas con la estrategia y prioridades institucionales. • Dar seguimiento al estado de las iniciativas y programas de proyectos, así como resolver los conflictos de recursos. • Evaluar el cumplimiento a los niveles de servicio. 2. Asegurar que se integre y funcione el grupo de trabajo para la dirección de las TIC y que éste reporte al servidor público designado en la dependencia o entidad. • El grupo de trabajo para la dirección de las TIC deberá integrarse con representantes de

	las unidades responsables sustantivas y de las unidades responsables de las áreas administrativas de la institución: finanzas, recursos materiales y recursos humanos. 3. Participar en el proceso de administración del portafolio de proyectos, con la responsabilidad de seleccionar y autorizar iniciativas, dar seguimiento y de evaluar el desempeño de dicho proceso. 4. Aprobar y asegurar la efectividad de los controles de alto nivel, tales como las políticas de los procesos de sistema de gestión de procesos de la UTIC, los indicadores del cuadro de mando integral de TIC y las estrategias para el control de los riesgos de TIC.
Relación de Productos	• Acta de constitución y operación del grupo de trabajo para la dirección de TIC • Lista de asuntos y acuerdos directivos

EEG-3 Establecer la estructura organizacional

Descripción	Establecer una estructura organizacional orientada a los procesos de la UTIC que responda a las necesidades de la dependencia o entidad y en sustento al sistema de gestión de procesos de la UTIC.
Factores Críticos	1. Establecer los roles y las responsabilidades de los servidores públicos involucrados en la ejecución de los procesos de la UTIC, para los usuarios y otros interesados, de manera que se delimite la autoridad entre el personal de la UTIC y los usuarios finales. • Determinar el conocimiento, experiencia, autoridad, responsabilidad y rendición de cuentas para cada función. • Asignar a las funciones uno o más roles del sistema de gestión de procesos y calidad de la UTIC. • Asignar los roles al personal de la UTIC. • Desarrollar descripciones de roles con descripción de metas clave y objetivos medibles. 2. Implementar la segregación de responsabilidades. • Establecer una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. • Los titulares de las unidades administrativas deberán asegurar que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas. • Identificar y documentar funciones en conflicto, tales como el iniciar, autorizar, ejecutar y verificar transacciones. Asegurar que la segregación de funciones se obligue, tanto física como lógicamente, cuando sea apropiado. 3. Supervisión. • Implementar prácticas adecuadas de supervisión dentro de la UTIC para asegurar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades. • Revisar la estructura organizacional de la UTIC de forma periódica, a fin de ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos

	institucionales y las circunstancias cambiantes.
Relación de Productos	• Descripciones de roles y responsabilidades • Procedimiento de segregación de responsabilidades

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.1.1.2.3 Descripción de roles

Rol	Descripción
Grupo de trabajo estratégico de TIC	Grupo de trabajo integrado por titulares de las unidades administrativas de la dependencia o entidad, con el conocimiento y la experiencia para valorar la contribución de las TIC en la institución, las oportunidades que genera y los riesgos derivados de la adopción, el uso, la propiedad, la seguridad y la operación de los activos y recursos de TIC.
Grupo de trabajo para la dirección de TIC	Grupo o grupos conformados por titulares de las unidades administrativas responsables y de la UTIC, que apoya y reporta al grupo de trabajo estratégico de TIC. Este grupo toma decisiones directivas, determina requerimientos, aprueba controles y evalúa los resultados de la UTIC, con el propósito de asegurar que la inversión y gasto en materia de TIC se encuentra alineada con los objetivos, la estrategia y prioridades de la dependencia o entidad.
Titular de la UTIC	El nivel más alto de responsabilidad de la UTIC de la dependencia o entidad.

7.1.1.2.4 Descripción de productos

Producto	Descripción
Acta de constitución y operación del grupo de trabajo estratégico de TIC	Documento que define el alcance, objetivos, participantes, roles y responsabilidades del grupo de trabajo estratégico de TIC. Incluyen las reglas para la operación del grupo de trabajo estratégico de TIC.
Acta de constitución y operación del grupo de trabajo para la dirección de TIC	Documento que define el alcance, objetivos, participantes, roles y responsabilidades del grupo de trabajo para la dirección de TIC. Incluyen los procedimientos para la operación del grupo de trabajo para la dirección de TIC.
Descripciones de roles y responsabilidades	Documento que define en una matriz de asignación los roles y responsabilidades para las actividades clave de un proceso. Esta matriz se conoce en inglés como RACI, acrónimo de *"Responsible, Accountable, Consulted and Informed"* define a los responsables de: rendir cuentas, de ejecutar, a los involucrados que son consultados y aquellos que deben ser informados.

Producto	Descripción
Procedimiento de segregación de responsabilidades	Procedimiento que identifica las funciones/actividades en conflicto para reducir la posibilidad de que un solo individuo afecte negativamente un proceso crítico.
Lista de Asuntos y acuerdos	Lista de asuntos y acuerdos resultantes de las sesiones de los grupos de trabajo estratégico de TIC y para la dirección de la TIC.

7.1.1.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de la Estructura de Gobierno de TIC	Medir el grado de cumplimiento de la estructura de gobierno de TIC	Es el porcentaje obtenido para alcanzar los objetivos establecidos	Eficacia	De gestión	Recomendación: (Estructura de Gobierno de TIC implantada / Estructura de Gobierno de TIC planeada) *100	Grupo de trabajo estratégico de TIC	Trimestral
Porcentaje de la Estructura de Dirección de TIC	Medir el grado de cumplimiento de la estructura de la dirección de TIC	Es el porcentaje obtenido para alcanzar los objetivos establecidos	Eficacia	De gestión	Recomendación: (Estructura de Dirección de TIC implantada / Estructura de Dirección de TIC adecuada) *100	Grupo de Trabajo estratégico	Trimestral

7.1.1.4 Reglas del proceso

1.1	La dependencia o entidad a través de la UTIC deberá integrar una estructura de gobierno de TIC con el propósito de determinar las prioridades de inversión en materia de TIC, así como mantener permanentemente alineado el ejercicio del gasto en materia de TIC con los objetivos de la dependencia o entidad.
1.2	La dependencia o entidad a través de la UTIC deberá establecer el grupo de trabajo estratégico de TIC y el grupo de trabajo para la dirección de TIC.
1.3	El titular de la UTIC deberá establecer, implementar y supervisar una estructura organizacional que responda a los roles y responsabilidades definidos en el Sistema de Gestión de Procesos de la UTIC con atención en el aseguramiento del control, la calidad, la administración de riesgos, la seguridad de la información, la propiedad de activos de TIC y la segregación de funciones.

7.1.1.5 Documentación soporte del proceso

No aplica

7.1.2 Planeación estratégica de TIC

7.1.2.1 Objetivos del proceso

General.-

Asegurar la contribución de las TIC al logro de los objetivos de la dependencia o entidad mediante la elaboración de un PETIC participativo, alineado a las directrices y disposiciones de los planes y programas federales.

que considere.

Específicos.-

1. Identificar los objetivos y prioridades de la dependencia o entidad con la finalidad de proponer proyectos eficaces e innovadores considerando especialmente aquellos relacionados con la mejora sustancial de los trámites y los servicios públicos.
2. Identificar las oportunidades y riesgos para el cumplimiento de los objetivos estratégicos de la dependencia o entidad en materia de TIC mediante el análisis del entorno y de la organización.
3. Establecer los mecanismos y temáticas a considerar para elaborar y operar el PETIC, especialmente estimaciones del presupuesto, de la inversión por proyecto, de las fuentes de financiamiento y de la estrategia de adquisición.
4. Instrumentar los mecanismos para asegurar que el personal de la UTIC entienda cabalmente el PETIC de la institución.
5. Establecer un cuadro de mando integral para controlar el cumplimiento del PETIC, que incluya las perspectivas financieras, de usuarios, de procesos, de crecimiento y de aprendizaje.

7.1.2.2 Descripción del proceso

7.1.2.2.1 Mapa general del proceso

Diagrama de flujo de información

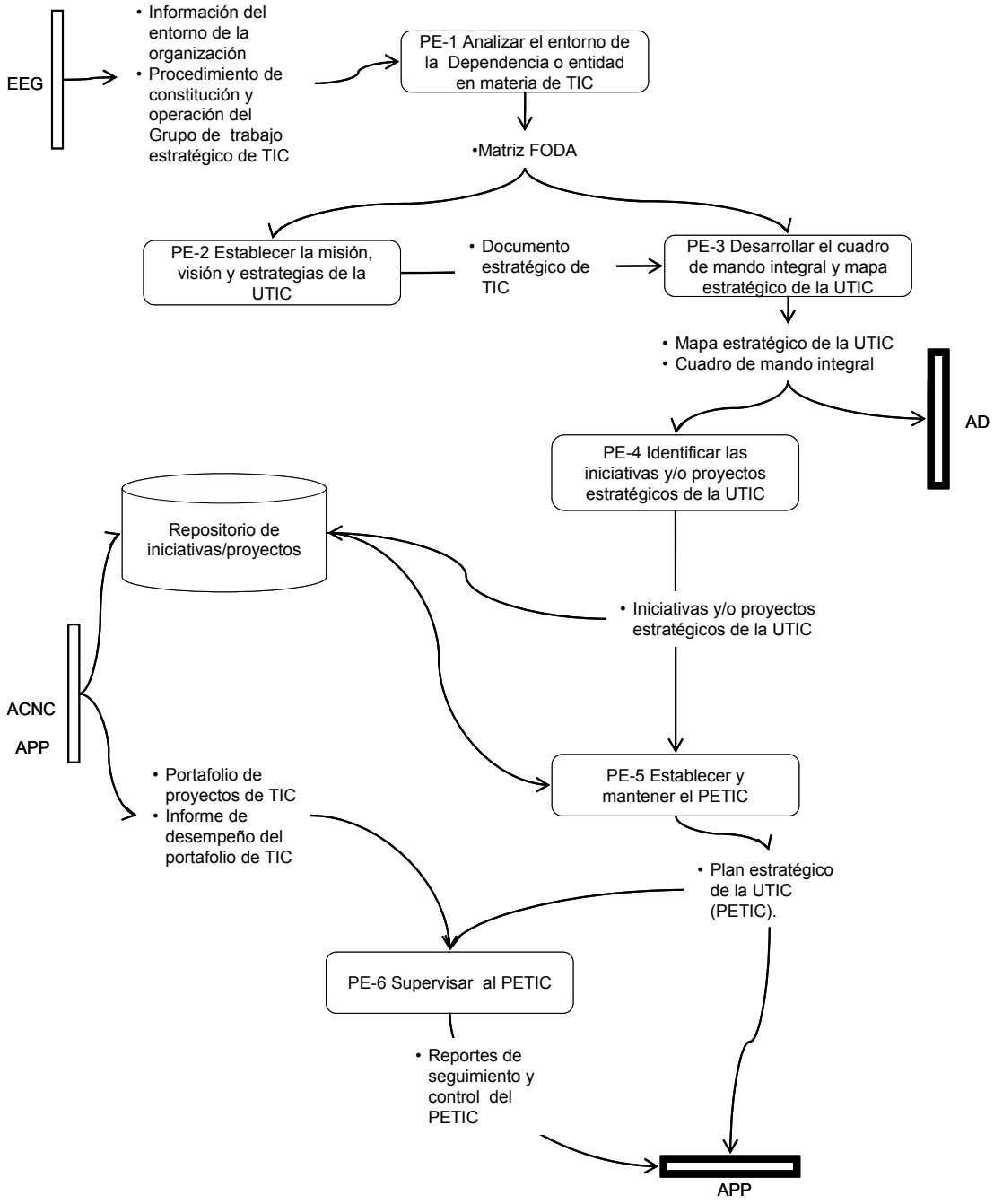
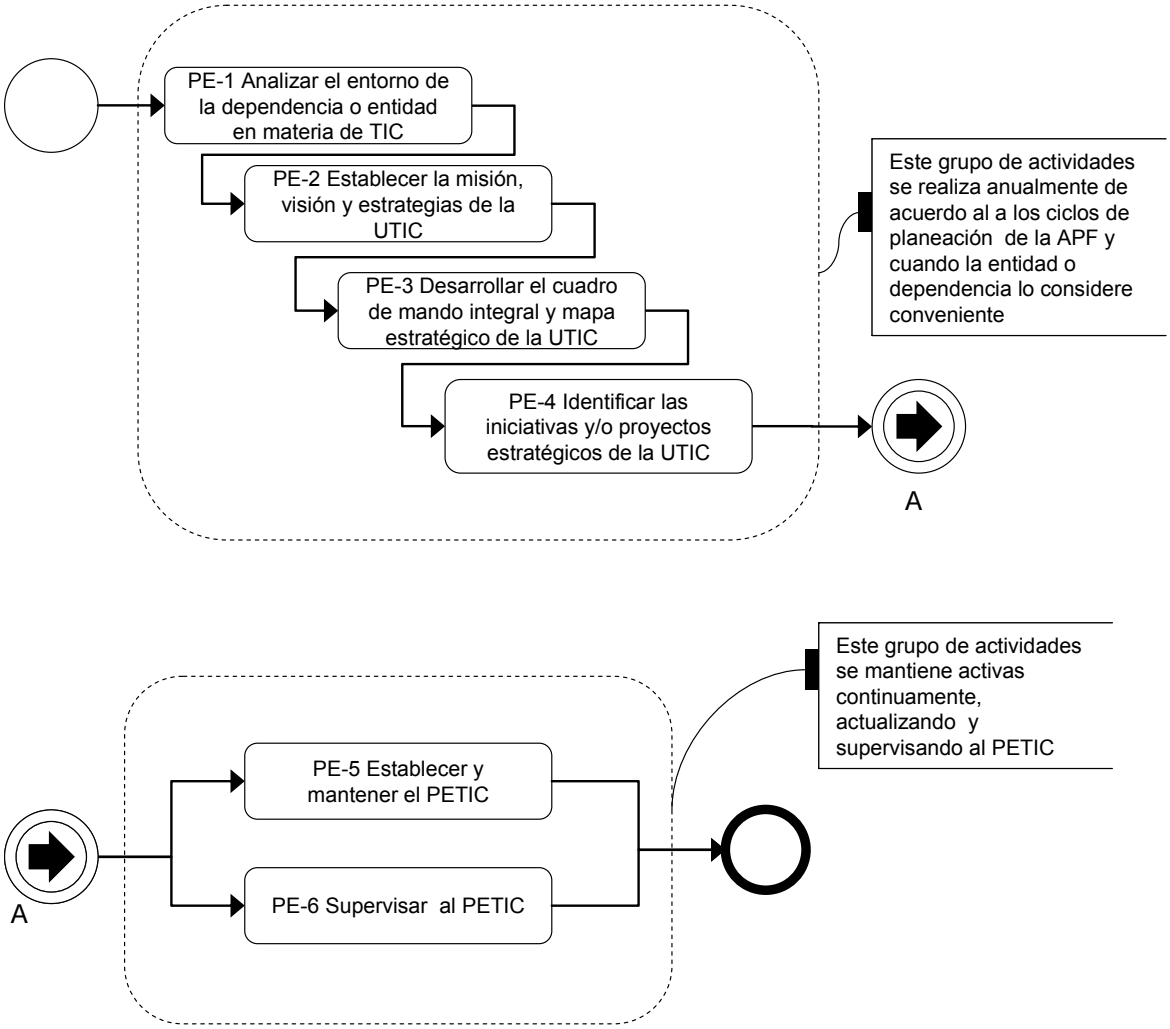


Diagrama de flujo de actividades



7.1.2.2.2 Descripción de las actividades del proceso

PE-1 Analizar el entorno de la dependencia o entidad en materia de TIC

Descripción	Identificar y analizar los factores que conforman el entorno de la organización en materia de TIC y la situación actual, esto incluye los elementos regulatorios, normativos y tecnológicos que influyen en la ejecución de las actividades y servicios que brinda la UTIC en apoyo a las funciones sustantivas de la dependencia o entidad.
Factores Críticos	1. Realizar un análisis de fortalezas, oportunidades, debilidades y amenazas que influyen en el cumplimiento de las funciones de la dependencia o entidad en materia de TIC. 2. Identificar los principales hechos o eventos del ambiente externo que podrían representar alguna amenaza u oportunidad para la dependencia o entidad. • Algunos factores a considerar pueden ser: legales, regulatorios, políticos, económicos, sociales, tecnológicos, entre otros. • Identificar a través del análisis del ambiente externo las principales oportunidades (situaciones externas positivas, que se generan en el entorno y que una vez identificadas pueden ser aprovechadas para generar valor). • Identificar a través del análisis del ambiente externo las principales amenazas (situaciones negativas, externas a la dependencia o entidad, que puedan afectar el cumplimiento de sus objetivos, planes y proyectos, por lo que llegado el caso, puede ser necesario diseñar una estrategia adecuada para poder enfrentarla). 3. Identificar las principales fortalezas y debilidades que están presentes en la dependencia o entidad, para el cumplimiento de sus objetivos y funciones. • Algunos factores a considerar pueden ser: disponibilidad de recursos tecnológicos, financieros, personal, activos, procesos, calidad de la infraestructura y/o de servicios, estructura interna y percepción de los usuarios). • Identificar durante el análisis del ambiente interno las principales fortalezas (elementos internos y positivos que le dan ventaja a la dependencia o entidad, para cumplir con sus funciones de manera efectiva y eficiente). • Identificar durante el análisis del ambiente interno las principales debilidades (problemas internos que constituyen barreras para lograr un mejor desempeño de la dependencia o entidad, que una vez identificados y desarrollando una adecuada estrategia pueden eliminarse).
Relación de Productos	• Matriz FODA

PE-2 Establecer la misión, visión y estrategias de la UTIC

Descripción	Establecer, documentar y comunicar la misión y visión de TIC, que transmita de manera efectiva los propósitos y objetivos de la UTIC.
Factores Críticos	1. Establecer la misión de la UTIC en la dependencia o entidad. • La misión deberá describir de manera clara y concreta el objetivo fundamental que persigue la UTIC, a fin de lograr el compromiso inmediato de los miembros que la conforman.

	2. Establecer la visión de la UTIC. • La visión de la UTIC deberá describir de manera breve, la situación deseada que busca alcanzar la UTIC a largo plazo, esta visión debe describir el futuro de la UTIC, ser fácil de recordar y estar alineada a los objetivos estratégicos. • La visión de la UTIC, deberá ser elaborada pensando en el escenario ideal de desempeño de manera efectiva, cumplimiento de sus objetivos y alineación de sus planes. 3. Documentar y difundir la misión y visión de la UTIC. • La misión y visión de la UTIC deberán estar documentadas formalmente y aprobadas por el titular de la dependencia o entidad (o en su caso por el grupo de trabajo estratégico de TIC) • La misión y visión de la UTIC, deberán ser difundidas y comunicadas a todos los miembros de la dependencia o entidad. • De manera constante se deberá difundir la misión y visión de la UTIC, a fin de que se mantenga presente en los servidores públicos de la dependencia o entidad. 4. Obtener el compromiso sobre la misión y visión de la UTIC. • Se deberá obtener el compromiso sobre la misión y visión de la UTIC por parte del grupo de trabajo estratégico de TIC, conformado por los mandos superiores y miembros clave de la dependencia o entidad. • Se deberán realizar actividades continuas que busquen transmitir y sensibilizar a los servidores públicos para trabajar alineados a la misión y visión de la UTIC
Relación de Productos	• Documento estratégico de TIC

PE-3 Desarrollar el cuadro de mando integral y mapa estratégico de la UTIC

Descripción	Establecer objetivos y metas claras a partir de la estrategia de la UTIC en términos operacionales, mediante el diseño e implementación de un cuadro de mando integral de TIC que abarque la perspectiva financiera, de usuario o cliente, procesos, desarrollo de personal y aprendizaje.
Factores Críticos	1. Analizar la situación actual y obtener información. 2. Analizar y determinar las funciones sustantivas de la dependencia o entidad. 3. Identificar las necesidades 4. Diseñar un mapa estratégico • Analizar la perspectiva financiera: analizar los factores críticos que permitan tener una situación económica saludable en la UTIC, esto incluye el uso adecuado de los recursos financieros, el análisis del costo de operación de los servicios de TIC y en su caso la salud financiera de la UTIC. • Analizar la perspectiva de cliente o usuario: analizar los factores críticos que permiten mantener niveles de satisfacción adecuados con los usuarios de los servicios de TIC, que son proporcionados por la dependencia o entidad. • Analizar la perspectiva de procesos: analizar los factores críticos que permitan

	mantener procesos y procedimientos adecuados para operar de manera efectiva, eficiente y con un adecuado nivel de control, a fin de cumplir con las necesidades de los usuarios de los servicios de TIC. • Analizar la perspectiva de desarrollo de personal y aprendizaje: analizar los factores críticos que permitan desarrollar las capacidades del personal de la dependencia o entidad y el conocimiento necesario para ejecutar los procesos y procedimientos que son empleados para operar en la dependencia o entidad. • Analizar las relaciones y dependencias entre los elementos de las cuatro perspectivas. 5. Identificar las variables e indicadores críticos en cada una de las perspectivas. 6. Establecer la correspondencia eficaz y eficiente entre las variables críticas y las medidas precisas para su control en un mapa estratégico de la UTIC 7. Configurar un cuadro de mando integral.
Relación de Productos	• Mapa estratégico de la UTIC • Cuadro de mando integral

PE-4 Identificar las iniciativas y/o proyectos estratégicos de la UTIC

Descripción	Identificar las principales iniciativas y/o proyectos que deben ser ejecutados por la dependencia o entidad, para cumplir con los objetivos estratégicos de la dependencia o entidad y el mapa estratégico de TIC.
Factores Críticos	1. Analizar los objetivos estratégicos de la dependencia o entidad y el mapa estratégico de la UTIC. • Antes de definir iniciativas, proyectos o presupuestar recursos para las actividades diarias de la dependencia o entidad, se deberán analizar los objetivos estratégicos de la dependencia o entidad y el mapa estratégico de la UTIC. 2. Determinar las iniciativas y/o proyectos estratégicos de TIC necesarios con el fin de cumplir con los objetivos estratégicos de la dependencia o entidad. • Realizar una lista y priorizar las iniciativas y/o proyectos estratégicos de TIC, a fin de cumplir con las funciones sustantivas y los objetivos estratégicos de la dependencia o entidad. • Para cada iniciativa y/o proyecto estratégico de TIC, se deberá identificar información de acuerdo a lo que se establezca en el proceso de Administración de portafolio de proyectos de TIC. 3. Estimar el presupuesto de alto nivel requerido por la iniciativa y/o proyectos estratégicos de la UTIC. • Para cada iniciativa y/o proyecto estratégico de la UTIC, se deberá estimar el presupuesto y los recursos necesarios para su ejecución, este presupuesto deberá considerar los recursos financieros para la contratación de los servicios o en su caso la adquisición, puesta en operación y mantenimiento de la solución tecnológica y/o el servicio de TIC. De igual forma se deberá estimar el esfuerzo interno y/o recursos humanos necesarios para adquirir, supervisar y administrar la solución tecnológica o el

	servicio de TIC. 4. Integrar las iniciativas y/o proyectos estratégicos al portafolio de proyectos de TIC para su evaluación, selección y autorización. • Se deberá priorizar las iniciativas y/o proyectos estratégicos de la UTIC, con base en su relevancia con respecto a los objetivos estratégicos y funciones sustantivas. • Se deberá realizar un análisis para asignar el nivel de prioridad de atención de las iniciativas y/o proyectos estratégicos de la UTIC. • Se deberá ponderar con mayor relevancia aquellos proyectos de la UTIC, que permitan cumplir los objetivos estratégicos de la dependencia o entidad, aporten mayor valor a los ciudadanos y sus organizaciones, permitan mejorar los trámites y servicios hacia los ciudadanos y cumplan con los aspectos legales y regulatorios.
Relación de Productos	• Iniciativas y/o proyectos estratégicos de la UTIC

PE-5 Establecer y mantener el PETIC

Descripción	Diseñar, documentar y mantener el plan estratégico de la UTIC que permita establecer los objetivos, misión, visión y líneas de acción estratégicas en materia de TIC, que guíen las actividades de la dependencia o entidad a corto, mediano y largo plazo.
Factores Críticos	1. Documentar la información relativa a la planeación estratégica de la UTIC de la dependencia o entidad. • El PETIC deberá contener información relativa a los siguientes aspectos: a. Descripción y beneficios de la implementación del proyecto. b. Análisis del ambiente externo e interno c. Misión y visión de la UTIC. d. Portafolio de iniciativas y/o proyectos estratégicos de la UTIC autorizados e. Presupuesto estimado f. Priorización de iniciativas y/o proyectos estratégicos de la UTIC g. Mecanismos de comunicación h. Descripción de roles y responsabilidades i. Mecanismos de seguimiento 2. Revisar y validar el plan estratégico de la UTIC • El personal clave de la dependencia o entidad, deberá participar en la elaboración y revisión del plan estratégico de la UTIC. • Es recomendable que la elaboración del plan estratégico de la UTIC, se realice mediante sesiones de trabajo colegiadas con la participación del grupo de trabajo para la dirección de TIC conformado en el proceso de estructura de gobierno. En estas sesiones participa personal clave de las áreas involucradas que incluye de ser posible a representantes de las áreas usuarias y/o normativas que influyen en los requerimientos tecnológicos y/o que sean receptores de los servicios o soluciones

	tecnológicas que la dependencia o entidad produce y opera • El plan estratégico de la UTIC deberá ser revisado de acuerdo a las decisiones de financiamiento y autorización del portafolio de proyectos de TIC. 3. Aprobar el plan estratégico de la UTIC • El plan estratégico de la UTIC deberá ser aprobado y firmado por los mandos superiores de la dependencia o entidad. 4. Mantener el plan estratégico de la UTIC • El plan estratégico de la UTIC deberá ser revisado y mantenerse actualizado y vigente. • El plan estratégico de la UTIC, podrá ser actualizado cuando: la estrategia cambie significativamente, la situación externa y/o interna afecte el cumplimiento de los objetivos, cuando se requiera afinar la estrategia definida, cuando exista un cambio en la administración de la dependencia o entidad, a fin de obtener nuevamente el compromiso de los mandos superiores.
Relación de Productos	• PETIC.

PE-6 Supervisar al PETIC

Descripción	Supervisar periódicamente los avances en el cumplimiento del plan estratégico de la UTIC
Factores Críticos	1. Dar seguimiento de manera planeada al PETIC y reportar trimestralmente su avance. 2. Informar periódicamente a los mandos superiores sobre el cumplimiento de las líneas de acción del plan estratégico de la UTIC y la situación que guardan los indicadores del cuadro de mando integral. 3. Identificar, registrar y administrar las acciones correctivas en caso de desviación. 4. Registrar y dar seguimiento a los acuerdos con los mandos superiores. 5. Implementar un sistema de medición para evaluar el desempeño de la incorporación de las TIC que permita la mejora continua del gobierno.
Relación de Productos	• Reportes de seguimiento y control del PETIC

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.1.2.2.3 Descripción de roles

Rol	Descripción
Director General /Alta Dirección	Es responsable de asegurar que las actividades de planeación estratégica se desarrollen en la dependencia o entidad
Responsable de la UTIC	Participar y Coordinar las sesiones de planeación estratégica de la UTIC y ejecutar sus actividades de acuerdo a lo definido en el PETIC

Responsable de la Planeación de la UTIC	Realizar investigación y análisis tecnológico y generar estrategias de TIC, así como convocar a los responsables de las Áreas administrativas clave, para definir conjuntamente el PETIC de la dependencia o entidad.
Equipo de Trabajo	Apoyar en la generación e integración del PETIC.
Grupo de Trabajo Estratégico de TIC	Equipo responsable conformado por los mandos superiores y miembros clave de la dependencia o entidad encargado de definir y establecer la visión y la misión de la UTIC

7.1.2.2.4 Descripción de productos

Producto	Descripción
Matriz FODA	Contiene la información de Fortalezas y debilidades, resultado del análisis del entorno interno así como, las amenazas y oportunidades resultado del análisis del entorno externo.
Documento estratégico de TIC	Documenta la visión y misión revisadas y aprobadas por el titular de la dependencia o entidad a quien el faculte.
PETIC	Documenta la información relativa a la planeación estratégica de la UTIC de una dependencia o entidad describe al menos los siguientes aspectos: a) Análisis del ambiente externo e interno b) Misión y visión de la UTIC c) Inventario de iniciativas estratégicas d) Portafolio de proyectos autorizados e) Presupuesto f) Priorización de iniciativas y proyectos g) Mecanismos de comunicación h) Mecanismos de seguimiento, control y evaluación
Mapa estratégico de la UTIC	Describe de manera gráfica la estrategia de la dependencia o entidad desde las siguientes perspectivas: a) Perspectiva financiera b) Perspectiva del usuario c) Perspectiva de procesos d) Perspectiva de desarrollo de personal y aprendizaje
Cuadro de mando integral	Describe de manera cuantitativa las metas y los indicadores que permiten medir el cumplimiento de la estrategia de la dependencia o entidad desde las siguientes perspectivas: a) Perspectiva financiera b) Perspectiva del usuario c) Perspectiva de procesos

Producto	Descripción
	d) Perspectiva de desarrollo de personal y aprendizaje
Iniciativas y/o proyectos estratégicos de la UTIC	Contiene la relación de iniciativas y/o proyectos estratégicos que han sido identificados y en su oportunidad evaluados y autorizados en sustento a la estrategia de la dependencia o entidad. Deberá contener al menos la información documentada de acuerdo a lo que se establezca en la ejecución del proceso de administración del portafolios de proyectos.
Reportes de seguimiento y control del PETIC	Contiene la evidencia de la realización de sesiones de presentación de avances sobre el cumplimiento del PETIC de la UTIC a los mandos medios y superiores, dichos reportes deberán contener información relativa a: a) Fecha y participantes b) Situación actual de los indicadores del cuadro de mando integral c) Identificación de desviaciones en caso de existir d) Registro y estado de las acciones correctivas

7.1.2.3. Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de cumplimiento del PETIC	Medir el grado de cumplimiento del PETIC	Es el porcentaje obtenido para alcanzar los objetivos establecidos	Eficacia	De gestión	(PETIC implantado / PETIC propuesto) *100	Titular de la UTIC	Trimestral

7.1.2.4 Reglas del proceso

1.1	Garantizar una planeación estratégica eficiente, considerando el modelo de gobierno digital y las estrategias planteadas en la AGD.
1.2	La UTIC deberá presentar a la UGD el PETIC a través del sistema que establezca la UGD para tal efecto.
1.3	La UTIC deberá asegurar la correcta dirección sobre las prioridades de los proyectos.
1.4	El titular de la UTIC deberá asegurar la comunicación y entendimiento del PETIC al personal de las áreas de la UTIC de manera formal.
1.5	La UTIC deberá establecer un cuadro de mando integral con indicadores que permitan dar seguimiento al cumplimiento de los objetivos y las estrategias definidas en el Documento estratégico de TIC y en el PETIC.
1.6	Las dependencias y entidades de la APF deberán mantener actualizada a la UGD acerca del avance en el PETIC y su proceso de planeación estratégica de TIC, de acuerdo a las fechas que establezca la UGD para tal efecto.

7.1.2.5 Documentación soporte del proceso

No aplica

7.1.3. Determinación de la dirección tecnológica

7.1.3.1. Objetivos del proceso

Generales.-

Determinar la dirección tecnológica de la institución para crear una arquitectura tecnológica que facilite la selección, el desarrollo, la aplicación y el uso de la infraestructura de TIC de manera que ésta responda a la dinámica de la dependencia o entidad.

Específicos.-

1. Determinar los requerimientos tecnológicos derivados de las necesidades de la dependencia o entidad que deberán ser incorporados en la creación de la arquitectura tecnológica.
2. Definir un modelo para la arquitectura tecnológica que incluya los diversos dominios tecnológicos necesarios para estandarizar y evolucionar la infraestructura de TIC de manera que ésta cuente con la capacidad necesaria para satisfacer las necesidades actuales y futuras de la dependencia o entidad.
3. Asegurar que el plan de tecnología tenga un balance entre necesidades, innovación, beneficios, riesgos y costos y dirija a la dependencia o entidad hacia el desarrollo de nuevas formas de cumplir con sus objetivos sustantivos.

7.1.3.2 Descripción del Proceso

7.1.3.2.1 Mapa general del proceso

Diagrama de flujo de información

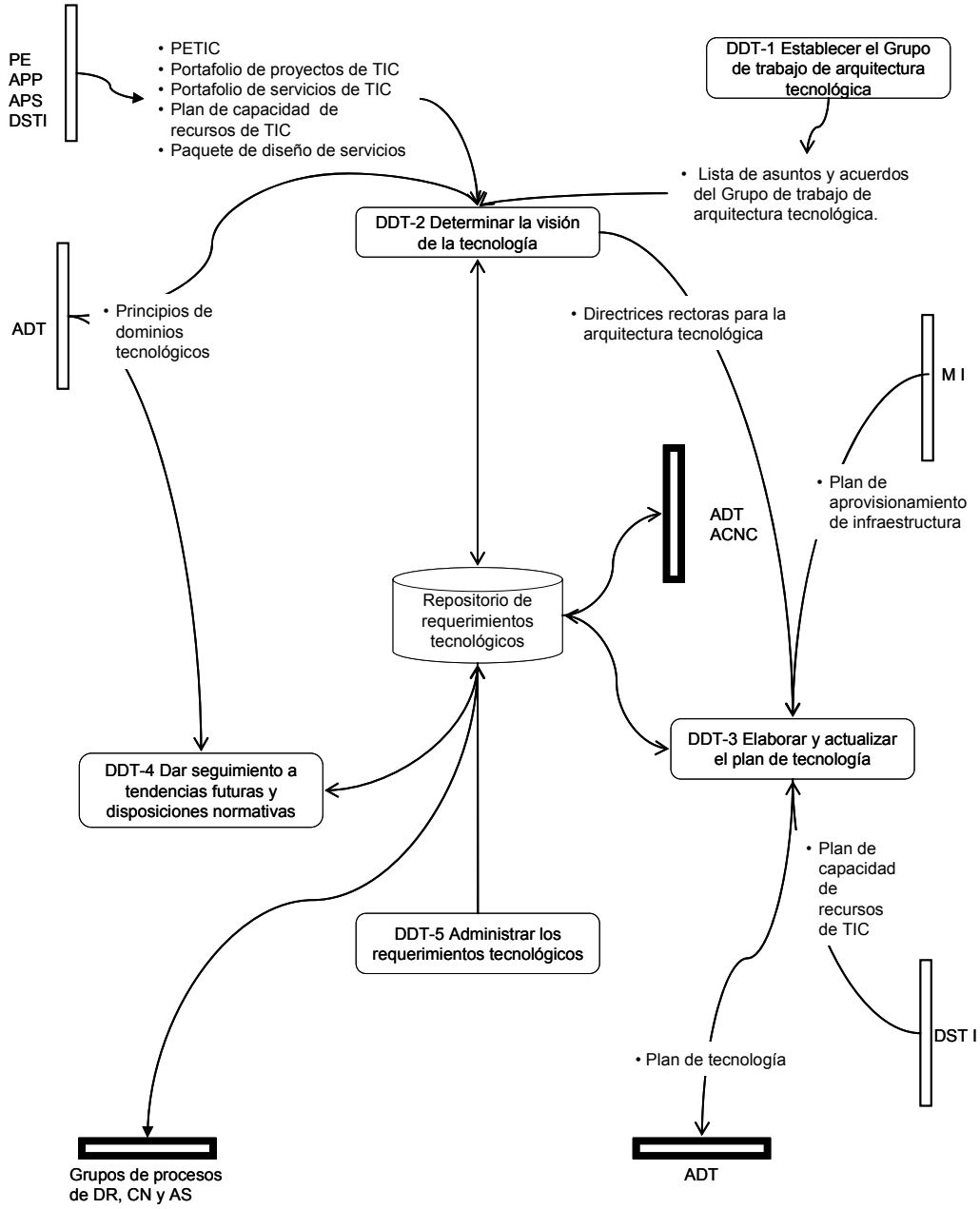
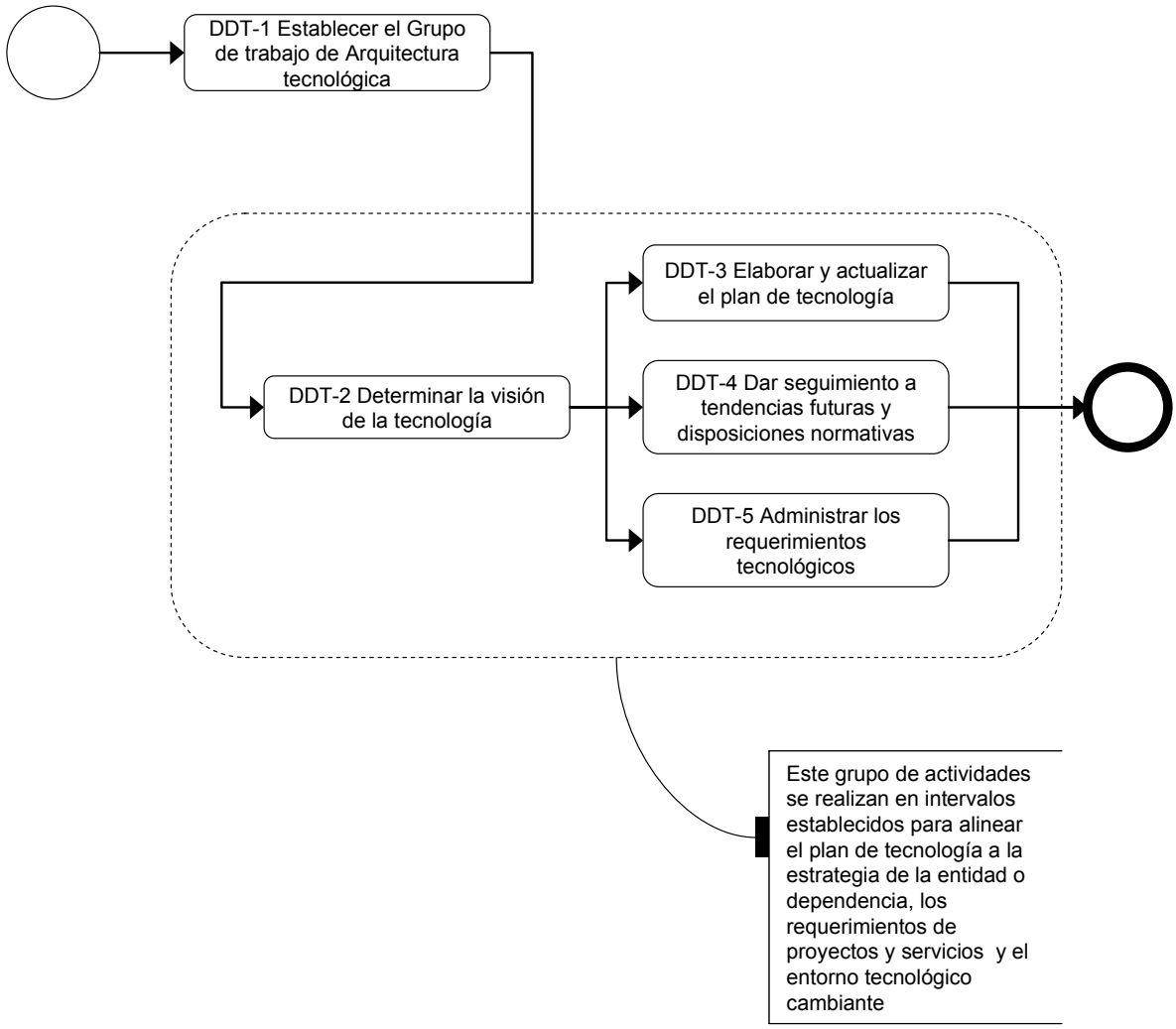


Diagrama de flujo de actividades



7.1.3.2.2 Descripción de las actividades del proceso

DDT-1: Establecer el grupo de trabajo de arquitectura tecnológica

Descripción	Proporcionar las directrices sobre la arquitectura tecnológica, asesoría sobre su aplicación, y que verifique el cumplimiento a estándares.
Factores Críticos	1. Establecer un grupo de trabajo de arquitectura tecnológica para proveer directrices relativas a las TIC y asesoría en su aplicación. 2. Acordar y documentar formalmente el rol y la autoridad del grupo de trabajo de arquitectura tecnológica. El grupo de trabajo de arquitectura tecnológica orienta el diseño de la arquitectura tecnológica garantizando que facilite la estrategia de la dependencia o entidad y tome en cuenta el cumplimiento regulatorio y los requerimientos tecnológicos de la dependencia o entidad. 3. Asegurar que el grupo de trabajo de arquitectura tecnológica se reúne regularmente y que se establecen formalmente los acuerdos y se da seguimiento a las acciones que se deriven de estas reuniones.
Relación de Productos	• Lista de asuntos y acuerdos del grupo de trabajo de arquitectura tecnológica

DDT-2: Determinar la visión de la tecnología

Descripción	Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada para materializar los objetivos y estrategia de la dependencia o entidad así como la provisión de los servicios de información acordes a los requerimientos de negocio. Esta práctica permite identificar cuales tecnologías tienen el potencial de crear oportunidades para la dependencia o entidad.
Factores Críticos	1. Determinar los requerimientos tecnológicos derivados de las necesidades de la dependencia o entidad, objetivos, estrategias, proyectos y servicios que deberán ser soportados por la dirección tecnológica En la identificación de los requerimientos tecnológicos de la dependencia o entidad puede ser útil desarrollar escenarios de uso que contemplen una descripción completa de la situación o necesidad de negocio en conjunto con la perspectiva tecnológica, esto permite analizar requerimientos específicos en relación al impacto que tienen en el negocio. 2. Traducir los requerimientos tecnológicos de la dependencia o entidad en términos de directrices rectoras para la arquitectura tecnológica. 3. Definir el alcance, estructura y nivel de detalle de los dominios de la arquitectura tecnológica. La arquitectura tecnológica deberá estar definida en niveles. El alcance y nivel de detalle de cada uno de los dominios de la arquitectura deberá ser consistente con el nivel de detalle necesario para sustentar los requerimientos tecnológicos determinados. Los niveles que típicamente se consideran en la arquitectura tecnológica son: • Arquitectura de datos/información: Entendida como la descripción del ciclo de vida integral de la información, es decir, debe representar como la información es capturada, modificada, agregada y distribuida a lo largo de dependencia o entidad, por lo que debe permitir identificar y describir las necesidades de información en términos

	de qué área y/o departamento genera y requiere qué información. En resumen, describe la estructura de los datos físicos y lógicos de la dependencia o entidad, y los recursos de gestión de estos datos. • Arquitectura de aplicaciones: Entendida como el modelo del portafolio de aplicaciones, actuales y futuras que la dependencia o entidad requiere para soportar sus capacidades sustantivas, la forma en que están/estarán organizadas y como están/estarán relacionadas, de tal manera, que cuándo la dependencia o entidad requiera incorporar nuevas aplicaciones pueda identificar la forma en la que está organizado su portafolio de aplicaciones. • Arquitectura de infraestructura tecnológica: Entendida como la definición de los marcos técnicos de referencia, principios, modelos, estándares, etc. necesarios para gobernar los recursos tecnológicos necesarios para la provisión de los servicios de TIC (hardware, software, redes, etc.) Mediante la inclusión de un cuarto dominio, la arquitectura de negocio puede extender el alcance de la arquitectura tecnológica a una arquitectura empresarial incluyendo la dimensión de los objetivos y procesos de la dependencia o entidad. Esta arquitectura es el resultado de la definición de estrategias, funciones, procesos y requerimientos funcionales. La arquitectura de negocio nos permite evaluar, e inclusive simular, cambios en los procesos sustantivos o, causados por posibles cambios de estrategia o metas. Tener una arquitectura de negocios permite asegurar calidad y consistencia en los esfuerzos de diseño y rediseño de los procesos sustantivos. Una de los beneficios clave de tener una arquitectura de negocios, desde la perspectiva de TIC, es que permite definir entregables relativos a información, contexto, y requerimientos tecnológicos necesarios para soportar los cambios propuestos 4. Realizar regularmente un análisis de las fortalezas, oportunidades, debilidades y amenazas (FODA) de todos los elementos críticos de la arquitectura tecnológica. 5. Dar seguimiento a la evolución del mercado y a las tecnologías emergentes con el propósito de identificar las tecnologías de punta que puedan tener un impacto en el éxito de la dependencia o entidad. 6. Realizar la selección de las áreas y tópicos de investigación de TIC en función de las iniciativas y/o proyectos de TIC identificados y/o de los requerimientos tecnológicos identificados. 7. Documentar las investigaciones en materia de TIC y derivar de las mismas las directrices rectoras que el grupo de trabajo de arquitectura tecnológica determine.
Relación de Productos	• Directrices rectoras para la arquitectura tecnológica

DDT-3: Elaborar y actualizar el plan de tecnología

Descripción	Crear y mantener un plan de tecnología que esté de acuerdo con los planes estratégicos y tácticos de la UTIC. El plan se basa en la dirección tecnológica e incluye directrices para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente

	competitivo, las economías de escala para inversiones y personal, en componentes tecnológicos, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.
Factores Críticos	1. Elaborar el Plan de tecnología basado en un análisis por cada uno de los dominios de la arquitectura tecnológica: • Describir el estado actual de los componentes del dominio para establecer una línea base para sustentar la planeación (de dónde partimos). • Desarrollar descripciones de la arquitectura meta para el dominio, conforme a la visión tecnológica de la dependencia o entidad. • Seleccionar y documentar las perspectivas arquitectónicas de la arquitectura objetivo de forma que demuestre que da respuesta a los requerimientos tecnológicos y a los objetivos de los interesados a un plazo determinado. Acordar la arquitectura objetivo con los interesados. • Analizar las brechas entre la arquitectura actual y la arquitectura objetivo. • Desarrollar una o más descripciones de arquitecturas en transición como incrementos o “estados”, alineados a la descripción de la arquitectura objetivo y describiendo los incrementos, resultando en una estrategia de transformación para llegar de la situación actual a la deseada, considerando aspectos de contingencia. 2. Integrar en el Plan de tecnología los planes de cada uno de los dominios de forma que conformen un marco integral de arquitectura de la dependencia o entidad que integra a las arquitecturas individuales. Esta integración permite: • Entender cómo los componentes de tecnología se integran en un enfoque sistémico, derivar modelos arquitectónicos que se enfocan en capacidad a nivel de la dependencia o entidad, definir los estándares que habilitarán la integración de componentes para maximizar el re-uso y potenciar la interoperabilidad, y asegurar que las descripciones de los diferentes dominios pueden combinarse en una sola representación lógica. 3. Evaluar y seleccionar la alternativa de implementación para el desarrollo de las arquitecturas meta. • Identificar los factores críticos para la transición y las iniciativas y/o proyectos de tecnología requeridos para pasar del estado actual al deseado así como evaluar las dependencias, costos y beneficios de los distintos proyectos. 4. Integrar las iniciativas de proyectos derivados de la planeación tecnológica en un programa de iniciativas de tecnología que considere la prioridad, el orden, las dependencias y los beneficios de las diferentes iniciativas/proyectos. 5. Incluir en el Plan de tecnología los costos relacionados con las iniciativas y/o proyectos de tecnología y otros costos derivados de la estrategia de transformación, complejidad, riesgos tecnológicos, economías de escala para el personal de sistemas e inversiones, y las mejoras esperadas en la interoperabilidad de plataformas y aplicaciones. 6. Someter el plan de tecnología y su programa de iniciativas y/o proyectos asociados al proceso de Administración de Portafolios de Proyectos para su evaluación, selección y autorización.

	7. Revisar el Plan de tecnología de acuerdo a las iniciativas y/o proyectos autorizados. 8. Dar seguimiento a la implementación del plan de tecnología. 9. Revisar y actualizar periódicamente el plan de tecnología. Asegurar que todos los grupos interesados se involucran en el desarrollo y aprobación de los planes de migración y de cambio, considerando el impacto en el personal y las operaciones. 10. Establecer un proceso de control de cambios en la arquitectura tecnológica, conforme al proceso Administración de cambios, para asegurar que los requerimientos de cambios se atienden en una forma integral desde la perspectiva arquitectónica. Se determinan las circunstancias bajo las cuáles componentes arquitectónicos podrán cambiarse una vez implementados así como los pasos para efectuar el cambio y el proceso para que esto suceda y las circunstancias para iniciar el ciclo de actualización de la arquitectura.
Relación de Productos	• Plan de tecnología

DDT-4: Dar seguimiento a tendencias futuras y disposiciones normativas

Descripción	Establecer un proceso para dar seguimiento, e incluir en el Plan de tecnología, a las tendencias del sector, tecnológicas, de infraestructura, legales y regulatorias.
Factores Críticos	1. Asegurar que se cuenta con personal capacitado dentro de la UTIC para dar seguimiento a los desarrollos y tendencias tecnológicas, programas y actividades del sector, asuntos de infraestructura y cambios a requerimientos y disposiciones normativas. 2. Consultar expertos externos para validar el entendimiento interno de la UTIC de las oportunidades y beneficios derivados de las nuevas tecnologías. 3. Participar en los foros y grupos de especialistas que se establezcan para determinar la política informática de la administración pública. 4. Proveer información relevante en materia de tendencias tecnológicas a los mandos medios y superiores y tomadores de decisiones de la dependencia o entidad. 5. Evaluar tecnologías emergentes en el contexto de su posible contribución al logro de los objetivos estratégicos y al crecimiento de la dependencia o entidad. 6. Asegurar que se da seguimiento a los cambios en las disposiciones y normas relativas a los componentes tecnológicos, que se analiza el impacto en el plan de tecnología y se hacen los cambios pertinentes para adecuar el cambio.
Relación de Productos	• Proceso de seguimiento a los desarrollos y tendencias tecnológicas.

DDT-5: Administrar los requerimientos tecnológicos

Descripción	Identificar, almacenar y comunicar los requerimientos tecnológicos derivados de las necesidades de la dependencia o entidad, objetivos, estrategias, proyectos y servicios que deberán ser soportados por la dirección tecnológica.
Factores Críticos	1. Registrar requerimientos tecnológicos incluyendo requerimientos para la arquitectura objetivo, es la base para la elaboración del Plan de tecnología.

	2. Priorizar requerimientos tecnológicos. 3. Determinar la prioridad de los requerimientos tecnológicos de acuerdo a su tipo y etapa en el ciclo de vida de la Arquitectura tecnológica. 4. Dar seguimiento a los requerimientos tecnológicos: En caso de ser necesario reasignar prioridades, agregar nuevos requerimientos, ajustar, modificar o dar de baja requerimientos. 5. Generar análisis de impacto de los cambios en los requerimientos para presentarlos al grupo de trabajo de arquitectura tecnológica.
Relación de Productos	• Repositorio de requerimientos tecnológicos administrado

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.1.3.2.3 Descripción de roles

Rol	Descripción
Grupo de trabajo de arquitectura tecnológica	Grupo de expertos que tendrá la responsabilidad de proporcionar directrices sobre la arquitectura tecnológica, dar asesoría sobre su aplicación y verificar el cumplimiento a estándares. El grupo de trabajo de arquitectura tecnológica integra representantes de los grupos de expertos de los distintos dominios tecnológicos (ver proceso de Administración de dominios tecnológicos).

7.1.3.2.4 Descripción de productos

Producto	Descripción
Plan de tecnología	El documento que contiene al menos: la dirección tecnológica de la dependencia o entidad, la visión de la arquitectura tecnológica, las directrices de la arquitectura tecnológica, el Programa de iniciativas y/o proyectos de tecnología, los Planes de adquisición de TIC, las Estrategias de migración y contingencias.
Directrices rectoras para la arquitectura tecnológica	Documentación de los principios tecnológicos de alto nivel, entendido como los principios y/o directrices que deben guiar la estrategia tecnológica, y los mecanismos de gobierno y selección de la plataforma tecnológica de la dependencia o entidad.
Registro de requerimientos tecnológicos	Registro de los requerimientos tecnológicos derivados de las necesidades de la dependencia o entidad.
Lista de asuntos y acuerdos del grupo de trabajo de arquitectura tecnológica	Incluye los acuerdos y decisiones tomados por el grupo de trabajo de arquitectura tecnológica.
Registro de	Lista de acuerdos y decisiones tomadas por grupo de trabajo de arquitectura tecnológica.

Producto	Descripción
acuerdos del grupo de trabajo de arquitectura tecnológica	Lista de acciones y asuntos pendientes.
Proceso de seguimiento a los desarrollos y tendencias tecnológicas	Proceso para dar seguimiento a los desarrollos y tendencias tecnológicas, programas y actividades del sector, asuntos de infraestructura y cambios a requerimientos y disposiciones normativas.
Repositorio de requerimientos tecnológicos administrado	Almacén de información contiene los requerimientos tecnológicos actualizados derivados de las necesidades de la dependencia o entidad, objetivos, estrategias, proyectos y servicios que deberán ser soportados por la dirección tecnológica. Es accedida por los grupos de procesos de DR, CN y AS.

7.1.3.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje del Plan de Tecnología	Medir el grado de cumplimiento del Plan de Tecnología	Es el porcentaje obtenido para alcanzar los objetivos establecidos	Eficacia	De gestión	(Plan de Tecnología implantado / Plan de Tecnología adecuado) *100	Grupo de trabajo de Arquitectura Tecnológica	Anual

7.1.3.4 Reglas del proceso

1.1	La UTIC deberá establecer una arquitectura tecnológica que asegure una respuesta eficiente a los cambios y requerimientos en materia de TIC de la dependencia o entidad.
1.2	La UTIC deberá integrar un grupo de trabajo de arquitectura tecnológica que proporcione las directrices sobre la dirección de la arquitectura tecnológica, asesoría sobre su aplicación y verificación de su cumplimiento.
1.3	La UTIC deberá designar a un responsable del proceso Determinar la dirección tecnológica.

7.1.3.5 Documentación soporte del proceso

	No aplica.

7.2 CONTROL

7.2.1 Administración del desempeño de TIC

7.2.1.1 Objetivos del proceso

General.-

Establecer sistemas de seguimiento y evaluación así como acciones de mejora, a partir de los resultados de la planeación estratégica, del desempeño de los procesos, de los proyectos, del uso y aprovechamiento de los activos, de los recursos así como de la entrega de los servicios de tecnologías de información y comunicaciones.

Específicos.-

1. Establecer un sistema que permita evaluar en forma integral o parcial el desempeño de TIC o de alguno de sus componentes.
2. Proporcionar a titulares y responsables informes de desempeño de TIC y de avance en el cumplimiento de objetivos, que les permita tomar decisiones oportunas e informadas.
3. Establecer y dar seguimiento a las acciones de mejora para prever y corregir desviaciones en el desempeño de las TIC.

7.2.1.2 Descripción del proceso

7.2.1.2.1 Mapa general del proceso

Diagrama de flujo de información

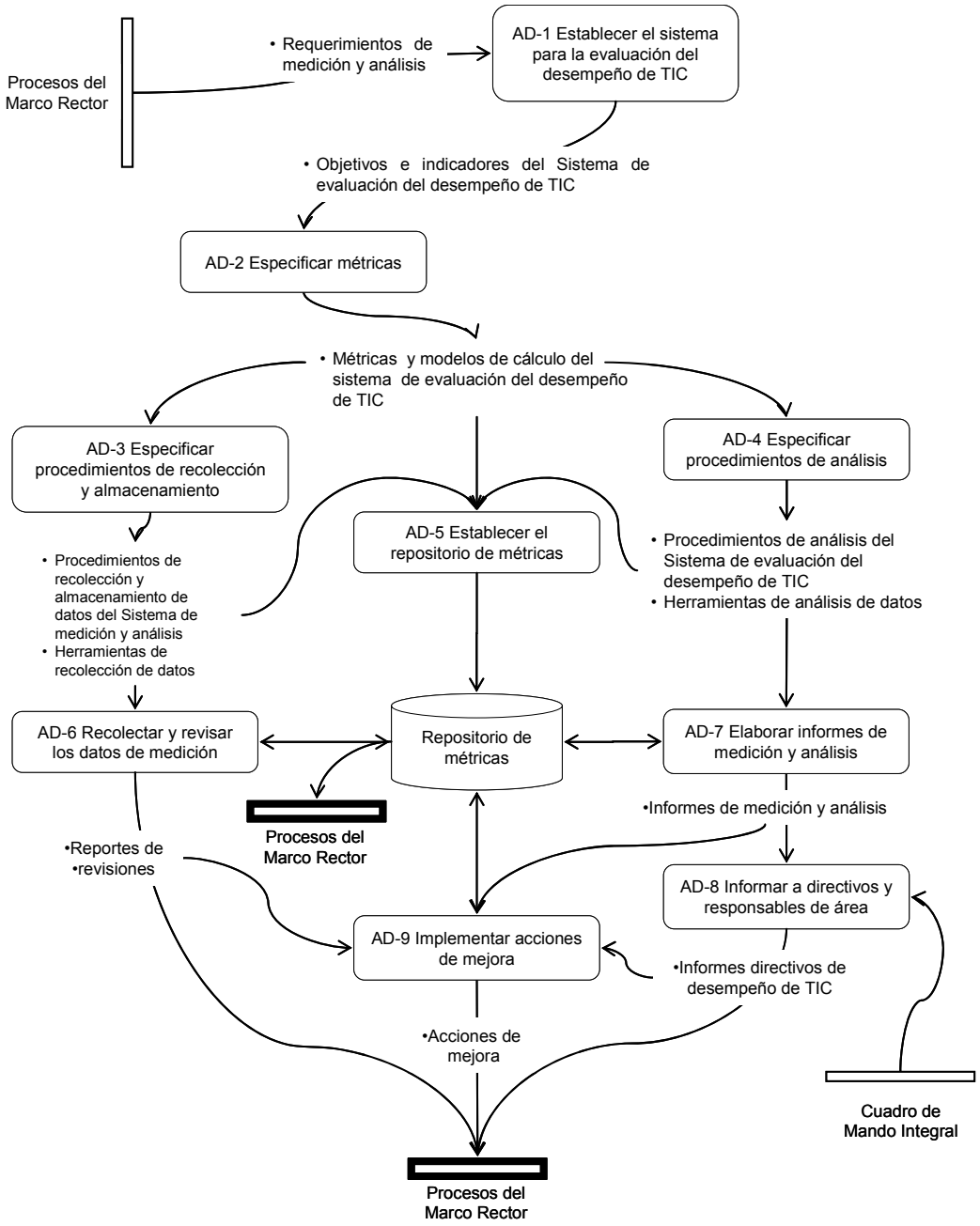
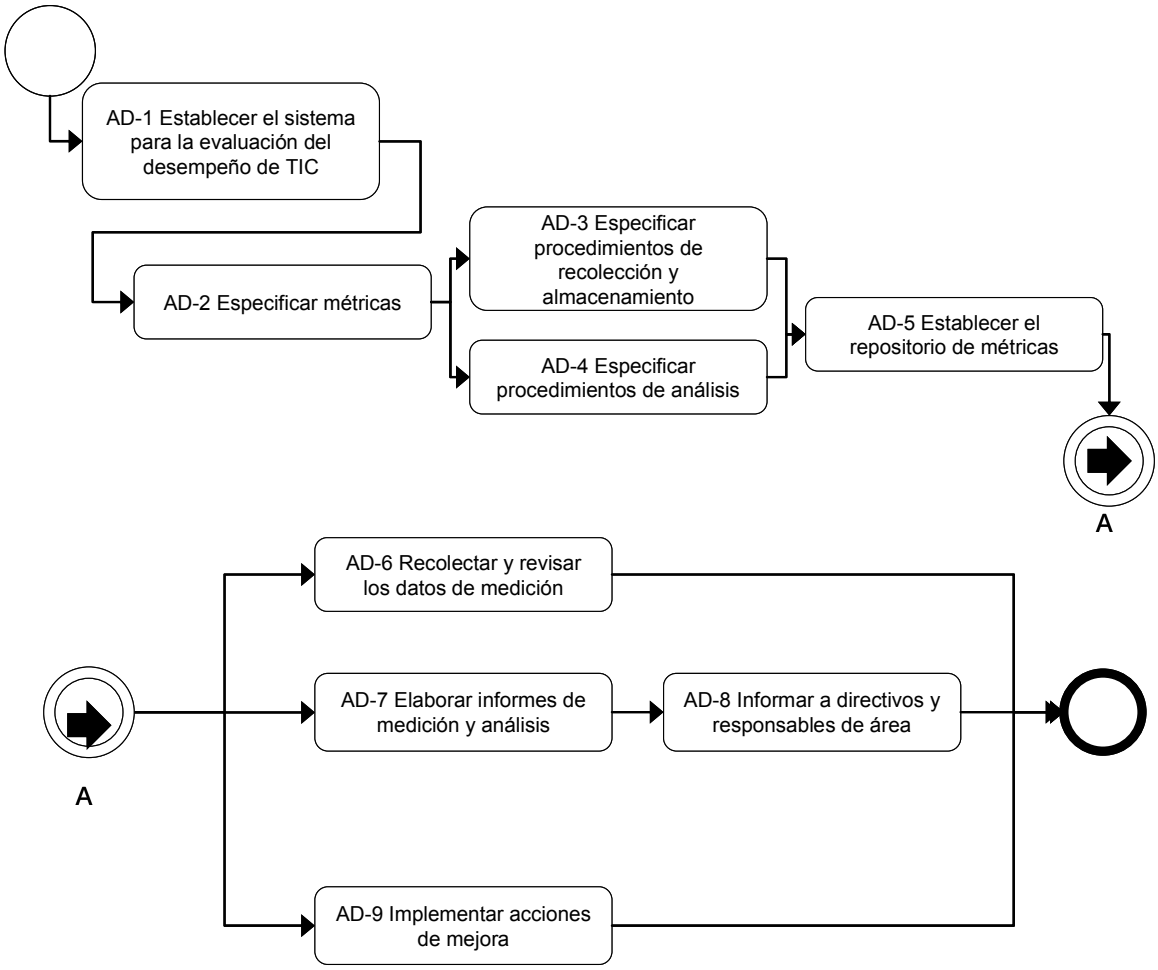


Diagrama de flujo de actividades



7.2.1.2.2 Descripción de las actividades del proceso

AD-1: Establecer el sistema para la evaluación del desempeño de TIC

Descripción	Establecer y mantener los indicadores necesarios para dar seguimiento al estado de la implementación de la estrategia, el desempeño de los procesos, el avance de los proyectos, el uso de los recursos y la entrega de los servicios de TIC.
Factores Críticos	1. Identificar, documentar y priorizar las necesidades de información de indicadores para definir un conjunto balanceado de éstos. 2. Diseñar los indicadores de manera que documenten cuáles métricas y análisis se realizarán, y especifican los tipos de acciones que pueden tomarse basadas en los resultados del análisis de datos. 3. Actualizar continuamente la información insumo de los indicadores, considerando datos de la continuidad de las operaciones normales y el tratamiento de riesgos asociados con el uso de las TIC. 4. Las necesidades de información deben ser clarificadas como resultado del establecimiento de los indicadores. 5. Los indicadores deben orientarse, de manera enunciativa pero no limitativa a proporcionar información de: la satisfacción de los usuarios, la reducción de costos, la optimización del proceso, la madurez del proceso, los niveles de servicio, el cumplimiento regulatorio, la responsabilidad social y el cumplimiento de los objetivos estratégicos. 6. Mantener el rastreo y la trazabilidad de los indicadores con las necesidades y objetivos de información determinados. 7. Formalizar y aprobar los indicadores. 8. Educar y sensibilizar al personal de la UTIC y a los interesados, incluyendo los titulares de las unidades responsables, los usuarios y los mandos superiores sobre la importancia de la evaluación del desempeño de TIC.
Relación de Productos	• Objetivos e indicadores del Sistema de evaluación del desempeño de TIC

AD-2: Especificar métricas

Descripción	Especificar métricas que cubran los indicadores documentados.

Factores Críticos	1. Identificar las métricas de los indicadores documentados, a éstas se debe dar una categoría y especificarse con un nombre, unidad de medida entre otros atributos. 2. Especificar los modelos o fórmulas de cálculo de las métricas. 3. Revisar, aprobar y formalizar las métricas definidas. 4. Verificar la prioridad y vigencia de las métricas periódicamente.
Relación de Productos	• Métricas y modelos de cálculo del sistema de evaluación del desempeño de TIC

AD-3: Especificar procedimientos de recolección y almacenamiento

Descripción	Especificar cómo son obtenidos y almacenados los datos de las métricas
Factores Críticos	1. Identificar orígenes de los datos. 2. Identificar métricas para las cuales se requieren datos que no se encuentran disponibles y revisar la definición de la métrica de ser necesario. 3. Especificar como recolectar y almacenar datos para cada métrica requerida. 4. Crear mecanismos y una guía de recolección de datos integradas en los procesos a ser medidos. 5. Soportar la recolección automática de datos cuando sea apropiado y viable. 6. Priorizar, revisar, aprobar y formalizar tanto las métricas como los procedimientos de recolección y almacenamiento de datos documentados. 7. Actualizar métricas e indicadores periódicamente.
Relación de Productos	• Procedimientos de recolección y almacenamiento de datos del Sistema de medición y análisis • Herramientas de recolección de datos

AD-4: Especificar procedimientos de análisis

Descripción	Especificar cómo son analizados y reportados los datos de las métricas.
Factores Críticos	1. Especificar y priorizar los análisis de información que serán realizados y los reportes que serán preparados. 2. Seleccionar métodos y herramientas apropiados de análisis de datos. 3. Especificar procedimientos administrativos para analizar los datos y comunicar los resultados. 4. Revisar y actualizar el contenido y formato propuesto de los informes necesarios para realizar los análisis especificados. 5. Actualizar métricas e indicadores como sea necesario. 6. Especificar los criterios para evaluar la utilidad de los resultados del análisis y de las actividades de medición y análisis.
Relación de Productos	• Procedimientos de análisis del Sistema de evaluación del desempeño de TIC

	• Herramientas de análisis de datos

AD-5: Establecer el repositorio de métricas

Descripción	Establecer y mantener el repositorio de métricas. El repositorio contiene las métricas definidas en el Sistema de evaluación del desempeño de TIC, también contiene o hace referencia a la información necesaria para entender, interpretar y evaluar las métricas. Este repositorio deberá ser diseñado como un componente del sistema de conocimiento de acuerdo a los procedimientos del proceso de Administración del Conocimiento.
Factores Críticos	1. Determinar las necesidades de almacenamiento, recuperación y análisis de métricas de la dependencia o entidad. 2. Diseñar e implementar el repositorio de métricas. 3. Especificar los procedimientos para almacenar, actualizar, y recuperar las métricas. 4. Hacer que el contenido del repositorio de métricas esté disponible para su uso por la dependencia o entidad y los proyectos según sea apropiado. 5. Revisar el repositorio de métricas y los procedimientos periódicamente y conforme las necesidades de la dependencia o entidad cambien.
Relación de Productos	• Repositorio de métricas

AD-6: Recolectar y revisar los datos de medición

Descripción	Obtener los datos de la especificación de las métricas y analizar e interpretar los datos de las métricas.
Factores Críticos	1. Obtener y/o generar los datos de las métricas 2. Examinar los datos para asegurar su integridad y exactitud. 3. Almacenar la información de acuerdo con los procedimientos de almacenamiento de datos. 4. Afinar criterios para análisis futuros.
Relación de Productos	• Reportes de revisiones

AD-7: Elaborar informes de medición y análisis

Descripción	Administrar y almacenar los datos de métricas, especificaciones de métricas y análisis de resultados, así como elaborar los informes de resultados de las métricas y análisis de actividades.
Factores Críticos	1. Poner a disposición los datos almacenados solo para uso del personal y grupos relevantes. 2. Elaborar los informes de manera que cumplan con los criterios de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. 3. Desarrollar análisis inicial, interpretar los resultados y desarrollar conclusiones preliminares. 4. Desarrollar mediciones y análisis adicionales, como sea necesario y preparar resultados

	para su presentación. 5. Revisar los resultados iniciales con los grupos relevantes. 6. Mantener informados a los grupos relevantes de los resultados de medición. 7. Asesorar a los grupos relevantes en el entendimiento de resultados.
Relación de Productos	• Informes de medición y análisis

AD-8: Informar a directivos y responsables de área

Descripción	Presentar informes directivos de desempeño de TIC con el fin de proporcionar a los titulares la información necesaria para determinar el logro de los objetivos, la eficiencia de los recursos de TIC y evaluar la calidad de los servicios de TIC y de las soluciones tecnológicas desarrolladas.
Factores Críticos	1. Establecer un proceso para informar a los directores y responsables de área en forma oportuna y confiable el estado del desempeño de TIC en términos de la contribución a los objetivos y prioridades de la dependencia o entidad. 2. Diseñar los informes directivos de desempeño de TIC para resaltar asuntos y riesgos clave relacionados con la contribución de TIC y particularmente con la capacidad de desarrollo de soluciones tecnológicas y la entrega de servicios de TIC así como el grado de cumplimiento de los objetivos de desempeño y como se han controlados los riesgos identificados. 3. Consolidar los resultados de las mediciones realizadas y traducirlos en informes de impacto a la operación de la dependencia o entidad (positivo o negativo) e incorporarlos en reportes periódicos a los mandos medios y superiores..
Relación de Productos	• Informes directivos de desempeño de TIC

AD-9: Implementar acciones de mejora

Descripción	Identifican desviaciones, problemas y oportunidades de mejora con base en los informes directivos de desempeño de TIC y datos recolectados de manera que se definan acciones correctivas y preventivas integradas en un plan de mejora.
Factores Críticos	1. Identificar desviaciones, problemas y oportunidades de mejora con base a los informes y datos recolectados. 2. Determinar las acciones correctivas y preventivas. 3. Efectuar la negociación y establecimiento de acciones de mejora, la asignación de las responsabilidades. 4. Definir claramente los resultados esperados del plan de mejora y conducir revisiones periódicas de avance. 5. Identificar desviaciones significativas en la implementación de acciones de mejora y escalar a los responsables de área involucrados. 6. Una vez concluidas las acciones, evaluar los resultados esperados y determinar lecciones aprendidas para disminuir la incidencia de desviaciones en el futuro.
Relación de Productos	• Acciones de mejora

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.2.1.2.3 Descripción de roles

Rol	Descripción
Administrador de métricas	Es responsable de establecer y administrar el Sistema de evaluación del desempeño de las TIC, comunica los resultados de las actividades de dicho plan y da monitoreo a la ejecución de las actividades de medición establecidas en el sistema de evaluación. El Administrador de métricas da seguimiento a las acciones de mejora hasta su conclusión.

7.2.1.2.4 Descripción de productos

Producto	Descripción
Acciones de Mejora	Registro de las acciones preventivas y correctivas que se definan, derivadas del análisis de los informes de evaluación del desempeño de TIC.
Repositorio de Métricas	Es un repositorio utilizado para recolectar y poner a disposición de los interesados los datos de las métricas del plan de evaluación del desempeño de TIC.
Informes de Medición y Análisis	Reportes generados periódicamente de acuerdo al sistema de evaluación del desempeño de TIC para informar a los interesados el resultado de las mediciones efectuadas.
Reportes de Revisión	Reportes con los resultados de las revisiones efectuadas al repositorio de métricas.
Informes directivos de desempeño de TIC	Reportes diseñados para presentar a los directores y titulares de las unidades responsables el grado en el que se han cumplido los objetivos estratégicos y los indicadores del Cuadro de mando integral de TIC y los controles para la administración de los riesgos de TIC.
Sistema de evaluación de desempeño de TIC	Sistema en el cual se establece la estrategia de las actividades de medición y análisis en la dependencia o entidad y su contenido es el siguiente: • Propósito del sistema de evaluación de desempeño de TIC • Alcance • Roles y responsabilidades • Objetivos de medición • Indicadores y Metas cuantitativas • Principales necesidades y Objetivos de Información • Necesidades de Información • Indicadores • Definición de métricas derivadas • Definición de métricas base • Matriz de Objetivos Estratégicos y Métricas • Procedimientos de recolección y Almacenamiento • Procedimientos de análisis • Cronograma de actividades • Recursos e Infraestructura • Reportes de medición y análisis • Repositorio organizacional de métricas

Producto	Descripción
	• Glosario de Términos
Herramientas de análisis de datos	Herramientas usadas para el análisis de los datos e información del repositorio de métricas con el propósito de elaborar informes de medición y análisis.
Herramienta de recolección de datos	Herramientas usadas para la recolección de los datos e información del repositorio de métricas.

7.2.1.3. Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Efectividad en la emisión de información para toma de decisiones	Determinar el grado de cumplimiento de los objetivos de la dependencia o entidad con referencia en los Informes de desempeño de TIC	Es el porcentaje obtenido para verificar el desempeño en alcanzar los objetivos establecidos	Eficacia	De gestión	(Informes directivos de desempeño de TIC que no contribuyen a los objetivos/ Informes directivos de desempeño de TIC planeado) *100	Administrador de métricas	Trimestral
Efectividad del Sistema de evaluación del desempeño	Determinar el grado de cumplimiento del Sistema de Evaluación del desempeño	Es el porcentaje obtenido sobre la eficiencia del Sistema de evaluación del desempeño	Eficacia	De gestión	(Sistema de Medición y Análisis implantado / Sistema de Medición y Análisis planeado) *100	Administrador de métricas	Trimestral

7.2.1.4. Reglas del proceso

1.1 La UTIC deberá asegurar que el Sistema de evaluación del desempeño de TIC integre mediciones y reportes que cubran al menos:

- Los indicadores de desempeño de los objetivos definidos del cuadro de mando integral resultado de la planeación estratégica de TIC.
- Riesgos de TIC y cumplimiento normativo.
- Niveles de satisfacción de usuarios de los servicios de TIC
- Indicadores de desempeño de los procesos clave de TIC, incluyendo los procesos de

	adquisición y desarrollo de soluciones tecnológicas y operación de servicios.
1.2	La UTIC deberá considerar en el diseño del Sistema de evaluación del desempeño de TIC los requerimientos de datos e información para el análisis de la aplicación de los procesos del marco rector.
1.3	La UTIC deberá asegurar que el Sistema de evaluación del desempeño de TIC sea consistente con el sistema de administración del desempeño de la dependencia o entidad.

7.2.1.5	Documentación soporte del proceso

No aplica

7.2.2. Cumplimiento regulatorio

7.2.2.1. Objetivos del proceso

General.-

Asegurar que el diseño y la operación de los servicios de TIC de la dependencia o entidad cumplan con la normatividad vigente mediante mecanismos de control y de supervisión

Específicos.-

1.
2. Establecer procedimientos, marcos de referencia metodológica, mejores prácticas y estándares que permitan identificar y aplicar oportunamente los requerimientos regulatorios en materia de TIC.
3. Evaluar por medios internos y de terceros el cumplimiento del marco regulatorio en los procesos del marco rector de este manual.
4. Establecer acciones correctivas para resolver los incumplimientos identificados.
5. Proveer informes periódicos sobre el cumplimiento de los requerimientos legales y regulatorios aplicables en materia de TIC a la dependencia o entidad.

7.2.2.2 Descripción del proceso

7.2.2.2.1 Mapa general del proceso

Diagrama de flujo de información

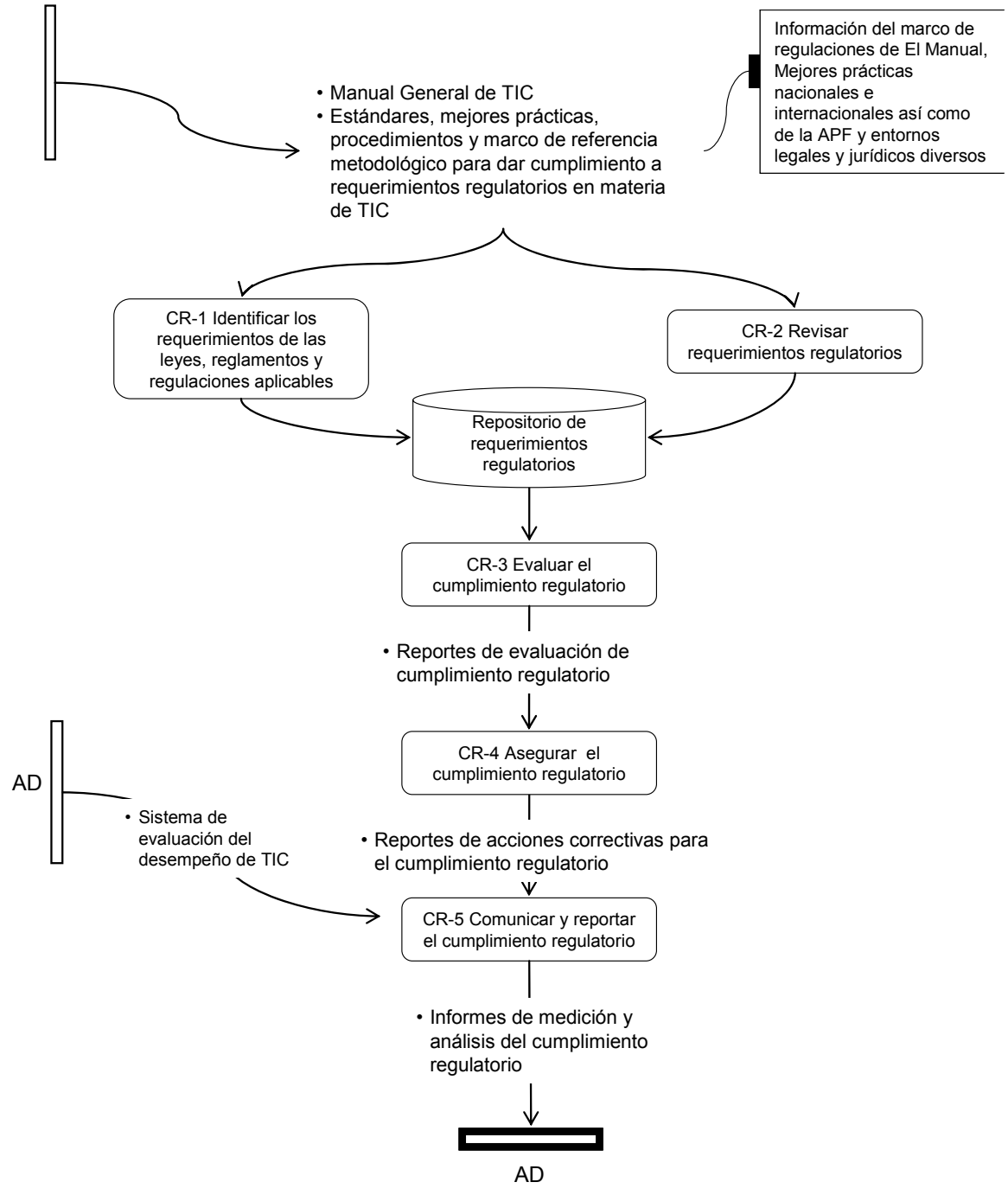
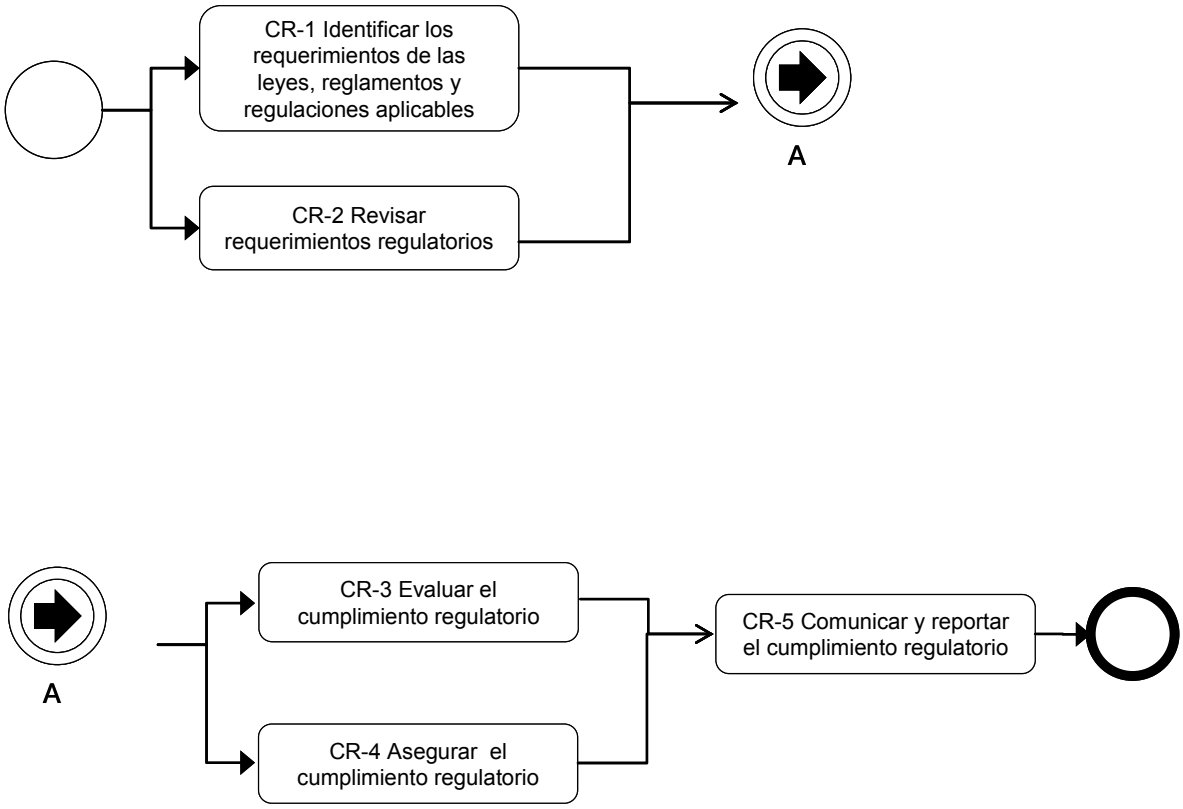


Diagrama de flujo de actividades



7.2.2.2.2 Descripción de las actividades del proceso

CR-1 Identificar los requerimientos de las leyes, reglamentos y regulaciones aplicables

Descripción	Identificar de manera continua los requerimientos en materia de TIC que se desprenden de las leyes aplicables a nivel federal, internacional, así como reglamentos, regulaciones y otras disposiciones que deban ser observadas por la dependencia o entidad, a fin de incorporar estándares, mejores prácticas, procedimientos y marco de referencia metodológico de TIC que sean necesarios en la dependencia o entidad para dar cumplimiento a los mismos.
Factores Críticos	1. Asignar las responsabilidades para la identificación de los requerimientos legales y regulatorios aplicables a las funciones, recursos y operaciones de TIC de la dependencia o entidad. 2. Considerar las Leyes Federales, las Leyes Locales e Internacionales, los Reglamentos y la Normatividad aplicable. 3. Considerar los aspectos relativos a la seguridad, la privacidad de la información, el nivel de acceso, control y procesamiento de los datos, propiedad intelectual y derechos de autor. 4. Implementar un catálogo que permita identificar y evaluar las leyes y requerimientos legales y regulatorios; así como determinar su impacto en los recursos, la operación y los servicios de TIC de la dependencia o entidad y sus proveedores de servicios. 5. Mantener actualizados los estándares, mejores prácticas, procedimientos y marco de referencia metodológico de acuerdo a los requerimientos legales y regulatorios aplicables. 6. Considerar las leyes y aspectos regulatorios en materia de TIC, con respecto a: comercio electrónico, flujos de información, seguridad, confidencialidad, reportes financieros o fiduciarios, regulaciones de la industria, firma electrónica, correo electrónico entre otras. 7. Evaluar el impacto de los requerimientos legales y regulatorios sobre acuerdos contractuales de servicios provistos por terceros. 8. Mantener un inventario de requerimientos legales y regulatorios para evaluar su impacto y las acciones requeridas. 9. Establecer un repositorio de requerimientos regulatorios de acuerdo los puntos anteriores.
Relación de Productos	• Repositorio de requerimientos regulatorios

CR-2 Revisar Requerimientos Regulatorios

Descripción	Revisar los estándares, mejores prácticas, procedimientos y marco de referencia metodológico de TIC para asegurar que los requisitos legales y regulatorios son observados, canalizados y comunicados de manera efectiva y oportuna.
Factores Críticos	1. Examinar los estándares, mejores prácticas, procedimientos y marco de referencia metodológico que se utilizan en la dependencia o entidad con el fin de asegurar que se cumple con los requerimientos legales y regulatorios aplicables, incluyendo Leyes Federales, Internacionales, Reglamentos, Normatividad y Regulaciones aplicables en materia de TIC.

	2. Examinar de manera continua los estándares, mejores prácticas, procedimientos y marco de referencia metodológico que se utilizan en la dependencia o entidad a fin de determinar su efectividad para asegurar el cumplimiento con los requerimientos legales y regulatorios aplicables en materia de TIC. 3. Obtener asesoría adicional cuando sea necesario sobre el contenido y la implementación de estándares, mejores prácticas, procedimientos y marco de referencia metodológico que apoyen al cumplimiento de los requerimientos legales y regulatorios aplicables en materia de TIC. 4. Actualizar con la información obtenida el repositorio de requerimientos regulatorios. 5. Comunicar de manera efectiva los nuevos requerimientos legales y regulatorios o cambios a los mismos en materia de TIC dentro de la dependencia o entidad
Relación de Productos	• Repositorio de requerimientos regulatorios

CR-3 Evaluar el cumplimiento Regulatorio

Descripción	Realizar las actividades necesarias de evaluación y análisis a fin de confirmar el cumplimiento de los estándares, mejores prácticas, procedimientos y marco de referencia metodológico de TIC con los requerimientos legales y regulatorios aplicables en materia de TIC.
Factores Críticos	1. Evaluar regularmente las actividades de TIC y los procesos a fin de asegurar el apego a los requerimientos legales y regulatorios en materia de TIC. 2. Efectuar auditorías internas o de terceros a los estándares, mejores prácticas, procedimientos y marco de referencia metodológico que se utilizan en la dependencia o entidad, para verificar el cumplimiento con los requerimientos legales y regulatorios aplicables en materia de TIC. 3. Asegurar que las brechas identificadas con respecto al cumplimiento de las regulaciones aplicables sean solventadas y se reflejen en actualizaciones a los estándares y procedimientos de manera periódica y continua. 4. Evaluar regularmente los patrones de hallazgos recurrentes. 5. Identificar, registrar y administrar propuestas de mejora a los estándares, mejores prácticas, procedimientos y marco de referencia metodológico que se utilizan en la dependencia o entidad en materia de TIC.
Relación de Productos	• Reportes de evaluación de cumplimiento regulatorio

CR-4 Asegurar el cumplimiento regulatorio

Descripción	Asegurar el cumplimiento regulatorio en materia de TIC y confirmar que se han tomado acciones correctivas y de mejora para resolver cualquier brecha de cumplimiento por el responsable del proceso correspondiente de forma oportuna y efectiva.
Factores Críticos	1. Obtener de manera periódica la confirmación del cumplimiento regulatorio por parte de los responsables de procesos de la dependencia o entidad en materia de TIC. 2. Asegurar regularmente que se han ejecutado revisiones internas y externas para evaluar los niveles de cumplimiento regulatorio. 3. Asegurar que en los contratos con terceros proveedores de bienes o servicios se incluya la obligatoriedad de un informe periódico del cumplimiento con las leyes y regulaciones

	aplicables a éstos. 4. Implementar procedimientos para vigilar e informar sobre incumplimientos de las regulaciones aplicables en materia de TIC, en la UTIC, por parte de los proveedores y en la dependencia o entidad, en materia de TIC; y en su caso realizar las actividades conducentes, así como identificar la causa raíz del incumplimiento.
Relación de Productos	• Reportes de acciones correctivas para el cumplimiento regulatorio

CR-5 Comunicar y reportar el cumplimiento regulatorio

Descripción	Integrar los reportes e informes en relación al cumplimiento legal y regulatorios.
Factores Críticos	1. Definir los requisitos de presentación de informes sobre el cumplimiento de los requerimientos legales y regulatorios aplicables a la dependencia o entidad, incluyendo el requisito de conservar información histórica en materia de TIC. 2. Asegurar la coherencia e integridad de la presentación de los informes de cumplimiento legal y regulatorio de manera completa conforme a los requisitos de información corporativa con aspectos tales como la distribución, frecuencia, alcance, contenido y formato de dichos reportes. 3. Comunicar y difundir los reportes de acuerdo a los niveles de distribución establecidos en el Sistema de evaluación del desempeño de TIC.
Relación de Productos	• Informes de medición y análisis del cumplimiento regulatorio

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.2.2.2.3 Descripción de roles

Rol	Descripción
Mandos medios y Superiores	Titulares de cargos de mandos medios, responsables de supervisar y dar seguimiento a las actividades de cumplimiento regulatorio en materia de TIC.
Responsables de área	Participan en la identificación de los requerimientos legales y regulatorios aplicables en materia de TIC, así como del establecimiento de los mecanismos para dar cumplimiento a los mismos. Participan en el apego a los procedimientos, estándares, mejores prácticas y marco de referencia metodológico aplicables para dar cumplimiento a los requerimientos legales y regulatorios.
Auditor interno	Responsable de realizar evaluaciones internas de apego a los requerimientos legales y regulatorios en materia de TIC.
Grupo interno de control regulatorio	Grupo responsable de realizar el inventario de requerimientos regulatorios, dar seguimiento a la implementación de procedimientos, estándares y metodologías aplicables en materia de TIC. Supervisar y dar seguimiento a las acciones correctivas para solventar las no conformidades de apego a los requerimientos legales y regulatorios en materia de TIC.
Personal de TIC	Atender en tiempo y forma los requerimientos regulatorios en materia de TIC.

7.2.2.2.4 Descripción de productos

Producto	Descripción
Repositorio de requerimientos regulatorios	Relación de requerimientos legales y regulatorios incluyendo leyes, reglamentos, regulaciones especiales, normatividad aplicable en materia de TIC. Este inventario deberá contener de manera ordenada y clasificada los requerimientos legales y regulatorios, la descripción del requerimiento, el tipo de regulación, la vigencia de dicha regulación y los responsables asociados al cumplimiento de dicha regulación.
Estándares, mejores prácticas, procedimientos y marco de referencia metodológico	Relación de estándares, procedimientos, mejores prácticas y marco de referencia metodológico que se encuentran documentados, están implementados y generan su respectiva evidencia. Asimismo deberá especificar el área responsable de su actualización, supervisión y control.
Reportes de cumplimiento regulatorio	Informe de los resultados de las revisiones internas o externas sobre el cumplimiento y adhesión de los requerimientos legales y regulatorios en materia de TIC. El reporte debe contemplar la documentación de acciones correctivas para resolver cualquier brecha de cumplimiento por el dueño responsable del proceso de forma oportuna y efectiva. El reporte debe contener el alcance de la revisión, la fecha de la revisión, el responsable de la revisión, los aspectos legales y regulatorios que se revisaron y su cumplimiento, así como la relación de las desviaciones y las acciones correctivas identificadas. Para las acciones correctivas se deberá establecer la fecha compromiso y el responsable de su ejecución y seguimiento.
Informes de medición y análisis de cumplimiento regulatorio	Reportes generados de acuerdo al Sistema de evaluación del desempeño de TIC (ver proceso Administración del desempeño de TIC), para informar sobre el cumplimiento de los requerimientos legales y regulatorios.

7.2.2.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de requerimientos legales y regulatorios	Medir el grado de cumplimiento de requerimientos legales y regulatorios	Es el porcentaje obtenido para alcanzar los objetivos establecidos	Eficacia	De gestión	(Requerimientos Legales y regulatorios no aplicables / Requerimientos Legales y regulatorios planeados) *100	Mandos Medios y Superiores	Trimestralmente

7.2.2.4 Reglas del proceso

1.1	La dependencia o entidad a través de la UTIC debe establecer procedimientos para administrar las actividades que aseguren el cumplimiento regulatorio en materia de TIC.
1.2	La UTIC deberá designar un responsable del proceso de Cumplimiento regulatorio.
1.3	El responsable del proceso de Cumplimiento regulatorio deberá dar seguimiento a la totalidad de los hallazgos de incumplimiento identificados, de acuerdo a la normatividad aplicable, con independencia de otras responsabilidades en las que se haya incurrido y que serán sancionadas por la autoridad competente.
1.4	La UTIC deberá mantener documentados, actualizados y aprobados los procedimientos y la evidencia al cumplimiento a los requerimientos legales y regulatorios en materia de TIC.

7.2.2.5 Documentación soporte del proceso

No aplica

7.2.3. Administración de riesgos de TIC

7.2.3.1. Objetivos del proceso

General.-

Disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la dependencia o entidad mediante la administración de los riesgos de TIC.

Específicos.-

1. Establecer en la dependencia o entidad, a través de la UTIC, un sistema de administración de riesgos en materia de TIC que permita identificar los riesgos en materia de TIC para su análisis, evaluación, atención, monitoreo y control.
2. Establecer medios para una toma de decisiones informada y oportuna sobre la mitigación de los riesgos en materia de TIC.

7.2.3.2 Descripción del proceso

7.2.3.2.1 Mapa general del proceso

Diagrama de flujo de información

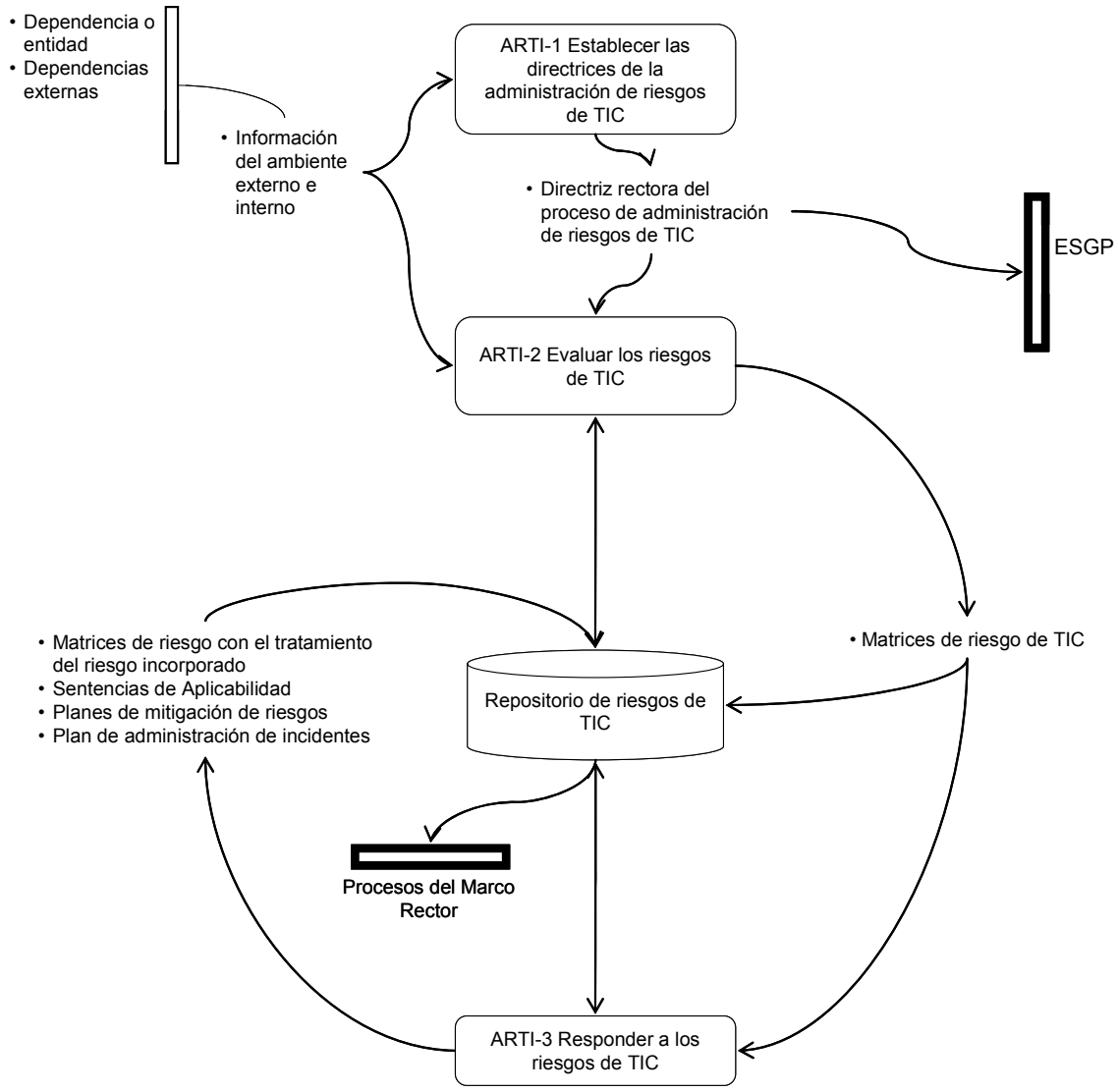
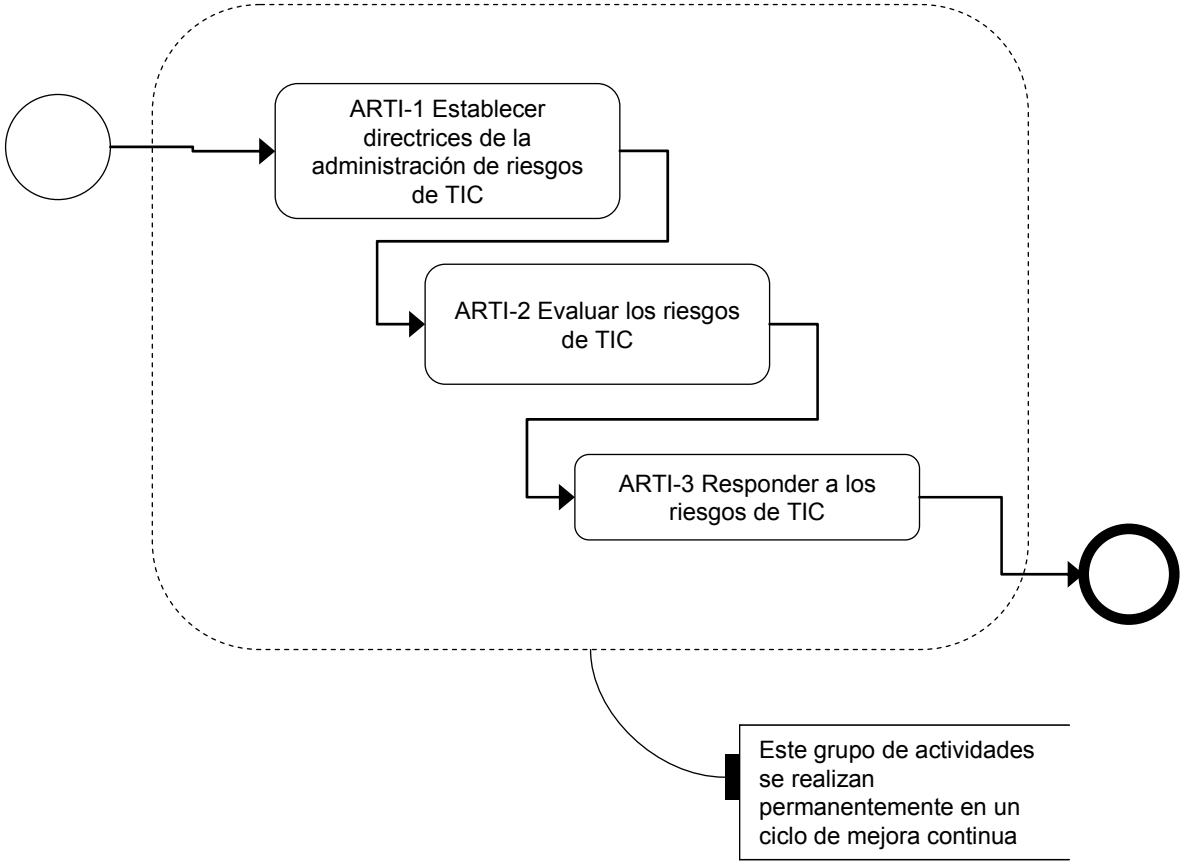


Diagrama de flujo de actividades



7.2.3.2.2 Descripción de las actividades del proceso

ARTI-1 Establecer las directrices de la administración de riesgos de TIC

Descripción	Establecer las directrices de la administración de riesgos de TIC en el contexto de la administración del riesgo de la dependencia o entidad.
Factores Críticos	1. Identificar el ambiente interno y externo de la dependencia o entidad. Aspectos del contexto externo incluyen, pero no están limitados a: • Identificar aspectos del contexto externo de la dependencia o entidad (legales, regulatorios, financieros, tecnológicos, económicos, naturales, competitivos) a nivel local, regional e internacional. • Identificar tendencias e impulsores externos que tienen impacto en los objetivos de la dependencia o entidad, así como las percepciones y valores que los involucrados externos tienen de la dependencia o entidad. • Definir los tipos de eventos externos y cambios a los ambientes de tecnologías que pueden poner en peligro el logro de los objetivos de la dependencia o entidad. Aspectos del contexto interno incluyen pero no limitados a: • Identificar los estándares y modelos de referencia adoptados por la dependencia o entidad. • Identificar las políticas y objetivos, así como las estrategias definidas para lograrlos. • Identificar las soluciones tecnológicas y flujos existentes necesarios de información, así como los procesos establecidos de toma de decisiones. 2. Documentar y difundir una directriz rectora del proceso de Administración de riesgos de TIC que defina la justificación de la dependencia o entidad para implantar la Administración de riesgos de TIC. La directriz rectora deberá: a) Garantizar la alineación con la administración del riesgo de la dependencia o entidad. b) Asegurar que existan los roles y responsabilidades para asegurar la aplicación y cumplimiento ésta. c) Integrar los requerimientos regulatorios identificados en el proceso de Cumplimiento regulatorio. d) Asegurar la definición de los elementos para la administración de riesgos de TIC, entre otros, los siguientes: • Los umbrales de tolerancia al riesgo en materia de TIC de la dependencia o entidad. • Los mecanismos o métodos en la que el proceso y la administración de riesgos en materia de TIC será medido. • Los proceso, métodos y herramientas que serán usados para administrar los riesgos en materia de de TIC • Las medidas que serán tomadas para corregir las desviaciones que se observen sobre los límites de exposición al riesgo o efectuar los ajustes preventivos a los niveles de tolerancia al riesgo. e) Asegurar la difusión por diversos medios a todo el personal que le aplique. f) Definir la forma y periodicidad con la que se deberá informar a las partes interesadas, sobre los riesgos en materia de TIC a los que se encuentran expuestos los procesos

	y servicios de la dependencia o entidad. g) Difundir las consecuencias y medidas correctivas aplicables derivadas de su no cumplimiento.
Relación de productos	• Directriz rectora del proceso de Administración de riesgos de TIC

ARTI-2 Evaluar los riesgos de TIC

Descripción	Asegurar que los riesgos en materia de TIC sean evaluados y presentados en términos del impacto a los procesos y servicios de la dependencia o entidad: financieros, transparencia y seguridad de la información, regulatorios, entre otros.
Factores Críticos	1. Recopilar datos relevantes a los riesgos de TIC. a) Recopilar datos del registro histórico de incidentes que hayan tenido algún impacto a la entidad o dependencia b) Recopilar el registro histórico de riesgos del activo o recurso a evaluar (si existe) c) Identificar los controles actualmente implementados en los activos o recursos a evaluar. 2. Identificar y analizar escenarios de riesgo que permitan identificar los impactos potenciales a la entidad o dependencia: a) Identificar activos o recursos inmersos en el alcance objetos de la evaluación, dichos activos pueden ser identificados al menos pero no limitado a las siguientes categorías: • Servicios • Procesos • Datos (operativos, nomina, contables, entre otros.) • Software (sistemas, aplicaciones, ,entre otros.) • Hardware • Equipos informativos que hospedan datos, aplicaciones y servicios. • Equipos de comunicaciones • Dispositivos de almacenamiento (cintas, CDs, DVDs, entre otros.) • Personas (empleados internos y terceros) b) Identificar amenazas para aquellos activos identificados, dichas amenazas pueden ser identificadas al menos pero no limitado a las siguientes categorías: • No causadas por el hombre: • Malfuncionamiento de TI (fallas de software y de hardware) • Naturales (terremotos, huracanes, entre otros.) • De origen industrial (fallas eléctricas, aire acondicionado) • Causados por el Hombre: • Maliciosas o Externas (espionaje industrial, hackers, entre otros.)

	o Internas (Personal mal intencionado) • No maliciosas o Errores humanos c) Identificar riesgos, algunos tipos de riesgos se mencionan a continuación: • Fraudes, • Robos • Degradación o perdida de continuidad en las operaciones • Fuga o modificación de información no autorizada • Accesos no autorizados • Falta o no cumplimiento de regulaciones, entre otros d) Identificar impactos a la entidad o dependencia, dichos impactos pueden al menos pero no limitado a los siguientes: • Financieros • Niveles de servicios • Imagen o reputación • Regulatorios
Relación de productos	• Matrices de riesgo de TIC • Repositorio de riesgos de TIC actualizado

ARTI-3 Responder a los riesgos de TIC

Descripción	Asegurar que se responde a los riesgos de TIC con base a su nivel de severidad, con base en las decisiones para su tratamiento y tomado los criterios de priorización de implantación de controles.
Factores Críticos	1. Identificar el nivel de severidad del riesgo. 2. Identificar opciones para el tratamiento del riesgo el cual involucra tomar las decisiones para: a) Aceptar el riesgo. No se efectúa ninguna acción debido a que el nivel de riesgo de acuerdo al apetito de riesgo aceptado está dentro de los niveles de riesgo aceptables por la entidad o dependencia. b) Evitar el riesgo: Se elimina la causa que produce el riesgo. c) Transferir el riesgo: Se transfiere y comparte el riesgo con una organización aseguradora o un tercero. d) Mitigar el riesgo: Se implementan controles para reducir el riesgo a un nivel aceptable por la entidad o dependencia 3. Identificar controles predictivos, preventivos y correctivos y mapearlos a cada uno de los escenarios de riesgos identificados. Estos controles deben ser documentados en la SoA. 4. Definir planes de mitigación del riesgo que consideren las actividades para implantar los controles identificados en la Sentencia de Aplicabilidad, para cada escenario de riesgo la prioridad de implantación debe ser definida y acordada. Algunos de los parámetros que pueden ser considerados en la priorización de la implantación de los controles o

	contramedidas son los siguientes: • Severidad del riesgo (nivel de riesgo) • Nivel de impacto positivo para los procesos y servicios de la entidad o dependencia con la implantación del control • Costo de implantación 5. Definir un plan de contingencia para reaccionar a eventos o incidentes en caso de la materialización de algún riesgo.
Relación de productos	• Matrices de riesgo con el tratamiento del riesgo incorporado • Sentencias de Aplicabilidad • Planes de mitigación de riesgos • Plan de administración de riesgos • Repositorio de riesgos de TIC actualizado

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.2.3.2.3 Descripción de roles

Rol	Descripción
Grupo de trabajo para la dirección de TIC	Grupo (o grupos) conformado por titulares de las unidades responsables y de la UTIC que apoya y reporta al grupo de trabajo estratégico de TIC. Este grupo es responsable de la aprobación de la Directriz rectora del proceso de administración de riesgos de TIC y asegurar su cumplimiento. Este grupo de trabajo es responsable sobre la colaboración y consenso a nivel dependencia o entidad requerida para dar soporte a las actividades y decisiones de la administración de riesgos de TIC.
Titular de la UTIC	Responsable del área administrativa de TIC y responsable de la implementación del marco de referencia metodológico de la administración de riesgos de TIC.
Grupos de control de riesgos de TIC	Responsables dentro de la dependencia o entidad para manejar dominios específicos de riesgos de TIC ejemplo: El Oficial de Seguridad de la Información, Responsable de la continuidad de los negocios y recuperación de desastres, responsable de la oficina de administración de proyectos, etc.
Personal de TIC	Responsables de realizar la evaluación del riesgo de TIC cuando sea requerido. Resguardan los recursos requeridos para la adquisición, procesamiento, almacenamiento y diseminación de datos/información en las TIC que tienen a su cargo.

7.2.3.2.4 Descripción de productos

Producto	Descripción
Directriz rectora del proceso de Administración de riesgos de TIC	Documenta las directrices para implantar la administración de riesgos de TIC en el contexto del riesgo de la dependencia o entidad; describe, al menos, los siguientes aspectos: a) Justificación para la implantación de la administración de riesgos de TIC. b) Propósito de la Directriz rectora del proceso de Administración de riesgos c) Alcance. d) Incluye los requerimientos regulatorios identificados en el proceso de Cumplimiento regulatorio. e) Los roles y responsabilidades para asegurar la aplicación su cumplimiento. f) Los elementos para la administración de riesgos en materia de TIC, entre otros: • Umbrales de la tolerancia al riesgo de TIC de la dependencia o entidad. • Los mecanismos y métodos por medio de los cuales se medirá el proceso y la administración de riesgos en materia de TIC. • Herramientas que serán usados para administrar los riesgos de TIC • Las medidas para corregir las desviaciones que ocurran arriba tanto de los límites de exposición al riesgo como de los niveles de tolerancia al riesgo. g) Un apartado donde asegure la difusión a todo el personal de la dependencia o entidad. h) Un apartado donde asegure su revisión periódica. i) Un apartado donde asegure que se realicen revisiones del cumplimiento y la definición de los responsables de dichas revisiones. j) Define acciones y consecuencias aplicables por su no cumplimiento.
Matrices de riesgo de TIC	Documenta los escenarios de riesgo de los activos evaluados, describe al menos los siguientes aspectos: a) Fecha de evaluación b) Área c) Proceso de negocio d) Activo evaluado e) Tipo de amenaza f) Agente de amenaza identificada g) Probabilidad de ocurrencia de la amenaza h) Descripción del riesgo i) Nivel de riesgo (severidad) j) Nivel de riesgo residual k) Impactos a la entidad o dependencia. l) Descripción del impacto m) Nivel de impacto (severidad) n) Tratamiento del riesgo
Sentencia de Aplicabilidad	Documenta para cada riesgo la identificación y selección de los controles que deberán implantarse para reducir el riesgo a niveles aceptables por la entidad o dependencia, describe al menos los siguientes aspectos: a) Activo b) Riesgo asociado c) Controles actualmente implementados

Producto	Descripción
	d) Control o controles seleccionados para mitigación del riesgo e) Razones para su selección
Planes de mitigación de riesgos	Documenta el plan de implantación de los controles seleccionados con el fin de mitigar los riesgos identificados, describe al menos pero no limitado a los siguientes aspectos: a) Riesgo asociado. b) Control o controles asociados c) Impacto a la dependencia o entidad. d) Plan de actividades para la implantación del control. e) Fecha de verificación de la implantación. f) Responsable de la implantación. g) Responsable de verificar su cumplimiento.
Plan de contingencia	Documenta las acciones y decisiones a llevar a cabo en caso de que se presente un evento o incidente no deseado que tenga un impacto potencial para la entidad o dependencia, documenta al menos pero no limitado a lo siguiente: a) Estructura del equipo de respuesta al riesgo. b) Responsabilidades del equipo de respuesta al riesgo. c) Procedimiento de notificación de respuesta en caso que ocurra un incidente o contingencia sobre un riesgo identificado previamente. d) Procedimiento de activación e) Evaluación preliminar del daño f) Asegurar la respuesta Inicial g) Evaluación de daños h) Ponerse en contacto y movilizar a las partes interesadas i) Lista de contactos externos j) Centro de control de crisis
Repositorio de riesgos de TIC	• Repositorio que integra todos los datos e información derivada del proceso de administración de riesgos.

7.2.3.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de las directivas de administración de riesgos de TIC	Grado de cumplimiento de las directrices de administración de riesgos de TIC	Es el porcentaje obtenido para alcanzar los objetivos establecidos	Efectividad	De gestión	(Directrices de Administración de riesgos de TIC implantadas / Directrices de la Administración de riesgos de TIC planeadas) *100	Grupo de administración de TIC	Trimestral

7.2.3.4	Reglas del proceso

1.1	Los mandos superiores de la dependencia o entidad deberán proveer a la UTIC de los recursos para establecer el proceso de Administración de riesgos de TIC.
1.2	La UTIC deberá establecer las directrices para la administración de riesgos de TIC de la dependencia o entidad.
1.3	La UTIC deberá designar un responsable del proceso de Administración de riesgos.
1.4	El responsable del proceso de Administración de riesgos deberá establecer y documentar el proceso de Administración de riesgos de TIC explicitando con precisión los objetivos de la UTIC y de la dependencia o entidad y compromiso con relación a la gestión de los riesgos en materia de TIC.
1.5	El responsable del proceso de Administración de riesgos deberá asegurar la definición de roles, su responsabilidad y autoridad, al establecer la administración de riesgos de TIC.
1.6	El responsable del proceso de Administración de riesgos de TIC deberá establecer mecanismos para el reporte de la gestión de los riesgos de TIC a las partes interesadas
1.7	El responsable del proceso de Administración de riesgos de TIC deberá documentar, actualizar y revisar el proceso de Administración de riesgos de TIC incluyendo la formalización de las decisiones sobre los riesgos.
1.8	El responsable del proceso de Administración de riesgos de TIC debe realizar una revisión periódica de riesgos de TIC.
1.9	El responsable del proceso de Administración de riesgos de TIC debe implementar mecanismos de identificación y valoración de amenazas y riesgos.
1.10	El responsable del proceso de administración de riesgos de TIC deberá implementar una repositorio y los informes correspondientes sobre incidentes y contingencias así como un reporte de análisis de los riesgos valorados; está información deberá estar a disposición de los responsables de la administración de riesgos en la dependencia o entidad.

7.2.3.5	Documentación soporte del proceso

No aplica

7.3 ADMINISTRACION PROYECTOS

7.3.1. Administración de portafolio de proyectos de TIC

7.3.1.1. Objetivos del proceso

General.-

Incrementar la probabilidad de seleccionar iniciativas que entreguen el máximo valor a la dependencia o entidad, mediante un proceso de evaluación, verificación de alineación estratégica, selección, asignación de prioridades y autorización.

Las iniciativas de inversión consideran erogaciones tanto por adquisiciones de bienes como por servicios.

Específicos.-

1. Establecer las directrices para la constitución del portafolio de proyectos de TIC y su administración.
2. Permitir una visión integral de los proyectos de TIC que genere sinergias y evite inversiones que no agreguen valor.
3. Actualizar el portafolio de proyectos para minimizar las consecuencias de las desviaciones respecto al PETIC y de riesgos emergentes.

7.3.1.2 Descripción del proceso

7.3.1.2.1. Mapa general del proceso

Diagrama de flujo de informacíón

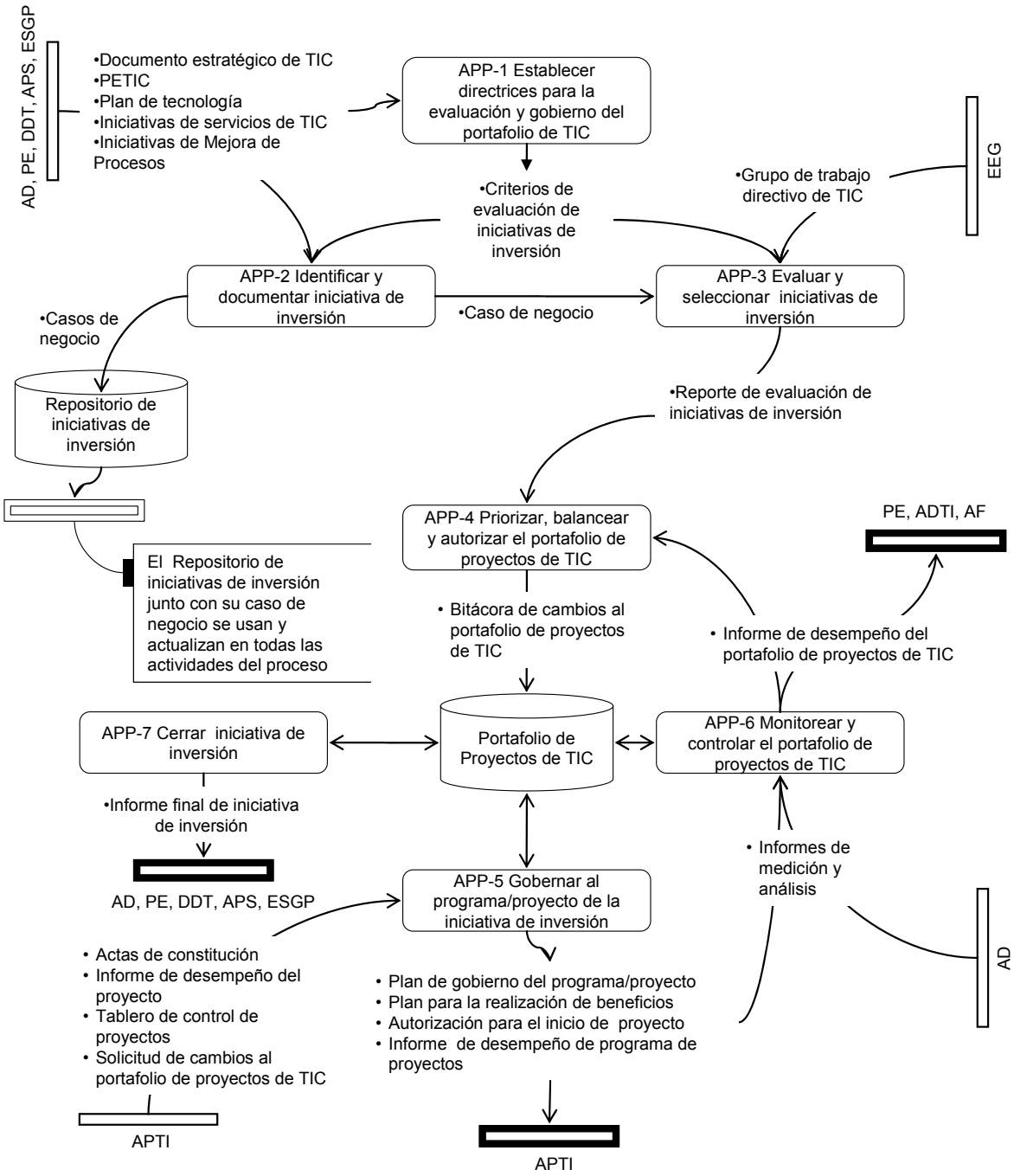
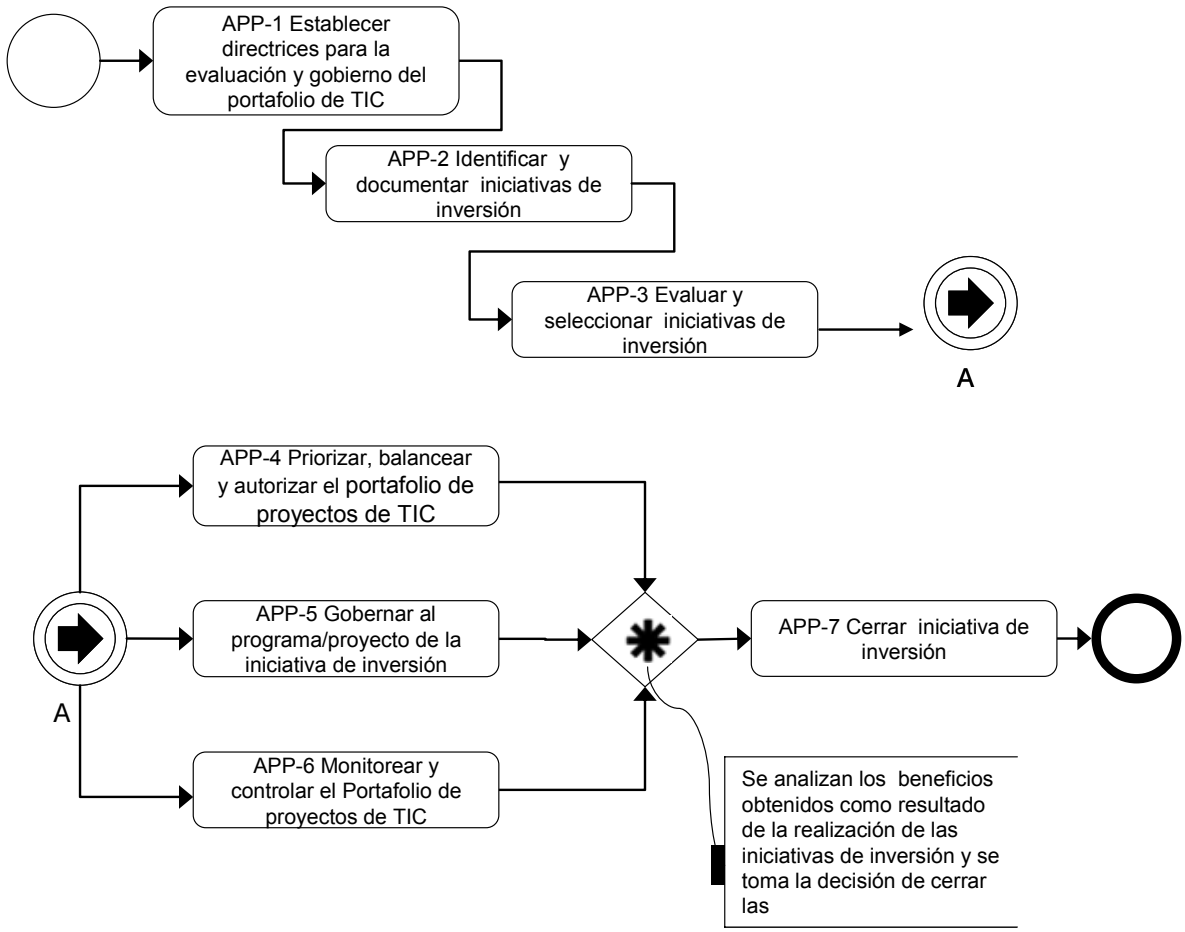


Diagrama de flujo de actividades



7.3.1.2.2. Descripción de las actividades del proceso

APP-1: Establecer las directrices para la evaluación y gobierno del portafolio de proyectos de TIC

Descripción	Dirigir y controlar al portafolio de proyectos de TIC, definir los criterios para la toma de decisiones sobre la asignación y uso de los recursos de la dependencia o entidad en proyectos de TIC y la realización de los beneficios de las inversiones propuestas.
Factores Críticos	1. Definir la forma de organización, los roles y las responsabilidades del grupo de trabajo directivo de TIC en el gobierno del portafolio de proyectos de TIC para la toma de decisiones acerca de: ◦ Prioridades de las iniciativas de inversión ◦ Inversión, asignación y reasignación de los recursos ◦ Alineación de las inversiones en proyectos de TIC a las necesidades y objetivos de la dependencia o entidad. 2. Autorización de nuevas iniciativas de inversión, la suspensión, cambios o cancelación a proyectos/programas y la reasignación de recursos entre proyectos. 3. Definir los grupos y categorías/tipos de iniciativas de inversión derivadas de los procesos de planeación estratégica de TIC, Determinación de la dirección tecnológica, Administración de portafolio de servicios y Sistema de gestión de Procesos, y de aquellas otras fuentes que detonen iniciativas que podrán ser presentadas al grupo de trabajo directivo de TIC para su autorización en el Portafolio de Proyectos, así como las características de las mismas. • La categoría de una iniciativa determina los criterios, niveles de aprobación y el procedimiento para la elaboración del Caso de Negocio, evaluación, selección y Autorización para el inicio del Proyecto. Las categorías pueden incluir sub-categorías denominadas tipos. 4. Definir para los criterios de evaluación de iniciativas de inversión de una categoría/tipo las propiedades para otorgar un rango, nivel o peso. • Alineación/contribución a los objetivos y estrategias de la dependencia o entidad. • Criterios financieros. • Criterios de riesgos. • Criterios de aspectos normativos y legales. • Criterios de recursos humanos. • Criterios técnicos. • Criterios de impacto y capacidad de la dependencia o entidad. • Criterio de contrataciones relacionadas. 5. Definir los parámetros de evaluación de criterios que será usados por cada categoría. • La asignación de los parámetros de evaluación de los criterios permitirán determinar un orden para la selección de iniciativas de inversión. • Pueden ser cualitativos yo cuantitativos y vienen de la variedad de las fuentes de información de la dependencia o entidad.
Relación de productos	• Criterios de evaluación de iniciativas de inversión.

APP-2: Identificar y documentar iniciativas de inversión

Descripción	Mantener un registro de las iniciativas de inversión de TIC y sus proyectos/programas relacionados que constituyen el portafolio de proyectos de TIC. Darle seguimiento al estado en que se encuentran las iniciativas de inversión a lo largo de su ciclo de vida.
Factores Críticos	1. Identificar e integrar todas las iniciativas de inversión de TIC que se detecten en la entidad y/o dependencia. 2. Se deberán incluir entre otras las iniciativas de inversión estratégicas derivadas de la planeación estratégica de TIC, las iniciativas de inversión provenientes de las necesidades de desarrollo de nuevos servicios de TIC o ajustes a servicios existentes, las iniciativas de inversión relativas a la continuidad de los servicios y las iniciativas de inversión en infraestructura y soporte de la dependencia o entidad. 3. Clasificar la iniciativa de TIC de acuerdo a los grupos y categorías/tipos definidos en los criterios de evaluación. 4. Documentar cada iniciativa de TIC teniendo como mínimo información de : • Identificación (como nombre, fuente de la iniciativa, patrocinador, cliente, principales interesados), • Alcance de alto nivel (como objetivos, alcance, plan de alto nivel, objetivos directivos que soporta, beneficios cuantitativos, beneficios cualitativos, recursos, entregables y riesgos), • De gobierno (estructura de gobierno recomendada para administrar, controlar y soportar la iniciativa), • De seguimiento (como el estado en el que se encuentra, cambios aprobados, administrador de la iniciativa). 5. Elaborar el Caso de Negocio de manera conjunta entre el Patrocinador de la iniciativa y la persona que sea designada por el grupo de trabajo directivo de TIC, considerando la justificación para realizar la inversión relacionada con una iniciativa. • Deberá contener la información suficiente para evaluar, seleccionar y priorizar la iniciativa. • Deberá documentar claramente los beneficios esperados por la dependencia o entidad y la manera en la que se va a medir la realización de los mismos. • Los responsables del Caso de Negocio son el Patrocinador de la iniciativa y la persona designada por el grupo de trabajo directivo de TIC. 6. Evaluar periódicamente, durante todo el ciclo de vida de la iniciativa, la vigencia del Caso de Negocio por cambios que se puedan presentar en la estrategia, en el entorno, costos, incremento en riesgos o a la reducción de los beneficios esperados. 7. De ser requerido, se actualiza el Caso de Negocio y si hay cambios significativos se presenta la información del impacto al grupo de trabajo directivo de TIC para que se evalúe si se continúa con la ejecución de la iniciativa y en su caso se aprueben los cambios al Caso de Negocio. 8. Mantener actualizado en el Repositorio de iniciativas de inversión, la información del estado en el que se encuentra la iniciativa a lo largo de todo su ciclo de vida, desde su identificación hasta su cierre y validación de beneficios. Incluyendo, en su caso, el registro de cancelación.
Relación de productos	• Caso de negocio.

APP-3: Evaluar y seleccionar iniciativas de inversión

Descripción	Las iniciativas de inversión son evaluadas por grupos y categorías/tipos para proveer comparaciones y determinar un orden de ejecución para facilitar el proceso de selección. Los resultados de la evaluación se usan para seleccionar a un subconjunto de iniciativas de inversión que serán propuestas al grupo de trabajo directivo de TIC para su priorización y autorización.
Factores Críticos	1. Evaluar cada una de las iniciativas de inversión de acuerdo a los criterios de selección y el esquema de evaluación y asignación de pesos correspondiente a su categoría/tipo. 2. Elaborar informes y representaciones gráficas de los resultados de las evaluaciones para facilitar la toma de decisiones al grupo de trabajo directivo de TIC. 3. Documentar recomendaciones resultantes del proceso de evaluación. 4. Seleccionar aquellas iniciativas de inversión que serán promocionadas para su priorización y autorización. 5. Para realizar esta selección se efectúan diversos análisis a nivel portafolio que contemplan los recursos con los que cuenta la organización para la ejecución de iniciativas de inversión, entre los que se encuentran: ◦ Análisis de capacidad de recursos humanos. ◦ Análisis de capacidad financiera. ◦ Análisis de capacidad de activos e infraestructura. 6. Identificar los requerimientos tecnológicos. 7. Identificar cuáles son las funciones sustantivas que soporta. 8. Identificar cuáles son los objetivos directivos que soporta y el nivel de aportación de valor a dichos objetivos. 9. Identificar los requerimientos regulatorios o legales que permitan sustentar la iniciativa.
Relación de productos	• Reporte de evaluación de iniciativas de inversión.

APP-4: Priorizar, balancear y autorizar el Portafolio de proyectos de TIC

Descripción	La asignación de prioridades permite comparar cada iniciativa del portafolio contra el resto de las seleccionadas, por grupo y categoría/tipo. Balancear y priorizar permite determinar cuáles de las iniciativas de inversión pueden ser realizadas dentro de las restricciones financieras, humanas y tecnológicas de la dependencia o entidad hasta encontrar la intersección de las expectativas que maximice los beneficios que deriven de su agrupación y organización, generando así un portafolio de proyectos de TIC que este alineado estratégicamente, maximizando su valor y balanceado en su conjunto.
Factores Críticos	1. Proponer y establecer un orden de acuerdo a la prioridad de las iniciativas de inversión seleccionadas. • Confirmar la clasificación de las iniciativas de inversión seleccionadas. • Revisar y analizar el resultado de la evaluación de las iniciativas de inversión seleccionadas • Determinar y acordar el orden de prioridad de las iniciativas de inversión seleccionadas. 2. Someter a revisión del grupo de trabajo directivo de TIC la propuesta de portafolio de proyectos de TIC para determinar cuáles iniciativas de inversión serán autorizadas para su ejecución, con base a los resultados de la evaluación, el orden de prioridad y aspectos complementarios como la alineación a los objetivos y estrategias de la dependencia o entidad.

	• Se toman decisiones sobre la asignación de recursos y se autoriza la ejecución de un conjunto de iniciativas de inversión. Si el nivel de precisión de la información de una iniciativa prioritaria es grande, se podría autorizar la realización de una fase de planeación que provea información más precisa para tomar una decisión sobre su realización. 3. Actualizar el portafolio de proyectos de TIC con las iniciativas de inversión autorizadas. • El portafolio de proyectos de TIC se compone de todos los proyectos y/o programas de la dependencia o entidad derivados de iniciativas de inversión autorizadas para su ejecución. 4. Balancear el portafolio de proyectos de TIC y los recursos con los que cuenta la dependencia o entidad para desarrollarlos. • Se deben incluir los siguientes aspectos al balancear el portafolio de proyectos de TIC: ° Agregar al portafolio de proyectos de TIC actual los programas de proyectos derivados de las nuevas iniciativas de inversión que han sido autorizadas. ° Identificar proyectos que se encuentren en ejecución pero que no hayan estado sujetos al proceso de autorización y aplicar las acciones correctivas derivadas del Balanceo del portafolio de proyectos de TIC. ° Revisar los informes de rendimiento del portafolio de proyectos de TIC y tomar decisiones para suspender, re-priorizar, continuar o cancelar. ° En base a los recursos disponibles, restricciones y a la valoración previa, los proyectos se categorizan, priorizan y se asignan recursos, el resultado conlleva a un ajuste de prioridades, y a partir de este punto se convierte en iterativo, hasta su finalización o cancelación. 5. Someter a revisión y autorización del grupo de trabajo directivo de TIC el portafolio de proyectos de TIC balanceado y priorizado para su autorización. 6. El grupo de trabajo directivo de TIC deberá asignar los proyectos y/o programas que integran al Portafolio de Proyectos de TIC a los Administradores de de Proyectos y/o Programas de TIC para su ejecución de acuerdo al proceso de Administración de Proyectos. 7. El administrador del portafolio de proyectos de TIC deberá comunicar a la UTIC el portafolio de proyectos de TIC y las decisiones tomadas por el grupo de trabajo directivo de TIC.
Relación de productos	• Bitácora de cambios al portafolio de proyectos de TIC.

APP-5: Gobernar al programa/proyecto de la iniciativa de inversión

Descripción	Se asigna a un responsable para la administración de la realización de la iniciativa quien establece un plan de alto nivel que determina el programa de proyectos que serán ejecutados. Se asigna a los responsables de la administración de los proyectos con apego a las prácticas establecidos en el proceso de Administración de Proyectos para su seguimiento y control por parte del Administrador del Portafolio de Proyectos. Si la realización de una iniciativa involucra a solo un proyecto frecuentemente el responsable de la administración de la iniciativa coincide con el responsable de la administración del único proyecto. Sin embargo si la realización de la iniciativa involucra a un programa de proyectos el responsable para la administración de la iniciativa es responsable de la administración del programa en su conjunto y se coordina con los administradores de los proyectos de su programa.
Factores	1. Revisar toda la información presentada para la autorización incluyendo el registro de la

Críticos	iniciativa, su caso de negocio y la asignación de recursos autorizados, validando el entendimiento con los interesados, incluyendo el patrocinador de la iniciativa y el cliente. 2. Identificar las distintas alternativas para lograr los objetivos establecidos en el caso de negocio de la iniciativa. • Se evalúan los beneficios, costos, riesgos y tiempo para cada alternativa. Se selecciona la alternativa con mayor potencial de valor, dentro de las restricciones de tiempo y el presupuesto autorizado. Se documenta la justificación de la selección de la alternativa. 3. Determinar el conjunto de proyectos necesarios para la realización de la iniciativa. • Se elabora la justificación del programa de proyectos a partir de la descripción de Caso de Negocio de cada uno de los proyectos del programa que considere información relacionada a los factores técnicos, de inversión y normativos que puedan aplicar a cada proyecto. 4. Elaborar un cronograma ejecutivo para el programa de proyectos que muestre la duración y las fechas de inicio y fin de cada proyecto. • Este cronograma incluye los hitos de control a fin de darle seguimiento puntual al programa, los cuales son puntos de control ejecutivo y se establecen de acuerdo a las restricciones, dependencias entre proyectos del programa y aquellos eventos sobre los que se desea tener visibilidad para la toma de decisiones. 5. Elaborar y emitir las autorizaciones para el inicio de los proyectos del programa y asignar a los administradores de proyectos siguiendo el proceso de Administración de Proyectos. 6. Elaborar un plan para gobierno del programa de proyectos. • Este plan de gobierno del programa de proyectos integra toda la información requerida para dirigir y controlar al programa con respecto a las finanzas, recursos, cronogramas, alcance, riesgos y comunicaciones. Este plan está sujeto a revisión y aprobación de los interesados, incluyendo al patrocinador de la iniciativa, el responsable de administrar el programa y los administradores de proyectos involucrados. La elaboración del plan para gobierno del programa se realiza en paralelo de la elaboración del plan de cada uno de los proyectos que lo constituyen siguiendo el proceso de Administración de Proyectos. Si el programa contiene un solo proyecto el plan de gobierno del programa es el mismo que el plan de administración del proyecto. 7. Elaborar un plan para la realización de beneficios del programa. • Este plan establece para cada resultado clave del programa la responsabilidad para el logro del resultado, la fecha estimada de obtención y el proceso de seguimiento el cual debe incluir un registro detallado de los beneficios esperados en conjunto con la explicación de los riesgos que pueden amenazar el cumplimento de cada resultado clave y como estos riesgos deben ser mitigados. 8. Dar seguimiento y controlar el rendimiento del programa para asegurar que la ejecución se lleva de acuerdo a los planes acordados. • El seguimiento se da a lo largo de toda la vida del programa e incluye la colección, medición y distribución de informes de rendimiento y la evaluación de las tendencias y los riesgos. 9. Administrar los asuntos del programa. 10. Evaluar la realización de beneficios de acuerdo al plan para la realización de beneficios del programa.

	• Se da seguimiento a la obtención de los resultados clave estipulados en este plan y validar que los beneficios asociados se estén cumpliendo. En caso de desviaciones se establecen acciones correctivas y de ser necesario se escalan los asuntos a los involucrados que convoque el Administrador del Portafolio de Proyectos de TIC.
Relación de productos	• Plan de gobierno del programa/proyecto • Plan para la realización de beneficios • Autorización para el inicio de proyecto • Informe de desempeño de programa de proyectos • Informes de medición y análisis

AP-6: Monitorear y controlar el Portafolio de proyectos de TIC

Descripción	Cada componente del portafolio se evalúa de manera individual para determinar su contribución al portafolio en su conjunto y se evalúa en forma global el portafolio para determinar si se están cumpliendo los objetivos de la dependencia o entidad. Proporcionar informes para evaluar el estado que guarda el portafolio y sustentar una adecuada toma de decisiones, sobre que componentes de portafolio (proyecto o programa de proyectos) se deben conservar, en cuales invertir, cuales reemplazar y cuales rechazar, cancelar o suspender.
Factores Críticos	1. Evaluar de manera individual para determinar su contribución al portafolio en su conjunto y se evalúa en forma global el portafolio para determinar si se están cumpliendo los objetivos de la dependencia o entidad. 2. Elaborar y revisar los informes de rendimiento de los componentes del portafolio de proyectos de TIC que se encuentran en ejecución. 3. Elaborar y revisar el orden de prioridad de los componentes del portafolio, las dependencias, alcance, riesgos, asuntos, logros, resultados y avances e integrar un informe global de rendimiento del portafolio de proyectos de TIC. 4. Presentar al grupo de trabajo directivo de TIC los informes de rendimiento para facilitar la toma de decisiones sobre la continuación de los componentes del portafolio de proyectos de TIC, la reasignación de prioridades y el uso de los recursos. 5. Escalar para la atención ejecutiva los asuntos y riesgos que impacten el portafolio de proyectos de TIC y los objetivos de la dependencia o entidad. 6. Comunicar a los involucrados en el portafolio de proyectos de TIC. Los ajustes o cambios que se decidan por el grupo de trabajo directivo de TIC para mitigar riesgos y/o aprovechar oportunidades
Relación de Productos	• Informe de desempeño del portafolio de proyectos de TIC

AP-7: Cerrar iniciativa de inversión

Descripción	Cerrar administrativamente la iniciativa mediante la integración del informe final que incluye la evaluación de los resultados y de beneficios desde la perspectiva de la dependencia o entidad y de acuerdo al caso de negocio autorizado.
Factores Críticos	1. Revisar los resultados y la documentación final de los proyectos asociados a la iniciativa. • Una vez concluidos y cerrados todos los proyectos asociados a una iniciativa se procede a evaluar los resultados obtenidos contra los esperados de acuerdo a los criterios de medición documentados en el caso de negocio de la iniciativa.

	2. Evaluar la realización final de los beneficios mediante revisiones posteriores a la conclusión y cierre de la iniciativa. • Las revisiones deberán efectuarse después de la implementación de los productos y servicios elaborados como resultado de la iniciativa, dejando un tiempo para erradicar los problemas que surjan posteriores a la implementación y para que los beneficios se perciban en la dependencia o entidad. 3. Realizar un informe final de la iniciativa. • El reporte integra los resultados y hallazgos de la revisión de los proyectos realizados, así como las lecciones aprendidas para mejorar la eficacia y eficiencia de la administración de portafolio de proyectos de TIC..
Relación de productos	• Informe final de iniciativa de inversión

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.3.1.2.3 Descripción de roles

Rol	Descripción
Grupo de trabajo directivo de TIC	Grupo de trabajo de la UTIC que tiene la responsabilidad, autoridad y conocimiento para seleccionar, autorizar iniciativas de inversión y tomar decisiones sobre el impacto y control del portafolio de proyectos de TIC. Este grupo toma las decisiones acerca de: • Prioridades de las iniciativas de inversión • Inversión, asignación y reasignación de los recursos • Alineación de las inversiones en proyectos de TIC a las necesidades y objetivos de la dependencia o entidad. • Autorización de nuevas iniciativas de inversión, la suspensión, cambios o cancelación a proyectos/programas y la reasignación de recursos entre proyectos.
Administrador del portafolio de proyectos de TIC	Responsable de la administración de uno o más portafolios, identifica, prioriza propone para autorización, administra y controla proyectos, programas y otras actividades para el logro de los objetivos del la dependencia o entidad. Convocará en caso de ser necesario a los responsables de la administración de programas y responsables de administración de proyectos, patrocinadores de la iniciativa y otros interesados para la toma de decisiones que impacten en el cumplimiento de los beneficios y objetivos del portafolio de proyectos de TIC.
Patrocinador de la Iniciativa	Área usuaria que define y propone la iniciativa de TIC, así como los requerimientos funcionales, operativos y beneficios.
Responsable de la administración del programa	Persona responsable de la dirección y control del proyecto o programa de proyectos que se determinan con el propósito de cumplir con los objetivos de la iniciativa y poder proporcionar un resultado final exitoso en tiempo y forma.
Administradores de proyectos	Persona responsable del la administración del proyecto de TIC con el propósito de cumplir con los objetivos del proyecto y poder proporcionar un resultado final exitoso en tiempo y forma.

7.3.1.2.4 Descripción de productos

Producto	Descripción
Criterios de evaluación de iniciativas de inversión	Se definen las propiedades cualitativas y/o cuantitativas a los criterios que se establecen para evaluar las iniciativas de inversión de una categoría/tipo determinado. Por cada criterio se definen como mínimo las propiedades de rango, nivel y peso. Criterios de mínimos de evaluación de iniciativas de inversión: • Alineación/contribución a los objetivos y estrategias de la dependencia o entidad. • Criterios financieros • Criterios de riesgos • Criterios de aspectos normativos y legales • Criterios de recursos humanos • Criterios técnicos • Criterios de impacto y capacidad de la dependencia o entidad • Criterio de contrataciones relacionadas
Repositorio de iniciativas de inversión	Incluye información de identificación (como nombre, fuente de la iniciativa, patrocinador, cliente, principales interesados), de alcance de alto nivel (como objetivos, alcance, plan de alto nivel, objetivos directivos que soporta, beneficios cuantitativos, beneficios cualitativos, recursos, entregables y riesgos) , de gobierno (estructura de gobierno recomendada para administrar, controlar y soportar la iniciativa) y de seguimiento (como el estado en el que se encuentra, cambios aprobados, administrador de la iniciativa).
Caso de negocio	Justificación técnica y económica de cómo se puede crear valor en la dependencia o entidad a través de la iniciativa, para garantizar la consecución de los resultados esperados. Para ello se apoya de indicadores cualitativos y/o cuantitativos. El contenido básico del caso de negocio consiste en los principales recursos a invertir y las capacidades técnicas, operativas y de negocio por desarrollar, dando como resultado la rentabilidad financiera u otros resultados no financieros pero factores de decisión.
Reporte de evaluación de iniciativa de inversión	Reporte que documenta el resultado de la evaluación de las iniciativas de inversión propuestas, fundamentos para la selección, priorización, autorización y balanceo: • Iniciativas de inversión autorizadas • Iniciativas de inversión no autorizadas Representación gráfica de la evaluación de las iniciativas de inversión.
Bitácora de cambios al portafolio de proyectos de TIC	Incluye información del portafolio de proyectos de TIC acerca de solicitudes de cambios, resultado de evaluación del impacto al cambio y autorización de los cambios. Incluye información de las decisiones que se tomaron de cada uno de los proyectos en cuanto a su suspensión, re-priorización, continuación o cancelación en base al resultado del balance del portafolio de proyectos.
Portafolio de proyectos de TIC	Se compone de todos los proyectos y/o programas de la dependencia o entidad derivados de iniciativas de inversión autorizadas para su ejecución.
Plan de gobierno del programa de	Integra toda la información requerida para dirigir y controlar al programa acerca de las finanzas, recursos, cronogramas, alcance, riesgos y comunicaciones.

Producto	Descripción
proyectos	
Autorización para el inicio del proyecto	Documento que autoriza formalmente que se dé inicio al proceso de administración del proyecto y emitir el Acta de constitución del proyecto.
Informes de desempeño del programa de proyectos	Informes y reportes que organizan y resumen la información recopilada del avance de los proyectos del programa y presentan los resultados del análisis de comparación del avance real contra lo planeado.
Informes de desempeño del portafolio de proyectos de TIC	Informes y reportes que organizan y resumen la información recopilada del avance global del portafolio.
Informe final de la iniciativa de inversión	Informe final elaborado al cierre de la iniciativa de inversión que integra los resultados y hallazgos de la revisión de resultados de los proyectos que la componen. Contiene las lecciones aprendidas para mejorar la eficacia y eficiencia de la administración de portafolios.
Plan para la realización de beneficios	Plan que establece para cada resultado clave del proyecto/programa la responsabilidad para el logro del resultado, la fecha estimada de obtención y el proceso de seguimiento, el cual debe incluir un registro detallado de los beneficios esperados en conjunto con la explicación de los riesgos que pueden amenazar el cumplimento de cada resultado clave y como estos riesgos deben ser mitigados.

7.3.1.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje del Portafolio de proyectos de TIC ejecutado	Obtener el porcentaje del portafolio de proyectos de TIC ejecutados en tiempo y forma	Porcentaje del portafolio de proyectos de TIC ejecutado con respecto al Portafolio de Proyectos de TIC programado	Eficacia operativa	De gestión	Iniciativas de inversión del Portafolio de Proyectos de TIC ejecutado / Total de Iniciativas de inversión del Portafolio de Proyectos de TIC programado	UTIC	Trimestral

7.3.1.4. Reglas del proceso

1.1.	El grupo de trabajo directivo de TIC, será responsable de autorizar las iniciativas de inversión que conformarán el portafolio de proyectos de TIC, así como de la aprobación en la toma de decisiones en caso de presentarse riesgos y oportunidades de alto impacto.
1.2.	El grupo de trabajo directivo de TIC deberá designar un responsable que administre cada iniciativa

	autorizada conforme al proceso de Administración de proyectos de TIC.
1.3	La autorización de iniciativas de inversión deberá estar sustentada en una justificación técnico económica o caso de negocio que presenta claramente los costos y beneficios, tangibles e intangibles esperados y deberá actualizarse cuando presente cambios.
1.4	El Administrador del portafolio de proyectos de TIC tendrá la responsabilidad de la identificación, evaluación, selección, determinación de prioridades y de la propuesta para autorización de las iniciativas de inversión del portafolio de proyectos de TIC así como de su balanceo, actualización y toma de decisiones en caso de presentarse riesgos, desviaciones y oportunidades.
1.5	Se deberá dar seguimiento y revisar periódicamente el estado y avance del portafolio de proyectos de TIC para tomar las decisiones y acciones preventivas, correctivas y oportunas sobre la continuidad de la inversión en recursos y de ser necesario ajustar, modificar, suspender o cancelar proyectos de TIC.
1.6	Deberá evaluar los resultados obtenidos de la ejecución del portafolio de proyectos de TIC y de la realización de los programas asociados a una iniciativa con el propósito de determinar el cumplimiento de los objetivos y beneficios esperados.
1.7	La UTIC deberá asegurar que la planeación y administración del portafolio de proyectos de TIC se apega a la normatividad para el uso y control de recursos financieros y humanos requeridos en los proyectos a implantar, así como del marco rector de procesos de TIC.

7.3.1.5. Documentación soporte del proceso

	No aplica.

7.3.2. Administración de proyectos de TIC

7.3.2.1. Objetivos del proceso

General.-

Incrementar la probabilidad de obtener los resultados esperados en los proyectos de TIC, mediante una planeación efectiva que asegure entrega oportuna, respeto del costo y la calidad acordada, asegurando la satisfacción del usuario.

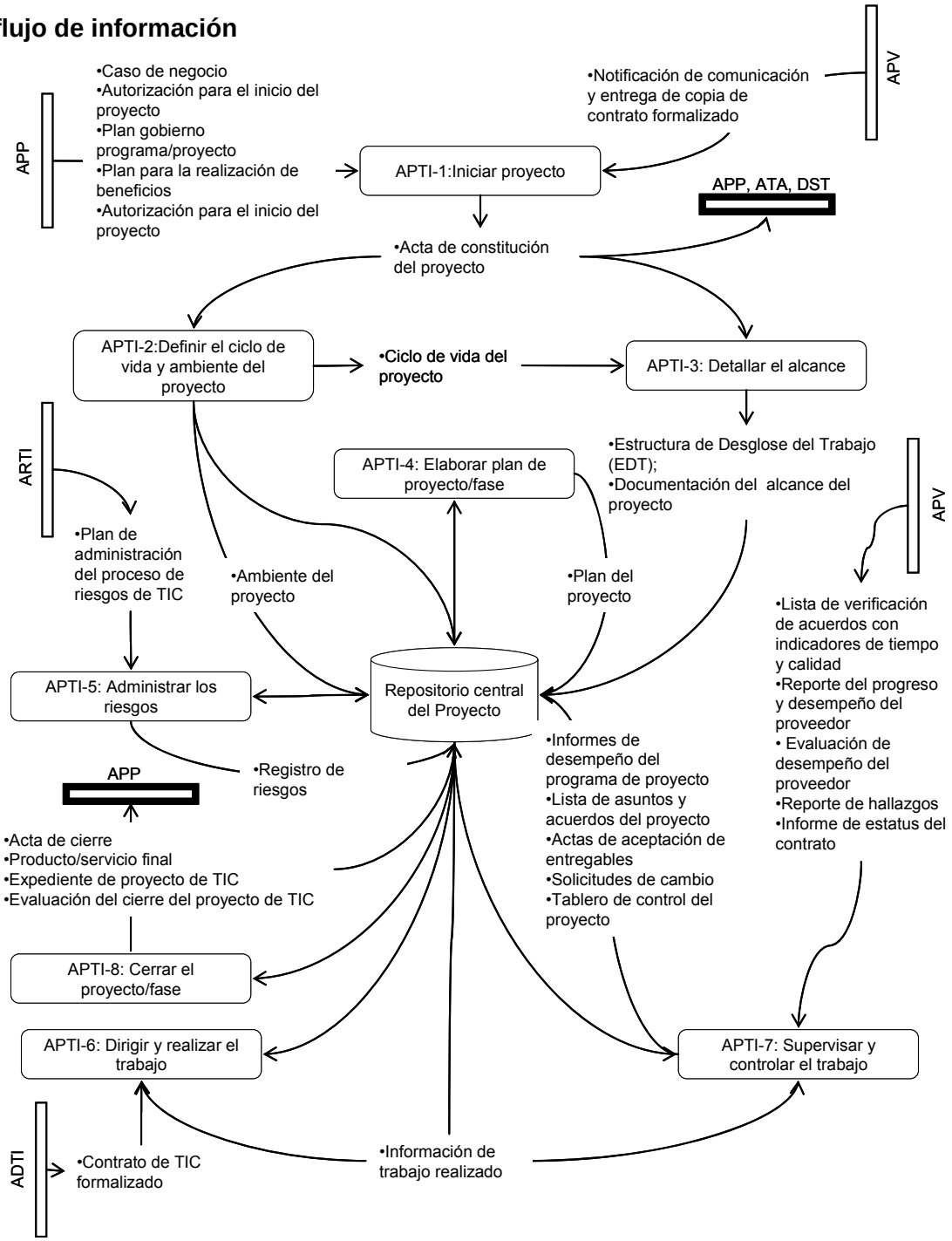
Específicos.-

1. Desarrollar y acordar con los involucrados el plan del proyecto.
2. Dirigir y controlar las actividades siguiendo el plan del proyecto, con el propósito de realizar el trabajo acordado respetando el alcance.
3. Asegurar que se cuenta con mediciones para detectar oportunamente desviaciones.
4. Ejecutar acciones preventivas y correctivas para evitar o subsanar desviaciones durante el proyecto.
5. Comunicar oportunamente a los interesados asuntos y riesgos para su análisis y atención.
6. Evaluar los cambios en los proyectos asegurando que se evalúe su impacto en el plan del proyecto antes de su autorización.
7. Asegurar la calidad del producto o servicio garantizando el cumplimiento de los criterios de satisfacción del usuario.

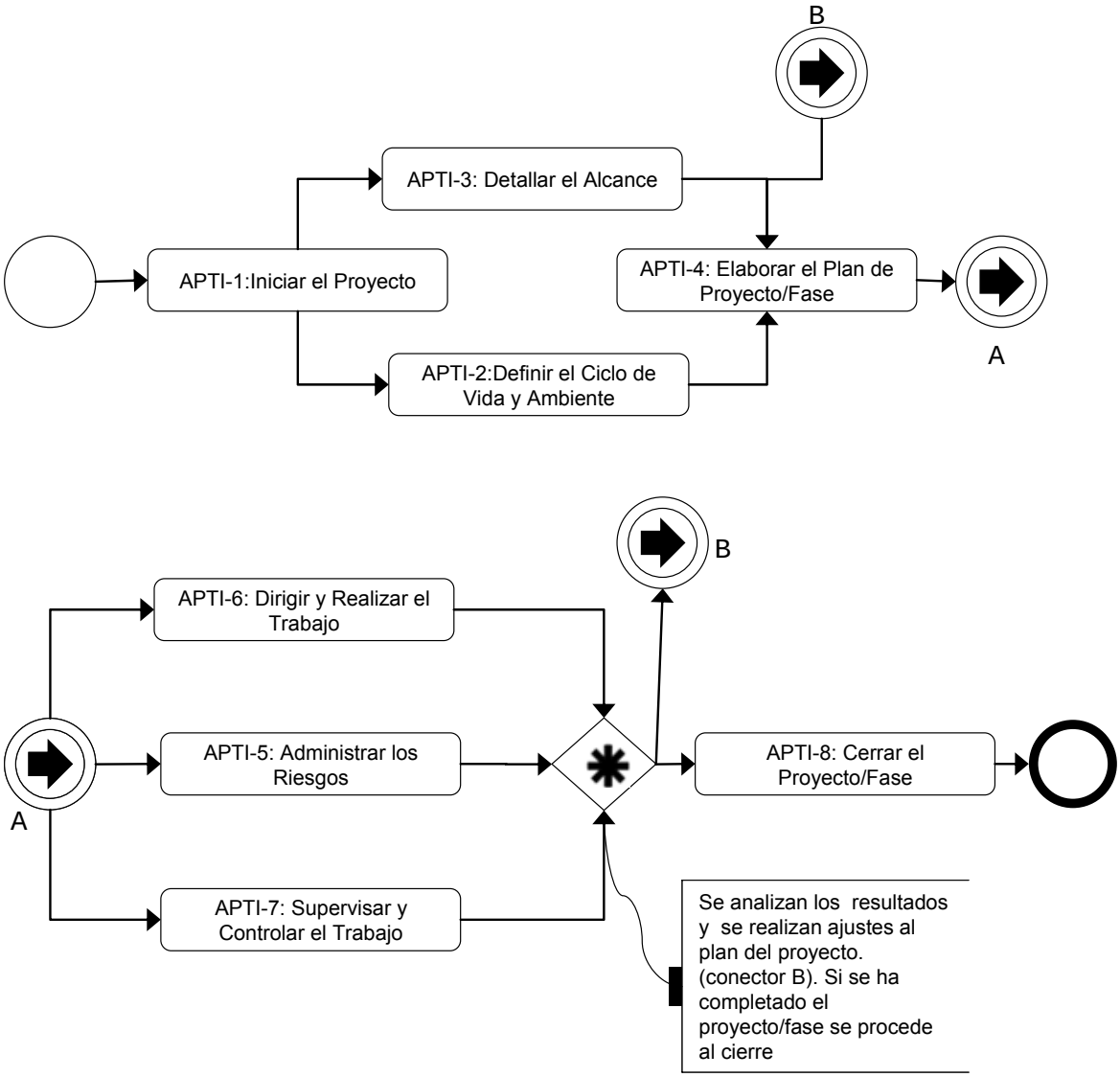
7.3.2.2. Descripción del proceso

7.3.2.2.1. Mapa general del proceso

Diagrama de flujo de información



Descripción del flujo de actividades



7.3.2.2.2. Descripción de las actividades del proceso

APTI-1: Iniciar el proyecto

Descripción	Tiene como propósito dar inicio formalmente a un proyecto.
Factores Críticos	1. Asignar formalmente a un responsable de llevar la administración del proyecto. 2. Para todo proyecto aprobado en el Portafolio de proyectos de TIC, deberá designarse a un Administrador de proyecto, que será responsable del desarrollo y cumplimiento del mismo. 3. Analizar la información de antecedentes del proyecto. 4. Facilitar al administrador del proyecto la información necesaria del proyecto, para que comprenda la importancia de éste para la dependencia o entidad y corrobore el alcance de acuerdo a los objetivos y requerimientos establecidos en los documentos que sustentaron la aprobación de la ejecución del proyecto, incluyendo si existen contratos. 5. Identificar proyectos relacionados con el propósito de determinar interdependencias, coordinar esfuerzos, identificar riesgos y explorar alternativas para evitar conflictos entre proyectos mientras se cumple con los objetivos del proyecto. 6. Identificar a los interesados o actores del proyecto que son afectados, que participan o son beneficiados, documentando y conciliando las expectativas sobre el proyecto. 7. Emitir el acta de constitución del proyecto con la finalidad de proveer al responsable de la administración del proyecto la autoridad de ejercer los recursos organizacionales acordados para realizar las actividades del proyecto.
Relación de productos	• Acta de constitución del proyecto

APTI-2: Definir el ciclo de vida y el ambiente del proyecto

Descripción	Definir el proceso para la realización del proyecto determinando su ciclo de vida así como establecer y mantener el ambiente del proyecto.
Factores Críticos	1. Definir el ciclo de vida del proyecto considerando entre otros factores, el tamaño del proyecto, experiencia y familiaridad del equipo en los procesos, tecnologías y productos a ser desarrollados y las restricciones como el tiempo y objetivos de calidad. • Si se cuenta con una base de activos organizacionales que contenga procesos estándar con modelos de ciclo de vida (ver proceso Establecimiento del sistema de gestión de procesos), el ciclo de vida del proyecto deberá ser una adaptación de éstos considerando los siguientes elementos:

	◦ Seleccionar de los procesos estándar que cubran mejor las necesidades del proyecto. ◦ De acuerdo con las guías de adaptación para establecer el proceso definido del proyecto. ◦ Utilizar los artefactos de la librería de procesos o repositorio organizacional como lecciones aprendidas, formatos, ejemplos de documentos, modelos de estimación, mecanismos de comunicación. ◦ Documentar el proceso definido. 2. Revisar el proceso definido del proyecto cada vez que sea necesario. • Pueden realizarse cualquier tipo de revisión determinado en la dependencia o entidad de acuerdo al proceso de establecimiento del sistema de gestión de procesos del presente manual. 3. Planear, diseñar, instalar y dar soporte al ambiente de trabajo.
Relación de productos	• Ciclo de vida del proyecto • Ambiente del proyecto • Repositorio central del proyecto

APTI-3: Detallar el alcance

Descripción	Tiene el propósito de recolectar, analizar y definir las necesidades y características del proyecto o servicio para establecer los principales elementos que definan la solución, orientadas a las necesidades del negocio y a la problemática actual. Esta práctica busca obtener una línea base de alcance del proyecto mediante el acuerdo detallado de las necesidades, objetivos y productos que forman parte del alcance del proyecto, así como las características que debe cumplir el producto o servicio a desarrollarse.
Factores Críticos	1. Acordar el alcance del producto, que corresponde a las características y funciones que caracterizan a un producto, servicio o resultado. 2. El alcance del producto deberá ser acordado con todos los interesados, particularmente con el cliente, el patrocinador y el equipo de trabajo. 3. Acordar con el equipo del proyecto y otros interesados el alcance del trabajo, que se refiere al trabajo que debe realizarse para entregar un producto, servicio o resultado con las funciones y características especificadas. 4. El alcance del trabajo se documenta en una Estructura de desglose del trabajo (EDT) que documenta el trabajo que será ejecutado por el equipo del proyecto, para lograr los objetivos del proyecto y crear los productos/entregables requeridos. 5. El EDT organiza y define el alcance total del proyecto.
Relación de productos	• Estructura de desglose del trabajo (EDT) • Documentación del alcance del proyecto

APTI-4: Elaborar el plan del proyecto/fase

Descripción	Consiste en establecer el plan del proyecto con el cual se guiará la ejecución, se dará seguimiento y se controlará la realización del proyecto a lo largo de todo el ciclo de vida del proyecto. El plan del proyecto establece como se cumplirá con los objetivos del proyecto, tomando en cuenta los factores, procesos e interacciones que lo componen o afectan durante su ciclo de vida.
Factores Críticos	1. Elaborar el cronograma del proyecto, partiendo de la EDT y de acuerdo con las

	restricciones establecidas en el acta constitutiva. Se deben definir las actividades, elaborar el diagrama de red con las actividades predecesoras y sucesoras, realizar los estimados, calcular las duraciones y las fechas de inicio y fin. El cronograma deberá ser elaborado con la participación de los interesados, particularmente con los responsables de desarrollar actividades. 2. Elaborar el presupuesto del proyecto, partiendo de la EDT y el cronograma del proyecto. Se elabora un estimado detallado que considera las estimaciones de los recursos necesarios para realizar las actividades programadas. El presupuesto deberá estar conforme al presupuesto autorizado en la carta de constitución del proyecto. Se debe ajustar el alcance del proyecto y el plan del proyecto (incluyendo el cronograma) en caso necesario. 3. Desarrollar el plan del proyecto. • Documentar un plan que en forma integral documente todos los procesos, métodos, herramientas, roles y responsabilidades para la administración y la realización del producto o servicio del proyecto. • El plan del proyecto debe integrar o hacer referencia a las líneas base para el control del tiempo (cronograma), costo (presupuesto) y alcance del proyecto (Documentación del alcance y la EDT). • El plan del proyecto deberá integrar o hacer referencia a los planes subsidiarios de (ver la descripción del producto plan del proyecto para mayor detalle del contenido de cada uno de estos planes): o Plan del alcance o Plan del tiempo o Plan del costo o Plan de calidad o Plan de recursos humanos o Plan de comunicaciones o Plan de riesgos o Plan de adquisiciones o Plan de configuración y cambios 4. Aprobar el plan del proyecto, ratificando los compromisos y acuerdos en los que se sustenta el plan. 5. Comunicar el plan del proyecto a todos los interesados. 6. Revisar el plan del proyecto cada vez que sea necesario cuidando de mantener el control de las versiones de las líneas base mediante solicitudes de cambios aprobadas y de comunicar los cambios a todos los interesados.
Relación de Productos	• Plan del proyecto

APTI-5: Administrar los riesgos

Descripción	Eliminar o minimizar los riesgos por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados.
Factores Críticos	1. Identificar riesgos. La identificación de riesgos es un proceso iterativo debido a que se pueden descubrir nuevos riesgos a medida que el proyecto avanza a lo largo de su ciclo de vida. El equipo del proyecto debe participar en la identificación de los riesgos para poder desarrollar y mantener un sentido de pertenencia y responsabilidad por los riesgos y las acciones asociadas con la respuesta a los riesgos. Los riesgos identificados se

	documentan en un registro de riesgos. 2. Clasificar riesgos. Los riesgos se categorizan por tipo de riesgo y se refina su descripción. Se identifica la causa raíz y se agrupan los riesgos por causa. Se pueden desarrollar respuestas efectivas a los riesgos si se aborda la causa del riesgo. (Ejemplo de Matriz FODA) 3. Responder a los riesgos. Se determina la prioridad de atención de los riesgos identificados y las acciones que serán realizadas para atender el riesgo, incluyendo las acciones de mitigación y la definición de un plan de contingencia. 4. Dar seguimiento y controlar riesgos. Realizar el seguimiento de los riesgos identificados, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto. 5. Adecuar el plan de proyecto, incluyendo la documentación del alcance, la EDT, el cronograma y el presupuesto para incorporar las decisiones derivadas de la administración de riesgos que impacten al plan.
Relación de productos	• Registro de riesgos

APTI-6: Dirigir y realizar el trabajo

Descripción	Consiste en la dirección y coordinación de las acciones para ejecutar el plan del proyecto y su cronograma respectivo, con el propósito de realizar el trabajo ahí descrito.
Factores Críticos	1. Asegurar que se realiza el trabajo necesario para elaborar los productos entregables y dar cumplimiento a los objetivos del proyecto. • Es fundamental que el responsable del proyecto garantice la realización exclusiva del trabajo previamente incluido en el plan y se asegure que se realice todo el trabajo planeado. 2. Durante la realización del trabajo se ejecutan las actividades de calidad de acuerdo a lo establecido en el Plan de Calidad. 3. El responsable de administrar el proyecto deberá supervisar la adquisición de los recursos y del equipo del proyecto necesario para la realización del trabajo. Es fundamental garantizar que el equipo de trabajo cuenta con las habilidades para realizar su trabajo mediante la provisión del entrenamiento y capacitación que requiera. 4. Durante la ejecución se distribuye la información requerida de acuerdo al plan de administración del proyecto con el propósito de mantener informados a los interesados y administrar adecuadamente sus expectativas.
Relación de productos	• Información de trabajo realizado

APTI-7: Supervisar y controlar el trabajo

Descripción	Comprende las bases para controlar efectivamente el proyecto a través del seguimiento del plan, reportando avances y manteniendo al día el control de cambios, y documentando las lecciones aprendidas a fin de recomendar acciones preventivas como anticipación de posibles problemas.
Factores Críticos	1. Dar seguimiento al rendimiento y avance del proyecto evaluando periódicamente los puntos de control que permitan identificar las variaciones respecto del plan del proyecto, para controlar los cambios y recomendar acciones preventivas como anticipación de posibles problemas y adoptar las acciones correctivas cuando sean necesarias, para controlar la ejecución del proyecto.

	2. Integrar los informes de rendimiento y realizar revisiones del progreso e hitos del proyecto. Los informes deben proporcionar la información sobre el estado de la situación, el progreso, y el nivel de detalles requeridos por los diversos interesados, según lo documentado en el plan de comunicaciones. 3. Entregar y revisar con el Administrador del Portafolio de Proyectos de TIC del proceso de Administración del Portafolio del Proyectos de TIC el informe del rendimiento del proyecto, así como los riesgos, hallazgos y oportunidades identificadas. 4. Analizar los asuntos del proyecto y dar seguimiento hasta su cierre. 5. Acordar formalmente la aceptación de entregables. Los entregables que se presenten para su aprobación deberán de haber sido sujetos a todas las actividades de calidad que se establezcan para éste en el Plan de de Calidad. 6. Realizar el control de cambios al proyecto, de tal modo que todos los cambios aprobados a las líneas base del proyecto (Ej. Costos (presupuesto), tiempo (cronograma), y alcance (documentación del alcance y EDT)) se revisen, aprueben e incorporen de manera apropiada al plan del proyecto. 7. Informar el seguimiento del proyecto y recibir retroalimentación de los Procesos de Administración de Proveedores, Adquisiciones de TIC, Administración Financiera y Establecimiento del Sistema de Gestión de Procesos del presente manual en materia de lo que a cada uno corresponde.
Relación de productos	• Informes de desempeño del programa de proyecto • Lista de asuntos y acuerdos del proyecto • Actas de aceptación de entregables • Solicitudes de cambio • Tablero de control del proyecto

APTI-8: Cerrar el proyecto/fase

Descripción	Comprende la importancia del cierre del proyecto o una fase del proyecto y los requerimientos para una entrega completa. El proceso de cierre verifica que los procesos definidos se completen en todas sus etapas para cerrar el proyecto o una fase del mismo, según corresponda y contempla desde la satisfacción del cliente, la entrega formal y recepción de los entregables y productos del proyecto, verificando y documentando los resultados del proyecto. El cierre considera la entrega ordenada de todos los documentos generados durante el desarrollo del proyecto, así como el cierre profesional de todos los acuerdos legales y evaluaciones de desempeño, dicho proceso comienza después de que el proyecto o su etapa cumplen con sus objetivos y es terminado, suspendido ó cancelado e incluye el cierre contractual y el cierre administrativo.
Factores Críticos	1. Revisar y validar que el expediente y documentación soporte del proyecto de TIC cumpla con lo definido en la Calidad del proceso Establecimiento del Sistema de Gestión de Procesos del presente manual como la documentación de lecciones aprendidas y la mejora continua. 2. Integrar el expediente del proyecto de TIC el cual contendrá la documentación soporte, resultados finales, archivos, cambios, directorios, evaluaciones y lecciones aprendidas entre otros. 3. Formalizar el cierre del proyecto a través del acta de cierre firmada por el cliente y/o patrocinador y los responsables de la administración y supervisión del proyecto. 4. Realizar las notificaciones correspondientes de término del proyecto a los procesos de Administración del Portafolio de Proyectos de TIC, Adquisiciones de TIC, Administración de Proveedores, Administración Financiera y Establecimiento del Sistema de Gestión de Procesos del presente manual para que se lleve acabo los procesos de cierre

	correspondientes. 5. Concluir y realizar el cierre contractual, en donde se verifiquen los entregables del proyecto. Los términos del contrato y sus condiciones pueden determinar procedimientos específicos para el cierre del contrato. Terminar antes de la fecha programada es un caso especial de cierre de contrato. 6. Concluir y realizar el cierre administrativo conforme a lo establecido en los Procesos de Administración de Proveedores y Adquisiciones de TIC del presente manual, asegurando y documentando los resultados del proyecto para formalizar la aceptación de los entregables, integrados por el Administrador del Proyecto los cuales incluirán las observaciones del cliente y/o el patrocinador ó el Administrador y Supervisor del Contrato, se incluye la recolección de documentos finales, así como el análisis de efectividad y éxito del proyecto. 7. Asegurar la calidad y disponibilidad del expediente y documentación soporte del Proyecto de TIC para su uso posterior con la finalidad de facilitar referencias, desarrollo futuros proyectos y auditorías externas o internas. 8. Considerar las actividades necesarias para lograr una transición efectiva del producto o servicio, incluyendo capacitación, materiales y demás herramientas necesarias con el propósito de que el usuario final utilice el producto o servicio generado. 9. Evaluar y documentar el cierre del proyecto en un formato de retroalimentación y discutirlo con el equipo, el cliente, el patrocinador, administrador y supervisor del contrato así como el administrador del proyecto. La evaluación servirá para documentar el desempeño del equipo del proyecto al cierre, como para capitalizar las lecciones aprendidas para futuros proyectos. Puntos a evaluar: • Retroalimentación del proceso de administración del portafolio de proyectos de TIC del presente manual. • Retroalimentación del cliente o usuario (cumplimiento de requerimientos) • Reportes ejecutivos, veraces, relevantes y a tiempo. • Distribución efectiva de roles y funciones. • Predicción y manejo adecuado de riesgos. • Entregas parciales y finales a tiempo. • Ahorro en costos. • Buena integración del equipo del proyecto. • Resultados predecibles. • Administración ordenada del proyecto. • Decisiones fundamentadas. • El plan del proyecto está completo y la información es correcta. • El producto del proyecto cumple adecuadamente con el estándar de calidad establecido. • Apego al plan del proyecto. • Evaluación de la relación con los involucrados al proyecto (equipo, cliente, proveedores, administrador del proyecto y demás participantes).
Relación de Productos	• Acta de cierre • Producto/servicio final • Expediente de proyecto de TIC • Evaluación del cierre del proyecto de TIC

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.3.2.2.3 Descripción de roles

Rol	Descripción
Administrador del Proyecto	Es el responsable de administrar el proyecto, de su desarrollo y cumplimiento, y es nombrado por la UTIC quien lidera al equipo del proyecto para alcanzar los objetivos, asegura la comunicación efectiva entre la administración y otras organizaciones y asegura que los problemas del proyecto sean identificados y resueltos a tiempo y adecuadamente, para proporcionar un resultado final exitoso en tiempo y forma. El administrador del Proyecto deberá contar con capacidades, conocimientos, habilidades, herramientas y técnicas de administración de proyectos.
Patrocinador del Proyecto	El patrocinador del proyecto es el ejecutivo responsable del proyecto, provee fondos para el proyecto y trabaja estrechamente con el administrador del proyecto para definir los factores críticos de éxito y métricas para el proyecto. Es la persona a cargo de la dirección del proyecto, asegura la toma de decisiones a tiempo, apoya la asignación de recursos, supera conflictos y barreras organizacionales para una mejor realización del proyecto, asigna y apoya al administrador del proyecto y provee la dirección estratégica al administrador del proyecto.
Cliente	Dependencia y/o entidad, persona, entidad externa o interna que define los alcances del proyecto, establecer los criterios funcionales de aceptación y recibe los resultados o productos de TIC del proyecto.
Usuario	Dependencia y/o Entidad, persona, entidad externa o interna que dará uso a los resultados y beneficios generados por el proyecto de TIC.
Equipo de Trabajo	Incluye los roles definidos en el proceso y son los encargados de planear, ejecutar, controlar y cerrar el ciclo de vida del proceso de Administración de Proyectos de TIC.

7.3.2.2.4 Descripción de productos

Producto	Descripción
Acta de constitución del proyecto	Documento que autoriza formalmente el inicio del proyecto y asigna al administrador del proyecto. El acta de constitución del proyecto es emitida por el patrocinador del proyecto cuando es autorizado en el proceso de administración del portafolio de proyectos de TIC.
Ciclo de vida del proyecto	Definen las fases en que se pueden dividir los proyectos, conectando el inicio de un proyecto con su fin, con el propósito de facilitar su gestión describiendo el entorno en el cual operan los proyectos.
Documentación del alcance del proyecto	Incluye la información necesaria y requerida para establecer el alcance del proyecto; la documentación del alcance incluye entre otros: • Los objetivos detallados del proyecto. • La especificación de los productos y entregables. • Los supuestos y restricciones. • La documentación de los requerimientos del proyecto. • Criterios de aceptación para entregables y fases del proyecto.
Plan del Proyecto	Establece de manera formal la estrategia, responsabilidades y planes a seguir para lograr los objetivos del proyecto, e integra toda la información requerida para administrar el proyecto.

Producto	Descripción
	Algunos puntos que deben ser considerados en este documento (ya sea integrados o referenciados) son: • Supuestos, dependencias, restricciones y exclusiones. • Adaptación del proceso (proceso definido adecuado al proyecto, estimados del proyecto, ciclo de vida) • Planes subsidiarios de: o Plan del alcance. Define la metodología para la definición del alcance, la creación de la EDT, la aprobación de entregables y el control de cambios al alcance. o Plan del tiempo. Define la metodología para la creación y el control de cambios al cronograma. o Plan del costo. Define la metodología para la creación y el control de cambios al presupuesto. o Plan de calidad. Define la metodología para la planeación de la calidad, el establecimiento de los objetivos de calidad y las actividades de aseguramiento y control de la calidad. o Plan de comunicaciones. En este plan se identifican los requerimientos de información de los interesados y se determina como se va proporcionar la información necesaria a lo largo de la realización del proyecto. El plan de comunicación detalla entre otros que información se va a comunicar, a quién, con que propósito, el medio y la frecuencia. o Plan de riesgos. Define la metodología para la identificación, clasificación, análisis, atención y seguimiento a los riesgos. o Plan de recursos humanos. Define la estructura organizacional del proyecto, establece roles y responsabilidades, define la metodología para la adquisición, integración, desarrollo y administración del equipo de trabajo. Incluye el plan de capacitación y entrenamiento así como el sistema de incentivos y recompensas. o Plan de adquisiciones. Define que se va a adquirir, cómo se van a contratar los servicios/productos, criterios de selección de proveedores, cuándo se debe contratar, cual es el presupuesto para cada contrato y el tipo de contrato, esquema de contratación. o Plan de configuración y cambios. Define la metodología para el control de versiones y la publicación y acceso a la base de información del proyecto. Define el sistema de control de cambios, incluyendo los tipos de cambios y los niveles para la autorización de cambios al proyecto. • Líneas base para el control del tiempo (cronograma), costo (presupuesto) y alcance (documentación del alcance del proyecto y la EDT) • Ambiente de Trabajo del Proyecto (servidores, equipos de desarrollo, equipos de pruebas, herramientas, infraestructura)
Ambiente del proyecto	Ambiente colaborativo para la administración de proyectos.
Repositorio central del proyecto	Es el conjunto de datos e información, resultado de la ejecución de las actividades a lo largo del Ciclo de vida del proyecto

Producto	Descripción
Estructura de desglose del trabajo	La Estructura de desglose de trabajo (EDT) es una descomposición jerárquica con orientación hacia el producto/entregable relativa al trabajo que será ejecutado por el equipo del proyecto para lograr los objetivos del proyecto y crear los productos entregables requeridos, internos y externos.
Lista asuntos y acuerdos del proyecto	Lista que permite el registro de asuntos y acuerdos de manera ordenada, facilitando la administración y cumplimiento de los mismos.
Informes de desempeño del programa de proyecto	Informes y reportes que organizan y resume la información recopilada del avance del proyecto y presentan los resultados del análisis de comparación del avance contra el plan.
Acta de cierre	Documento en el que los involucrados relevantes reconocen el cierre del proyecto y dan conformidad de que el proyecto ha cumplido de manera completa el producto y/o servicios establecidos.
Producto/servicio final	Es la aceptación formal y entrega de producto, servicio o resultado final que el proyecto debe producir.
Registro de Riesgos	Lista ordenada de riesgos del proyecto, ordenados y asociados con la mitigación o las acciones de contingencia. Un ejemplo del contenido del registro de riesgos es: • ID del riesgo. • Fecha de registro. • Estado. • Descripción detallada del riesgo. • Tipo de riesgo. • Descripción del impacto a actividades, productos, u objetivos en caso de presentarse el riesgo. • Probabilidad. • Medición de impacto. • Prioridad. • Disparadores/síntomas que indican la posibilidad latente del riesgo. Responsable del riesgo. • Plan de mitigación. • Plan de contingencia. • Fecha de seguimiento • Observaciones • Reserva del riesgo.
Información del trabajo realizado	Registro de información del estado del trabajo del proyecto para proveer datos para informar el rendimiento y el estado del proyecto a los interesados. Esta información incluye, entre otros: • Productos entregables que han sido completados y aquellos que no han sido completados. • Actividades del cronograma que se han iniciado y aquellas que se han finalizado.

Producto	Descripción
	• Actividades del cronograma que se han retrasado. • Alcance del cumplimiento de los estándares de calidad. • Costos autorizados e incurridos. • Estimaciones del esfuerzo remanente hasta la conclusión de las actividades del cronograma. • Porcentaje físicamente completado de las actividades del cronograma en desarrollo. • Lecciones aprendidas documentadas registradas en la base de conocimientos de lecciones aprendidas. • Detalle de la utilización de recursos. • Bitácoras de trabajo.
Acta de aceptación de entregables	Carta que se emite por el cliente para reconocer que un conjunto de entregables se han realizado de acuerdo a lo establecido y que cumple con los requerimientos acordados, mediante la firma de un oficio de aprobación de entregables. Un ejemplo del contenido de esta acta es: • Nombre del proyecto • Fecha • Objetivo del documento • Lista de entregables generados • Firmas de conformidad del servicio
Solicitudes de Cambios	Solicitudes para ampliar o reducir el alcance de un proyecto. Únicamente se procesan las solicitudes de cambio formalmente documentadas, y sólo se implementan las solicitudes de cambio aprobadas. Un ejemplo del contenido de una solicitud de cambio es: • Fecha de solicitud • Número de solicitud • Nombre del proyecto • Nombre del solicitante y rol en el proyecto • Tipo de cambio • Descripción del cambio • Análisis del impacto (tiempo, costo, alcance, calidad) • Respuesta • Firmas • Anexos En forma complementaria se puede integrar la bitácora de control de cambios con la fecha de recepción, número de solicitud, breve descripción, solicitante, autoriza, fecha acordada, recursos (Hrs/hombre, costo), estado y observaciones.
Tablero de control del proyecto	Se identifican los puntos de control que permitan identificar las variaciones con respecto al plan del proyecto, con el propósito de dar seguimiento al rendimiento y al avance del proyecto.

Producto	Descripción
Expediente del proyecto de TIC	Contiene toda la documentación generada por el proyecto desde su concepción hasta el cierre.
Evaluación del cierre del proyecto de TIC	Formato de retroalimentación que integra la evaluación del equipo, el cliente, el patrocinador, administrador y supervisor del contrato así como el administrador del proyecto. La evaluación servirá para documentar el desempeño del equipo del proyecto al cierre, como para capitalizar las lecciones aprendidas para futuros proyectos. Puntos a evaluar: • Retroalimentación del Proceso de Administración del Portafolio de Proyectos del presente manual. • Retroalimentación del cliente o usuario (cumplimiento de requerimientos) • Reportes ejecutivos, veraces, relevantes y a tiempo. • Distribución efectiva de roles y funciones. • Predicción y manejo adecuado de riesgos • Entregas parciales y finales a tiempo • Ahorro en costos • Buena integración del equipo del proyecto • Resultados predecibles • Administración ordenada del proyecto • Decisiones fundamentadas • El plan del proyecto esta completo y la información es correcta • El producto del proyecto cumple adecuadamente con el estándar de calidad establecido • Apego al plan del proyecto • Evaluación de la relación con los involucrados al proyecto (equipo, cliente, proveedores, administrador del proyecto y demás participantes).

7.2.2.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de proyectos a tiempo y dentro del presupuesto	Conocer el porcentaje de proyectos realizados en tiempo y dentro del presupuesto de acuerdo a lo programado en el portafolio de proyectos de TIC	Porcentaje de proyectos de TIC desarrollados en tiempo y dentro del presupuesto con respecto a los programado en el portafolio de proyectos de TIC.	Eficiencia operativa	De gestión	Porcentaje de proyectos a tiempo y dentro del presupuesto =(Número de proyectos realizados en tiempo y dentro del presupuesto / Total de proyectos programados en tiempo y presupuesto del Portafolio de Proyectos de TIC) * 100	UTIC	Trimestral

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Índice del rendimiento del costo del proyecto	Indicador de eficiencia de costos más comúnmente utilizado	Un valor inferior a 1 indica un sobre costo con respecto a las estimaciones. Un valor superior a 1 indica un costo inferior con respecto a las estimaciones.	Eficiencia operativa	De gestión	CPI= EV/AC, donde: - CPI: Índice de rendimiento del costo; - EV: Valor ganado.- La cantidad presupuestada para el trabajo realmente completado de la actividad del cronograma o el componente de la EDT durante un periodo de tiempo determinado; - AC: Costo real.- Costo total incurrido en la realización del trabajo realmente completado de la actividad del cronograma o el componente de la EDT durante un periodo de tiempo determinado	Administrador del proyecto	Trimestral
Índice del rendimiento del cronograma del proyecto	Predecir la fecha de conclusión y, a veces, para predecir las estimaciones de conclusión del proyecto.	Un valor inferior a 1 indica un sobre costo con respecto a las estimaciones. Un valor superior a 1 indica un costo inferior con respecto a las estimaciones. La variación del cronograma al final del proyecto será igual a cero porque ya se habrán ganado todos los valores	Eficiencia operativa	De gestión	SPI= EV/PV, donde: - SPI índice de rendimiento del cronograma; - EV: Valor ganado.- La cantidad presupuestada para el trabajo realmente completado de la actividad del cronograma o el componente de la EDT durante un periodo de tiempo determinado; - PV: Valor planificado.- Costo presupuestado	Administrador del proyecto	Trimestral

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
		planificados.			del trabajo programado para ser completado de una actividad o componente de la EDT hasta un momento determinado		

7.3.2.4 Reglas del proceso

1.1	Deberá designarse un Administrador del proyecto para cada proyecto de TIC que se inicie en la UTIC. El Administrador del proyecto será responsable de las actividades de dirección, planificación y seguimiento y control del proyecto para asegurar cumpla según lo establecido en el Plan del proyecto.
1.2	Los administradores de proyecto asignados deberán asegurarse de que todos los proyectos tengan asociado un plan del proyecto aprobado formalmente. Los cambios al plan del proyecto deberán realizarse mediante un proceso de control cambios.
1.3	Los administradores de proyecto asignados deberán asegurarse de que cualquier cambio al plan del proyecto autorizado se realice mediante un proceso de control cambios.
1.4	El administrador del proyecto deberá administrar y dar seguimiento al avance del proyecto a fin de dar cumplimiento a lo planeado, utilizando eficientemente los recursos asignados e identificando desviaciones, riesgos y oportunidades para tomar las acciones que correspondan en cada caso.
1.5	El administrador del proyecto deberá asegurar que se elaboren informes periódicos que incluyan como mínimo: el progreso al cronograma, las listas de riesgos, asuntos y cambios ocurridos durante el ciclo de vida del proyecto.
1.6	El administrador del proyecto deberá informar y recibir retroalimentación del seguimiento al plan del proyecto según el plan de comunicaciones y de los procesos de administración del portafolio de TIC, proceso de administración de proveedores, proceso de adquisiciones, proceso de administración financiera, procesos establecimiento del sistema de gestión de procesos del presente manual, en lo que a cada uno corresponda.
1.7	El administrador del proyecto deberá contar con el expediente del proyecto de TIC debidamente documentado y actualizado conforme a cada actividad desde su inicio, durante su ciclo de vida hasta su cierre.

7.3.2.5 Documentación soporte del proceso

No aplica.

7.4 ADMINISTRACIÓN-PROCESOS

7.4.1 Establecimiento del sistema de gestión de procesos

7.4.1.1 Objetivos del proceso

General.-

Establecer un sistema de gestión de procesos en la UTIC, apegado al marco rector de procesos de TIC, para mejorar la eficiencia operativa de la UTIC y entregar soluciones tecnológicas y servicios de TIC de calidad.

Específicos.-

1. Identificar los procesos de la UTIC.
2. Definir los procesos de la UTIC.
3. Determinar la secuencia e interacciones de estos procesos.
4. Determinar los criterios y los métodos necesarios para asegurar que tanto la operación como el control de estos procesos son efectivos.
5. Asegurar la disponibilidad de los recursos y de la información necesaria para la operación y el monitoreo de estos procesos.
6. Establecer indicadores para estos procesos.
7. Monitorear los resultados de los procesos.
8. Analizar los resultados de estos procesos.
9. Determinar las oportunidades de mejora y lecciones aprendidas.
10. Implementar las acciones de mejora.

7.4.1.2 Descripción del proceso

7.4.1.2.1 Mapa general del proceso

Diagrama de flujo de información

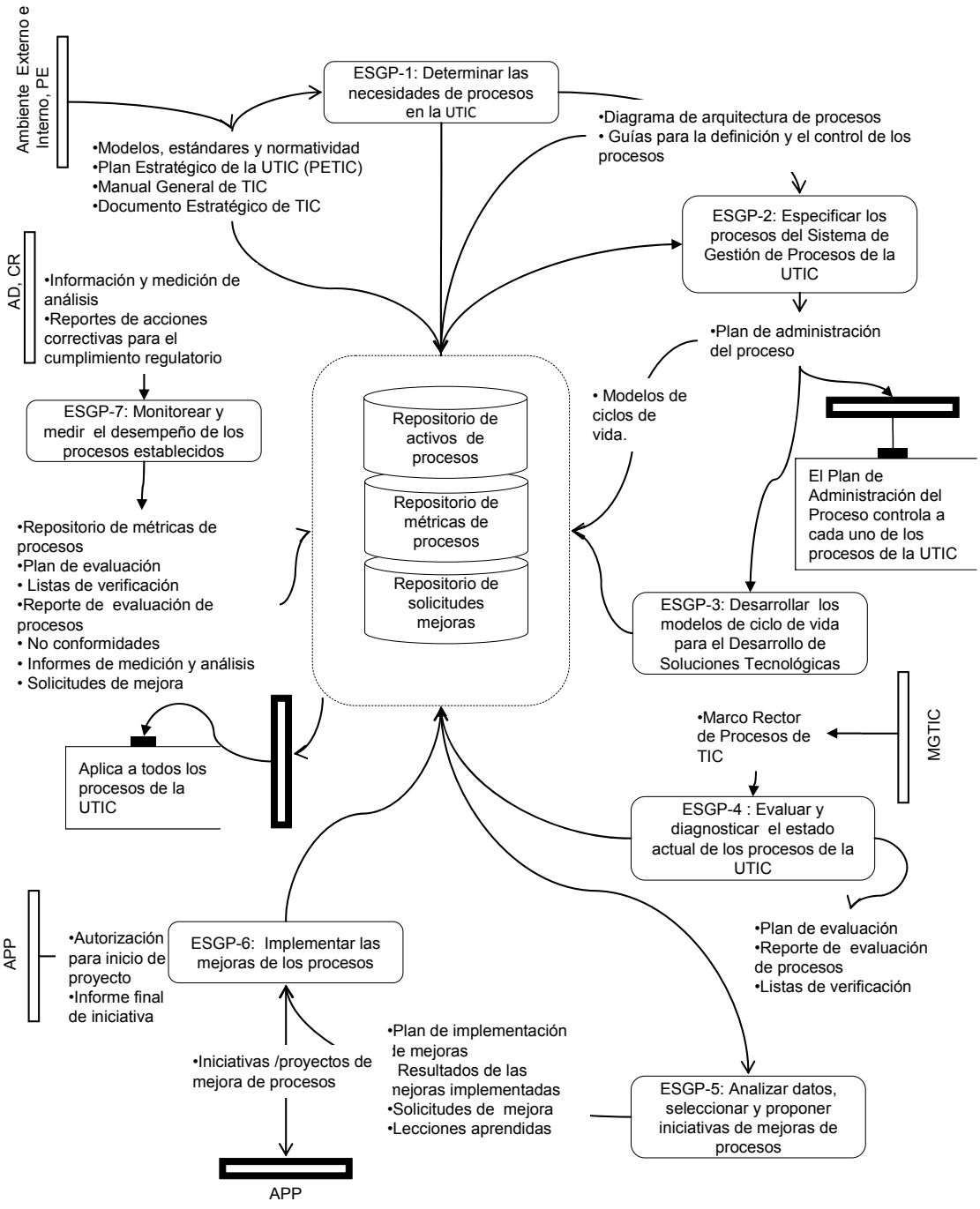
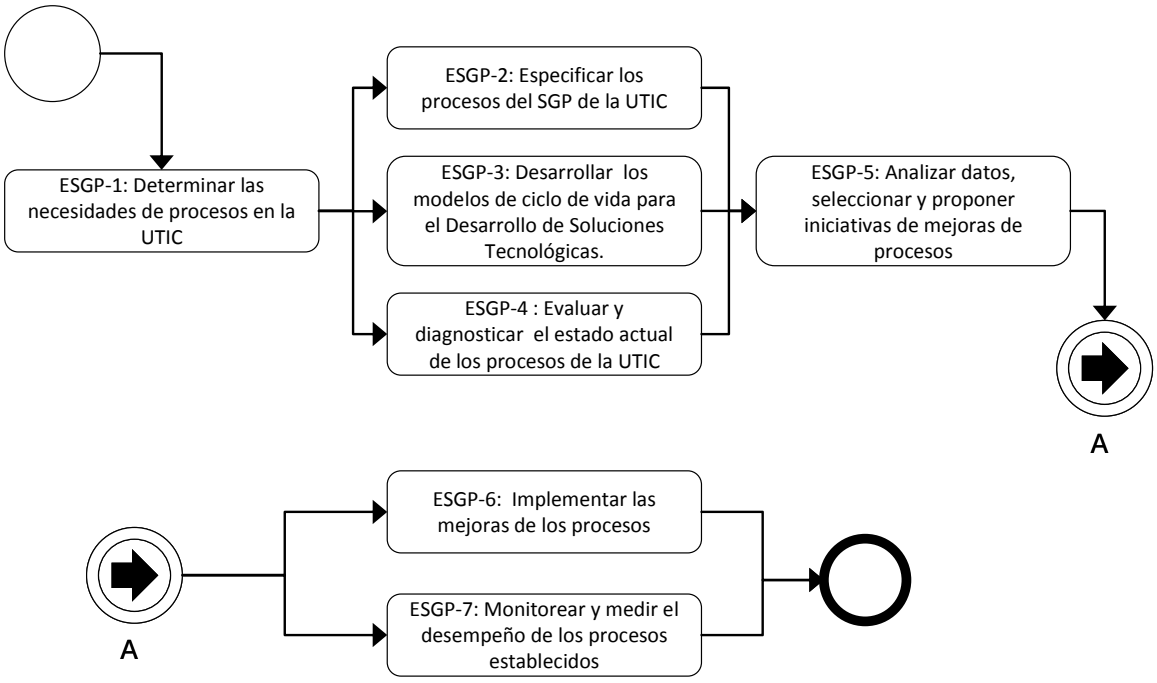


Diagrama de flujo de actividades



7.4.1.2.2 Descripción de las actividades del proceso

ESGP-1: Determinar las necesidades de procesos en la UTIC

Descripción	Definir los procesos del sistema de gestión de procesos de la UTIC con un enfoque sistémico (necesariamente del marco rector de procesos de este manual).
Factores Críticos	1. Determinar los procesos que formarán parte del sistema de procesos de la UTIC con base a los siguientes criterios: • Asegurar que se consideran los procesos necesarios para dar cumplimiento a los objetivos, misión, visión y líneas de acción estratégica en materia de TIC establecidas en el PETIC y en el Documento estratégico de TIC. • Incluir el conjunto de procesos de UTIC necesarios para asegurar la entrega consistente de soluciones tecnológicas y servicios de TIC de calidad que cumplen con los objetivos de calidad y la normatividad vigente • Apegarse al marco rector de procesos del presente manual • Considerar los estándares y modelos de referencia de mejores prácticas nacionales e internacionales que se hayan seleccionado para su adopción en la institución. 2. Especificar las características esenciales de los procesos determinados, en el contexto de la UTIC de la dependencia o entidad, incluyendo: • El objetivo y propósito para cada uno de los procesos • La secuencia e interacciones de los procesos con el propósito de asegurar que existe una apropiada integración entre los procesos incluyendo: o límites (inicio y el fin del proceso), o entradas y salidas, o proveedores y usuarios (clientes), o subprocesos, o conexiones con procesos internos y externos. 3. Modelar los procesos en forma gráfica a través de un diagrama de arquitectura de procesos, en donde muestre la jerarquía, relación e interacción entre los procesos. 4. Determinar y comunicar las guías para la definición y el control de los procesos. 5. Diseñar el repositorio de activos de procesos, identificar y mantener el conocimiento y transferir el conocimiento. • Este factor crítico se lleva a cabo en colaboración y bajo la dirección del proceso de administración del conocimiento. 6. Revisar en forma periódica las necesidades de definición y control de los procesos de TIC de la dependencia o entidad.
Relación de Productos	• Diagrama de arquitectura de procesos • Guías para la definición y el control de los procesos

	• Repositorio de activos de procesos • Repositorio de métricas de procesos • Repositorio de solicitudes de mejoras

ESGP-2: Especificar los procesos del ESGP de la UTIC

Descripción	Desarrollar/mejorar la definición de los procesos constituyentes del sistema de gestión de la UTIC.
Factores Críticos	1. Definir y comunicar para cada proceso metas y objetivos específicos, medibles, viables, orientados a resultados y en tiempo para la ejecución efectiva de cada proceso. Asegurando que se encuentre asociados a las metas de establecidas en el PETIC y que se soportan por métricas adecuadas. 2. Asignar un responsable para cada proceso, y definir claramente los roles y responsabilidades del dueño del proceso. Incluye, por ejemplo, responsabilidad del diseño del proceso, interacción con otros procesos, rendición de cuentas de los resultados finales, medición del desempeño del proceso y la identificación de mejora de las oportunidades. 3. Diseñar y establecer cada proceso de tal manera que sea repetible y consecuentemente produzca los resultados esperados. Proveer una secuencia lógica pero flexible y escalable de actividades que lleve a los resultados deseados y que sea lo suficientemente ágil para manejar las excepciones y emergencias. Usar procesos consistentes, cuando sea posible, y ajustarlos de ser necesario de acuerdo a criterios y guías de adaptación formalmente aprobadas. 4. Definir las actividades clave y productos resultantes del proceso. Asignar y comunicar roles y responsabilidades no ambiguas para la ejecución efectiva y eficiente de las actividades clave y su documentación, así como la rendición de cuentas para los entregables finales del proceso. 5. Definir los documentos y activos del proceso que se encontrarán bajo control de cambios y versiones, incluyendo las políticas, planes y procedimientos que controlan los procesos, los documentos de origen externo necesarios para la planeación y operación del proceso y los registros necesarios para proveer evidencia de la conformidad a los requerimientos del proceso y de su operación efectiva. Se deberá definir y comunicar cómo estos documentos y activos serán documentados, identificados, revisados, mantenidos, aprobados, almacenados, comunicados y usados para el entrenamiento (de ser el caso). 6. Asegurar: a) la definición de los objetivos de calidad y los requerimientos para el producto resultante, b) las necesidades de establecimiento de procesos, activos y de provisión de recursos específicos para el producto, c) las actividades de verificación, validación, monitoreo, inspección y pruebas específicos para el producto, d) los criterios para la aceptación de los productos y, e) los registros para proveer evidencia que los procesos y los productos resultantes

	cumplen con los requerimientos. 7. Identificar un conjunto de métricas que proporcionen visión de los resultados y el desempeño del proceso. Establecer objetivos que se reflejen en las metas del proceso y los indicadores de desempeño de tal manera que permitan el logro de las metas de los procesos. Definir como se obtienen los datos. Comparar las medidas actuales con los objetivos y tomar las acciones sobre las desviaciones cuando sea necesario. Alinear métricas, objetivos y métodos con el enfoque de monitoreo global del desempeño de TIC establecido en el proceso de evaluación del desempeño de TIC (ver proceso Administración del desempeño). 8. Determinar, proveer y mantener la infraestructura necesaria para la realización de los procedimientos. La infraestructura incluye, cuando sea aplicable: a) instalaciones, espacio de trabajo y herramientas asociadas, b) equipo del proceso incluyendo software e infraestructura, c) servicios de soporte (como transporte, comunicación o sistemas de información) • Se sugiere evaluar estándares de ambientes de trabajo colaborativos apropiados para la realización de los procesos de la UTIC. 9. Determinar las competencias de los recursos humanos que realizará trabajo que afecte la calidad de los productos y determinar la capacitación requerida para lograr estas competencias 10. Integrar el Plan de administración del proceso (también llamado Plan de calidad del proceso en un sistema de gestión de procesos, según ISO 9001) los elementos necesarios para la dirección, realización y control del proceso.
Relación de Productos	• Plan de administración del proceso • Modelos de ciclo de vida

ESGP-3: Desarrollar los modelos de los ciclo de vida para el desarrollo de soluciones tecnológicas y sus guías de adaptación

Descripción	Establecer y mantener los modelos estándares de ciclo de vida para usar en la UTIC de acuerdo a criterios y guías de adaptación aprobadas.
Factores Críticos	1. Seleccionar, documentar y revisar los modelos de ciclo de vida estándares para el desarrollo de una solución tecnológica para una variedad de tipos de proyectos que determine el grupo de trabajo de mejora continua de TIC con base en los procesos y lineamientos del este manual y las mejores prácticas de TIC aplicables 2. Establecer y mantener los criterios y guías de adaptación para crear un proceso definido para un proyecto de desarrollo de una solución tecnológica con base a los modelos de ciclo de vida estándares que este de acuerdo a las necesidades específicas del tipo de proyecto y las características del producto resultante. Los criterios y guías de adaptación deben especificar los requerimientos obligatorios que deben ser satisfechos por el proceso definido, opciones que pueden ser usadas y criterios para selección y los procedimientos que deben seguirse para desarrollar y documentar la adaptación de los modelos de ciclo de vida estándares.

	3. Revisar y detectar mejoras en forma periódica a los criterios y guías de adaptación.
Relación de Productos	• Repositorio de activos de procesos • Repositorio de métricas de procesos • Repositorio de solicitudes de mejora

ESGP-4: Evaluar y diagnosticar el estado actual de los procesos de la UTIC

Descripción	Evaluar periódicamente los procesos de la UTIC con el propósito de: • Contar con un diagnóstico del estado actual de los procesos de la UTIC • Identificar procesos que se necesitan definir o que tienen oportunidades de mejoras • Confirmar el progreso y hacer visibles los beneficios de mejora de procesos • Generar conciencia del valor y los beneficios potenciales de la inversión en el establecimiento y mejora de procesos, motivar a los involucrados y facilitar la aceptación del cambio
Factores Críticos	1. Obtener el compromiso de los funcionarios de alto nivel para la evaluación de los procesos de la UTIC 2. Realizar la evaluación de los procesos de la UTIC • La evaluación de los procesos de la UTIC deberá considerar un análisis comparativo de los procesos operando actualmente contra los procesos y lineamientos definidos en el MGTIC. • El alcance de la evaluación de procesos deberá considerar lo siguiente: o Cobertura de la evaluación con respecto a los procesos y lineamientos del presente manual y de ser el caso, los otros estándares y modelos de referencia de mejores prácticas nacionales e internacionales que se hayan seleccionado para su adopción en la institución. o Áreas y personal de la UTIC participantes en la evaluación. o Identificación de los proyectos, funciones, procesos, servicios, activos y recursos que conformarán el universo objeto de la evaluación. 3. Planear, conducir la evaluación y documentar en el reporte de la evaluación los resultados de la evaluación identificando los hallazgos y las oportunidades de mejoras detectadas. 4. Comunicar los resultados de la evaluación realizada.
Relación de Productos	• Plan de evaluación • Reporte de evaluación de procesos • Listas de verificación

ESGP-5: Analizar datos, proponer y seleccionar iniciativas de mejoras de procesos

Descripción	Identificar mejoras a los procesos, elaborar los planes de acción para su implementación y

	desplegar los procesos mejorados.
Factores Críticos	1. Identificar las mejoras a los procesos a ser implementadas. • Las posibles mejoras a los procesos se obtienen de diversas fuentes, incluyendo las mediciones a los procesos, lecciones aprendidas en la implementación de los procesos, propuestas y solicitudes de mejora elaboradas por los involucrados en la dirección, control y ejecución del proceso, resultados de las evaluaciones hechas a los procesos, los informes de medición y análisis de la evaluación del desempeño de los procesos, resultados de análisis comparativos contra otros procesos dentro de la institución y recomendaciones provenientes por otras iniciativas de mejora de procesos en la APF. 2. El grupo de trabajo de procesos y mejora continua de la UTIC tendrá la responsabilidad de administrar las mejoras a los procesos de la UTIC de una forma ordenada y siempre en beneficio de la dependencia o entidad mediante un proceso de control de cambios. • Las solicitudes de mejora de procesos deberán ser registradas y analizadas para determinar el impacto en la dependencia o entidad, los beneficios de su implantación, los costos y esfuerzos involucrados. 3. Priorizar y seleccionar las mejoras candidatas a ser implementadas considerando los siguientes criterios: • Costo y esfuerzo para implementar las mejoras propuestas • Beneficios tangibles e intangibles resultantes de las mejoras propuestas • Contribución de las mejoras propuestas al cumplimiento del Plan estratégico de la UTIC (PETIC) • Barreras potenciales en la implementación de las propuestas 4. De ser necesario, por tamaño y magnitud del esfuerzo, documentar las mejoras de los procesos propuestas como iniciativas/proyectos de mejora de procesos de acuerdo a las guías que se establezcan para la administración del portafolio de proyectos de TIC para su evaluación, selección y autorización de la inversión por las autoridades correspondientes (ver proceso Administración de portafolio de proyectos de TIC).
Relación de Productos	• Plan de implementación de mejoras • Resultados de las mejoras implementados • Solicitudes de mejora • Lecciones aprendidas

ESGP-6: Implementar las mejoras a los procesos

Descripción	Elaborar los planes para la implementación de las mejoras y el despliegue de los procesos mejorados.
Factores Críticos	1. Elaborar las estrategias y planes de acción detallados que permitan alcanzar las mejoras de proceso identificadas en un plan de implementación de mejora de procesos. • Establecer los equipos para implementar las acciones del proyecto de mejora.

- Desarrollar el plan del proyecto de mejora para la implementación y despliegue siguiendo las guías del proceso de administración de proyectos.
- Planear pruebas pilotos de las mejoras de proceso seleccionadas, en caso de ser necesario.
- Revisar y negociar los planes y compromisos con los involucrados relevantes y con los equipos involucrados.

2. Comunicar y revisar el plan de implementación de mejora de procesos conforme sea necesario y negociar los compromisos con los involucrados.
3. Dirigir, supervisar y controlar el trabajo de los equipos y los involucrados para monitorear el progreso y los resultados del proyecto de implementación de mejora de procesos.
4. Determinar el alcance del despliegue de las mejoras de los procesos.
   - El desplegar mejoras a los procesos involucra la determinación de los proyectos, servicios y actividades que serán afectados y de cuál manera por el despliegue de las mejoras. En esta determinación se debe considerar el estado de los proyectos, servicio, actividades con respecto a su ciclo de vida incluyendo:
     - Servicios en etapa de diseño o en su ejecución
     - Proyectos que están iniciando actividades
     - Proyectos activos que se podrían beneficiar de la implementación de los procesos actuales
     - Actividades de operación críticas en la provisión de los servicios de TIC
5. Definir las actividades para el despliegue de las mejoras de los procesos de TIC en los proyectos, servicios y actividades identificados.
   - En las actividades para el despliegue se debe considerar los siguientes aspectos:
     - Actividades de asesoría y soporte para la adaptación de los procesos, de ser necesaria, de acuerdo a las guías de adaptación e para satisfacer las necesidades propias de los proyectos y servicios
     - Mantener registros de la adaptación e implementación de los procesos
     - Asegurar que el proceso resultado de la adaptación de procesos, sea considerado en la ejecución de las auditorías de proceso
     - Desplegar los activos de los procesos dentro del alcance del despliegue, documentar cambios que se realicen y proporcionar asesoría sobre el uso de los activos de proceso
     - Con el propósito de permitir la comunicación de los cambios, entender la relación de los cambios en los activos de proceso de la dependencia o entidad y los cambios en el desempeño de los procesos y resultados.
6. Asegurar que los resultados de los proyectos de mejora de procesos satisfacen los objetivos de la mejora y entregan los beneficios esperados.
7. Recopilar las lecciones aprendidas a partir de la definición, pilotaje, implementación y despliegue de las mejoras de los procesos y hacer que las lecciones aprendidas estén disponibles a los interesados.

Relación de Productos	• Repositorio de activos de procesos • Repositorio de métricas de procesos • Repositorio de solicitudes de mejora

ESGP-7: Monitorear y medir el desempeño de los procesos establecidos

Descripción	Monitorear y medir los procesos y los productos/servicios y demostrar cumplimiento a la normatividad y a los estándares, políticas, planes y procedimientos. Esta actividad deberá cumplir con los planes y procedimientos del proceso de administración del desempeño de TI que le apliquen.
Factores Críticos	1. Monitorear y medir los productos/servicios • La UTIC deberá monitorear y medir las características de los productos/servicios resultantes de sus procesos establecidos para verificar que los requerimientos se han cumplido. Esto debe realizarse de momentos apropiados durante la realización del proceso de acuerdo a un plan acordado por todos los involucrados. Se debe conservar evidencia de la conformidad con los criterios de aceptación. Estos registros deberán indicar la persona (o personas) que autorizan la entrega del producto/servicio. 2. Monitorear y medir los procesos • La UTIC deberá aplicar métodos apropiados para monitorear sus procesos establecidos. Estos métodos deberán demostrar la habilidad de los procesos para lograr los resultados planeados, cuando no se alcanzan estos resultados se deben tomar acciones para corregir la desviación y eliminar de ser posible la causa raíz del problema mediante acciones correctivas. Para verificar que los requerimientos se han cumplido. Esto debe realizarse en los momentos apropiados durante la realización del proceso de acuerdo a un plan acordado por todos los involucrados. Se debe conservar evidencia de la conformidad con los criterios de aceptación. Estos registros deberán indicar la persona (o personas) que autorizan la entrega del producto/servicio. Seleccionar los productos de trabajo que serán evaluados, basándose en un criterio de muestras de documentos si se utilizan muestras. 3. Realizar evaluaciones (auditorías internas y de tercera parte de ser el caso) en intervalos planeados para determinar si los procesos establecidos se apegan a la normatividad vigente y a las políticas, planes y procedimientos que controlan los procesos de acuerdo a los estándares establecidos por la UTIC y determinar si su implementación es efectiva. • Estas evaluaciones deberán de ejecutarse de manera independiente para asegurar su objetividad. • La selección de los evaluadores deberá asegurar la objetividad y la imparcialidad de la evaluación. Los evaluadores no deberán evaluar su propio trabajo. Los evaluadores deberán estar debidamente calificados. o En caso de que la evaluación tenga como propósito demostrar objetivamente el cumplimiento de un estándar ante terceros (tal como CMMI, ISO 9001, ISO 20000, ISO 27001, etc) la persona física y/o moral que realice la evaluación deberá contar con las credenciales actualizadas que le acrediten como evaluador reconocido por las entidades u organizaciones que determinen los dueños de los derechos de autor del estándar en cuestión.

	• Se deberá establecer un programa de evaluaciones tomando en consideración el estado y la importancia de los procesos y las áreas a ser evaluadas, así como los resultados de evaluaciones anteriores. Los criterios para las evaluaciones, el alcance, la frecuencia y los métodos de las evaluaciones deberán estar definidas. • Se deben registrar y comunicar los resultados de las evaluaciones. • El funcionario responsable del área/ proceso evaluado deberá asegurar que se realizan las acciones para corregir las no conformidades encontradas durante las evaluaciones y que se toman las acciones correctivas para evitar que las desviaciones vuelvan a ocurrir. Se entiende por no conformidad los problemas identificados en las evaluaciones que reflejan la falta de observancia a los estándares, procesos o procedimientos. El estatus de las no conformidades provee un indicador de las tendencias de calidad. • Dar seguimiento a las no conformidades hasta su cierre y validar que las acciones correctivas tomadas son efectivas.
Relación de Productos	• Repositorio de métricas de procesos • Plan de evaluación • Listas de verificación • Reporte de evaluación de procesos • No conformidades • Informes de medición y análisis • Solicitudes de mejora

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.4.1.2.3 Descripción de roles

Rol	Descripción
Responsable de Mejora de Procesos	Coordina y administra las tareas de evaluación, definición, implementación y despliegue de las iniciativas/proyectos de mejora de los procesos de la UTIC, así como la administración de las solicitudes de mejora y lecciones aprendidas.
Responsable de Aseguramiento de Calidad	Coordina las actividades de evaluación que son ejecutadas por el grupo de aseguramiento de calidad, desarrolla la planeación de actividades y se asegura de su ejecución. Reporta a la dirección los resultados de las actividades de evaluación.
Evaluador de calidad	Responsable de realizar actividades dentro de un plan de evaluación.
Grupo de Trabajo de Mejora Continua de TIC	Responsable de planear, pilotear y desplegar el plan de mejora de procesos establecido para la dependencia o entidad. Apoya en la definición los procesos de la UTIC y asesora en la ejecución de los procesos.
Responsable del proceso	Responsable de asegurar que el proceso establecido se ejecute de acuerdo al plan de administración del proceso y que éste cumple con sus objetivos.

7.4.1.2.4 Descripción de productos

Producto	Descripción
Diagrama de arquitectura de procesos	Diagrama que muestra visualmente la arquitectura de procesos del sistema de procesos de la UTIC, muestra la jerarquía, relación e interacción entre los proceso e incluye la documentación de las características esenciales de los procesos, entre otros: • El objetivo y propósito para cada uno de los procesos. • La secuencia e interacciones de los procesos con el propósito de asegurar que existe una apropiada integración entre los procesos incluyendo: o límites (inicio y el fin del proceso), o entradas y salidas, o proveedores y usuarios (clientes), o subprocesos, o conexiones con procesos internos y externos.
Guías para la definición y control de los procesos	Guías que establecen las directrices para la documentación y definición de los procesos de la UTIC incluyendo las directrices para la elaboración del plan de administración del proceso.
Repositorio de activos de procesos	Ejemplos de activos a incluir en el repositorio son: • Políticas y normatividad de la institución. • Documentación de los procesos estándares incluyendo los planes de administración de procesos. • Materiales de capacitación. • Lecciones aprendidas. • Plantillas, listas de verificación, etc.
Plan de Administración del proceso	Plan que integra los elementos necesarios para la dirección, realización y control del proceso. El contenido típico de este plan es: • Objetivos y metas del proceso • Normatividad y estándares que le aplican • Roles y responsabilidades de los involucrados en el proceso incluyendo los roles y responsabilidades del dueño del proceso • Guías, procesos, procedimientos, instrucciones de trabajo requeridas para documenten las actividades del proceso así como las guías de adaptación y manejo de excepciones • Documentos y registro sujetos a control de cambios y versiones • La definición de los objetivos de calidad y los requerimientos para el producto

Producto	Descripción
	resultante • Las actividades de verificación, validación, monitoreo, inspección y pruebas específicos para el producto • Los criterios para la aceptación de los productos • Los registros para proveer evidencia que los procesos y los productos resultantes cumplen con los requerimientos • Métricas e informes de medición y análisis • Recursos (infraestructura y personal) necesarios para la realización del proceso incluyendo las competencias de los recursos humanos
Plan de evaluación	Documento que se genera para planear y establecer las evaluaciones y auditorías en la dependencia o entidad. Algunos puntos que deben de ser considerados en este documento son: a) Tabla de contenido b) Objetivo del documento c) Aprobación del documento d) Acrónimos y definiciones e) Objetivo de la evaluación f) Objetivo de mejora g) Alcance de la dependencia o entidad h) Alcance sobre el modelo i) Identificación de proyectos a evaluar j) Actividades k) Roles y responsabilidades: l) Patrocinador m) Grupo evaluador n) Participantes o) Restricciones de la evaluación p) Riesgos de la evaluación q) Confidencialidad de la evaluación r) Acuerdo de confidencialidad s) Entregables de la evaluación t) Actividades u) Instalaciones

Producto	Descripción
	v) Calendario detallado
Iniciativa/proyecto de mejora	Propuesta de inversión en un proyecto de mejora de procesos que se integra al portafolios de proyectos de TIC para su priorización y evaluación (ver el proceso de administración del portafolio de proyectos de TIC)
Plan de implementación de mejoras	Plan que se desarrolla para ejecutar el despliegue e implementación de procesos en la dependencia o entidad: a) Objetivo del documento b) Aprobación del documento c) Acrónimos y definiciones d) Alcance e) Situación actual f) Identificación de proyectos piloto g) Áreas de proceso a pilotear h) Estrategia general y cronograma ejecutivo • Capacitación formal: - Preparación y ejecución de talleres de despliegue • Liberación de procesos definidos • Difusión del proceso • Oficialización del proceso • Junta de inicio de la fase de despliegue • Ejecución de proyectos • Soporte y asesoría a proyectos - Soporte técnico a proyectos (primer nivel) - Soporte técnico a proyectos (segundo nivel) - Políticas para el soporte a pilotos • Mecanismos de comunicación y administración básica del cambio • Administración de cambios y mejora continua del proceso • Conducir auditorias de aseguramiento de la calidad a proyectos piloto • Revisiones periódicas i) Roles y responsabilidades j) Agenda de actividades
Resultados de las mejoras implementadas	Resultados obtenidos de la ejecución del plan de implementación de mejoras.

Producto	Descripción
Listas de verificación	Documento en el cual se establecen los criterios y puntos críticos a revisar en una auditoría, revisión o evaluación, para determinar el adecuado desempeño.
Reporte de evaluación de procesos	Proporciona un registro completo y define las conclusiones de la evaluación o auditoría. Debe incluir o hacer referencia al Plan de Evaluación en lo referente a los objetivos, alcance, equipo, fechas y criterios. También puede incluir o hacer referencia, según sea apropiado, al resumen del proceso de evaluación o auditoría, la confirmación de que se han cumplido los objetivos, las áreas no cubiertas, las opiniones divergentes sin resolver, las no conformidades encontradas, las recomendaciones para la mejora y los planes de acción del seguimiento acordados.
Lecciones aprendidas	Documento en el que se registra las lecciones aprendidas que aportan valor a para incrementar el conocimiento de la UTIC con respecto a sus procesos y activos de procesos.
Solicitud de mejora de procesos	Documento que se utiliza para hacer el registro y llevar la administración de las oportunidades de mejora a los procesos de la UTIC.
Repositorio de métricas de procesos	Repositorio utilizado para recolectar y mantener disponible para los interesados las métricas de procesos de acuerdo al Sistema de evaluación del desempeño de TIC (ver proceso Administración del desempeño de TIC).
Informes de medición y análisis	Reportes generados periódicamente de acuerdo al Sistema de evaluación de desempeño de TIC (ver proceso Administración del desempeño de TIC), para informar a los interesados el resultado de las mediciones de procesos.
Repositorio de solicitudes de mejora	Repositorio utilizado para recolectar y dar seguimiento al estado de las solicitudes de mejoras de procesos durante todo su ciclo de vida.
Modelo de ciclo de vida	Definición del proceso estándar que describe la metodología que deberá ser usada, por tipo de proyecto, para desarrollar y/o adquirir soluciones tecnológicas. Los modelos de ciclo de vida deberán estar acorde a las guías de los procesos del grupo de procesos de desarrollo y adquisición de soluciones del marco rector de procesos. Estos modelos se utilizan en el proceso Administración de proyectos de TIC para definir el ciclo de vida y el ambiente del proyecto. El modelo de ciclo de vida incluye las guías de adaptación entre las cuales se encuentran guías para: • Modificar el modelo de ciclo de vida • Modificación de elementos del proceso tales como artefactos / productos • Reordenamiento de actividades
No conformidad	Se refiere a los problemas identificados en las evaluaciones que reflejan la falta de observancia a los estándares, procesos o procedimientos.

7.4.1.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Número de Procesos de la UTIC establecidos de acuerdo al marco rector de procesos del presente manual	Conocer el número de procesos de TI establecidos en la UTIC de acuerdo al MGTIC	Notificar los números de procesos de TI que han sido establecidos de acuerdo y que son equiparables a los definidos en el marco rector de procesos de TI	Eficacia	De gestión	Número de procesos de TI instrumentados	Dirección de TIC	Trimestral
Tasa de mejoras implementadas	Evaluar eficacia de la implementación de mejoras	Medición de la eficacia en la implementación de mejoras	Calidad	De gestión	Índice de mejoras= Total mejoras implementadas / Total de mejoras recopiladas x 100	Dirección de TIC	Trimestral
Porcentaje de cumplimiento	Evaluar porcentaje de cumplimiento de procesos al marco rector	Evaluar el cumplimiento de los procesos al marco rector del presente manual.	Calidad	De gestión	Índice de cumplimiento = Procesos apegados al marco rector / Procesos establecidos por la entidad o dependencia x 100	Dirección de TIC	Trimestral

7.4.1.4 Reglas del proceso

1.1	La UTIC deberá regir su gestión de acuerdo a los procesos del marco rector de procesos de TIC.
1.2.	Los procedimientos e instrucciones de trabajo que defina la UTIC sobre cada proceso en su contexto deberán estar alineados al marco rector de procesos.
1.3	Todos los procesos establecidos deberán de contar con indicadores y métricas para poder evaluar su desempeño en forma periódica.
1.4	Todos los participantes en la ejecución de los procesos deberán de contar con las capacidades, habilidades y conocimientos para la realización de las actividades y tareas asociadas a su rol.
1.5	El responsable de cada proceso establecido en la UTIC deberá revisar y aprobar el Plan de administración del proceso correspondiente.
1.6	Se deberán realizar evaluaciones y/o auditorias documentadas a fin de verificar el cumplimiento de los procesos en operación a los planes de administración del proceso.

7.4.1.5	Documentación soporte del proceso
	No aplica

7.5 ADMINISTRACIÓN DE RECURSOS

7.5.1 Administración financiera de TIC

7.5.1.1 Objetivos del proceso

General.-

Administrar y controlar de manera eficiente los recursos financieros asignados a TIC, a fin de maximizar su contribución a los objetivos de la planeación estratégica.

Específicos.-

1. Identificar y consolidar los requerimientos financieros de proyectos y servicios de TIC en los portafolios correspondientes.
2. Solicitar a la unidad administrativa encargada de los recursos financieros, recursos materiales y servicios generales los recursos financieros necesarios para la ejecución del portafolio proyectos y servicios de TIC.
3. Organizar los portafolios de proyectos y servicios de TIC a fin de mejorar su rentabilidad considerando minimizar los costos, maximizar los beneficios y utilizar las estrategias adecuadas.
4. Facilitar la toma de decisiones de inversión de TIC al grupo de trabajo para la dirección de TIC y al titular de la UTIC mediante la priorización de proyectos que optimicen costos y maximicen beneficios.
5. Elaborar y mantener actualizado el presupuesto de TIC en el repositorio de iniciativas de TIC para cada rubro de gasto e inversión, considerando las presiones de gasto.
6. Establecer indicadores y monitorear los resultados del gasto en TIC y su correlación con los beneficios.
7. Ejecutar acciones correctivas cuando los costos se desvían de los presupuestos asignados y/o preventivas cuando las tendencias presenten oportunidades de mejora.
8. Asegurarse la existencia de un presupuesto suficiente para los servicios complementarios a las TIC.

7.5.1.2 Descripción del proceso

7.5.1.2.1 Mapa general del proceso

Diagrama de flujo de información

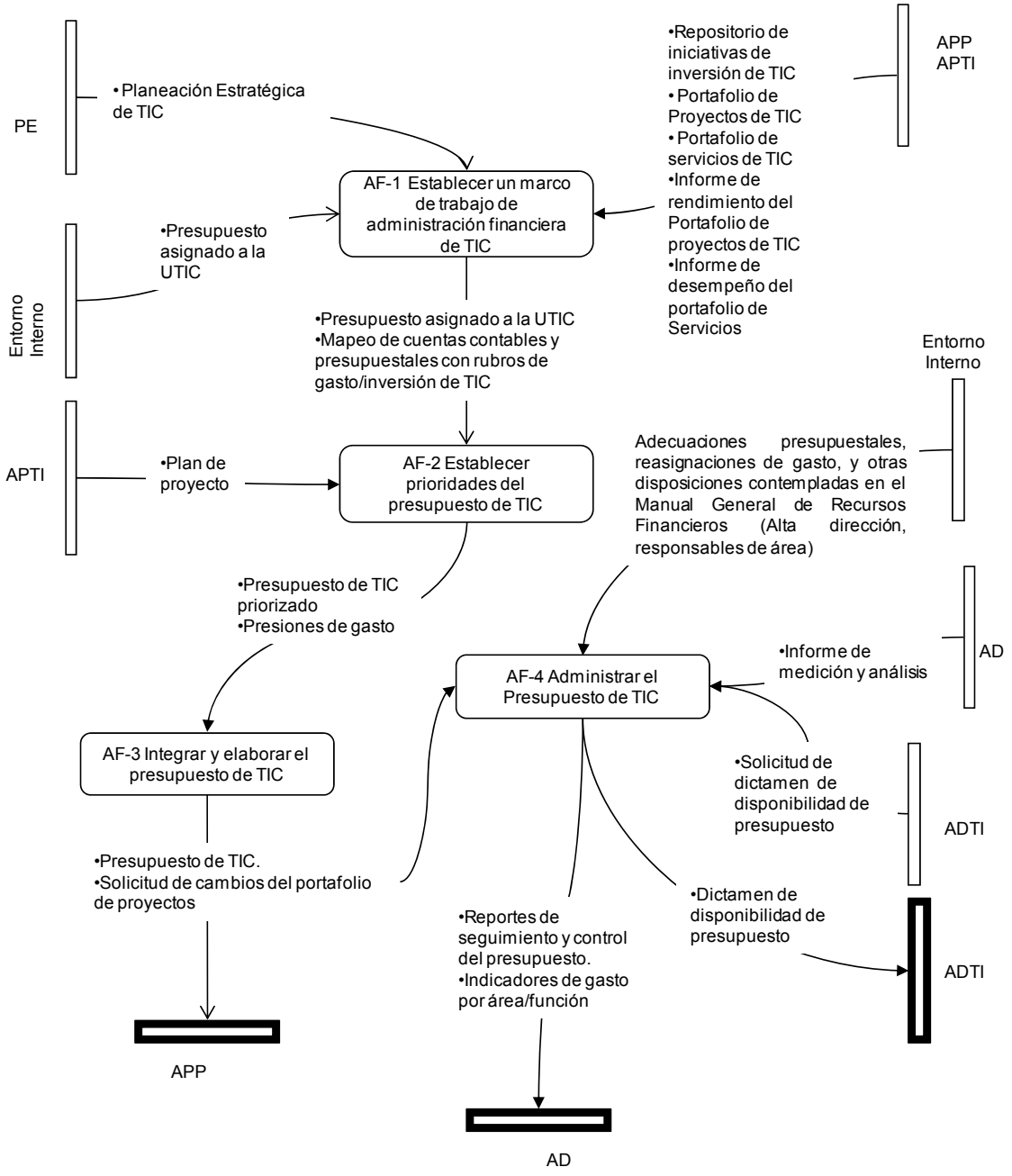
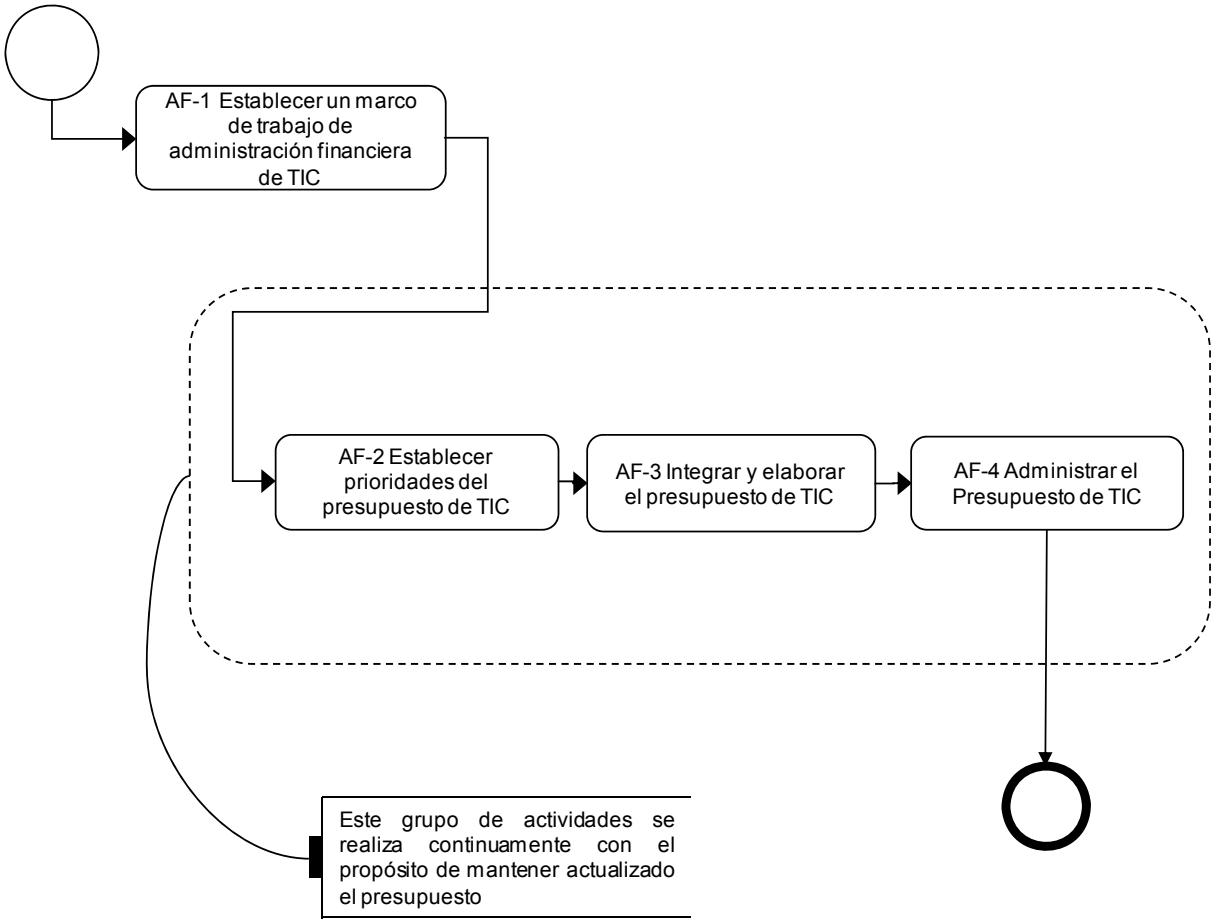


Diagrama de flujo de actividades



7.5.1.2.2 Descripción de las actividades del proceso

AF-1 Establecer un marco de trabajo de administración financiera de TIC

Descripción	Establecer y mantener un marco de trabajo para la administración financiera de TIC a través del portafolio de inversiones de TIC integrado por las inversiones y el costo de los activos y servicios de TI organizados y estructurados en los portafolios de proyectos de TIC y portafolio de servicios de TIC.
Factores Críticos	1. Mantener la comunicación efectiva con las áreas que desempeñen las funciones relativas a la administración financiera y de recursos materiales y servicios generales de la dependencia o entidad, para obtener, dar seguimiento y administrar el presupuesto asignado a la UTIC. 2. Solicitar a la unidad administrativa encargada de los Recursos financieros, recursos materiales y servicios generales el presupuesto necesario para la ejecución del portafolio de inversión de TIC. 3. Asegurar que se realicen las siguientes funciones para la administración financiera de los recursos de TIC considerando al Manual de Recursos Financieros. • Administrar el presupuesto y los costos de TIC. • Administrar los beneficios de las inversiones de TIC. • En base a los portafolios de proyectos y servicios de TIC, establecer estimaciones transparentes y comparables de los costos y beneficios de TIC. • Mantener actualizados costos de los activos de TIC y los portafolios de proyectos y de servicios de TIC, así como asegurar que el costo de su mantenimiento esté adecuadamente reflejado en los presupuestos y planes de inversión. 4. Realizar el mapeo de cuentas contables y presupuestales del portafolio de inversión de TIC, el inventario de servicios y activos de TIC que conforman las bases para establecer el presupuesto de TIC y dar cumplimiento a la planeación estratégica de TIC definida en el grupo de procesos de Dirección. 5. Actualizar y realizar los ajustes periódicos al plan de inversión de TIC para su adecuada y oportuna administración financiera. 6. Informar a los Administradores de los portafolios de proyectos y de servicios de TIC si se cuenta con recursos para evaluar nuevas inversiones de TIC considerando todo el ciclo de vida que les corresponda. 7. Mantener registros del presupuesto de TIC incluyendo gastos comprometidos, fechas de pago, gastos a la fecha que abarquen nuevos proyectos, operación y mantenimiento a los activos, portafolio de proyectos de TIC y portafolio de servicios de TIC. 8. Proveer de información financiera, costos y beneficios para el análisis de los casos de negocio de iniciativas de TIC en colaboración con las áreas que tengan bajo su responsabilidad su elaboración. 9. Comunicar la información financiera, los costos, beneficios, riesgos e información relevante para la priorización del presupuesto y administración de costos de TIC a los grupos de procesos de Gobierno y de organización estratégica para que sean

	contemplados en la planeación, administración y toma de decisiones.
Relación de Productos	• Presupuesto asignado a la UTIC • Mapeo de cuentas contables y presupuestales con rubros de gasto/inversión de TIC

AF-2 Establecer prioridades del presupuesto de TIC

Descripción	Abarca el proceso de toma de decisiones con el objetivo de definir las prioridades en la asignación de recursos a TIC para operaciones, proyectos y mantenimiento, a fin de maximizar su contribución para optimizar el retorno de inversión del portafolio de proyectos, servicios y activos de TIC. Durante el análisis es necesario identificar e informar las posibles presiones de gasto (insuficiencias presupuestales a gastos recurrentes o comprometidos, y de soporte a aquellas iniciativas que no contasen con suficiencia presupuestal para su ejecución).
Factores Críticos	1. Identificar todos los requerimientos de TIC que demanden asignación presupuestal correspondientes al portafolio de proyectos de TIC, portafolio de servicios de TIC, y servicios complementarios a las TIC (mantenimiento a instalaciones, aire acondicionado, energía eléctrica, energía sin interrupción, extinción de incendios, control de acceso, en su caso suministros o insumos requeridos, etcétera). 2. Asignar prioridades a los requerimientos e iniciativas de TIC dentro del portafolio de proyectos de TIC y de servicios TIC basándose en los casos de negocio, criterios de evaluación de cada uno y en la planeación estratégica de TIC de la UTIC y de la dependencia o entidad. 3. Crear propuesta para la asignación del presupuesto al portafolio de proyectos de TIC, portafolio de servicios de TIC y servicios complementarios de TIC incluyendo el presupuesto requerido para operación, mantenimiento y nuevas tecnologías, así como las presiones de gasto y solicitudes emergentes con posibles insuficiencias presupuestales. 4. Establecer escenarios de asignaciones presupuestales, indicando claramente los gastos indispensables para garantizar la continuidad de la operación, los riesgos operativos y las correspondientes a iniciativas derivadas de la planeación estratégica para revisión con los involucrados. 5. Presentar al Titular de la UTIC y al grupo de trabajo para la dirección de TIC la propuesta de inversiones de TIC para su aprobación. 6. Identificar, comunicar y resolver los impactos significativos de las decisiones tomadas sobre la asignación presupuestal. 7. Obtener la confirmación y aprobación del grupo de trabajo para la dirección de TIC sobre las prioridades del presupuesto y sobre los cambios que puedan afectar o impactar el cumplimiento de los objetivos de la planeación estratégica de TIC y de cada uno de los portafolios: Portafolio de proyectos de TIC y Portafolio de servicios de TIC.
Relación de Productos	• Presupuesto de TIC priorizado • Presiones de gasto

AF-3 Integrar y elaborar el presupuesto de TIC

Descripción	Con base en las prioridades establecidas en el portafolio de inversión en TIC, producto del proceso de planeación estratégica, elaborar y mantener actualizado el portafolio de inversión de TIC que contiene el presupuesto para cada rubro de gasto e inversión, considerando el presupuesto global asignado a TIC, e incluyendo los costos recurrentes de operar y mantener la infraestructura actual. Se debe contemplar el presupuesto general de TIC, así como el desarrollo de presupuestos para los diferentes portafolios de proyectos y servicios de TIC. En este proceso se incluye la toma de decisiones con el objetivo de asignar los recursos presupuestales de TIC de acuerdo a las prioridades acordadas institucionalmente para operaciones, proyectos y mantenimiento, a fin de maximizar la contribución de TIC para optimizar el retorno de inversión de los portafolios de proyectos, y servicios de TIC.
Factores Críticos	1. Seguir un mecanismo formal para establecer, cambiar y aprobar un presupuesto de TIC, incluyendo los costos de los portafolios de proyectos y servicios de TIC. 2. El portafolio de inversión de TIC deberá considerar al menos los siguientes componentes: • Los mecanismos autorizados de financiamiento • Los costos de recursos internos, incluyendo el personal, activos de información y físicos • Costos de servicios de terceros • Costos de servicios complementarios e insumos requeridos • Apego a la normatividad vigente en materia de Adquisiciones, Arrendamientos y Servicios, Administración Financiera, así como de los Manuales generales de recursos materiales y finanzas • Identificar los gastos fijos asociados a la operación y mantenimiento tanto recurrentes y plurianuales, y sus tendencias: los requeridos por única vez (equipos, infraestructura, sistemas, desarrollo y licenciamiento), servicios básicos prioritarios (seguridad, monitoreo y control, hospedaje, entre otros), y servicios complementarios (suministro eléctrico, extinción de incendios, control de acceso, mantenimiento de instalaciones, etc.), para con ellos estimar el costo operativo básico anual de TIC 3. Documentar el racionamiento y las presiones de gasto para justificar posibles contingencias y revisarlas constantemente. 4. Monitorear la efectividad de la administración del presupuesto considerando (asignaciones de costos a proyectos, asignaciones de costos a servicios y el análisis de la variación de costos y presupuestos). 5. Instruir a los responsables de los portafolios de proyectos y servicios de TIC realizar la planeación del presupuesto. 6. Revisar los planes de presupuesto, tomar las decisiones necesarias acerca de la asignación, compilación y comunicación del presupuesto a los responsables involucrados.
Relación de Productos	• Presupuesto de TIC • Solicitud de cambios del portafolio de proyectos

AF-4 Administrar el presupuesto de TIC

Descripción	Dar seguimiento, monitorear y controlar los costos reales contra los presupuestados. Los costos se deben monitorear y reportar de manera periódica y de acuerdo a la periodicidad requerida por cada dependencia y/o entidad y en correspondencia a los tiempos que determine la normatividad vigente en la materia a fin de tener oportunidad de establecer medidas preventivas, correctivas y de mejora.
Factores Críticos	1. Dar seguimiento a los costos y presupuesto de TIC asignado al portafolio de inversión de TIC, en los respectivos portafolios de proyectos y servicios de TIC y aquéllos, que corresponden a otros rubros, para que su registro, análisis, control y seguimiento. • Se deberá establecer los elementos de costo de los proyectos que serán asignados a la unidad responsable de las TIC, y aquellos que correspondan a las áreas usuarias que reciben los servicios de TIC. • Establecer los esquemas de reporte de los costos incluyendo indicadores, periodicidad, los responsables de reportar la información y a quien se deberá reportar la información. • Dar seguimiento a la ejecución del programa anual de adquisiciones, arrendamientos y servicios de TIC de la UTIC para actualizar su estatus el portafolio de inversión de TIC. 2. Recopilar información relevante para identificar desviaciones con respecto al presupuesto tales como: • Control del gasto: diferencias entre lo presupuestado y lo ejercido. • Administración de los beneficios del uso del presupuesto. • Avance actual del presupuesto con respecto a las metas de inversión expresadas en términos análisis de indicadores tales como análisis del retorno de inversión, análisis de valor presente y/o análisis de la tasa de retorno (ROI, VPN, IRR). • Las tendencias de los costos de servicio para optimización de servicios. • Tendencias del costo de portafolio de servicios para mejora de la productividad. • Distribución de costos directos e indirectos. 3. Recopilar la información relativa a los costos y presupuesto mediante los mecanismos y sistemas apropiados. 4. Consolidar los costos a niveles apropiados de control para identificar desviaciones de manera oportuna para tomar acciones correctivas. 5. Instruir y habilitar a los responsables para el registro, captura y consolidación de la información de costos y presentar los reportes a los mandos medios y superiores. 6. Analizar las desviaciones y comparar el desempeño mediante comparativos internos y de la industria a fin de sugerir acciones correctivas. • Control del presupuesto entre lo actual y lo estimado. Asegurar que los mandos medios y superiores participan y revisan los resultados del análisis de los resultados de la administración del presupuesto y establecer acciones correctivas, preventivas o de mejora. 7. En caso de que existan desviaciones, éstas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre el plan de inversión de TIC y los portafolios de proyectos y servicios de TIC. Se deberán evaluar para que junto con los involucrados se

	tomen las medidas correctivas, preventivas y de mejora. 8. En caso de ser necesario, el caso de negocio del programa de inversión deberá ser actualizado conforme a las adecuaciones presupuestales, reasignaciones de gasto, y otras disposiciones contempladas en el Manual Administrativo de Aplicación General en Materia de Recursos Financieros así como a leyes y reglamentes que apliquen.
Relación de Productos	• Reportes de seguimiento y control del presupuesto • Indicadores de gasto por área / función

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.5.1.2.3 Descripción de roles

Rol	Descripción
Grupo de trabajo para la dirección de TIC	Responsable de tomar las decisiones de alto nivel con respecto a la priorización de los recursos y asignación del presupuesto a iniciativas de inversión de TIC.
Responsables de área	Participan en el establecimiento del presupuesto estimado para los programas, proyectos y servicios de TIC. Responsable de documentar los casos de negocio para justificar los beneficios de la inversión de TIC en programas, proyectos o servicios específicos. Responsables de establecer el presupuesto estimado para la operación y mantenimiento de la infraestructura de TIC. Responsables de dar seguimiento a los costos y presupuesto estimado durante la ejecución de los programas, proyectos y servicios de TIC.
Administrador del presupuesto	Responsable de realizar las actividades administrativas para establecer el presupuesto asignado y el calendario de gasto de TIC, así como monitorear el ejercicio y reportar la información asociada al presupuesto y las desviaciones en el mismo.

7.5.1.2.4 Descripción de productos

Producto	Descripción
Procedimientos de administración financiera de TIC	Procedimientos que formalizan las reglas internas para: • Manejar el presupuesto y los costos de TIC • Mapeo de cuentas contables y presupuestales con rubros de gasto/inversión de TIC • Administrar los beneficios de las inversiones de TI • Establecer estimaciones transparentes y comparables de los costos y beneficios de TIC • Establecer los presupuestos, planes y calendario de gasto e inversión
Presupuesto de TIC priorizado	Lista de iniciativas de inversión de TIC presupuestadas y calificadas con nivel de prioridad

Producto	Descripción
	para el uso de los recursos financieros disponibles en la dependencia o entidad. Esta lista deberá contener un estimado preliminar a alto nivel que permita establecer el corte en base a las prioridades de la dependencia o entidad para las cuales habrá recursos, una vez que se defina el presupuesto y calendario de gasto e inversión definitivo asignado a la dependencia o entidad.
Presupuesto de TIC	Documento que formaliza las iniciativas de inversión de TIC que serán realizados por la dependencia o entidad y el presupuesto asignado calendarizado para ser ejercido para cada uno de ellos.
Reportes de seguimiento y control del presupuesto TIC	Reportes periódicos que informan sobre el uso de los recursos financieros en comparación con el presupuesto establecido, indicando el flujo de efectivo de los compromisos establecidos ejercidos y/o por devengar. Igualmente deberá señalar las desviaciones con respecto a las estimaciones de costo y programación del presupuesto. Estos reportes deberán contener información de seguimiento a las acciones correctivas establecidas para controlar y administrar el presupuesto.
Caso de negocio	Documento que contiene la justificación de los objetivos de las iniciativas de inversión de TIC, así como la descripción de su contribución al negocio, en su caso establece la información sobre el costo beneficio, el análisis de retorno de inversión y/o análisis que sustente los beneficios de la inversión.
Reporte de costo / beneficio	Informe que contiene los criterios de evaluación de alternativas así como el análisis en términos de costo / beneficio.
Mapeo de cuentas contables y presupuestales con rubros de gasto/inversión de TIC	Documento que constituye la guía de rubros de gasto en materia de TIC, y de aquellos gastos en bienes, servicios e insumos complementarios a las TIC que resultan indispensables.
Presiones de gasto	Documento que señala las insuficiencias presupuestales y sus impactos en la operación, seguridad y apoyo a programas sustantivos, este deberá presentarse a los mandos medios y superiores y en su oportunidad al grupo de trabajo para la dirección de TIC, para efectos de que reconsidere la asignación presupuestal o en su caso modifique los alcances de los proyectos en el portafolio de proyectos de TIC.
Indicadores de gasto por proyecto/área/función	Establecimiento de un mecanismo de seguimiento y emisión de reportes donde se señale la asignación y avance del gasto corriente y de inversión para cada proyecto, área o función, su comparación y las desviaciones que pudieran presentarse contra los estimados, para la toma de decisiones.
Solicitud de cambios del portafolio de proyectos	Solicitud de cambio al presupuesto asignado a un proyecto del portafolio de proyectos de TIC.

7.5.1.3 Indicadores

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de presupuesto ejercido real del programa de adquisiciones y servicios de TIC	Evaluar el porcentaje ejercido del presupuesto conforme a lo programado	Porcentaje de presupuesto ejercido real del programa de adquisiciones y servicios de TIC, conforme a lo programado	Eficacia	De gestión	Porcentaje presupuesto ejercido real del programa de adquisiciones y servicios de TIC = (presupuesto comprometido + Presupuesto pagado / total del presupuesto asignado) * 100	Titular de la UTIC	Conforme al calendario del programa de adquisiciones y servicios de TIC
Presupuesto sub ejercido	Identificar el presupuesto sub ejercido	Presupuesto sub ejercido a la fecha en que se evalúa el indicador	Eficacia	De gestión	Presupuesto sub ejercido = Presupuesto programado al período de evaluación – presupuesto ejercido al período de evaluación	Titular de la UTIC	Conforme al calendario del programa de adquisiciones y servicios de TIC

7.5.1.4 Reglas del proceso

1.1	Se deberá realizar la administración financiera de TIC que tome como base el Portafolio de proyectos establecido mediante las actividades de planeación estratégica de la dependencia o entidad de TIC.
1.2	La UTIC deberá administrar el presupuesto asignado a las TIC en la dependencia o entidad. Asimismo, integrará la distribución presupuestal de la dependencia o entidad en lo correspondiente a TIC con base en los recursos que se establezcan en el Presupuesto de Egresos de la Federación para el año correspondiente, y coordinará la planeación del presupuesto en materia de TIC de la dependencia o entidad conforme al portafolio de proyectos de TIC, con la finalidad de definir sus necesidades de inversión en materia de TIC de corto, mediano y largo plazo.
1.3	Para cada programa de inversión en TIC se deberá contar un caso de negocio a fin de justificar la contribución de valor al negocio y el costo beneficio. El área correspondiente deberá de informar a la UTIC la asignación de presupuesto en los rubros relacionados con Tecnologías de Información y Comunicaciones.
1.4	Se deberá establecer las prioridades en el uso del presupuesto conforme al lo especificado en el Proceso de administración de portafolio de proyectos de TIC.

1.5	Anualmente se deberá analizar la manera más efectiva y eficiente de asignar el presupuesto al portafolio y/o proyectos de TIC tomando en cuenta la ponderación y prioridades definidas para maximizar la contribución de valor, consolidando los criterios y aprobaciones integrales: de las áreas usuarias de negocio (sustantivas y adjetivas), áreas técnicas normativas en materia de TIC, y áreas financiero presupuestales.
1.6	Se deberá formalizar y documentar el presupuesto establecido de TIC y difundirlo a todos los participantes relevantes tales como responsables área, líderes y responsables de áreas operativas y/o de servicio.
1.7	Se deberán documentar los riesgos asociados en la asignación del presupuesto.
1.8	Cualquier cambio en la asignación de presupuesto deberá ser evaluado y analizado en términos de su impacto en la contribución de valor establecida en su caso de negocio.
1.9	Se deberá recopilar y presentar información de manera periódica para medir el desempeño del uso del presupuesto y el monitoreo de los costos incurridos.
1.10	Periódicamente se deberán evaluar los costos a fin de establecer un análisis interno y/o de comparación de mejores prácticas externas a fin de procurar hacer más efectivo el uso de los recursos financieros.
1.11	Se deberá monitorear y controlar los costos en comparación con el presupuesto establecido y en caso de desviación tomar las acciones correctivas de manera oportuna.
1.12	El proceso de administración de inversiones de TIC será mejorado continuamente con base en las lecciones aprendidas provenientes del análisis del desempeño real de las inversiones.
1.13	Las decisiones de inversiones deberán considerar las tendencias de mejora de precio/desempeño.
1.14	Se investigarán y evaluarán formalmente las alternativas de financiamiento dentro del contexto de la estructura de capital existente en la institución, mediante el uso de métodos formales de evaluación.
1.15	Se deberá informar y someter a los responsables de la asignación presupuestal global de las posibles presiones de gasto (insuficiencias presupuestales a gastos recurrentes o comprometidos) y de soporte a aquellos proyectos estratégicos que no cuenten con suficiencia presupuestal para su ejecución.
1.16	Se deberá asegurar que los presupuestos relativos a bienes y servicios complementarios sean suficientes para mantener la operación y los programas de expansión. La UTIC deberá solicitar al área correspondiente la integración de recursos presupuestales en materia de TIC en el anteproyecto de presupuesto que se presenta a la Secretaría de Hacienda y Crédito Público.
1.17	Las presiones de gasto se deberán identificar y someter al grupo de trabajo para la dirección de TIC, indicando los riesgos en la operación y afectación en programas prioritarios, tácticos y estratégicos.
1.18	En el caso de presupuestos para sistemas y tecnologías especializados, así como para actividades específicas no estandarizadas en la industria de cómputo y comunicaciones (por ejemplo: equipamiento biomédico, de laboratorio, de investigación y desarrollo, de control y potencia, radio-enlaces, etc.), deberán establecerse claramente los criterios de excepción al cumplimiento de normas y reglas generales aplicables a las TIC, pero siempre estableciendo las normas aplicables al caso y definiendo los responsables de establecer estándares y criterios técnico-económicos que garanticen la optimización del uso de recursos financieros en beneficio de la institución.
1.19	Sin perjuicio de lo establecido en este manual, las dependencias y entidades deberán observar, en lo conducente, las disposiciones emanadas del manual general de recursos financieros.

7.5.1.5	Documentación soporte del proceso
	No aplica

7.5.2. Administración de proveedores

7.5.2.1 Objetivos del proceso

General.-

Establecer los mecanismos de comunicación con los proveedores necesarios para asegurar el adecuado cumplimiento de los compromisos contractuales.

Específicos.-

1. Definir los canales de comunicación con los proveedores.
2. Establecer mecanismos de revisión preventiva para evitar retrasos en la ejecución del programa de adquisiciones y de corrección para asegurar la calidad del producto o servicio.

7.5.2.2 Descripción del proceso

7.5.2.2.1 Mapa general del proceso

Diagrama de flujo de información

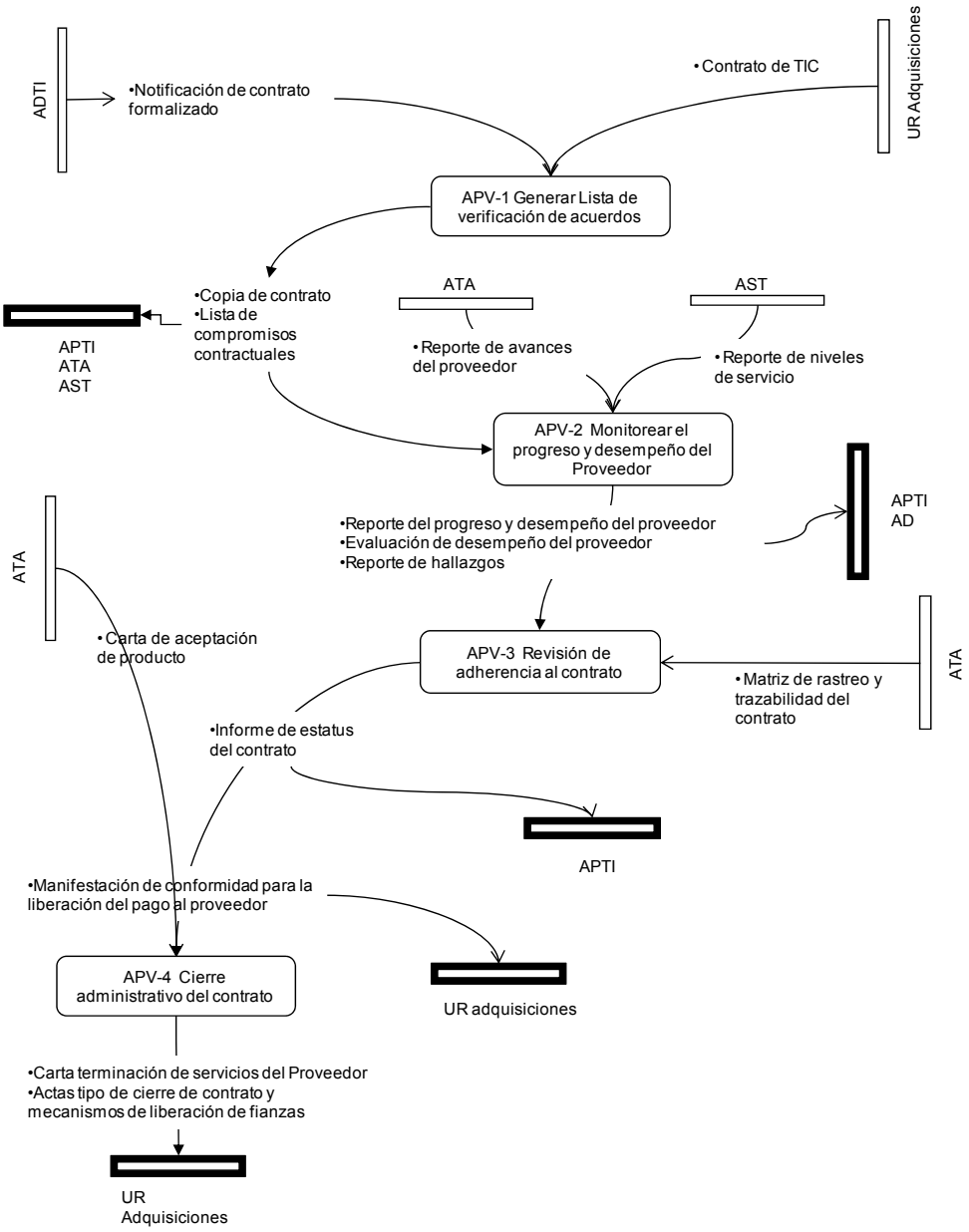
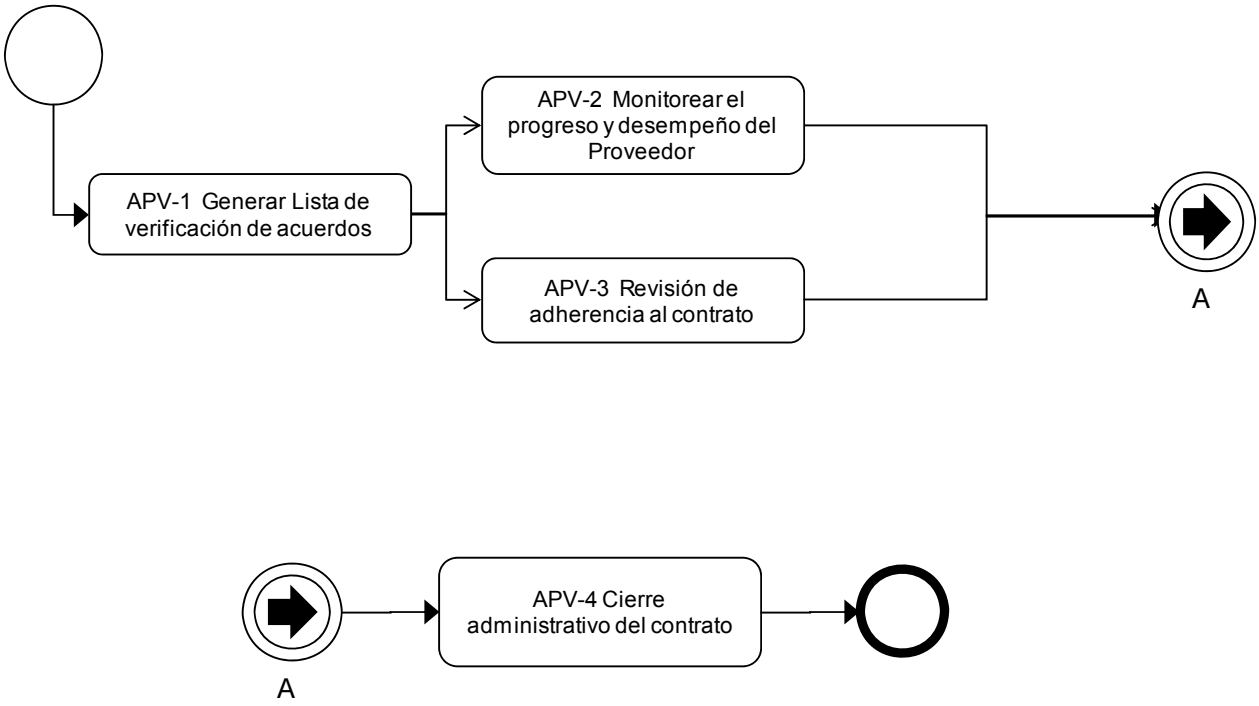


Diagrama de flujo de actividades



7.5.2.2.2 Descripción de las actividades del proceso

APV-1 Generar lista de verificación de acuerdos

Descripción	Con base al contrato establecido, se elabora una lista de verificación para dar seguimiento al desarrollo del contrato.
Factores Críticos	1. Verificar que el contrato que contenga a detalle los términos y condiciones que normarán la adquisición. Así como el detalle de los requerimientos contractuales especificados por el Solicitante. 2. Asegurar que los involucrados con el desarrollo y seguimiento del contrato dispongan de una copia del contrato firmado y un resumen de las obligaciones establecidas y firmadas por los participantes. 3. Identificar los compromisos y responsabilidades contractuales que permitan darle seguimiento y monitorear la ejecución del contrato. 4. Identificar a los responsables como supervisor(es) y administrador(es) del contrato por parte del Proveedor y Solicitante. 5. Identificar los escenarios o condiciones, sobre las cuales se estarían aplicando penalizaciones al (los) Proveedores. 6. Documentar los entregables, compromisos y responsabilidades contractuales. 7. En los casos en los que se presenten múltiples proveedores en el desarrollo de la solución, es necesario definir que requerimientos serán cubiertos por cada tipo de proveedor y sus características particulares.
Relación de Productos	• Copia de contrato TIC • Lista de verificación de compromisos contractuales

APV-2 Monitorear el progreso y desempeño del proveedor

Descripción	Verificar que las actividades del Proveedor son desempeñadas como fue especificado en el contrato.
Factores Críticos	1. Validar que se cuenta con la carta de confidencialidad 2. Revisar y analizar la información del Proveedor que le proporcionen los involucrados en el desarrollo del contrato. 3. Revisar con los responsables de los proyectos, los reportes del progreso y desempeño del Proveedor. 4. Revisar el desempeño de los servicios y/o soluciones tecnológicas. a) Evaluar el desempeño real contra el desempeño esperado. b) Realizar análisis causal, para identificar las raíces de las desviaciones. c) Establecer planes de acciones preventivas y/o correctivas que permitan que el desempeño de los servicios y soluciones tecnológicas de los objetivos establecidos. 5. Verificar la aplicación de penalizaciones. 6. Identificar y registrar riesgos y problemas 7. Establecer las acciones preventivas / correctivas pertinentes y monitorearlas hasta su

	cierre. 8. Evaluar el desempeño general del Proveedor o Desarrollar encuestas para evaluar al Proveedor. o Aplicar encuestas de evaluación. o Revisar con el Proveedor el resultado de la evaluación. o Usar los resultados de las revisiones para mejorar el desempeño de los Proveedores. 9. Integrar información y preparar informe. 10. Contar con la documentación soporte que avale la experiencia y habilidades del proveedor para cumplir con lo especificado en el contrato. 11. Revisar periódicamente los resultados con los mandos superiores.
Relación de Productos	• Reporte de hallazgos • Reporte del progreso y desempeño del proveedor • Evaluación de desempeño del proveedor

APV-3 Revisión de adherencia al contrato TIC

Descripción	Evaluar que las actividades desarrolladas se realicen con apego en lo estipulado en el contrato, con la finalidad de detectar riesgos, oportunidades, problemas, tan temprano como sea posible, que puedan afectar el cumplimiento contractual, ya sea por parte del Proveedor o del Solicitante.
Factores Críticos	1. En puntos de control seleccionados, conducir revisiones de cumplimiento de los acuerdos contractuales. a) Asegurar que los involucrados clave, estén en la revisión. b) Utilizar la información del contrato como base para la revisión. c) Analizar los posibles incumplimientos y determinar si aplican deducciones, penalizaciones, o incluso la rescisión del contrato. 2. Informar los resultados de la revisión, a las partes involucradas, incluyendo al Proveedor, para establecer acciones correctivas o preventivas. a) Dar seguimiento a las acciones hasta su cierre. 3. Escalar los asuntos no resueltos al nivel de autoridad adecuado, de tal manera que se garantice la resolución.
Relación de Productos	• Informe de estatus del contrato

APV-4 Cierre administrativo del contrato

Descripción	Asegurar que efectivamente el proveedor ya cumplió con la totalidad de sus compromisos y se procede a que el contrato se declare terminado.
Factores Críticos	1. Verificar que el servicio y/o soluciones tecnológicas se han entregado conforme lo

	especificado y de conformidad con el contrato. 2. Validar que todas las inconformidades, defectos y/o desviaciones han sido cerrados. 3. Asegurar que no exista alguna deducción y/o penalización por aplicar. 4. Confirmar que todos los accesos y/o cuentas proporcionados al proveedor han sido dados de baja. 5. Se valida lo correspondiente a las garantías. 6. Se elabora y aprueba la carta de terminación de los servicios y/o soluciones tecnológicas por parte del proveedor.
Relación de Productos	• Carta terminación de servicios del Proveedor • Actas tipo de cierre de contrato y mecanismos de liberación de fianzas

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.5.2.2.3 Descripción de roles

Rol	Descripción
Administrador del contrato	Realiza la administración exclusiva de los compromisos de un contrato que pueda estar relacionado a servicios suministrados por uno o más proveedores.
Administrador del proveedor	Monitorea el avance así como el rendimiento del proveedor con base a los acuerdos establecidos. Identificando los riesgos e incidencias que sean consiguientes de la revisión del avance, permitiendo establecer líneas de acción para su resolución.
Área jurídica	Instancia que brinda soporte en los aspectos legales del contrato.
Área de adquisiciones	Responsables de integrar el programa de adquisiciones, de ejecutar y vigilar el procedimiento de licitación correspondiente y asegurarse que se elabore el contrato.

7.5.2.2.4 Descripción de productos

Producto	Descripción
Carta terminación de servicios del proveedor	Instrumento para formaliza el cierre del contrato y el cual está basado en lo establecido por los Manuales de Generales de Recursos Financieros. Los siguientes puntos deben de estar considerados en el detalle del contenido del documento: a) Nombre del responsable de la aprobación b) Fecha c) Características de la solución tecnológica y/o servicio adquirido d) Referencias a las descripciones de las garantías y condiciones de su aplicación
Evaluación de	Reporte que indica el concentrado de las evaluaciones al desempeño del proveedor

Producto	Descripción
desempeño del proveedor	realizadas por los involucrados en el desarrollo de las actividades del proveedor. Los siguientes puntos deben de estar considerados en el detalle del contenido del documento: a) Muestra el nivel de satisfacción, al menos en las siguientes dimensiones o Comercial o Calidad o Capacidad técnica
Manifestación de conformidad para la liberación del pago al proveedor	Escrito que avala la aprobación del pago a un proveedor por un servicio y/o solución tecnológica proporcionado.
Informe de estatus del contrato	Describe, el grado de apego al contrato que se está manteniendo tanto por parte del Proveedor así como del Solicitante. Los siguientes puntos deben de estar considerados en el detalle del contenido del documento: a) Muestra las desviaciones críticas, y la manera en que se están o deberían de solventar b) Indica riesgos potenciales, así como las acciones para su mitigación c) Señala las recomendaciones, y en su caso dictamen, por parte del departamento Jurídico d) Establece incidencias, penalizaciones y deducciones con los términos establecidos en el contrato para su aplicación
Lista de verificación de compromisos contractuales	Identifica los compromisos contractuales de los que se conforma el contrato, este documento ayuda para el monitoreo y ejecución de las actividades del Proveedor. Los siguientes puntos deben de estar considerados en el detalle del contenido del documento: a) Indica nombre del Administrador del contrato b) Indica nombre(s) y el (os) Administrador(es) y el (los) proyecto (s) c) Indica número de contrato d) Indica el nombre del proveedor e) Indica la fecha de formalización y la de término del contrato f) Señala el compromiso contractual así como quién es responsable de su desarrollo g) Describe las condiciones sobre las cuales se tienen que aplicar penas o deducciones
Notificación de contrato formalizado	La notificación se realiza según el medio definido por la dependencia o entidad. Algunos ejemplos son: oficio, nota informativa o algún otro medio de comunicación formal. Los siguientes puntos deben de estar considerados en el detalle del contenido del documento: a) Descripción detallada del asunto b) Indicación de acciones a tomar
Reporte de hallazgos	Contiene el registro de las desviaciones y/o defectos encontrados durante las evaluaciones de capacidades efectuadas al Proveedor. Los siguientes puntos deben de estar

Producto	Descripción
	considerados en el detalle del contenido del documento: a) Indica los hallazgos de forma univoca b) Clasifica el hallazgo con base a su criticidad c) Muestra el estatus del hallazgo d) Señala las acciones para la resolución del hallazgo así como el responsable de su ejecución
Reporte del progreso y desempeño del proveedor	Documento ejecutivo que muestra el resumen del progreso así como el desempeño del Proveedor en un periodo determinado. Los siguientes puntos deben de estar considerados en el detalle del contenido del documento: a) Señala los principales logros alcanzado en el periodo b) Muestra el desempeño en término de los niveles de servicio c) Indica las penalizaciones y/o deducciones, aplicadas y/o por aplicar d) Indica los principales riesgos y problemáticas
Reporte del progreso y desempeño del proveedor	Documento ejecutivo que muestra el resumen de los resultados de la evacuación efectuada a las capacidades del proveedor.
Compromisos contractuales	Relación de acuerdos generados en el contrato en términos de obligaciones, restricciones, tiempos, entre otros; con el proveedor del servicio o solución tecnológica.

7.5.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de cumplimiento del proveedor	Medir el porcentaje de cumplimiento del proveedor conforme al contrato	Porcentaje de entregables cumplidos en tiempo con respecto a los entregables y tiempos definidos en el contrato.	Eficacia	De gestión	Porcentaje de cumplimiento del proveedor=(Número de entregables cumplidos/ Número de Entregables totales del contrato)*100	UTIC	Conforme al plan de trabajo y calendario de entregables
Grado de satisfacción de los entregables del proveedor	Medir la calidad de los bienes y servicios respecto a las especificaciones de	Nivel de satisfacción de los productos entregables por parte de los proveedores	Eficacia	De gestión	Σ (Número de requisitos cumplidos con calidad por producto / Número de requisitos por entregable x 100)	UTIC	Conforme al plan de trabajo y calendario de entregables

	entregables esperados				/ Total de número de entregables		

7.5.2.4 Reglas del proceso

1.1	La dependencia o entidad deberá de establecer e implementar actividades de administración de contratos, para asegurar que se cumple con todos los aspectos establecidos en los mismos.
1.2	Ninguna prestación de servicio o recepción de producto se podrá hacer sin el debido contrato que lo avale.
1.3	Todos los involucrados deberán de conocer y tener acceso al contrato.
1.4	Se deberá establecer un responsable único, que verifique el cumplimiento contractual. Se monitoreará el cumplimiento de las condiciones operativas, legales y de control, para implementar acciones correctivas.
1.5	El proveedor estará sujeto a revisiones periódicas independientes y se le retroalimentará sobre su desempeño para mejorar la prestación del servicio; se deberá asegurar que en el contrato queden establecidos los términos para poder efectuar dichas revisiones.
1.6	Las mediciones ayudarán a la detección temprana de problemas potenciales con los servicios que presten los proveedores.
1.7	Ningún pago a proveedor se deberá realizar sin la validación y aceptación del servicio y/o solución tecnológica, y sin la respectiva validación del cumplimiento contractual
1.8	Se deberán identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente, sobre una base de continuidad. Esto implicará asegurarse de que los contratos estén de acuerdo con los requerimientos legales y regulatorios de los estándares universales de TIC.
1.9	La administración de riesgos del proveedor deberá considerar, como mínimo, acuerdos de confidencialidad, contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos.
1.10	Sin perjuicio de lo establecido en este manual, las dependencias y entidades deberán observar, en lo conducente, las disposiciones emanadas de los manuales administrativos de aplicación general en materia de adquisiciones y arrendamientos y de recursos materiales y servicios generales", según sea el caso.

7.5.2.5 Documentación soporte del proceso

No aplica

7.5.3. Adquisiciones de TIC

7.5.3.1 Objetivos del proceso

General.-

Establecer, de acuerdo a los portafolios de servicios y proyectos, el programa de adquisiciones y servicios de TIC y ejecutarlo.

Específicos.-

1. Definir el programa de adquisiciones y servicios de TIC, en apego a la normatividad vigente en materia de adquisiciones, arrendamientos y servicios de la APF.
2. Cumplir con los requerimientos del procedimiento administrativo de adquisiciones y los compromisos contractuales que se deriven.

7.5.3.2 Descripción del proceso

7.5.3.2.1 Mapa general del proceso

Diagrama de flujo de información

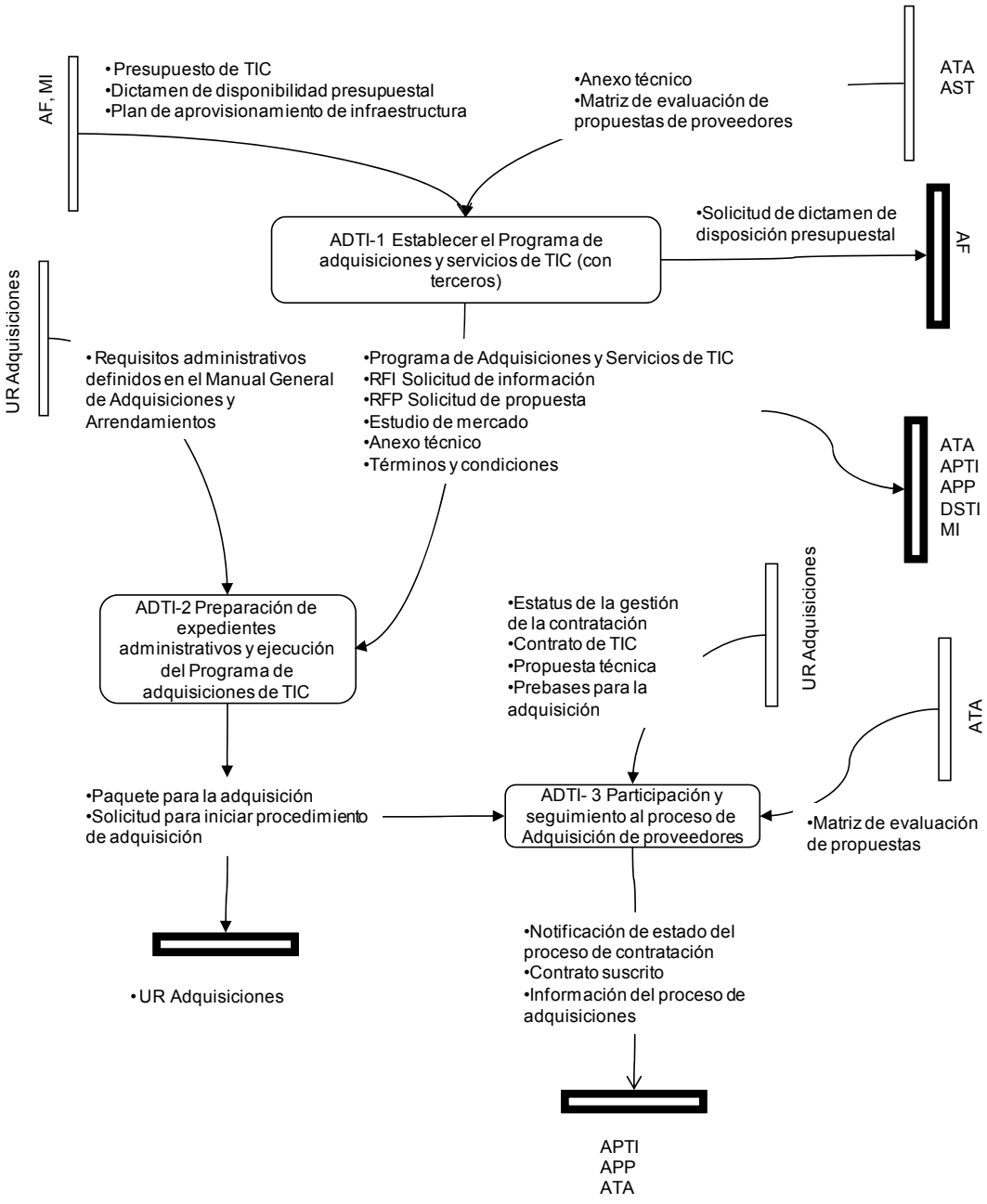
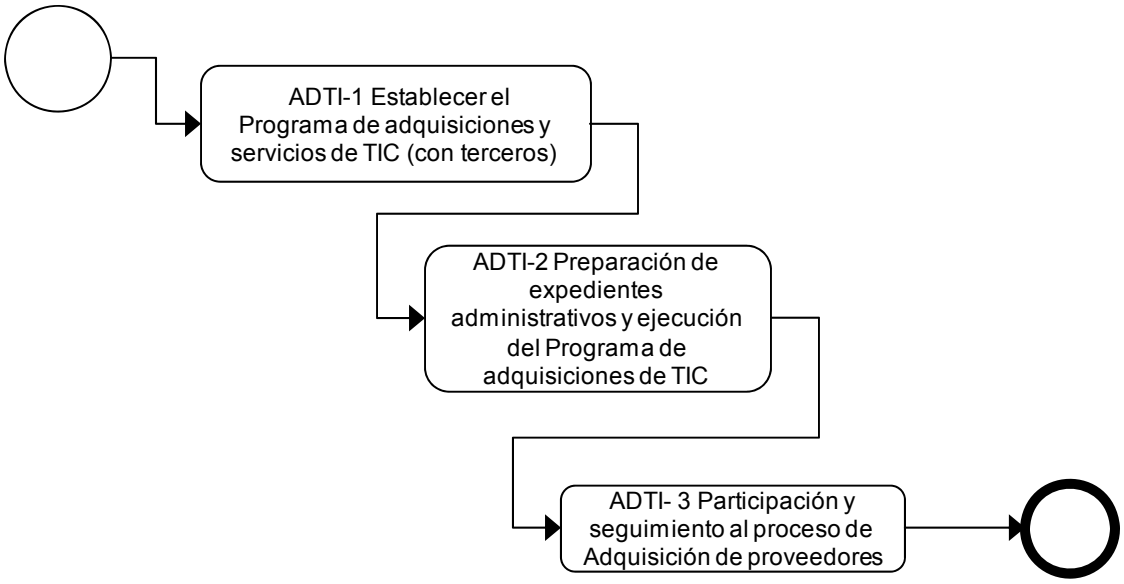


Diagrama de flujo de actividades



7.5.3.2.2 Descripción de las actividades del proceso

ADTI-1 Establecer el programa de adquisiciones y servicios de TIC (con terceros)

Descripción	Establecer el programa de adquisiciones y servicios de TIC que se utilizará para llevar a cabo el procedimiento de contratación o adquisición de los servicios, soluciones tecnológicas o bienes que cubran las necesidades detectadas en materia de TIC conforme al portafolio de proyectos de TIC de la dependencia, y bajo las mejores condiciones para la misma.
Factores Críticos	1. Confirmar que las necesidades a cubrir se encuentran en un Anexo técnico que incluya con los requerimientos funcionales, técnicos, criterios de calidad, niveles de servicio, términos y condiciones de entrega y aceptación de la solución tecnológica, con los resultados del estudio de mercado, que incluya los requisitos, estableciendo los criterios de evaluación de propuestas ya sea: por puntos y porcentajes, costo/beneficio o método binario. Este Anexo deberá contar con el visto bueno del área usuaria así como del responsable del paquete de servicio. 2. Verificar que se cuenta con una Estrategia de adquisición con base a la Investigación de mercado realizada, la cual deberá considerar: a. La definición precisa de la necesidad funcional y operativa del área usuaria. b. El análisis de viabilidad técnica y financiera confirmado mediante investigación de mercado consistente en análisis de las mejores prácticas e identificación de posibles proveedores realizando solicitudes de información sobre sus soluciones tecnológicas y servicios relacionados con la necesidad a cubrir. c. Solicitud de propuesta específica a potenciales proveedores representativos del mercado, con un planteamiento detallado preliminar del requerimiento, para confirmar que el requerimiento es claro y susceptible de atender por el mercado y proveedores específicos. d. Análisis de las propuestas y los costos asociados a ellas para afinar los requerimientos, estimar el rango presupuestal requerido. 3. Validar que el área usuaria ha especificado los criterios de calidad, criterios de aceptación y niveles de servicio esperados del producto, servicio o bien a ser adquirido. 4. Seleccionar el tipo del procedimiento de adquisición que se estará realizando, conforme lo establece la normatividad en materia de adquisiciones, arrendamientos y servicios del sector público. 5. Conforme al tipo del procedimiento de adquisición, se establecen, en conjunto con el área usaría los términos y condiciones para la adquisición del servicio y/o producto o se elaboran la documentación que da sustento al tipo de procedimiento de adquisición seleccionado. 6. Se integra la información, para conformar el Programa de adquisiciones y servicios de TIC, el cual deberá mantenerse actualizado conforme a la normatividad en la materia.
Relación de productos	• Programa de adquisiciones y servicios de TIC • RFI solicitud de información • RFP solicitud de propuesta

	• Estudio de mercado • Anexo técnico • Términos y condiciones

ADTI- 2 Preparación de expedientes administrativos y ejecución del programa de adquisiciones de TIC

Descripción	Integrar el expediente con la documentación soporte del Programa de adquisiciones y servicios de TIC conforme al tipo del procedimiento de adquisición y lo especificado en la normatividad en materia de adquisiciones, arrendamientos y servicios del Sector público, y dar trámite ante la Unidad responsable de las funciones relativas a los procesos mencionados en la dependencia y/o entidad.
Factores Críticos	1. Preparar los expedientes administrativos de TIC conforme al procedimiento adquisición y de acuerdo al Programa de adquisiciones y servicios de TIC. 2. Tramitar autorizaciones aplicables de acuerdo al tipo de adquisición y la normatividad vigente en la materia, así como las consultas a otras áreas de la Dependencia y/o Entidad interesadas en consolidar sus requerimientos de TIC. 3. El expediente administrativo de TIC deberá integrar y asegurar los requisitos solicitados por la normatividad en materia de Adquisiciones, Arrendamientos y Servicios de contrataciones del Sector Público, vigilando que estos cumplan con lo establecido por el procedimiento administrativo como: ▪ Currícula, experiencia, descripción de los bienes o servicios, tiempo y lugar de entrega, cartas compromiso sobre la entrega de los bienes o servicios, garantías, etc. ▪ Fecha de entrega de los bienes ó inicio y finalización de los servicios. ▪ Normas oficiales de calidad (normas mexicanas o internacionales) ▪ Las penas convencionales, sanciones o deductivas que se aplicarán por incumplimiento, así como la eficacia de la garantía de cumplimiento. ▪ Y las demás establecidas en la normatividad. 4. Ejecutar y gestionar en tiempo y forma el Programa de adquisiciones y Servicios de TIC con la Unidad responsable que gestiona los procedimientos de contratación de la Dependencia y/o Entidad conforme a la normatividad vigente en la materia y estándares de operación de la misma. 5. Colaborar con la Unidad responsable a lo largo del procedimiento de contratación, e involucrar al área jurídica y responsables de los procesos de adquisiciones en el análisis, preparación y documentación de la información y, en su caso, los fundamentos legales y motivos técnicos.
Relación de productos	• Paquete para la adquisición • Solicitud para iniciar procedimiento de adquisición

ADTI- 3 Participación y seguimiento de procesos de adquisición de proveedores

Descripción	Dar seguimiento a la gestión de contratación realizado por la Unidad responsable del

	procedimiento de contratación hasta su formalización con la dependencia o entidad.
Factores Críticos	1. Dar seguimiento al procedimiento de contratación que realiza la Unidad responsable de las contrataciones hasta su formalización 2. En caso de que la Unidad responsable encargada de la gestión del procedimiento de contratación tenga dudas técnicas en materia de TIC sobre el expediente y documentación soporte, la UTIC deberá resolver las dudas que se generen y realizar las precisiones correspondientes en la documentación que sea necesaria. 3. Revisar que el contrato contenga las responsabilidades y obligaciones de ambas partes. • Considerar lo especificado por la normatividad en materia de adquisiciones, arrendamientos y servicios del Sector Público. • Validar que las especificaciones técnicas donde se estipulan los deberes del proveedor y sus compromisos, queden plasmados en el contrato • Revisar, y aprobar el contrato por las partes involucradas 4. Formalizar el contrato
Relación de productos	• Notificación de estado del proceso de contratación • Contrato suscrito • Información del proceso de adquisiciones

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.5.3.2.3 Descripción de roles

Rol	Descripción
UR Adquisiciones	Responsables de integrar el programa de adquisiciones, de ejecutar y vigilar el procedimiento de licitación correspondiente y asegurarse que se elabore el contrato.
Áreas usuarias	Las personas y dependencias o entidades que tienen la necesidad a ser cubierta y las características funcionales y de servicio que requieren de los soluciones tecnológicas/servicios a adquirir. Aprobación del anexo técnico y convocatoria al proceso de licitación, participación en el proceso de evaluación de propuestas en cuanto al cumplimiento de requisitos funcionales y operativos.
Área jurídica	Instancia encargada de la revisión de los aspectos legales y normativos del procedimiento de contratación, así como la elaboración y/o revisión de los aspectos legales del contrato.
Área TIC	Incorporación e interpretación de las necesidades del área usuaria, conducción de la investigación de mercado, integración del anexo técnico, evaluación de aspectos técnicos de la propuesta, elaboración del dictamen, seguimiento del proceso con áreas involucradas. Preparación del expediente plurianual y sustento de justificaciones en caso de requerir aprobación de la SFP y SHCP.

Proveedor	Persona o sociedad que proporciona servicios y/o soluciones tecnológicas que deben satisfacer especificaciones de calidad y determinados requisitos de acuerdo a lo estipulado con el solicitante.

7.5.3.2.4 Descripción de productos

Producto	Descripción
Programa de adquisiciones y servicios de TIC	Documento que contiene la información acerca de las adquisiciones que en materia de TIC, serán realizados por la dependencia y/o entidad.
Expediente administrativo de TIC y documentación soporte	Documentos que contienen los requisitos solicitados por la Ley de Adquisiciones, Arrendamientos y Servicios y normatividad vigente en la materia que soportan su contratación, donde se describen entre otras cosas el objeto y alcance de la contratación, los requisitos legales y administrativos, los criterios y metodología de evaluación de las proposiciones, los requisitos técnicos y operativos, el modelo de contrato y el calendario de eventos que conforman el procedimiento. a) Anexo Técnico b) Requisitos técnicos c) Términos y condiciones d) Documentación Soporte, y e) Demás documentación solicitada en la normatividad.
Registro de dudas técnicas en materia de TIC	Documento que registra las preguntas, respuestas y precisiones derivadas del proceso de dudas y aclaraciones de la Unidad responsable que lleva a cabo el proceso de contratación.
RFI Solicitud de información	Documento donde solicita la descripción de bienes y servicios que el proveedor ofrece en relación con las necesidades generales de la institución relativos a los bienes o servicios que requiere, así como el conocimiento de la experiencia y capacidad del mismo a fin de considerarlo para participar en el estudio de mercado y en el procedimiento de licitación.
RFP Solicitud de propuesta	Documento de solicitud de propuesta específica a potenciales proveedores representativos del mercado, con un planteamiento detallado preliminar del requerimiento, para participar en la investigación de mercado específica con el objeto de: confirmar que el requerimiento es claro, susceptible de atender por el mercado y proveedores específicos; así como conocer los precios, tiempo y esfuerzo que el suministro del bien o servicio demanda.
Estudio de mercado	Documento que conjunta los hallazgos de la solicitud de información y de propuesta que concluye con el análisis de viabilidad técnica y financiera, permitiendo conocer el rango de costo/inversión para determinar los requerimientos de suficiencia presupuestal y afinar los requerimientos, para la elaboración del expediente plurianual, suficiencias presupuestales, autorizaciones a la SFP y SHC, oficios de inversión y elaboración del anexo técnico de la convocatoria y bases de licitación.
Anexo técnico	Documento que detalla la descripción de los bienes y servicios a adquirir, los requerimientos técnicos, operativos, especificaciones, condiciones, criterios de evaluación de propuestas, criterios de aceptación de entregables, niveles de servicio esperados y las

Producto	Descripción
	condiciones generales, de las bases de licitación que conforman la convocatoria a participar en el procedimiento.
Notificación de estado del proceso de contratación	Documento que comunica el estado en el que se encuentra el proceso de contratación a los grupos interesados.
Solicitud para iniciar procedimiento de adquisición	Documento oficial para realizar la gestión del procedimiento de contratación.
Información del proceso de adquisiciones	Documentos técnicos, requerimientos, especificaciones que proporcionan información del proceso de adquisiciones (servicio o soluciones tecnológicas).
Contrato suscrito	Contrato firmado y aceptado por el proveedor y el solicitante.

7.5.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de contrataciones de TIC	Evaluar el porcentaje de contrataciones realizadas conforme al programa de adquisiciones y servicios	Evaluar el apego a los tiempos de contratación requeridos por cada solicitud recibida	Eficacia	De gestión	Porcentaje de contrataciones de TIC = (Solicitudes de Adquisición formalizadas / Total de solicitudes del programa de Adquisiciones y servicios de TIC) * 100	UTIC	Anual
Porcentaje de solicitudes gestionadas en tiempo	Evaluar la efectividad del procedimiento de adquisiciones y servicios de TIC	Evaluar el cumplimiento en tiempo y forma del programa de adquisiciones y servicios de TIC	Eficacia	De gestión	Porcentaje de contratos gestionados en tiempo = (Σ solicitudes gestionadas(Tiempo real del procedimiento de adquisición por solicitud recibida / Tiempo de procedimiento de contratación programada) * 100)/ Total de solicitudes del programa de adquisiciones y	UTIC	Anual

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
					servicios de TIC		

7.5.3.4	Reglas del proceso
1.1	Sin perjuicio de lo establecido en el presente manual, todas las actividades desarrolladas para la adquisición de soluciones tecnológicas o servicios, y demás actividades descritas en este proceso, deberán de apegarse –en lo conducente- al manual administrativo de aplicación general en materia de adquisiciones y arrendamientos, leyes y reglamentos que apliquen.
1.2	Se deberá contar con la definición de los requerimientos funcionales, operativos y volumetría de las áreas usuarias, y sus correspondientes requerimientos técnicos desarrollados por las áreas responsables de las TIC para conducir los estudios de viabilidad y de mercado, y en función de las conclusiones de éstos iniciar formalmente el procedimiento de adquisición de bienes y servicios TIC.
1.3	Todos los acuerdos entre proveedor y solicitante deberán quedar plasmados en el contrato y anexos respectivos. Si se trata de servicios deberá incluirse un acuerdo de nivel de servicio donde detalle los parámetros aceptables y las métricas acordadas de así como los estándares y metodologías para su control y seguimiento.
1.5	Se deberá revisar que el contrato cumpla con todas los requisitos administrativos, técnicos y funcionales antes de que sea firmado por la UTIC.
1.6	Se deberán observar las prácticas claves definidas en el proceso de administración de proveedores del presente manual.
1.7	Se deberán observar las prácticas claves definidas en el proceso de administración financiera de TIC del presente manual.

7.5.3.5	Documentación soporte del proceso
	No aplica

7.6 ADMINISTRACIÓN DE SERVICIOS

7.6.1 Administración de portafolio de servicios de TIC

7.6.1.1 Objetivos del proceso

General.-

Definir las prioridades, compromisos e inversiones en servicios de TIC, necesarias para el logro de los objetivos estratégicos de la dependencia o entidad.

Específicos.-

1. Asegurar la gestión del ciclo de vida de los servicios de TIC desde su conceptualización, diseño, elaboración y entrada en operación hasta que entre en desuso.
2. Establecer mecanismos para la toma de decisiones de carácter estratégico relacionadas con los servicios provistos por la UTIC.
3. Establecer un esquema de evaluación, adecuado, comparable, transparente y repetible, que considere el valor financiero, los beneficios y los riesgos implícitos de los casos de negocio, de acuerdo a lo establecido en el proceso de administración del portafolio de proyectos.
4. Implementar mecanismos que aseguren la comunicación y el involucramiento de la UTIC con los mandos superiores de la dependencia o entidad, para la toma de decisiones acerca de las inversiones en servicios de TIC.
5. Proporcionar a los mandos medios y superiores información clara y concreta sobre los servicios que se proveen a los usuarios de TIC.

7.6.1.2 Descripción del proceso

7.6.1.2.1 Mapa general del proceso

Diagrama de flujo de información

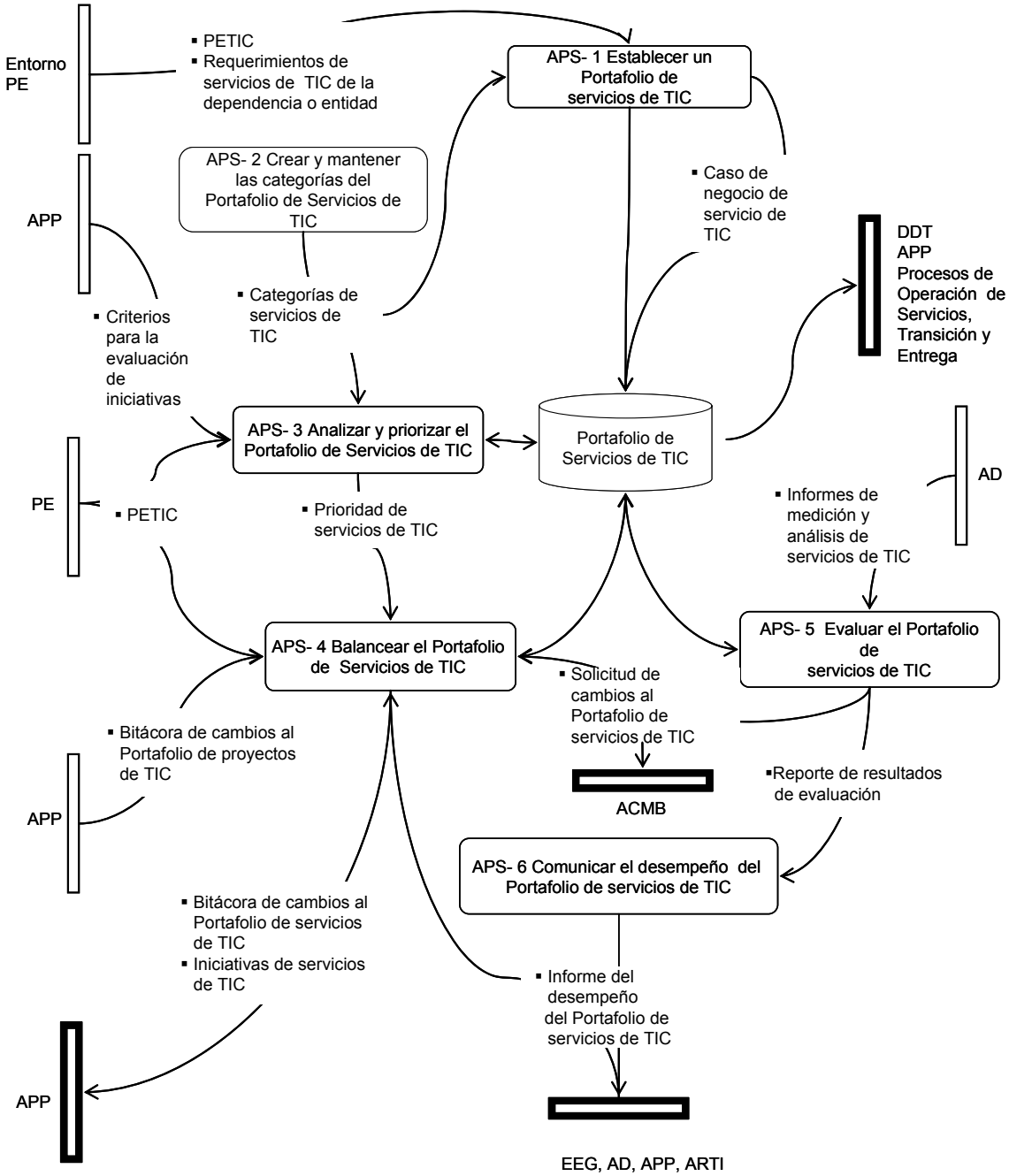
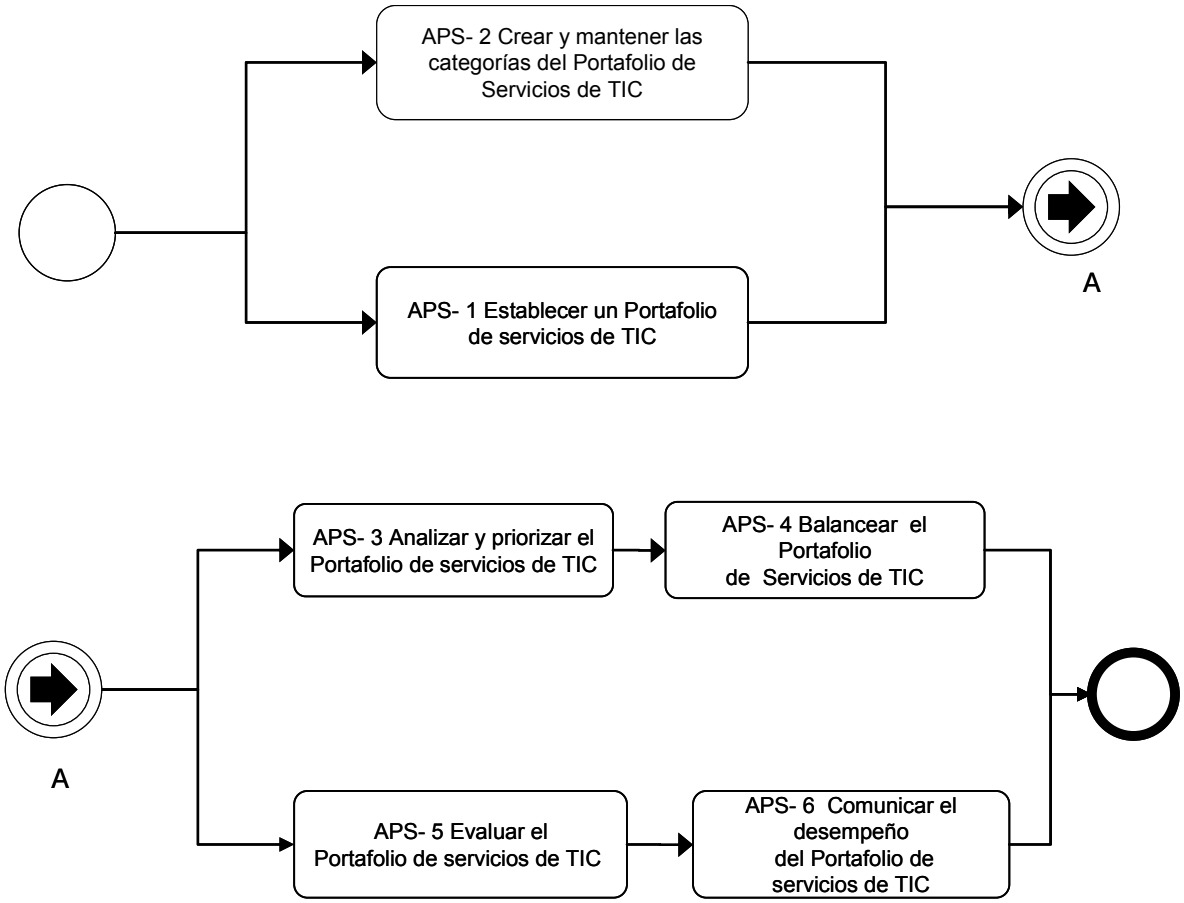


Diagrama de flujo de actividades



7.6.1.2.2 Descripción de las actividades del proceso

APS- 1 Establecer un Portafolio de Servicios de TIC

Descripción	Crear y mantener un registro detallado de los servicios de TIC existentes, así como de aquellas iniciativas/proyectos que estén destinados a la creación de nuevos servicios de TIC.
Factores Críticos	1. Elaborar la propuesta estratégica del Portafolio de servicios de TIC; para esto se deben formular las siguientes preguntas: • ¿Cuáles son los objetivos a largo plazo de la entrega de servicio? • ¿Qué servicios son necesarios para alcanzar esas metas? • ¿Qué capacidades y recursos son necesarios para que la dependencia o entidad alcance estos servicios? • ¿Cómo vamos a llegar? 2. Recolectar información de todos los servicios de TIC existentes y de los propuestos, con el propósito de proveer una fuente única y consistente de información de los servicios de TIC. 3. Elaborar para cada servicio definido en el Portafolio de servicios de TIC su correspondiente caso de negocio. • Documentar los requerimientos de información para los servicios existentes y los nuevos • En la elaboración del caso de negocio se deben considerar los costos de oportunidad de los servicios existentes. • Las definiciones de los servicios de TIC deberán ser acordadas por todos los involucrados. 4. Considerar si se deben incluir aquellos servicios que prestan terceros a la dependencia o entidad.
Relación de Productos	• Caso de negocio de servicio de TIC

APS- 2 Crear y Mantener las categorías del portafolio de servicios de TIC

Descripción	Determinar las categorizaciones que estarán disponibles en el Portafolio de servicios de TIC.
Factores Críticos	• Definir las categorías en las que se agruparan los servicios del Portafolio de servicios de TIC, con base en las prioridades estratégicas y los supuestos relacionados con el uso de los servicios de TIC en la dependencia o entidad. Considerar el uso de las categorías siguientes: canal de entrada de servicios (propuestos o en desarrollo); catálogo de servicios de TIC (actuales o disponibles para su despliegue); y Servicios retirados • Mantener actualizadas las categorías dentro del portafolio de servicios de TIC según las necesidades en la dependencia o entidad, y mantener actualizados los servicios respecto a esas categorías. Estas categorías deben apoyar a la administración del portafolio en la evaluación cubriendo los servicios de TIC actuales, así como aquellas

	iniciativas/proyectos destinados a la introducción o modificación de Servicios de TIC, y su contribución relativa a la maximización del valor, el equilibrio y el alineamiento estratégico de la empresa. • Al momento de crear las categorías de servicios de TIC hay que tomar en cuenta los criterios necesarios para la administración del catálogo de servicios de TIC, incluyendo las categorías necesarias para distinguir los tipos de servicios del Catálogo de servicios al ciudadano, el Catálogo de servicios a los procesos de las Unidades Responsables y el Catálogo de servicios técnicos. • Determinar para cada categoría las propiedades de datos e información que será documentada y administrada dentro del Portafolios de servicios de TIC.
Relación de Productos	• Categorías de servicios de TIC

APS- 3 Analizar y Priorizar el Portafolio de servicios de TIC

Descripción	Realizar un análisis para determinar las prioridades del Portafolio de servicios de TIC con el propósito de sustentar las decisiones de inversión en iniciativas de servicios de TIC.
Factores Críticos	1. Considerar las siguientes categorías para la evaluación de priorización de los servicios incluidos en el Portafolio: • Operar el servicio - Las inversiones se centran en el mantenimiento de las operaciones de servicio. • Crecer el servicio - Las inversiones están destinadas al crecimiento del alcance de los servicios. • Transformar el negocio - Inversiones se mueve en nuevos espacios de atención. 2. Determinar la prioridad de los servicios de TIC asignando un valor único en términos de riesgo y desempeño para cada servicio o iniciativa/proyecto de servicios de TIC y que identifique su contribución para lograr los objetivos de la dependencia o entidad. 3. Esta actividad se debe realizar con la participación de mandos medios y los expertos en la materia, para responder satisfactoriamente a estos factores críticos.
Relación de Productos	• Prioridad de servicios de TIC

APS- 4 Balancear el Portafolio de Servicios de TIC

Descripción	El grupo de trabajo para la dirección de TIC analiza las propuestas de iniciativas de inversión de Servicios de TIC para decidir sobre las propuestas con base en el valor, beneficios, recursos y riesgos implícitos en cada uno. Esta actividad se realiza en forma coordinada con la Administración del portafolio de proyectos de TIC.
Factores Críticos	1. Analizar el desempeño del Portafolio de servicios de TIC y el logro de los objetivos trazados sobre el mismo. Los criterios de análisis deberán tener como base, las necesidades y objetivos estratégicos de la dependencia o entidad. 2. El grupo de trabajo para la dirección de TIC, debe autorizar y/o cancelar las iniciativas/proyectos de servicios de TIC, liberar recursos comprometidos y autorizar el financiamiento de las operaciones de TIC, esto en coordinación con el proceso de

	Administración del portafolio de proyectos de TIC. 3. Con las aprobaciones realizadas, se procede al correspondiente diseño y/o modificación de Servicios de TIC. 4. Registrar en la bitácora de cambios al Portafolio de servicios de TIC los resultados de decisiones sobre los servicios existentes, pueden dividirse en cinco categorías: • Conservar – Son servicios y/o activos definidos en su totalidad y que se encuentran alineados con la estrategia de la dependencia o entidad. • Reemplazar – Estos servicios tienen objetivos de la dependencia o entidad, poco claros y una superposición de funcionalidades. • Racionalizar – A menudo las organizaciones descubren que están ofreciendo servicios que se componen de múltiples presentaciones de un mismo sistema operativo, múltiples versiones del mismo software y / o varias versiones del sistema de las plataformas de prestación de funciones similares. • Renovar – Estos servicios satisfacen los criterios de aptitud funcional, pero quizá pudieran necesitar el reemplazo de algunos componentes técnicos. • Retirar – Servicios que no cumplen los niveles mínimos técnicos y funcionales.
Relación de Productos	• Solicitud de cambios al portafolio de servicios de TIC • Bitácora de cambios al portafolio de servicios de TIC • Iniciativas de servicios de TIC

APS- 5 Revisar el Portafolio de servicios de TIC

Descripción	Identificar si las prioridades establecidas se mantienen alineadas con la estrategia y objetivos de la dependencia o entidad y validar que exista un balance adecuado entre los servicios disponibles para usarse y los que se desarrollan.
Factores Críticos	1. Los criterios para la evaluación del portafolio deberán estar correctamente definidos y actualizados de acuerdo a las necesidades de la dependencia o entidad. 2. La revisión deberá determinar correcciones necesarias a la combinación de iniciativas/proyectos de servicios de TIC, Servicios de TIC y se establecerán los ajustes requeridos, con el objetivo de optimizar al máximo el Portafolio y reflejar el equilibrio deseado. 3. Establecer evaluaciones periódicas sobre el Portafolio de servicios de TIC con fines de calidad.
Relación de Productos	• Reporte de resultados de evaluación

APS- 6 Comunicar el desempeño del Portafolio de servicios de TIC

Descripción	Comunicar los resultados de la revisión hecha al Portafolio de Servicios de TIC, con la finalidad de informar sobre los resultados alcanzados referente a los objetivos del Portafolio y demostrar el valor que TIC le está proporcionando a la dependencia o entidad.

Factores Críticos	1. Los informes elaborados deben indicar claramente la alineación con las metas y objetivos de TIC y de la dependencia o entidad. Los informes que se elaboren deberán cumplir con los criterios del proceso de Administración del Desempeño de TIC. 2. Publicar el resultado de la revisión al desempeño del Portafolio de servicios de TIC. Esta actividad la realiza el Administrador de Portafolio de servicios de TIC o los mandos medios o superiores
Relación de Productos	• Informe del desempeño del portafolio de servicios de TIC

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.6.1.2.3 Descripción de roles

Rol	Descripción
Administrador de portafolio de servicios	Asegurar que los requerimientos actuales y futuros del cliente sean identificados, entendidos y documentados en los Acuerdos del Nivel de Servicios y en los documentos de los Requerimientos del Nivel de servicios. Negociar y acordar con el cliente los niveles de servicios a ser entregados y documentarlos formalmente. Asistir en la producción y mantenimiento del Portafolio de servicios de TIC.
Grupo de trabajo para la dirección de TIC	Grupo o grupos de trabajo conformados por los mandos medios de la UTIC y de las unidades responsables que toman las decisiones de inversión de TIC con respecto a la administración del Portafolio de servicios de TIC este grupo tiene las siguientes responsabilidades: • Elaborar la propuesta estratégica del Portafolio de servicios de TIC. • Asegurar que la evaluación y priorización del Portafolio de servicios de TIC, fue realizada alineados a los objetivos de la dependencia o entidad. • Evaluar el desempeño y los objetivos trazados sobre el Portafolio de servicios de TIC en colaboración con los Administradores de las líneas de servicio. • Dar a conocer el Portafolio de servicios de TIC, así como de las modificaciones que se realicen.
Administrador de Línea de Servicio/Servicio	Responsable de administrar los servicios de TIC como un producto sobre su ciclo de vida completo, desde su concepto hasta su retiro a través de su diseño, transición y operación. Los administradores de servicio son responsables de los datos e información contenidos en el Portafolio de servicios de TIC referente a su servicio (o línea de servicio). Debe interactuar muy de cerca con los usuarios en la determinación de los requerimientos de información para elaborar los casos de negocio de los servicios de TIC.

7.6.1.2.4 Descripción de productos

Producto	Descripción
Portafolio de servicios de TIC	Repositorio de conocimientos con información sobre los servicios de TIC. Incluye los servicios a lo largo de su ciclo de vida desde su conceptualización, diseño, transición hasta los que se encuentran actualmente en operación o en desuso. El Portafolio de Servicios de TIC incluye al catálogo de servicios de TIC. Una alternativa para la implementación del Portafolios de servicios de TIC es integrar la información de éste, de manera estructurada, en base de datos de configuraciones (CMDB) administrada en el proceso de Administración de la configuración.
Catálogo de servicios de TIC	Es el elemento del portafolio de servicios que se publica para conocimiento de los usuarios, apoya la comunicación con éstos y la entrega de servicios de TIC. El catálogo de servicios incluye información como la siguiente: Propietario del servicio Descripción resumida del servicio Descripción detallada del servicio Arquitectura del servicio Horario del servicio Horario de mantenimiento del servicio Calidad del servicio Métricas y Reportes del servicio Disponibilidad Roles y responsabilidades de los involucrados en el servicio
Iniciativa de servicios de TIC	Documentación de las iniciativas de proyectos destinados a la creación, mantenimiento o modificación de servicios de TIC, de acuerdo a las categorías de servicios del Portafolio de servicios de TIC y a los criterios de evaluación que se establecen en el proceso de Administración del portafolio de proyectos de TIC. La documentación de la iniciativa incluye los requerimientos de información del servicio y la documentación de su caso de negocio.
Caso de negocio	Justificación técnica y económica de cómo se puede crear valor a la entidad o dependencia y/o a los usuarios de un servicio de TIC. Incluye información de costos, beneficios, riesgos y contribución a los objetivos de la entidad o dependencia. Sustenta las decisiones, según sea el caso, acerca de la construcción de un servicio desde cero, adquisición de solución en el mercado, adecuación de un servicio existente, mantenimiento en la operación o retiro de un servicio.
Bitácora de cambios al Portafolio de Servicios de TIC	Incluye información acerca del estado de las solicitudes de cambio al Portafolio de servicios de TIC. Registra el resultado de las decisiones tomadas con respecto a conservar, reemplazar, racionalizar, renovar y/o retirar servicios de TIC

Producto	Descripción
Informe de desempeño del portafolio de servicios de TIC	Informes y reportes que comunican el estado global del desempeño y el cumplimiento a los objetivos y metas del Portafolio de servicios de TIC.
Reporte de evaluación del portafolios de Servicios de TIC	Reporte de la evaluación periódica que se realiza al Portafolio de servicios de TIC con el propósito de determinar si las prioridades asignadas a los servicios de TIC permanecen vigentes y validar que existe un equilibrio adecuado en las inversiones autorizadas.
Solicitud de cambios al portafolio de servicios de TIC	Solicitud para realizar un cambio al Portafolio de servicios de TIC.
Categorías de servicios de TIC	Grupos de servicios del Portafolio de servicios de TIC usados para facilitar la administración del Portafolios de servicios de TIC.
Prioridad de servicios de TIC	Valor único que se asigna a los servicios de TIC dentro del portafolio para denotar su prioridad de acuerdo a su contribución para lograr los objetivos de la entidad o dependencia, sus beneficios, costos, nivel de riesgo y su desempeño (actual o potencial).

7.6.1.3. Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de Servicios de TIC	Medir el grado de cumplimiento del Portafolio de Servicios de TIC	Es el porcentaje obtenido de los servicios de TIC para alcanzar los objetivos establecidos	Eficacia	De gestión	(Servicios de TIC entregados/ Servicios de TIC planeados) *100	Administrador del Portafolio de Servicios de TIC	Semestral

7.6.1.4 Reglas del proceso

1.1	La UTIC deberá designar a un responsable de la administración del Portafolio de servicios de TIC.
1.2	El grupo de trabajo para la Dirección de TIC debe designar un responsable para cada iniciativa de servicio de TIC, será denominado Administrador de Línea de Servicio/Servicio.
1.3	Cualquier cambio al Portafolio de Servicios de TIC deberá ser aprobado por el responsable de la Administración del portafolio de servicios y se deberá llevar a cabo mediante el proceso de Administración de Cambios.
1.4	El Administrador de Línea de Servicio/Servicio será responsable de la revisión del Caso de Negocio.

7.6.1.5 Documentación soporte del proceso

No aplica

7.6.2 Diseño de servicios de TIC

7.6.2.1 Objetivos del proceso

General.-

Diseñar y desarrollar servicios, así como mantener o mejorar los existentes, conforme a las necesidades, prioridades y posibilidades de la dependencia o entidad, a fin de mantener e incrementar la calidad de los bienes y servicios que la institución ofrece a la sociedad..

Específicos.-

1. Diseñar servicios que respondan a las necesidades y programas de la dependencia o entidad, considerando requerimientos especificados por el usuario y la normatividad vigente.
2. Diseñar servicios que contemplen seguridad de TIC, continuidad, disponibilidad, capacidad de la UTIC y proveedores.
3. Definir especificaciones de los servicios de TIC que permitan construirlos y desplegarlos en función de las necesidades de la dependencia o entidad.
4. Identificar y administrar riesgos para que puedan ser eliminados, transferidos y/o mitigados, antes de que los servicios de TIC, pasen al ambiente de producción.
5. Diseñar la arquitectura del ambiente del servicio de TIC, para satisfacer las necesidades actuales y futuras de la dependencia o entidad.
6. Elaborar planes de TIC, procedimientos, arquitecturas, y documentos para el diseño de soluciones tecnológicas de calidad que satisfagan las necesidades de la dependencia o entidad.
7. Asegurar una comunicación transparente de las definiciones y estado de los servicios diseñados.

7.6.2.2 Descripción del proceso

7.6.2.2.1 Mapa general del proceso

Diagrama de flujo de información

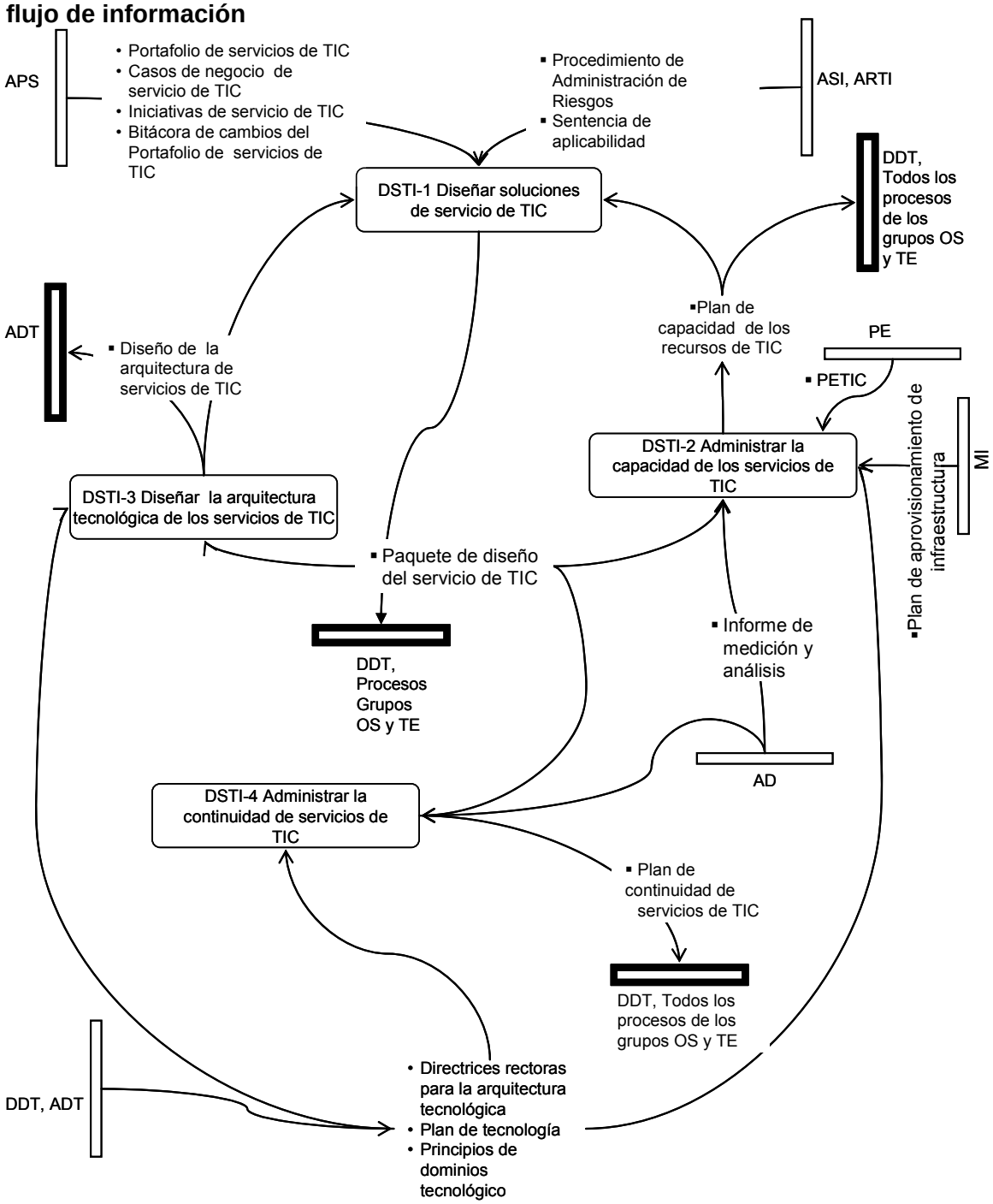
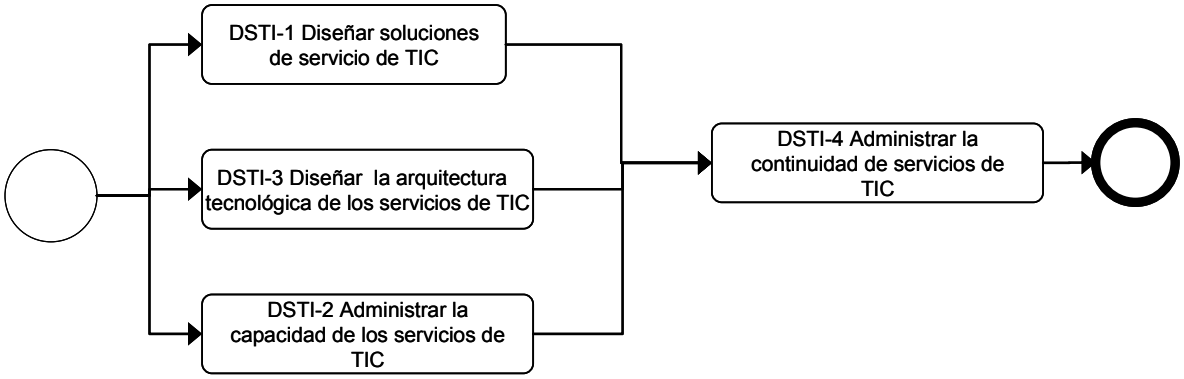


Diagrama de flujo de actividades



7.6.2.2.2 Descripción de las actividades del proceso

DSTI-1 Diseñar soluciones de servicio de TIC

Descripción	Elaborar planes y especificaciones de diseño de servicios nuevos o mejorados que cumplan con las necesidades y requerimientos de información, presupuestos, programas y límites de tiempo que la dependencia o entidad tiene. Las especificaciones del servicio de TIC y las expectativas puntuales sobre éste, deberán ser identificadas, definidas, acordadas, documentadas y medidas en requerimientos de servicio y criterios de aceptación.
Factores Críticos	1. Acordar los requerimientos del servicio. Realizar un análisis de los requerimientos asociados al servicio, asegurando que se documenten y acuerden formalmente por todas las partes interesadas. Estos requerimientos forman la base para todas las actividades de diseño posteriores y deberán encontrarse bajo control formal de cambios. • Para servicios existentes se incluyen, entre otros, requerimientos de: – Requerimientos nuevos de funcionalidad o infraestructura. – Cambios en los procesos de la dependencia o entidad, dependencias, prioridades, importancia e impacto. – Cambios en los volúmenes de transacciones del servicio. – Cambios en los niveles de servicio y sus metas asociadas. • Para servicios nuevos se incluyen, entre otros, requerimientos de: – Requerimientos de funcionalidad y de infraestructura. – Requerimientos para la administración del servicio. – Procesos de la dependencia o entidad que soporta, dependencias, prioridades, importancia e impacto. – Requerimientos de niveles de servicios y sus metas. – Niveles de transacciones, números de usuarios de acuerdo a su tipo y su crecimiento anticipado. – Caso de negocio, incluyendo aspectos financieros y de estrategia. – Estimaciones sobre la frecuencia de cambios. – Niveles de capacidad o de soporte que va a requerir (por ejemplo soporte local). 2. Analizar la madurez, capacidades y estado de la infraestructura y servicios de TIC existentes con una perspectiva de reuso para utilizar siempre que sea posible componentes y servicios existentes. 3. Elaborar las especificaciones de las soluciones de servicios, considerando todos los aspectos inherentes al servicio, incluyendo, pero no limitando: • Instalaciones, funcionalidad e información para monitoreo. • Los procesos que soportan o soportarán los servicios internos y externos y el impacto y beneficios esperados. • Los ciclos de servicios: su demanda planeada o definida por las regulaciones, leyes y normas del organismo y los indicados por los diversos organismos rectores de la

Administración Pública Federal.

- Los Requerimientos de Niveles de Servicios SLR y las metas de Nivel de Servicio esperadas y acordadas o comprometidas.
- Las escalas de tiempo, o límites de tiempo acordados o establecidos internamente o externamente.
- Los requerimientos para realizar las pruebas del servicio, sobre todo las de aceptación del usuario.
- Los OLA acordados dentro de TIC.
- Los contratos con proveedores externos, documentados en los Contratos de Soporte actuales.
- El nivel de escalabilidad del servicio para satisfacer las necesidades futuras de la dependencia o entidad.

4. Documentar los Criterios de aceptación del servicio.
5. Evaluar diversas opciones de solución en cuanto a tiempo, costo, beneficios a la dependencia o entidad y al ciudadano y el grado de cumplimiento a los requerimientos del servicio para seleccionar la alternativa de solución que se considere más apropiada.
6. Analizar, re-evaluar y de ser necesario acordar cambios al presupuesto y recursos autorizados en el proceso de Administración del portafolio de servicios de TIC para la iniciativa correspondiente al servicio que se está diseñando.
7. Validar que la solución seleccionada se encuentra alineada a las estrategias de TIC, el Plan de tecnología, ver proceso Determinar la dirección tecnológica, los principios y las directrices de la arquitectura tecnológica, ver proceso Administrar dominios tecnológicos.
8. Asegurar que la solución seleccionada cumple con todos los controles de gobierno y de seguridad que le apliquen de acuerdo a su categoría.
9. Realizar una evaluación para determinar que tan preparada se encuentra la dependencia o entidad para asegura que la solución seleccionada para el servicio puede ser operada de manera que cumpla con las metas de los niveles de servicio requeridas. Esta evaluación deberá incluir:
   - Un análisis del impacto, beneficios y contribución de la solución, así como de los costos involucrados a lo largo de todo el ciclo de vida del servicio, incluyendo los costos del diseño, desarrollo, continuidad de la operación y soporte del servicio.
   - Evaluación y mitigación de los riesgos asociados a un servicio nuevo o modificado, particularmente con respecto a su operación, seguridad, disponibilidad y continuidad.
   - La capacidad y madurez de la dependencia o entidad con respecto al servicio bajo diseño. La evaluación de este aspecto es realizado por los responsables de unidades de responsables usuarias del servicio con respecto a la existencia de procesos, estructura, personal, roles, responsabilidades e instalaciones apropiadas para operar el servicio.
   - La capacidad y madurez de la infraestructura de TIC. La evaluación de este aspecto considera:
     - La evaluación del impacto del servicio en todas las áreas de TIC y recursos

	involucrados. – Los procesos, roles y responsabilidades propios de la UTIC. – Las habilidades, conocimiento y competencia del personal. – Las herramientas de soporte y gestión necesarias para el servicio. 10. Definir las métricas y métodos de medición requeridos para validar el cumplimiento de los acuerdos de niveles de servicio. 11. Determinar contratos con proveedores externos necesarios para operar el servicio. 12. Integrar en el Paquete del diseño de servicio, toda la información resultante de esta actividad en soporte a los procesos involucrados en el desarrollo de la solución tecnológica, la transición y entrega y la operación del servicio. 13. Los datos e información del conocimiento resultante del Diseño del servicio; incluyendo el paquete del diseño se deberá incorporar y administrar en un repositorio de conocimiento del Sistema de conocimiento de la UTIC.
Relación de Productos	• Paquete de diseño del servicio de TIC

DSTI-2 Administrar la capacidad de los recursos de TIC

Descripción	Revisar periódicamente el desempeño actual y la capacidad de los recursos de TI con el propósito de optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades de los servicios de TIC, para asegurar que cumple con los niveles de servicio acordados. Este proceso incluye el pronóstico de necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias.
Factores Críticos	1. Desarrollar un Plan de capacidad que le permita a la UTIC proporcionar servicios que cumplan con los niveles y metas de servicio acordadas y para cumplir con el crecimiento previsto de la demanda, la mejora de los niveles de servicio y nuevos servicios incluidos en el Portafolio de servicios de TIC. En la elaboración del Plan de capacidad se deben considerar: • La información suficiente para habilitar la toma de decisiones con respecto a: – Cuales activos y/o recursos requieren ser mejorados (por ejemplo: más memoria, dispositivos de almacenamiento más veloces, procesadores más poderosos, mayor ancho de banda). – Cuándo se requiere la mejora. – Cuánto costará la mejora. Los planes de capacidad se usan para la planificación del presupuesto y las inversiones. • El balance entre los costos involucrados y los recursos requeridos de forma que las adquisiciones y los costos involucrados se pueden justificar para procesar las cargas de trabajo acordadas tal como se determina en los niveles de servicio acordados, • El balance entre la oferta y la demanda, necesario para asegurar que la capacidad de los recursos está de acuerdo a la demanda que se tiene sobre ellos, y • La participación de los responsables y expertos de los dominios tecnológicos dentro del

	alcance del Plan de capacidad. 2. Revisar el desempeño y capacidad actual. Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados. • Incluye el monitoreo del desempeño actual y capacidad usada, soportada de ser necesario por soluciones automatizadas. • Identificar y dar seguimiento a incidentes causados por problemas de falta de capacidad. • Evaluar los niveles de capacidad a nivel demanda, servicio y componente contra los niveles de servicio acordados y tendencias. 3. Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TIC en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad. 4. Garantizar la disponibilidad de los recursos de TIC. Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TIC. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La UTIC debe garantizar que los planes de contingencia consideren de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TIC. 5. Monitorear continuamente el desempeño y la capacidad de los recursos de TIC. La información reunida sirve para dos propósitos: • Mantener y poner a punto el desempeño actual dentro de TI y atender temas como flexibilidad, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos. • Para reportar la disponibilidad hacia el servicio prestado como se requiere en los SLA. Acompañar todos los reportes de excepción con recomendaciones para acciones correctivas.
Relación de Productos	• Plan de capacidad de los recursos de TIC

DSTI-3 Diseñar la arquitectura tecnológica de los servicios de TIC.

Descripción	Proveer los modelos arquitectónicos para el desarrollo y despliegue de la infraestructura de TIC necesaria para la operación de un servicio o una línea de servicios, que satisfaga las necesidades actuales y futuras del servicio y se encuentre alineado a las directrices de la Arquitectura tecnológica de la dependencia o entidad y su plan de tecnología.
Factores Críticos	1. Adoptar una metodología para el desarrollo de modelos de arquitectura de servicios de TIC que permita la estandarización, soporte y consistencia en el establecimiento y evolución de la infraestructura de TIC necesaria para sustentar el diseño y la provisión de un servicio de TIC. 2. Diseñar, usando la metodología establecida, los modelos de arquitectura tecnológica necesarios para sustentar el diseño y la operación de una solución para un servicio nuevo

	o modificado. 3. Asegurar que las infraestructuras de TIC, ambientes, datos, aplicaciones y servicios externos involucrados en el modelo de arquitectura de un servicio de TIC se alinean a las directrices de la Arquitectura tecnológica y los principios de los dominios tecnológicos y que los requerimientos tecnológicos derivados de éstas se consideren en la elaboración del Plan de tecnología, ver proceso Determinación de la dirección tecnológica. 4. Asegurar el apego a marcos de referencia arquitectónicos adoptados por la dependencia o entidad, estrategias, procedimientos y estándares.
Relación de Productos	• Diseño de la arquitectura de servicios de TIC

DSTI-4 Administrar la continuidad de servicios de TIC

Descripción	Asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI mediante el desarrollo y mantenimiento de los planes de contingencia en materia de TIC, el entrenamiento y pruebas de los planes de contingencia en materia de TIC y asegurando que la disponibilidad de copias de los planes de contingencia y de los datos requeridos fuera de las instalaciones.
Factores Críticos	1. Desarrollar y establecer un sistema de continuidad de servicios, consistente a lo largo de toda la dependencia o entidad, para asegurar la continuidad de los servicios de TIC que incluya las directrices, los procedimientos, estructuras, roles y responsabilidades necesarios para soportar la continuidad de los servicios de TIC. • El Sistema de continuidad de servicios de TIC tiene el propósito de ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. • El Sistema de continuidad de servicios de TIC, debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. • El Sistema de continuidad de servicios de TIC, debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación. • El Sistema de continuidad de servicios de TIC debe considerar los resultados del análisis de impacto al negocio (BIA) y la estrategia de recuperación que se determine en el proceso de Administración de riesgos de TIC. 2. Desarrollar el Plan de continuidad de TIC con base en el Sistema de continuidad de servicios de TIC, diseñados para reducir el impacto de una interrupción mayor de las funciones y los procesos clave de la dependencia o entidad. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas. 3. Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TIC, para construir resistencia y establecer prioridades en situaciones de

recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias de la dependencia o entidad, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

4. Revisar el Plan de continuidad de TIC mediante un procedimiento de control de cambios, para asegurar que el plan de continuidad de TIC se mantenga actualizado y que refleje de manera continua los requerimientos actuales de la dependencia o entidad. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.
5. Probar el plan de continuidad de TI de forma regular para asegurar que los servicios de TIC pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.
6. Entrenar en el Plan de continuidad de TIC, para asegurar que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procedimientos, actividades y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.
7. Asegurar que el Plan de continuidad de TIC se distribuye de manera apropiada y segura y que está disponible entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlo accesibles bajo cualquier escenario de desastre.
8. Planear las acciones a tomar durante el período en que se están recuperando y reanudando los servicios de TIC. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los titulares de las Unidades responsables entienden los tiempos de recuperación de los servicios críticos de TIC y las inversiones necesarias en materia de TIC para soportar las necesidades de recuperación y reanudación de los servicios de TIC.
9. Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TIC críticos, necesarios para la recuperación de los servicios de TIC y para los planes de continuidad de la dependencia o entidad. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos sustantivos de la dependencia o entidad y el personal de TIC. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la dependencia o entidad. El titular de la UTIC debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos dos veces por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

	10. Activar el Plan de continuidad cuando sea necesario y una vez lograda una exitosa reanudación los servicios de TIC después de un desastre, evaluar el desempeño contra el plan, los problemas encontrados y lo adecuado del Plan de continuidad. Actualizar el plan en consecuencia con los hallazgos y lecciones aprendidas.
Relación de Productos	• Plan de continuidad de servicios de TIC

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.6.2.2.3 Descripción de roles

Rol	Descripción
Responsable del diseño de servicios de TIC	Es responsable de la calidad del proceso de diseñar servicios de TIC y supervisa tanto su administración como el cumplimiento con los procesos, los modelos de datos, así como las disposiciones y tecnologías asociadas con este proceso.
Propietario del Servicio	Es responsable por la entrega de un servicio en específico, sin importar en donde residan los componentes subyacentes, procesos o capacidades profesionales que lo soportan.
Arquitecto de TIC	Responsable de la arquitectura que seguirá el servicio desde el punto de vista tecnológico con fines de integración en la solución.
Administrador de Proyectos	Persona encargada de gestionar todos los aspectos relacionados a un proyecto incluyendo recursos monetarios, tiempo, tareas, actividades, seguimiento, reporte de avance, entre otros.
Responsable del diseño de un servicio	Responsable de elaborar el paquete de Diseño del servicio y supervisar el programa de proyectos que se deriven del mismo.

7.6.2.2.4 Descripción de productos

Producto	Descripción
Requerimientos SLR	Es un requerimiento del usuario respecto a un aspecto de un servicio y tiene como base los objetivos del negocio, son necesarios para negociar las metas de niveles de servicio.
Acuerdos de SLA	Acuerdo entre un Proveedor de TIC y un usuario. El SLA describe el Servicio TIC, documenta los Objetivos de niveles de servicio y especifica las responsabilidades de la UTIC, del proveedor de TIC y del usuario. Un único SLA puede cubrir varios Servicios TIC o varios usuarios.
Acuerdos OLA	Consiste en el Acuerdo entre la UTIC y otra parte de la misma Dependencia o entidad. El OLA contiene la descripción de los Servicios TIC que se ofrecen a los usuarios, e incluye la definición de los bienes y Servicios que se proveen, así como los compromisos de ambas partes.
Contratos de Soporte (UC)	Es un Contrato entre la UTIC y un Tercero. El Tercero proporciona bienes o Servicios que soportan la entrega de un Servicio al usuario. El Contrato de Soporte define

Producto	Descripción
	objetivos y responsabilidades que son requeridos para alcanzar los Objetivos de Nivel de Servicio en un SLA.
Plan de capacidad	El Plan de capacidad se usa para gestionar los recursos de TIC requeridos para proveer los servicios de TIC incluidos en el Portafolio de servicios de TIC. El Plan contiene escenarios para distintas predicciones de demanda de los servicios, y las opciones valoradas para proveer los niveles y metas de servicios acordados. El Plan de capacidad incluye los factores para cumplir los requerimientos de desempeño y disponibilidad actuales y futuros de los servicios. El contenido típico del Plan de capacidad incluye: • Descripción del entorno y alcance considerado en el Plan de capacidad incluyendo: o Los servicios actuales, tecnología y recursos. o Los niveles actuales de capacidad de la dependencia o entidad. o Incidentes y problemas experimentados debido a una falta o exceso de capacidad. o El grado de cumplimiento de los niveles de servicio. o Los cambios que se han realizado desde la última emisión del plan. • Resumen ejecutivo, incluyendo una síntesis de los principales asuntos, opciones, recomendaciones y costos. • Escenarios de demanda y provisión de los servicios. • Alcance de los recursos de TIC que están considerados en el plan. • Métodos usados para recolectar la información que sustenta al plan. • Supuestos. • Resumen de los servicios considerados en el plan. • Uso actual de los recursos de TIC y predicciones de los niveles de uso futuros. • Opciones para mejorar la eficacia y la eficiencia de la entrega de servicios de TIC. • Estimados de costos. • Recomendaciones en términos de : o Beneficios para la dependencia o entidad. o Impacto potencial si se lleva a cabo la recomendación. o Riesgos involucrados. o Recursos requeridos. o Costos de adquisición y de operación asociados.
Requerimientos de servicios de terceros	Documento en el que se describen los servicios que se requerirán de terceros para la construcción y/o provisión del servicio de TIC.
Entendimiento de los requerimientos de seguridad de la	Documento en el que se describen las necesidades de seguridad que se requerirán implementar para el nuevo o modificado servicio, y que se genera a partir del proceso de Administración de la seguridad.

Producto	Descripción
dependencia o entidad	
Plan de continuidad	Plan que define los pasos necesarios para recuperar uno o más servicios. El Plan además identificará los disparadores de la invocación del plan, las personas que han de ser involucradas, las comunicaciones necesarias entre otros. El Plan de continuidad de los servicios deberá ser parte de un sistema de continuidad de la operación en la dependencia o entidad, y contemplar: • Las condiciones y las responsabilidades para activar y/o escalar el plan. • Estrategias de recuperación, incluyendo la secuencia de actividades necesarias. • Requerimientos mínimos para mantener un nivel adecuado de operación y de niveles de servicio con recursos disminuidos. • Procedimientos de emergencia. • Procedimientos de respaldo. • Procedimientos temporales de operación. • Procedimientos para la recuperación del servicio. • Plan de pruebas y mantenimiento. • Actividades de entrenamiento, educación y concientización. • Responsabilidades de los individuos. • Regulaciones. • Inventario de recursos críticos, incluyendo información actualizada de los contactos necesarios para ejecutar los procedimientos de emergencia, recuperación y respaldo. • Instalaciones alternativas de acuerdo a lo establecido en el plan. • Proveedores alternativos para recursos críticos. • Plan de comunicaciones.
Paquete de diseño del servicio de TIC	Documentación integrada de los resultados del diseño de soluciones de servicios de TIC. El contenido típico del Paquete de diseño del servicio es: • Requerimientos: o Requerimientos de información desde la perspectiva del usuario. o Requerimientos del uso del servicio. o Contactos del personal clave y otros involucrados en el diseño, transición y operación del servicio. • Diseño del servicio: o Requerimientos funcionales del servicio. o Requerimientos de niveles de servicio. o Requerimientos de operación y de administración del servicio. o Arquitectura y diseño del servicio, incluyendo: ▪ El modelo y definición del servicio para la transición y

Producto	Descripción
	operación. ▪ Todos los componentes del servicio e infraestructura (de preferencia dentro de la base de datos para la administración de la configuración. ▪ Requerimientos de documentación necesaria para los usuarios, procesos, servicios, componentes, transición, soporte y operación. ▪ Procesos, procedimientos, métricas y mediciones y reportes asociados al servicio. • Evaluación del grado de preparación de la dependencia o entidad incluyendo: beneficios, evaluación financiera, evaluación técnica, evaluación de recursos y evaluación organizacional, en conjunto con detalles de las habilidades, competencias y conocimientos requeridos por la UTIC, sus proveedores, los servicios de tercero y contratos. • Planes del ciclo de vida del servicio. o Planes generales de alto nivel para cada una de las fases del ciclo de vida del servicio, incluyendo un cronograma de alto nivel para la transición, la operación y mejoras subsecuentes de los servicios. • Criterios de aceptación del servicio.
Portafolio de servicios de TIC	Conjunto de todos los servicios que son gestionados por la UTIC. El Portafolio de Servicios de TIC se emplea para gestionar el ciclo de vida completo de los Servicios, e incluye al Catálogo de servicios (servicios en uso).
Requerimientos de servicios de TI	Son necesidades específicas que necesitarán ser cubiertas por el servicio.
Diseño de la arquitectura de servicios de TIC	Modelos que describen los componentes de la arquitectura tecnológica y las relaciones entre ellos a considerar para la solución del diseño de los servicios de TIC.

7.6.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de Servicios en Operación de TIC	Medir el grado de cumplimiento del catálogo de servicios de TIC	Es el porcentaje obtenido de los servicios en operación alcanzar los objetivos establecidos	Eficacia	De gestión	(servicios de TIC en operación / servicios de TIC registrados en el catalogo de servicios) * 100	Responsable del diseño de un servicio	Semestral

7.6.2.4	Reglas del proceso

1.1	La UTIC deberá designar un responsable del proceso de diseño de servicios de TIC.
1.2	El responsable del proceso de Diseño de servicios de TIC incluirá solamente en un proceso, el diseño de servicios aprobados por el responsable del Portafolio de servicios de TIC, tanto nuevos servicios como modificaciones a servicios existentes.
1.3	El grupo de trabajo para la dirección de TIC, deberá designar a un responsable del diseño del servicio.

7.6.2.5	Documentación soporte del proceso

No aplica

7.7 DESARROLLO Y ADQUISICIÓN DE SOLUCIONES

7.7.1. Administración técnica de las adquisiciones

7.7.1.1 Objetivos del proceso

General.-

Definir los criterios para la adquisición de una solución tecnológica, desde la definición de los requerimientos para la adquisición hasta la aceptación de la solución tecnológica adquirida.

Específicos.-

1. Identificar las necesidades, expectativas, restricciones e interfaces y transformarlas en requerimientos contractuales para la adquisición de una solución o servicio.
2. Definir las características técnicas de la solución tecnológica o servicio a ser adquirido, para asegurar que cubre las necesidades, expectativas y restricciones identificadas.
3. Evaluar técnicamente las soluciones o servicios propuestos por los diferentes proveedores para asegurar la cobertura de los requerimientos contractuales e identificar la mejor respuesta a las necesidades de la dependencia o entidad.
4. Dar seguimiento y revisar las actividades de los proveedores para asegurar el cumplimiento de los acuerdos establecidos en el contrato.
5. Evaluar las soluciones tecnológicas o servicios entregados por el proveedor para asegurar el cumplimiento de los requerimientos y aprobarlos.

7.7.1.2 Descripción del proceso

7.7.1.2.1 Mapa general del proceso

Diagrama de flujo de información

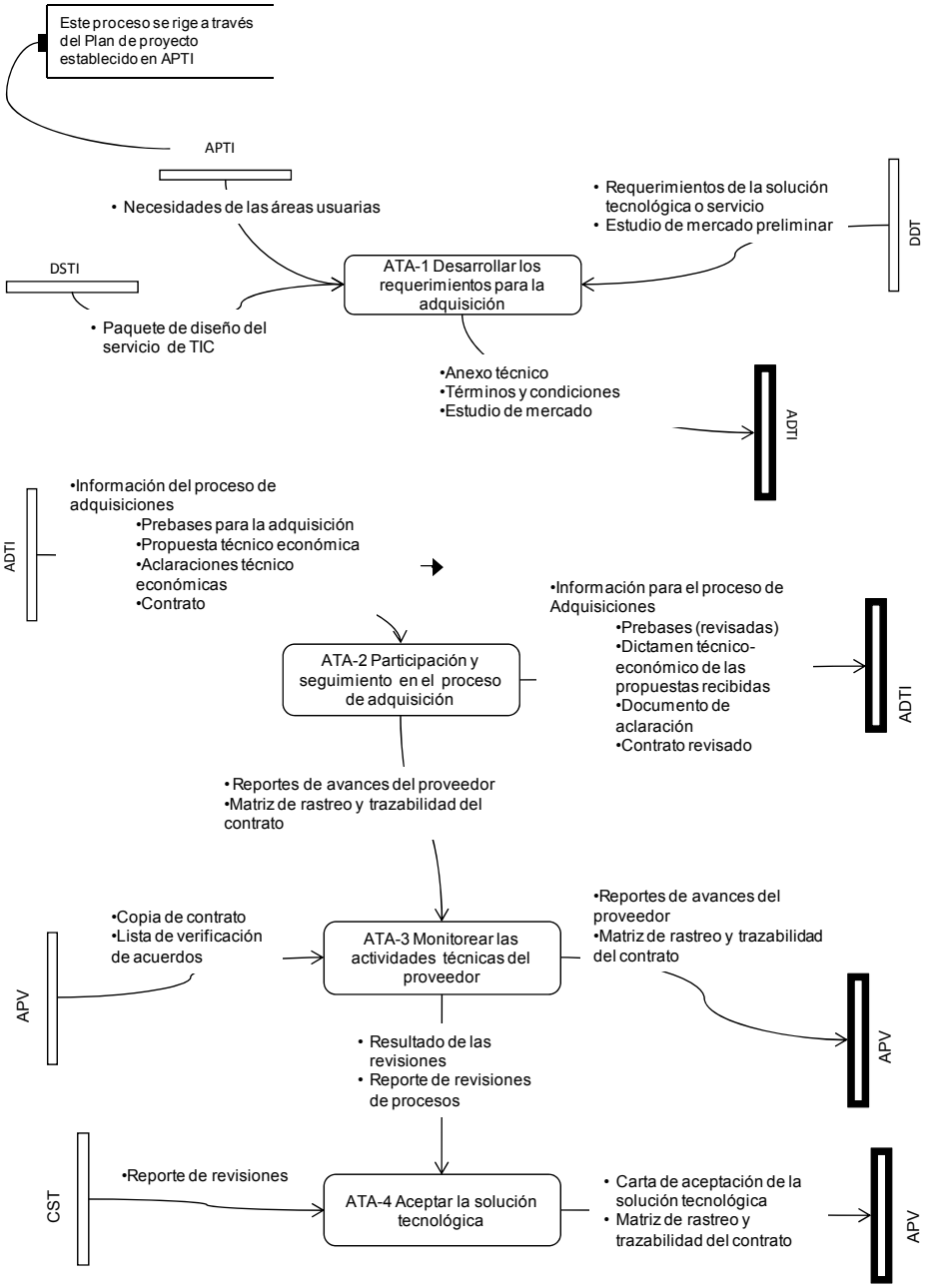
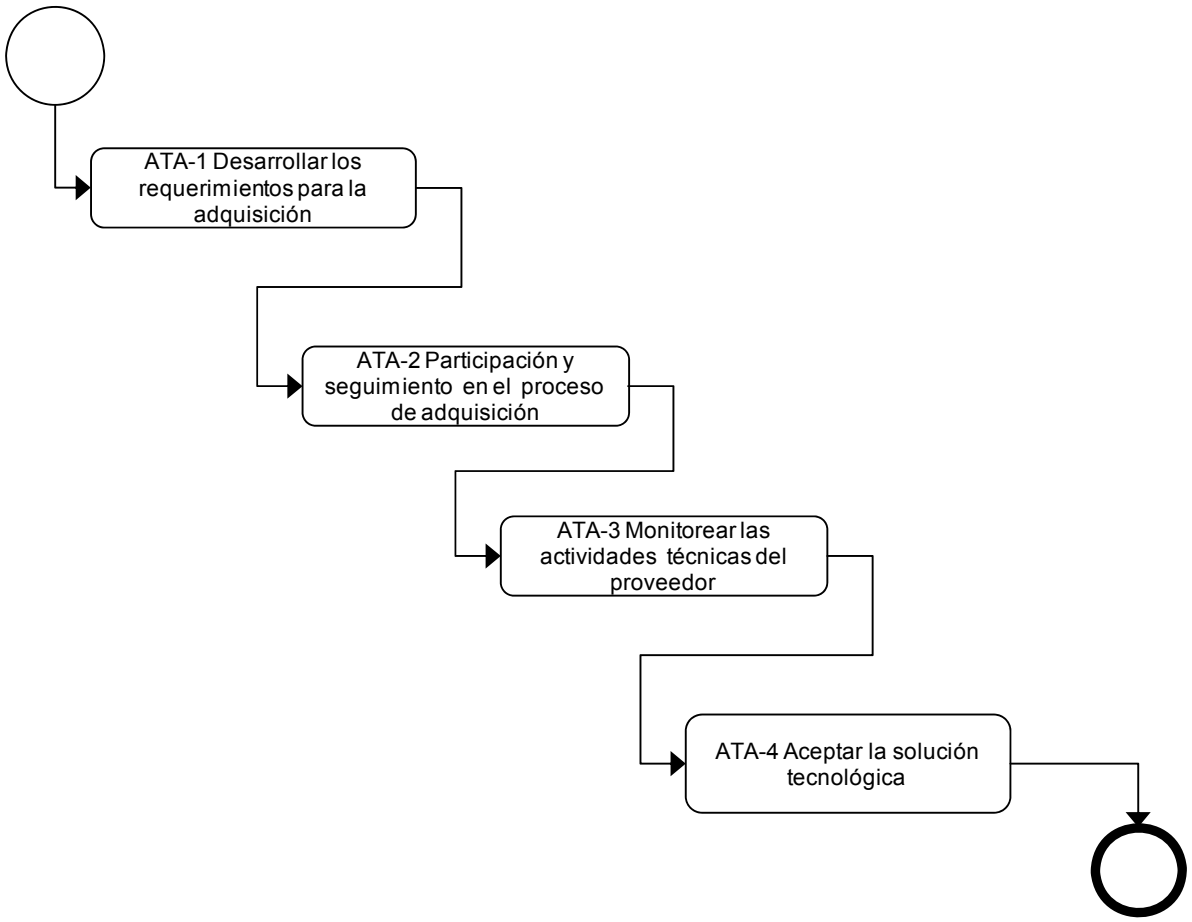


Diagrama de flujo de actividades



7.7.1.2.2 Descripción de las actividades del proceso

ATA-1 Desarrollar los requerimientos para la adquisición

Descripción	Identificar las necesidades y la información relacionada para definir el alcance y las restricciones que servirán como parámetros para desarrollar los anexos técnicos
Factores Críticos	1. Identificar las necesidades de las áreas usuarias. 2. Priorizar los requerimientos para la adquisición. • Priorizar requerimientos de la solución tecnológica y/o servicios, ó en caso de ser requerido un ajuste de alcance por diversos factores como tiempo, costo y/o calendario. • Definir criterios generales y específicos de aceptación para definir cuando se considera cubierta la funcionalidad de una solución tecnológica y/o servicio adquirido. 3. Establecer y mantener los términos y condiciones a partir de los requerimientos para la adquisición acordados con las Áreas usuarias. • Definir la especificación de los requerimientos de soluciones tecnológicas y/o servicios. • Definir los métodos a través de los cuales se corroborará la (s) entrega (s) de la solución tecnológica y/o servicios así como el cumplimiento de los requerimientos técnicos así como los, términos y condiciones especificados. 4. Analizar y validar los requerimientos para asegurarse que son necesarios y suficientes para cubrir las necesidades identificadas. • Asegurarse que los requerimientos definidos cubren todos los escenarios operacionales necesarios para solventar la necesidad, así como que se encuentren definidos y documentados los métodos de operación de la solución y/o servicio. • Identificar y analizar los posibles riesgos en los requerimientos definidos, así como las estrategias de mitigación y/o contingencia de los mismos. 5. Desarrollar Anexo Técnico • Proporcionar a la Unidad responsable de adquisiciones los requerimientos técnicos de la adquisición y colaborar con un enfoque técnico en el desarrollo de la estrategia de adquisición. • Colaborar en la selección de posibles proveedores a ser invitados para solucionar los requerimientos, y proporcionar información desde el punto de vista técnico identificando la capacidad de los Proveedores.
Relación de productos	• Anexo técnico • Términos y condiciones • Estudio de mercado

ATA-2 Participación y seguimiento en el proceso de adquisición

Descripción	Colaborar en el seguimiento del proceso de adquisición de la solución tecnológica y/o servicio de acuerdo a las especificaciones del contrato.
Factores Críticos	1. Validar las pre-bases para la adquisición. • Revisar la consistencia entre los requerimientos de la solución tecnológica y/o servicio, y los términos y condiciones. 2. Realizar la evaluación identificando la propuesta técnica más apropiada conforme a los requerimientos definidos y que cubra con las restricciones establecidas. 3. Realizar el reporte de avance del proceso de adquisición con respecto a la propuesta técnico económica del proveedor. 4. Actualizar la matriz de rastreo y trazabilidad del contrato.
Relación de productos	• Reportes de avances del proveedor • Matriz de rastreo y trazabilidad del contrato • Prebases (revisadas) • Dictamen técnico-económico de las propuestas recibidas • Documento de aclaración • Contrato revisado

ATA-3 Monitorear las actividades técnicas del proveedor

Descripción	Dar seguimiento constante a la ejecución de la solución tecnológica elegida y verificar el cumplimiento de los acuerdos establecidos.
Factores Críticos	1. Revisiones de avances con el proveedor: • Revisar el cumplimiento de los términos y condiciones establecidos con el proveedor para el desarrollo de la solución tecnológica. • Registrar los avances, problemas y riesgos detectados en la construcción de la solución tecnológica adquirida, así como su seguimiento correspondiente. • Mantener un registro del estatus, acciones preventivas/ correctivas tomadas, responsabilidades y resultados obtenidos. 2. Monitorear los procesos seleccionados del proveedor • Seleccionar procesos a ser monitoreados • Planear y ejecutar revisiones periódicas a los procesos seleccionados para asegurar el cumplimiento con los requerimientos establecidos en el acuerdo. • Analizar los resultados del monitoreo de los procesos seleccionados con el objetivo de detectar tempranamente cualquier riesgo que pueda afectar las habilidades del proveedor para satisfacer los requerimientos establecidos en el acuerdo. 3. Ejecutar revisiones de cumplimiento con los requerimientos contractuales • Revisar el cumplimiento de los requerimientos a través de la matriz de rastreo y trazabilidad del contrato, para así poder mapear y controlar los requerimientos

	contra los productos entregados. • Utilizar la información contenida en el contrato como criterios de revisión. • Registrar el cumplimiento con los términos y condiciones o en su caso incumplimientos que se han presentado. • Informar los resultados de las revisiones, al proveedor y al responsable de las adquisiciones de TIC para que en caso de aplicar ejecuté las penalizaciones correspondientes.
Relación de productos	• Reporte de avances del proveedor • Matriz de rastreo y trazabilidad del contrato • Resultado de las revisiones • Reporte de revisiones de procesos

ATA-4 Aceptar la solución tecnológica

Descripción	Asegurarse que la solución adquirida cumple técnicamente con los requerimientos y acuerdos establecidos en el contrato.
Factores Críticos	1. Validar la solución tecnológica. • Revisar la solución tecnológica entregada contra los términos y condiciones establecidos en el contrato. • Formalizar el cumplimiento de la solución tecnológica con respecto a lo establecido en el contrato. • Comunicar los resultados de las actividades a los involucrados. 2. Elaborar la carta de aceptación de la solución tecnológica. • La carta de aceptación de la solución tecnológica deberá ser presentada al proveedor y al área responsable de la facturación y pago para que procedan con las acciones correspondientes. • Se deberá de referir a las garantías especificadas en el contrato.
Relación de productos	• Carta de aceptación de la solución tecnológica • Matriz de rastreo y trazabilidad del contrato

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.7.1.2.3 Descripción de roles

Rol	Descripción
Analista de requerimientos para la adquisición	Realiza el levantamiento de requerimientos por medio de la definición del alcance de la funcionalidad requerida para el producto o servicio a adquirir, así como los aspectos necesarios externos e internos, asociados al requerimiento o necesidad. Identifica los criterios de verificación y validación para los productos/ servicios adquiridos.

Líder técnico para la adquisición	Es responsable de la elaboración y seguimiento del plan de adquisición de producto/ servicio, asignación de los recursos y prioridades a las actividades del proyecto. Deberá coordinar todas las actividades asociadas del proyecto tales como control de avance, medición y análisis, solución de problemas, administración de riesgos, etc. La persona responsable de la ejecución del proyecto debe tener habilidades de liderazgo y conducción de equipos, Debe conocer del dominio de la aplicación y conocer el proceso que se utilizará para la adquisición, es decir, las técnicas de análisis, diseño e implementación y conocimiento de los estándares organizacionales aplicables al proyecto. Debe de tener capacidad de análisis para evaluar técnicamente las soluciones provistas por los proveedores, así como solventar cualquier duda con respecto a los requerimientos técnicos de la solicitud hecha a los proveedores.
Responsable de aseguramiento de calidad	Es el responsable de revisar y supervisar las soluciones tecnológicas y las actividades para verificar que cumplan los estándares y procedimientos aplicables, y proveer los resultados de esas revisiones al Líder técnico para la adquisición. Ayudará a asegurar que los planes, estándares y procedimientos que se han definido sean adecuados para las necesidades del proyecto y a verificar que sean utilizables para la ejecución de revisiones a lo largo del ciclo de vida del proyecto.
Usuario	Dependencia y/o Entidades, persona, entidad externa o interna que dará uso a los resultados y beneficios generados por el proyecto de TIC.
Unidades responsables	Las personas unidades administrativas y dependencias o entidades, que tienen la necesidad a ser cubierta y son los beneficiados con la adquisición de productos o servicios.

7.7.1.2.4 Descripción de productos

Producto	Descripción
Términos y Condiciones	Es el conjunto de especificaciones de la solución tecnológica y/o servicio según sea el caso 1. Garantía 2. Soporte a fallas 3. Actualizaciones 4. Especificaciones no funcionales 5. Especificaciones de operación 6. Tiempos de respuesta 7. Niveles de servicio • Penalizaciones aplicables • Condiciones de pago Que deberán ser incorporados a los compromisos contractuales que se deriven de la adquisición de la solución tecnológica y/o servicio.
Anexo técnico	Recopila la especificaciones técnicas de la solución tecnológica y/o servicio a adquirir, en la cual se especifican: 1. Requerimientos funcionales

Producto	Descripción
	2. Requerimientos operacionales 3. Requerimientos no funcionales 4. Requerimientos de Arquitectura 5. Restricciones e interfaces con otros elementos
Reporte de revisiones de procesos	Este documento es el resultado de la revisión de los procesos seleccionados del proveedor, en él que deberán de registrarse: 1. Proceso revisado 2. Fechas de revisión 3. Revisor 4. Criterios para la revisión 5. Hallazgos detectados 6. Estado de los hallazgos 7. Impacto y prioridad
Reporte de resultados de revisiones	Es un informe que se presenta para reportar los avances en el desarrollo de las actividades del proveedor, en el cual se refleja el cumplimiento o no cumplimiento de los acuerdos establecidos. 1. Compromisos planeados por cumplir en el periodo 2. Compromisos cumplidos en el periodo 3. Asuntos y su estatus 4. Riesgos y su estatus
Matriz de rastreo y trazabilidad del contrato.	Es el documento que permite relacionar los requerimientos, con los términos y condiciones, así como con los niveles de servicios establecidos en el contrato, de igual forma contiene información necesaria para poder relacionar los requerimientos con los productos entregados y los criterios de aceptación establecidos para asegurar la calidad del producto entregado.
Carta aceptación de la solución tecnológica	Es el documento que avala que la solución tecnológica adquirida fue entregada y satisface plenamente los requerimientos definidos. 1. Nombre y firma del responsable técnico de la verificación. 2. Nombre y firma del responsable de la aceptación de la solución tecnológica adquirida. 3. Fecha 4. Características de la solución tecnológica adquirida 5. Entregables recibidos.
Reportes de avances del proveedor	Reporte con el indicador de nivel de cumplimiento del proveedor contra los requerimientos

Producto	Descripción
Estudio de Mercado	Investigación concluyente que tiene como objetivo principal la descripción legal, económica, tecnológica y de infraestructura

7.7.1.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
ICR	Reducir la desviación del producto respecto a la especificación original	Medir el cumplimiento de requerimientos	Eficacia	De gestión	(Requerimientos del producto que cumplen especificaciones) / Requerimientos solicitados)	UTIC	Trimestral
DDP	Reducir los defectos encontrados por requerimientos	Medir densidad de defectos en pruebas	Eficacia	De gestión	Requerimentos com defectos encontrados / Requerimientos	UTIC	Trimestral
IRAT	Medir la desviación en la entrega de requerimientos	Medir Requerimientos atendidos a tiempo	Eficacia	De gestión	Requerimientos atendidos a tiempo / Requerimientos entregados	UTIC	Trimestral

7.7.1.4 Reglas del proceso

1.1	Las actividades para la adquisición de productos y/o servicios deberán ser planeadas y monitoreadas formalmente, en base a la Especificación de requerimientos de soluciones tecnológicas (ERST).
1.2	Todas las actividades para la adquisición de productos o servicios deberán realizarse con apego a la Ley de adquisiciones, arrendamientos y servicios del sector público y su Reglamento, así como los marcos regulatorios aplicables a la dependencia o entidad.
1.3	Para la aplicación del pago y la facturación de productos y/o servicios se deberá de contar con la respectiva carta de aceptación de producto
1.4	Las dependencias y entidades en relación a la adquisición, desarrollo e intercambio de software, sistemas y aplicativos, considerarán por igual, a las soluciones comerciales, propietarias, libres o de código abierto, debiendo considerar en su evaluación las mejores prácticas y el nivel de valor que ofrezcan a la dependencia, en ahorros, mitigación de riesgos, o mejoras del servicio al usuario.
1.5	Los nuevos desarrollos de software, sistemas o aplicativos, que efectúen las UTIC de las dependencias y entidades, deberán ser inscritos en el Instituto Nacional del Derecho de Autor, en un plazo de 45 días naturales después de su liberación, siendo la dependencia o entidad la propietaria de tales derechos.
1.6	Deberá preverse la condición de la disposición anterior en los contratos que para efectos del software, sistemas o aplicativos se realicen.

1.7	La adquisición y el desarrollo de software, sistemas y/o aplicativos deberá efectuarse considerando la arquitectura tecnológica definida por la UTIC; deberán quedar asentados en el dictamen técnico correspondiente a la adquisición o al desarrollo que se trate.
1.8	La UTIC deberá asegurarse de inscribir el proyecto de adquisición y/o desarrollo de software, sistemas y/o aplicativos en el PETIC, en el portafolio de proyectos de la UTIC y/o en el apartado que corresponda al Plan estratégico de tecnologías de la información y comunicaciones de la dependencia o entidad.
1.9	Como parte de la metodología de desarrollo de sistemas y aplicativos que las áreas responsables de la UTIC utilicen para la adquisición, desarrollo o mantenimiento de software, sistemas y/o aplicativos, deberán someter a todo módulo o componente desarrollado o adquirido a pruebas unitarias, de integración, de funcionalidad, de volumen, de aceptación del usuario y de seguridad y toda aquella prueba que asegure la calidad de la solución tecnológica.
1.10	Las UTIC deberán asegurarse de que las áreas requirentes de la adquisición o desarrollo de software, sistemas y/o aplicaciones los desarrollos tomen la responsabilidad de proporcionar los elementos necesarios que apoyen el desarrollo del sistema (documentación, bases de datos, desarrollos previos, etcétera) cumpliendo con los tiempos establecidos en los planes de trabajo.
1.11	Para todos los casos en los que se integren o adicionen componentes de software, sistemas y/o aplicativos a un sistema, se deberán ejecutar pruebas integrales de funcionalidad, para asegurar la preservación de las funciones ya existentes
1.12	Las áreas responsables de la adquisición de un software sistema y/o aplicativo o que haya desarrollado o dado mantenimiento a éstos deberán documentar la liberación de éste para uso del área responsable de la operación.
1.13	Toda adquisición de soluciones tecnológicas debe de estar sustentada a través de un caso de negocio.
1.14	Toda adquisición debe de estar consolidada a nivel de la UTIC de cada dependencia de acuerdo al portafolio de proyectos.
1.15	Toda adquisición de soluciones deberá de observar los lineamientos de seguridad emitidos por la UTIC de la dependencia.
1.16	Se deberá de incluir la especificación de los requerimientos de seguridad establecidos tanto en la política de seguridad como en las políticas de nivel medio relacionadas al desarrollo seguro de soluciones tecnológicas.
1.17	Se deberán de realizar verificaciones y validaciones a los productos y soluciones tecnológicas adquiridas por equipos independientes a los involucrados en la ejecución o elaboración de los productos y soluciones tecnológicas.
1.18	Se deberán de realizar verificaciones y auditorias para asegurar el cumplimiento de los procesos establecidos y de acuerdo a los términos y condiciones especificados en el contrato. Estas verificaciones y auditorias deberán de ser realizadas por equipos independientes a los involucrados en la ejecución de los procesos.
1.19	La plataforma de cómputo y de comunicaciones, el software de desarrollo y de ejecución, así como la configuración sobre la cual operarán las soluciones tecnológicas y aplicativos adquiridos o desarrollados deberá ser aprobada por el Titular de la UTIC, a fin de conservar asegurar el rendimiento y los tiempos de respuesta de las plataformas mencionadas y de las redes de comunicaciones.
1.20	La UTIC deberá asegurarse de inscribir el proyecto de adquisición y/o desarrollo de software, sistemas y/o aplicativos en el PETIC, en el portafolio de proyectos de la UTIC y/o en el apartado que corresponda al Plan estratégico de tecnologías de la información y comunicaciones de la dependencia o entidad.
1.21	Las UTIC que requieran efectuar adquisiciones de software, sistemas y/o aplicativos deberán efectuar éstas previa evaluación técnica y aprobación por el o las áreas de la UTIC facultadas.

1.22	Las UTIC que requieran efectuar adquisiciones de software, sistemas y/o aplicativos solicitadas por usuarios deberán efectuar éstas previa evaluación y aprobación de la funcionalidad solicitada. La solicitud aprobada por parte del usuario deberá ser por escrito y por personal facultado.
1.23	Para el caso de las adquisiciones de software, sistemas y/o aplicativos, independientemente de que no requieran personalización, deberán ser sometidos a pruebas de volumen, de estrés e integrales de funcionalidad, en los ambientes de pruebas de la UTIC hasta asegurar su correcta funcionalidad, reunir las evidencias necesarias y suficientes para que éstas sean aprobadas por el personal de la UTIC y del área usuaria, debiéndose obtener en ambos casos aprobación escrita.

7.7.1.5 Documentación soporte del proceso

No aplica

7.7.2 Desarrollo de soluciones tecnológicas

7.7.2.1 Objetivos del proceso

General.-

Realizar las actividades para la construcción de una solución tecnológica, incluyendo la especificación de los requerimientos, el diseño, el desarrollo, la verificación, la validación y la integración de los componentes o productos necesarios para su entrega.

Específicos.-

1. Especificar los requerimientos
2. Desarrollar los requerimientos
3. Especificar el diseño de la solución tecnológica
4. Administrar los cambios de requerimientos
5. Administrar el ambiente de la configuración y cambios en los componentes de la solución tecnológica
6. Desarrollar y construir los componentes de la solución tecnológica.
7. Verificar y validar los componentes de la solución tecnológica, en coordinación con el proceso de calidad de soluciones tecnológicas.
8. Integración de los componentes y entrega de la solución tecnológica.

7.7.1.2 Descripción del proceso

7.7.1.2.1 Mapa general del proceso

Diagrama de flujo de información

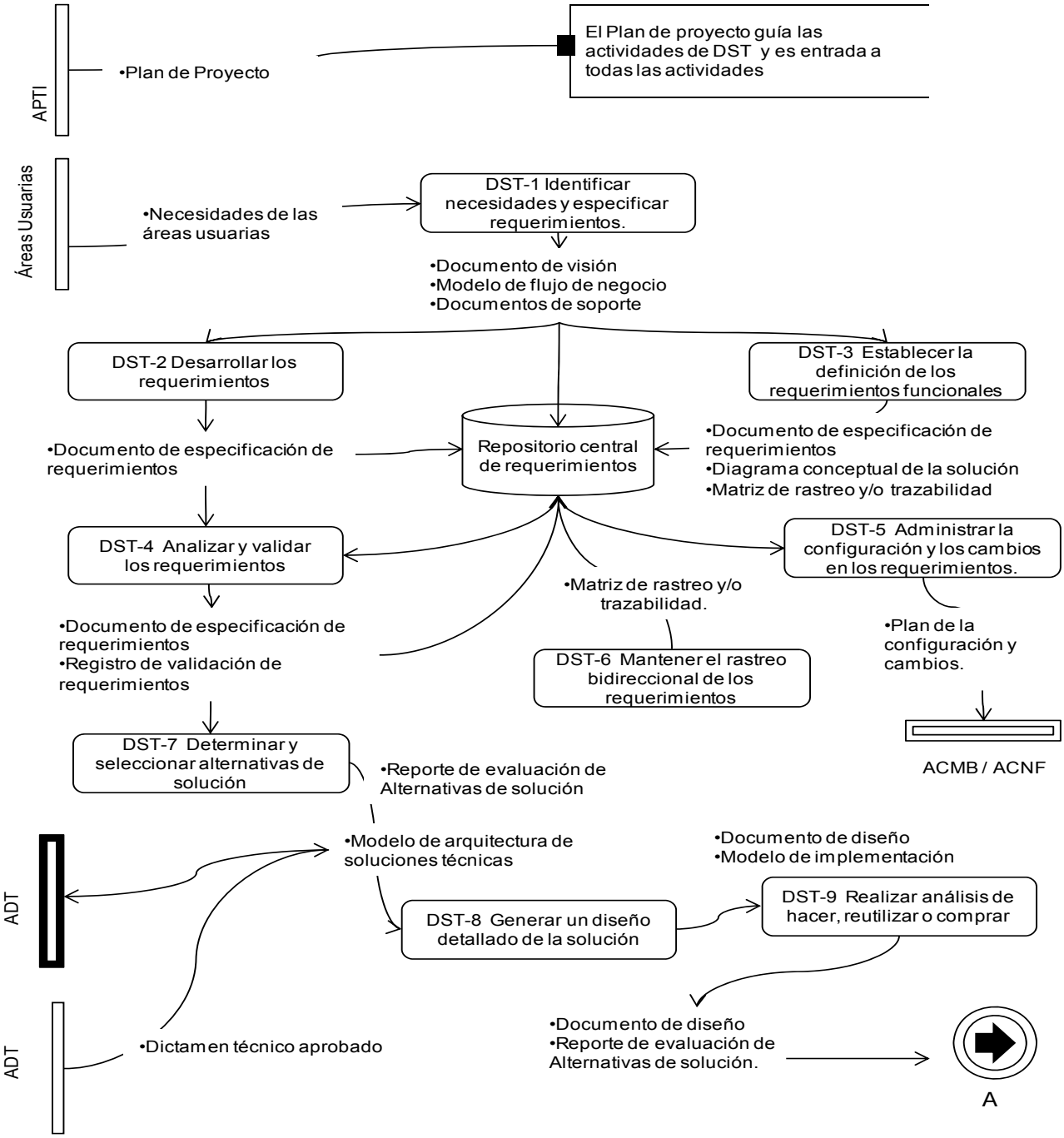


Diagrama de flujo de información

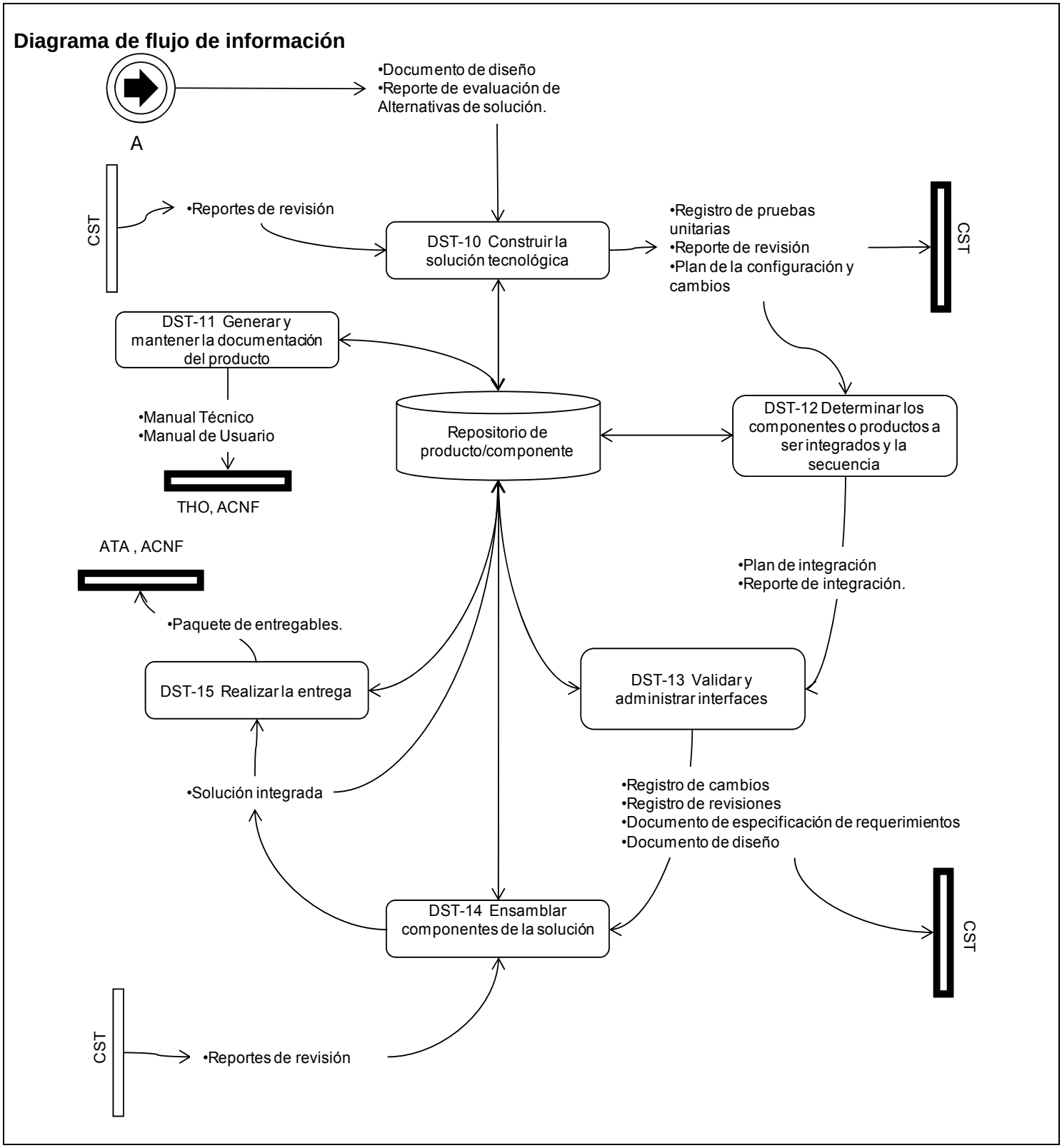
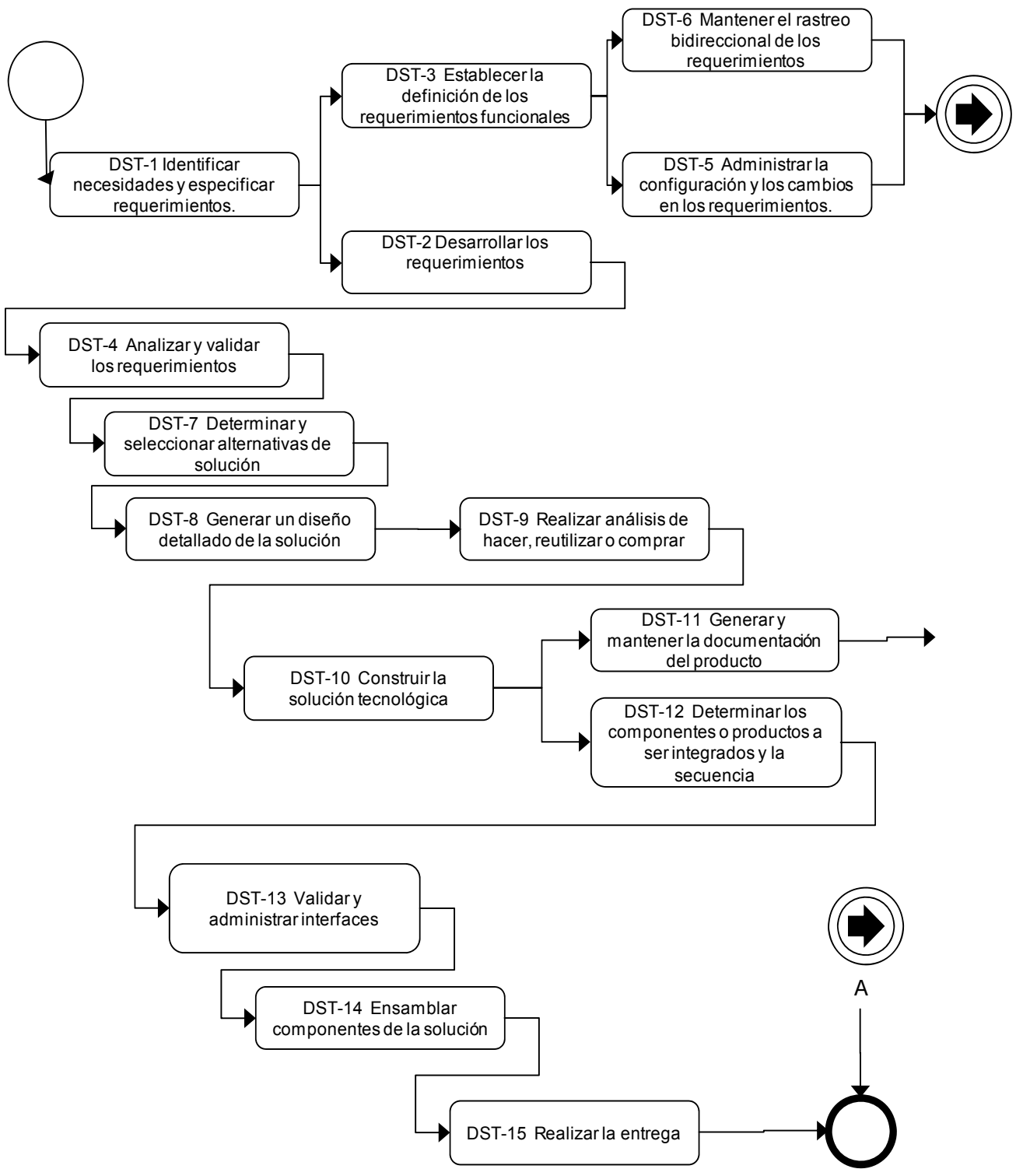


Diagrama de flujo de actividades



7.7.2.2.2 Descripción de las actividades del proceso

DST-1 Identificar necesidades y especificar requerimientos.

Descripción	Identificar las necesidades, expectativas, restricciones e interfaces para cada una de las fases del ciclo de vida de la elaboración de la solución tecnológica y especificar los requerimientos de manera detallada.
Factores Críticos	1. Identificar, modelar y recopilar las necesidades de las áreas usuarias. • Identificación y modelación de las necesidades a partir del análisis de las funciones sustantivas de la dependencia o entidad, las necesidades de automatización del proceso que mejoren la operación diaria y los servicios que se brinda a la ciudadanía. • Las necesidades específicas deberán ser proporcionadas por el área que hace el requerimiento, quien, para su solicitud, deberá considerar el marco normativo (leyes, reglamentos, estándares, reglas de negocio, procedimientos, etc.) que incidirá en la solución. • Identificar y documentar las expectativas y restricciones que pudieran estar presentes. • El detalle de las necesidades puede ser obtenido mediante técnicas tales como: entrevistas, cuestionarios, prototipos, etc. 2. Especificar los requerimientos. • Traducir las necesidades identificadas en requerimientos específicos. • Documentar, revisar y validar con las áreas usuarias los requerimientos específicos. 3. Generar la visión • Documentar la visión de la solución tecnológica que solventará las necesidades especificadas así como los requerimientos específicos a alto nivel.
Relación de productos	• Documento de visión • Modelo de flujo de negocio • Documentos de soporte

DST-2 Desarrollar los requerimientos.

Descripción	Establecer, mantener y asociar los componentes o productos asociados a los requerimientos del Usuario.
Factores Críticos	1. Desarrollar los requerimientos. • Analizar la información de las necesidades de las áreas usuarias. • Especificar y detallar los requerimientos y características de la solución tecnológica. • Identificar los requerimientos necesarios para cada producto o componente de la solución identificado, realizando el diseño de la arquitectura, asociando las características de calidad del producto, así como las características de rendimiento, capacidad y disponibilidad necesarias. • Registrar la trazabilidad de los requerimientos en el ciclo de desarrollo. 2. Identificar interfaces externas e internas. Identificar requerimientos funcionales y/o no funcionales resultado del diseño de la arquitectura, y documentarlos en términos técnicos para su posterior desarrollo 3. Establecer las relaciones entre los requerimientos. • Con el fin de considerarlos durante su asociación, así como, los cambios que surjan durante el ciclo de vida del desarrollo del componente o producto 4. Facilitar la gestión de las necesidades y requerimientos bajo un entorno de colaboración.

Relación de productos	• Documento de especificación de requerimientos

DST-3 Establecer la definición de los requerimientos funcionales.

Descripción	Establecer y mantener la descripción de la funcionalidad de la solución tecnológica.
Factores Críticos	1. Analizar y especificar los requerimientos funcionales La definición de la funcionalidad en ocasión referida como "Análisis funcional", es la descripción de "lo que el producto debe de hacer". La definición de la funcionalidad puede incluir acciones, secuencias, entradas, salidas, o cualquier otra información que comunique la forma en que el producto deberá de ser usado. 2. Generar grupos de requerimientos basados en criterios establecidos, (funcionalidades similares) para facilitar y enfocar el análisis de los requerimientos. 3. Considerar la secuencia y ruta critica de las funciones, desde su inicio y su secuencia durante el desarrollo de los componentes. • Considerar la simulación del requerimiento como un mecanismo de apoyo para la definición del requerimiento • Asociar los requerimientos a grupos de funcionalidades, objetos y/o componentes. 4. Asociar los requerimientos funcionales y no funcionales a funciones o sub funciones.
Relación de productos	• Documento de especificación de requerimientos • Diagrama conceptual de la solución • Matriz de rastreo y/o trazabilidad

DST-4 Analizar y validar los requerimientos.

Descripción	Analizar los requerimientos para asegurar que son los necesarios y suficientes, que están asociados y corresponden con las necesidades y restricciones descritas por los involucrados. Así como, validarlos para asegurar que el producto resultado se podrá ejecutar en los ambientes especificados de operación de acuerdo a como se contempla en su definición.
Factores Críticos	1. Analizar los requerimientos y determinar cuáles de ellos satisfacen los objetivos o los requerimientos de alto nivel. 2. Analizar los requerimientos y asegurar que están completos, son factibles de realizar y pueden ser verificados, además de realizar los escenarios de prueba. 3. Identificar los requerimientos clave, los cuales tienen una fuerte influencia en costo, tiempo, funcionalidad, riesgo o de rendimiento. 4. Identificar los indicadores de rendimiento que serán monitoreados durante el desarrollo de la funcionalidad. 5. Analizar los conceptos de la operación y los escenarios para adecuar las necesidades del Usuario, las restricciones, y las interfaces y con ello descubrir nuevos requerimientos. 6. Establecer la simulación del modelo operacional, facilitando el entendimiento y corroboración de la necesidad por parte del usuario mediante el requerimiento funcional propuesto.

	7. Analizar los requerimientos y balancear entre las necesidades del Usuario y las restricciones (tiempo, costo, recursos tecnológicos y/o humanos, etc.). 8. Realizar una evaluación de los riesgos de los requerimientos. 9. Analizar los requerimientos para determinar el riesgo de que el producto resultado no pueda ejecutarse apropiadamente en el ambiente propuesto. 10. Todos los requerimientos deberán de ser validados y aprobados por los participantes en su definición, la aprobación deberá de documentarse y resguardarse.
Relación de productos	• Documento de especificación de requerimientos • Registro de validación de requerimientos

DST-5 Administrar la configuración y los cambios en los requerimientos.

Descripción	Administrar los activos asociados a la solución y las solicitudes de cambios en los requerimientos a lo largo del ciclo de vida del desarrollo de la solución tecnológica mediante la documentación del análisis, evaluación del impacto en términos técnicos, tiempo, costo y esfuerzo, así como los riesgos asociados con dichos cambios.
Factores Críticos	1. Identificar los componentes y productos que estarán bajo configuración. 2. Establecer líneas base de los componentes y productos identificados. 3. Establecer un ambiente para la administración de los requerimientos, sus cambios y rastreabilidad. 4. Establecer los estatus asociados a los componentes y productos para la administración de los cambios. 5. Identificar los cambios en los requerimientos. ▪ Registrar todas las solicitudes de cambios (ver el proceso ACMB). 6. Analizar y evaluar el impacto de los cambios, haciendo uso de los registros de rastreo y trazabilidad bidireccional de los requerimientos, y comunicarlos a los involucrados relevantes. 7. Revisar, autorizar y/o rechazar las solicitudes de cambio. 8. Actualizar los planes de trabajo en caso de ser necesario. 9. Administrar la configuración de los productos afectados por los cambios. 10. Administrar las solicitudes de cambio hasta su incorporación o cierre. 11. Verificar que los cambios realizados sean los especificados en la solicitud de cambios y evaluar el cambio realizado.
Relación de productos	• Plan de la configuración y cambios

DST-6 Mantener el rastreo bidireccional de los requerimientos

Descripción	Mantener un registro de rastreo bidireccional entre los requerimientos y los componentes de la solución a lo largo de todo el ciclo de vida de la solución.
Factores Críticos	1. Mantener un registro de rastreo entre los requerimientos y los diversos elementos que componen la solución tecnológica. • La Matriz de rastreo y/o trazabilidad debe contener información relativa a la relación entre las necesidades, los requerimientos, los módulos, los componentes, los objetos, productos, procesos y versiones de los productos de trabajo de la solución. • Considerar el rastreo de las relaciones tanto en forma horizontal como vertical, así como a través de las interfaces. 2. Realizar y mantener una matriz de rastreo y/o trazabilidad. • La Matriz de rastreo y/o trazabilidad deberá ser creada desde el inicio de la solución y se deberá mantener actualizada a lo largo de todo el ciclo de vida. • La Matriz de rastreo y/o trazabilidad deberá ser utilizada para el análisis de impacto cuando se presenten solicitudes de cambio. • La Matriz de rastreo y/o trazabilidad deberá de ser periódicamente verificada de acuerdo a la planificación de la solución tecnológica.
Relación de productos	• Matriz de rastreo y/o trazabilidad.

DST-7 Determinar y seleccionar alternativas de solución

Descripción	Analizar e identificar alternativas de solución así como criterios de selección, para contar con un medio que cumpla con los requerimientos establecidos y que esté balanceada en términos de costo, tiempo y rendimiento.
Factores Críticos	1. Definir criterios de evaluación para seleccionar un conjunto de alternativas de solución para ser consideradas. 2. Identificar tecnología actualmente en uso y/o nuevos productos en el mercado con ventajas competitivas. 3. Identificar productos o componentes existentes candidatos disponibles que satisfagan los requerimientos. 4. Generar alternativas de solución. 5. Realizar una asociación de cada una de las alternativas para cada requerimiento. 6. Analizar posibles cambios en los requerimientos basados en las alternativas de solución. 7. Determinar los criterios para la selección de la mejor alternativa de solución. 8. Documentar la selección, las evaluaciones y aprobación de la misma.
Relación de productos	• Reporte de evaluación de Alternativas de solución • Modelo de arquitectura de soluciones técnicas

DST-8 Generar un diseño detallado de la solución

Descripción	Generar el diseño detallado de la solución, esto incluye la arquitectura, el diseño funcional, el diseño de interfaces, las estructuras de datos, las relaciones entre los componentes y/o objetos y flujos de información necesarios.
Factores Críticos	1. Identificar y adoptar los métodos de diseño apropiados para cada tipo de solución. 2. Determinar las capas de diseño y el nivel apropiado para la generación de la documentación de cada capa. 3. Desarrollar el Diseño de la solución. • El diseño de componentes o productos proveen el contenido apropiado no sólo para la fase de implementación o desarrollo, sino también para las etapas subsecuentes del ciclo de vida del producto, tales como, mantenimientos, migraciones, reinstalaciones, etc. • La documentación del diseño debe ser generada en términos técnicos y debe incluir las características y los parámetros necesarios, incluyendo: tamaños, funciones, interfaces, patrones, etc. 4. Asegurar que el diseño se apega a los estándares y criterios establecidos 5. Asegurar que el diseño se apega a los requerimientos definidos y aprobados. 6. Generar un compendio de documentos técnicos que permitan comprender el diseño y realizar las actividades necesarias para el mantenimiento de la solución. 7. Identificar las interfaces asociadas con otros componentes o productos, así como con entidades externas. 8. Aplicar criterios establecidos para el diseño de las interfaces. 9. Documentar el diseño con sus capas, paquetes e interfaces, incluyendo las razones de la decisión de la alternativa seleccionada.
Relación de productos	• Documento de diseño • Modelo de implementación

DST-9 Realizar análisis de hacer, reutilizar o comprar.

Descripción	Analizar y evaluar que elementos o componentes de la solución requieren ser desarrollados y cuáles pueden ser reutilizados o comprados.
Factores Críticos	1. Establecer criterios de decisión para el reuso o adquisición de componentes de diseño, así como establecer el método de análisis y valoración. 2. Determinar las implicaciones de implementar componentes “no desarrollados” en caso de mantenimiento. 3. Documentar qué elementos y componentes serán reutilizados y cuales serán comprados. • Se deberá documentar en tal caso el resultado de este análisis aún cuando no exista componentes a reutilizar y/o comprar.
Relación de productos	• Documento de diseño

	• Reporte de evaluación de Alternativas de solución.

DST-10 Construir la solución tecnológica

Descripción	Construir la solución tecnológica en base a los requerimientos especificados y a partir de los documentos de diseño.
Factores Críticos	1. Establecer y usar métodos efectivos para la implementación e integración de los componentes y /o productos. 2. Aplicar estándares y criterios establecidos para el desarrollo. 3. Construir los componentes de la solución. 4. Ejecutar pruebas unitarias de los productos o componentes que sean apropiadas. 5. Realizar las revisiones necesarias de productos y componentes. 6. Establecer un ambiente de colaboración para la re-utilización de componentes propios de la construcción de la solución (ver el proceso ACNC). 7. Ejecutar pruebas (ver el proceso CST).
Relación de productos	• Repositorio de producto/componente • Registro de pruebas unitarias • Reporte de revisión • Plan de la configuración y cambios

DST-11 Generar y mantener la documentación del producto

Descripción	Desarrollar y mantener la documentación que va a ser utilizada para realizar la instalación, soportar la operación y dar mantenimiento a la solución tecnológica.
Factores Críticos	1. Generar la documentación de instalación, operación y mantenimiento de la solución tecnológica. 2. Generar la documentación necesaria para el uso de la solución tecnológica por el área usuaria. 3. Aplicar estándares en la generación de la documentación. 4. Realizar revisiones entre colegas de los documentos de instalación, operación y mantenimiento (ver el proceso CST).
Relación de productos	• Repositorio de producto/componente • Manual Técnico • Manual de Usuario

DST-12 Determinar los componentes o productos que serán integrados y su secuencia

Descripción	Establecer la secuencia y los pasos que requieren seguirse para realizar la integración de los

	diversos productos y/o componentes que constituyen la solución tecnológica.
Factores Críticos	1. Identificar los productos o componentes que serán integrados. Pueden existir productos o componentes a ser entregados, la integración puede ser algún elemento externo, accesorios o herramienta de prueba. Una vez analizadas las alternativas de pruebas de la integración y la secuencia de ensamblaje para la integración, se selecciona la mejor secuencia de integración. La integración puede implicar componentes en diferentes fases del ciclo de vida de desarrollo del producto. Se deberá de evaluar la mejor alternativa a llevar a cabo para la integración. 2. Identificar los tipos de verificación que serán ejecutadas durante la integración. 3. Identificar las alternativas de integración y de secuencia. 4. Seleccionar la mejor alternativa para la integración y secuencia, que deberá ser organizada de forma centralizada, con capacidad de documentarse. 5. Seleccionar la mejor alternativa para la integración y su secuencia. 6. Realizar revisiones periódicas de la secuencia de integración y realizar las validaciones necesarias. 7. Registrar las justificaciones de la toma de decisión.
Relación de productos	• Repositorio de producto/componente • Plan de integración • Reporte de integración.

DST-13 Validar y administrar interfaces

Descripción	Revisar y mantener la consistencia de las especificaciones de las interfaces a lo largo de la vida del producto y administrar los cambios a las mismas.
Factores Críticos	1. Identificar y documentar el flujo del proceso de modificación y notificación para la actualización de las interfaces. 2. Revisar las especificaciones de las interfaces manteniendo su registro en forma centralizada y asegurar su actualización en forma periódica. 3. Asegurar la compatibilidad de las interfaces a lo largo de la vida del producto. 4. Verificar el cumplimiento de la interfaces identificadas, así como favorecer la comunicación de los cambios y activos. 5. Administrar los cambios en las especificaciones de interfaces.
Relación de productos	• Repositorio de producto/componente • Registro de cambios • Registro de revisiones • Documento de especificación de requerimientos • Documento de diseño

DST-14 Ensamblar componentes de la solución

Descripción	Asegurar que el ensamblado de los componentes dentro de la solución deberá incorporarse de acuerdo a la secuencia de integración establecida y de acuerdo a los procedimientos estipulados.
Factores Críticos	1. Dar seguimiento al estatus de cada uno de los componentes tan pronto como estén disponibles para realizar la integración. 2. Asegurar que los componentes son liberados al ambiente de integración de acuerdo con la secuencia de integración y los procedimientos disponibles. 3. Confirmar la recepción de cada componente identificado adecuadamente. 4. Asegurar que cada componente recibido cumpla con la descripción correcta. 5. Validar que los componentes cumplan con la configuración establecida. 6. Asegurar la disponibilidad del ambiente de integración. 7. Asegurar que la secuencia de ensamblado es ejecutada de forma adecuada. 8. Seleccionar la mejor alternativa para la integración y secuencia, que deberá ser organizada de forma centralizada, con capacidad de documentarse. 9. Llevar a cabo evaluaciones del ensamblado de los componentes siguiendo la secuencia de integración del producto así como los procedimientos disponibles. 10. Mantener un registro de los resultados de la evaluación.
Relación de productos	• Repositorio de producto/componente • Solución integrada

DST-15 Realizar la entrega

Descripción	Generar un paquete con los productos o componentes ensamblados y realizar la entrega de la solución tecnológica.
Factores Críticos	1. Realizar una revisión de los requerimientos, diseño, productos, resultados de las verificaciones, y de la documentación generada en cada fase del desarrollo del producto. • Para asegurar que los aspectos que puedan afectar el empaquetado y la entrega del producto han sido identificados y resueltos. 2. Usar procedimientos probados para generar el paquete y la entrega del producto ensamblado. 3. Realizar la entrega del producto y la documentación relacionada y confirmar la recepción. 4. Seleccionar la mejor alternativa para la integración y secuencia, que deberá ser organizada de forma centralizada, con capacidad de documentarse.
Relación de productos	• Paquete de entregables

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.7.2.2.3 Descripción de roles

Rol	Descripción
Analista de requerimientos	Ejecuta la obtención de requerimientos por medio de la definición del alcance de la funcionalidad de la solución tecnológica, identificando los roles asociados, así como los aspectos necesarios externos e internos, asociados al requerimiento o necesidad. Detalla los requerimientos funcionales y no funcionales, plasmando en los documentos establecidos el entendimiento.
Arquitecto de soluciones tecnológicas	El Arquitecto es una persona con amplios conocimientos técnicos, conocedor del negocio de los proyectos y que, probablemente, esté asignado a uno o varios proyectos al mismo tiempo. Algunas de sus responsabilidades suelen ser: definir los lineamientos de diseño, su arquitectura y demás cuestiones técnicas de los proyectos.
Diseñador de soluciones tecnológicas	El diseñador realiza las tareas asociadas al diseño de los componentes de las soluciones tecnológicas asociados a los requerimientos, la estructura y relaciones del repositorio, así como, las Interfaces de Usuario.
Administrador de la configuración.	Es responsable de la elaboración y monitoreo y control de la ejecución del plan de la configuración y cambios, así como responsable de revisar el estado de la configuración de los productos y componentes y generar las líneas base que se hayan establecido a lo largo del ciclo de vida de este.
Desarrollador	Es responsable del desarrollo y pruebas de los componentes de la solución tecnológica, acorde con los estándares adoptados en el proyecto, para su integración en subsistemas mayores. Cuando los componentes de pruebas deben ser creados para soportar las pruebas, el desarrollador es también responsable del desarrollo y pruebas de los componentes de pruebas y los correspondientes subsistemas.
Integrador de la solución tecnológica.	Dentro de sus actividades están el confirmar la preparación de los componentes para su integración y ensamblaje, ejecutar pruebas de integración, asegurar el cumplimiento de los estándares para la integración y documentación que comprende, realizar la integración de todos los componentes que se entregan y notificar al finalizar para su entrega.
Ingeniero de pruebas de soluciones tecnológicas	Responsable de ejecutar los escenarios de prueba y dar seguimiento a los defectos de pruebas hasta su cierre, así como llevar la trazabilidad de los casos de prueba.
Revisor	Revisa que los productos y/o entregables generados tengan la calidad esperada, cumplan con los criterios de calidad definidos, y cubran los requerimientos del solicitante, antes de ser entregados; a su vez reporta las inconformidades detectadas y les da seguimiento hasta su cierre.
Unidades responsables	Las personas y organizaciones que tienen algún interés o influencia en los resultados del proyecto o procesos. Los proyectos o procesos tienen más de un interesado y cada uno de ellos tendrá necesidades, expectativas y actividades diferentes.

7.7.2.2.4 Descripción de productos

Producto	Descripción
Documento de especificación de requerimientos	Describe los requerimientos funcionales y no funcionales a detalle de productos o servicios, algunos de los puntos que deben de ser considerados en este documento son: • Situación actual • Solución propuesta • Suposiciones y dependencias • Requerimientos funcionales • Requerimientos no funcionales • Diagrama de flujo del negocio • Reglas del negocio • Glosario de términos
Registro de validación de requerimientos	En este documento se registran los datos asociados a las validaciones de cada uno de los requerimientos, y el involucrado responsable reconoce que un conjunto de entregables se ha realizado de acuerdo a lo establecido y que cumple con lo acordado.
Documento de visión	Define la visión del producto/servicio, se detalla en términos de sus principales necesidades y características. Contiene un panorama general de los requerimientos esenciales, restricciones de la solución tecnológica, además proporciona las bases para establecer el alcance del proyecto y detallar los requerimientos tecnológicos. Los siguientes puntos deben ser considerados en el detalle del contenido del documento: • Definiciones, abreviaturas y referencias • Situación actual • Objetivo • Oportunidades de negocio • Descripción del problema • Identificación de involucrados y unidades responsables • Cobertura y características del ambiente del usuario • Principales necesidades de los involucrados y unidades responsables. • Estándares aplicables • Requerimientos funcionales, características del producto • Requerimientos no funcionales: ▪ Requerimientos del sistema ▪ Requerimientos de desempeño y capacidad ▪ Requerimientos de ambiente • Requerimientos de documentación
Documento de diseño	Describe las realizaciones de las especificaciones de los requerimientos a nivel diseño, sirve como una abstracción del diseño detallado y su código fuente. Se emplea como una entrada esencial para las actividades de implementación y pruebas.

Producto	Descripción
Registro de cambios	Documento o repositorio que contendrá los registros de los todos los cambios detectados durante la ejecución y desarrollo del proyecto o producto, este será de acuerdo al proceso Administración de cambios.
Repositorio central de requerimientos	Espacio físico que permite el almacenamiento del total de las necesidades establecidas para el área usuaria sustantiva, mismo que permite la explotación y administración de los cambios de los mismos, bajo un espacio seguro y controlado en un entorno de colaboración.
Matriz de rastreo y/o trazabilidad	Es una vista que se realiza con el fin de asociar los requerimientos y los productos de trabajo relacionados a los mismos (tales como casos de uso, clases, componentes, casos de prueba, entre otros) a lo largo del ciclo de vida. Esta matriz es importante para identificar las dependencias e inconsistencias que pudieran surgir en los requerimientos; así como para evaluar el impacto de un cambio en los requerimientos. Algunos aspectos que cubre este documento son: • Descripción del requerimiento. • Tipo de requerimiento • Prioridad • Estatus • Producto de trabajo de X nivel (repetible) • Estado del producto de trabajo • Solicitud de cambio asociada
Reporte de evaluación de alternativas de solución.	Contiene el resultado del análisis que se realiza para identificar la mejor opción para la adopción de una solución durante el proyecto, entre los datos que puede contener el documento están: • Responsable del Análisis • Fecha del análisis. • Tipo de análisis • Resultado del análisis. • Listado de criterios de evaluación. • Justificación
Documento de arquitectura	Contiene la información específica del diseño de la solución técnica de la solución, estableciendo la relación con los diversos dominios establecidos por la arquitectura de TI
Modelo de implementación	Representa la composición física de la implementación en términos de Subsistemas y Elementos como: Directorios y archivos, incluyendo código fuente, datos y archivos ejecutables. • Diagramas de actividad. • Diagramas de estados. • Diagramas de componentes. • Diagrama de clases

Producto	Descripción
Registro de pruebas unitarias	Es el documento en donde se especifica si las pruebas unitarias fueron exitosas o si se encontraron defectos.
Registro de pruebas	Es el documento en donde se especifica si las pruebas realizadas fueron exitosas o si se encontraron defectos.
Solución integrada	Es una versión operacional de una solución tecnológica o parte de una.
Registro de las revisiones	Contiene el registro de los defectos encontrados durante las revisiones, revisiones entre colegas y aprobaciones realizadas a los productos de trabajo y productos del proyecto, a su vez se utiliza para dar seguimiento a los defectos hasta su cierre.
Manual de usuario	Contiene la estructura e información acerca de la funcionalidad del sistema. Algunos puntos relevantes que debe considerar este documento son: • Definiciones, abreviaciones y referencias. • Identificación de los usuarios finales del sistema. • Identificación de la funcionalidad del sistema. • Por cada una de las funcionalidades o módulos contemplar: ▪ Condiciones iniciales ▪ Interfaces ▪ Acciones requeridas ▪ Condiciones finales
Manual técnico	Documentación técnica de la solución tecnológica que será utilizada para la instalación, soporte a la operación y el mantenimiento de la solución tecnológica.
Plan de integración	Es el documento que describe las actividades y secuencia para la integración de los componentes de la solución tecnológica.
Paquete de entregables	El documento del compendio de documentación para liberación los ambientes de pruebas de usuario contiene información de la relación de programas que se instalaran.
Plan de la configuración y cambios	Documento donde se plasman la forma de versionar y nombrar los artefactos, así como la definición del o los repositorios de información del proyecto.
Documentos de soporte en la identificación de necesidades	Documentos que ayudaran a obtener y documentar la información de los usuarios que servirán de entrada para la elaboración del Documento de especificación de requerimientos. Incluye entre otros minutas de reunión, cuestionarios, entrevistas, prototipos, etc.
Reporte de revisión	Resultado con el estatus de las revisiones realizadas a la solución tecnológica (productos o componentes) en base a los requerimientos especificados.
Modelo de flujo de negocio	Modelo con las funciones sustantivas de la dependencia o entidad y requerimientos de acuerdo al flujo de negocio a seguir.
Repositorio de productos/ componentes	Espacio físico que permite el almacenamiento de los productos y/o componentes de los productos desarrollados para su resguardo y uso. Este repositorio se deberá encontrar bajo

Producto	Descripción
	control de configuraciones.
Reporte de integración	Documento que detalla la secuencia y forma de integración de los componentes, productos, herramientas o accesorios a entregar.
Repositorio de productos/componentes	Espacio físico que permite el almacenamiento de los productos, y/o componentes de productos desarrollados para su resguardo , consulta y/o reutilización
Manuel técnico	Documentación técnica que va a ser utilizada para la instalación, soporte a la operación y el mantenimiento a la solución tecnológica.

7.7.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Productividad en requerimientos	Mejorar la capacidad y productividad en desarrollo de software	Medir la productividad del grupo al conocer la producción de requerimientos	Eficiencia	De gestión	Requerimientos entregados / Requerimientos planeados	Líder de proyecto	Al cierre del proyecto
Índice de validación	Reducir las no conformidades en validación	Medir la proporción de defectos en la validación	Calidad	De gestión	(Criterios de validación que no cumplen) / Criterios de validación totales	Líder de proyecto	Al cierre del proyecto
Índice de cumplimiento de alcance	Medir el alcance final con respecto a los requerimientos originales	Medir lo requerimiento entregados	Calidad	De gestión	(Requerimientos validados correctamente / requerimientos especificados originalmente	Líder de proyecto	Al cierre del proyecto
Índice de cambios en requerimientos	Reducir los cambios realizados en los requerimientos durante el proyecto	Medir los cambios realizados a los requerimientos originales	Calidad	De gestión	Requerimientos con cambios/ Requerimientos originales	Líder de proyecto	Al cierre del proyecto

7.7.2.4 Reglas del proceso

1.1	El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurar que las necesidades de negocio que motivan el desarrollo de soluciones tecnológicas esten claramente identificadas y documentadas
1.2	Las especificaciones de los requerimientos de las soluciones tecnológicas deben estar alineadas a las necesidades de negocio identificadas El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurarse de inscribir el proyecto de adquisición y/o desarrollo de software, sistemas y/o aplicativos en el PETIC,

	en el portafolio de proyectos de la UTIC y/o en el apartado que corresponda al Plan Estratégico de Tecnologías de la Información y Comunicaciones de la dependencia o entidad.
1.3	El desarrollo de soluciones tecnológicas debe de realizarse de acuerdo a lo especificado en el presente manual.
1.4	Las soluciones tecnológicas deben estar alineadas a la arquitectura de aplicaciones de la dependencia o entidad.
1.5	El desarrollo de soluciones solamente podrá ser ejecutado cuando se haya confirmado que no existen productos comerciales en el mercado con una funcionalidad similar a la requerida por el área solicitante y cuando se haya validado y demostrado que no existen aplicaciones de software dentro de la APF que puedan satisfacer las necesidades del área usuaria.
1.6	El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurar que los requerimientos de las unidades responsables y los requerimientos técnicos de la solución tecnológica sean identificados, documentados y validados, para todo desarrollo a efectuarse.
1.7	El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurar que se realice una evaluación de las diversas alternativas de solución mediante un proceso estructurado de toma de decisiones, para todo desarrollo a efectuarse
1.8	El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurar que se genera y documenta el diseño de la solución tecnológica, para todo desarrollo en curso.
1.9	El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurar que reestablecen criterios de aceptación y procedimientos de verificación y validación que permitan asegurar que la solución tecnológica no presenta defectos y funciona correctamente, para todo desarrollo en curso.
1.10	El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurar que se establecen procedimientos documentados para realizar la integración de los productos y/o componentes de la solución tecnológica, para todo desarrollo en curso.
1.11	El administrador del proceso de desarrollo de soluciones tecnológicas deberá asegurar que toda solución tecnológica desarrollada, integrada y validada siga los procesos del grupo de Transición y Entrega.

	Reglas de aplicación a procedimientos regidos por el proceso
	Previo al inicio del desarrollo de cualquier software (sistema, aplicativo, componente), ya sea por desarrollo interno, o bajo contrato, se deberá contar con la autorización escrita del Titular de la UTIC o responsable facultado y el dictamen correspondiente.
	Las UTIC deberá evaluar el software, sistemas o aplicativos que utilizará en sus procesos o proyectos, conforme a los siguientes criterios: a). que satisfaga las necesidades de la dependencia o entidad; b). la capacidad y calidad del software, sistema o aplicativo para integrarse a otros sistemas existentes en operación; c). la interoperabilidad con otros sistemas de las dependencias o entidades, y el costo inicial y el costo de su implantación, mantenimiento y soporte a lo largo de su vida útil.
	La UTIC deberá asegurar que, desde la conceptualización en el proceso de desarrollo, el software, sistemas o aplicativos que estén orientados a funcionarios de la dependencia o entidad, sean accedidos como mínimo mediante un hipervínculo a la Intranet o Portal de la dependencia o entidad .
	La UTIC deberá asegurar que, desde la conceptualización en el proceso de desarrollo, el software, sistemas o aplicativos que estén orientados a ciudadanos, empresarios o cualquier entidad externa a la dependencia o entidad, sean accedidos como mínimo mediante un hipervínculo al Portal de la dependencia o entidad .
	Todas las áreas que desarrollen, implementen o proporcionen mantenimiento a las soluciones tecnológicas deberán revisar las disposiciones descritas en el presente manual, y será

	responsabilidad la ejecución de los ajustes necesarios para asegurar que las soluciones tecnológicas estén alineadas a las definiciones de desarrollo que se especifiquen en el presente manual.
	Las disposiciones del presente manual aplican para todo sistema que esté en fase de gestión de requerimientos, análisis, diseño, codificación, pruebas, liberación o mantenimiento.
	Las soluciones tecnológicas que estén en producción y cuyo proceso de desarrollo no cumpla en su totalidad con las disposiciones del presente manual deberán ser revisados por el área responsable de la interoperabilidad y la arquitectura tecnológica de la UTIC. El área responsable del sistema tendrá la obligación de seguir las recomendaciones dictaminadas por el área responsable de la interoperabilidad y la arquitectura tecnológica.
	De manera enunciativa, pero no limitativa, deberá aplicar las mejores prácticas en lo referente a: desarrollo iterativo; administración de requerimientos; utilización de arquitecturas basadas en componentes; modelado visual basado en UML; evaluación continua de la calidad; administración de cambios.
	Para la aplicación de las mejores prácticas, las UTIC deberán seguir una metodología de desarrollo de sistemas que integre la aplicación y seguimiento de las mejores prácticas en el desarrollo de sistemas y aplicativos, está metodología deberá estar apegada a MOPROSOFT, R.U.P., CMM dev., inclusive una personalización de éstas siempre y cuando se asegure la integralidad del desarrollo y el control en cada una de sus fases, recursos y entregables.
	Como parte de su metodología de desarrollo de sistemas y aplicativos las áreas responsables de la UTIC que adquieran, desarrollen o proporcionen mantenimiento de software, sistemas y/o aplicativos deberán someter a todo modulo o componente desarrollado a pruebas unitarias, de integración, de funcionalidad, de volumen y de seguridad.
	Las UTIC deberán asegurarse de que las áreas requirentes de la adquisición o desarrollo de software, sistemas y/o aplicaciones los desarrollos tomen la responsabilidad de proporcionar los elementos necesarios que apoyen el desarrollo del sistema (documentación, bases de datos, desarrollos previos, entre otros) cumpliendo con los tiempos establecidos en los planes de trabajo
	Las UTICS deberán asegurarse de que las áreas requirentes de la adquisición o desarrollo de software, sistemas y/o aplicaciones al realizar su solicitud de desarrollo o mantenimiento de sistemas hayan establecido sus requerimientos detallados y alcance de los servicios automatizados por escrito. Así mismo la UTIC deberá asegurarse de que el documento que entregue el área requirente cumpla con lo dictado por as mejores prácticas.
	Como parte de su metodología de desarrollo de sistemas y aplicativos las áreas responsables de la UTIC que adquieran, desarrollen o proporcionen mantenimiento de software, sistemas y/o aplicativos deberán observar que para todo componente de software deberán proporcionar evidencias de pruebas unitarias para poder verificar sus funciones principales.
	Siempre que se unan o adicionen los componentes de software al sistema, se deberán ejecutar pruebas integrales, para asegurar la preservación de las funciones ya existentes. La frecuencia de realización de pruebas deberá ser como mínimo dos veces al día.
	La frecuencia de ejecución de las pruebas funcionales deberá ser como mínimo de manera semanal. La especificación de toda prueba funcional deberá ser documentada mediante un caso de prueba.
	Las áreas responsables de la UTIC que adquieran, desarrollen o proporcionen mantenimiento de software, sistemas y/o aplicativos deberán administrar la configuración de sus productos, con apego a las mejores prácticas.
	Las dependencias o entidades de la Administración Pública Federal, deberán contar con un catálogo de software de sistemas, para promover un mejor aprovechamiento en su uso, por lo que deberán contener los datos que a continuación se detallan: Nombre del software de sistemas; Descripción; Descripción de los licenciamientos que cubren los derechos de su uso según

	corresponda; Requerimientos de hardware y software comercial, propietario, libre o de código abierto, para su operación y uso; Nombre y ubicación del responsable del software de sistemas; Nombre del propietario del software de sistemas; y Memoria técnica, incluyendo actualizaciones.
	Las dependencias y entidades de la APF, efectuarán una revisión periódica, al menos anual, de su catálogo de software, de sistemas y aplicativos; y lo colocarán a disposición de la UGD, para que aquel software, sistema o aplicativo que pueda ser utilizado en alguna otra dependencia o entidad se aproveche.
	Los sistemas y aplicativos desarrollados en las dependencias y entidades, deberán definir e implementar una estrategia de desarrollo de aplicaciones, basada en la utilización de las herramientas de software de propósito especifico, con la finalidad de que los desarrollos, sigan una directriz que se justifique en el tipo de proceso que se automatiza, el volumen de usuarios, el volumen de transacciones y el volumen de datos a almacenar; asimismo que permita la agilización de los tiempos de desarrollo y mantenimiento de aplicaciones: Desarrollos para bases de datos transaccionales; Desarrollos de aplicaciones de Inteligencia de Negocios; Desarrollos aplicaciones y servicios para flujos de trabajo o procesos; Desarrollo de aplicaciones para manejo de contenido; Desarrollo de aplicaciones para manejo de datos geo referenciados; Desarrollos de aplicaciones y servicios web para interoperabilidad; Desarrollos de aplicaciones para servidores de aplicaciones web; Desarrollos de aplicaciones para servidores de portales.
	Los sistemas y aplicativos de las dependencias y entidades se conceptualizarán desde su diseño y a través de su desarrollo e implementación de sistemas y aplicativos del mismo tipo; por lo que deberán realizarlo de forma escalable en cuanto a la plataforma de desarrollo, desempeño de las herramientas de desarrollo y software de sistemas que se utilizará para su operación.
	Las UTICS deberán definir e implementar las mediciones de eficiencia en el proceso de desarrollo de sistemas, de forma que éstas se trasladen a indicadores de desempeño, que permitan establecer acciones de mejora y aprovechamiento máximo de los recursos que se aplican en el ciclo de desarrollo de sistemas y aplicativos.
	Las áreas de las UTICS correspondientes en coordinación con él área de las UTICS responsables del centro de datos, deberán considerar durante las etapas correspondientes del ciclo de desarrollo de sistemas, la adecuada previsión de las actividades de instalación, configuración y puesta en operación de los ambientes de desarrollo, pruebas, preproducción y producción.
	Las áreas de desarrollo y de producción correspondientes de las UTICS, deberán conjuntamente asegurarse de planear y documentar las actividades enunciadas en el párrafo anterior, de manera que se programe en el centro de datos, el uso de cada elemento necesario, con el propósito de medir y verificar el mejor uso de los recursos de cómputo, almacenamiento y comunicaciones, entre otros.
	Las UTICS como responsables del desarrollo de sistemas y aplicativos en las dependencias y entidades, deberán asegurarse de las capacidades de reutilización de código de las soluciones tecnológicas , aplicativos, servicios web, componentes y demás código existente antes de iniciar un nuevo desarrollo, con la finalidad de que se optimice el uso de los elementos ya existentes y se agilice el tiempo de desarrollo de nuevas aplicaciones.
	Para el caso de los desarrollos de software, sistemas y/o aplicativos por fábrica, las UTIC deberán asegurar, previo a la contratación, que el proveedor cuenta con metodologías y mejores prácticas probadas mediante la presentación de la documentación que soporte su decir en el proceso de licitación que se efectúe.
	La UTIC deberá considerar la capacitación de todos aquellos que estén involucrados en el manejo de un software, sistema o aplicativo en desarrollo y el responsable del proyecto deberá integrar esta actividad en su proyecto de desarrollo. Las personas a ser capacitadas serán aquellas que alimentan de datos el sistema, quienes lo operan, quienes lo administran funcionalmente y quienes se benefician de sus resultados. La capacitación técnica deberá ser considerada como una actividad independiente de la capacitación dirigida al usuario.

	Las UTIC podrán utilizar el software libre que así lo especifique en su licencia, previa autorización por escrito del responsable del portafolio de proyectos y de la arquitectura tecnológica de la UTIC; respetando las condiciones establecidas dentro de la licencia para su uso, previa autorización por escrito de la UTIC.
	Para el caso de las UTIC que efectúen desarrollos aprobados mediante fábricas de software, deberán asignar un responsable de proyecto. El responsable de proyecto deberá seguir una metodología de administración de proyectos apegada a las mejores practicas para dar seguimiento al desarrollo de la fabrica y controlar los recursos, tiempos y entregables comprometidos.
	El responsable del proyecto de desarrollo de una solución tecnológica deberá: lograr la Implantación total del mismo; prever las medidas necesarias para el periodo de transición del sistema que se implantará; establecer la fecha de entrega definitiva del proyecto al usuario; fijar la fecha compromiso de entrega de resultados de los programas; coordinar e integrar el desarrollo de la documentación de sistemas apegándose a las normas y procedimientos de la documentación de la etapa de liberación; elaborar y actualizar la documentación asociada con el sistema.
	El responsable del desarrollo deberá obtener una carta de conformidad del usuario, solicitante del sistema o aplicativo desarrollado mediante la cual éste acepta el producto recibido.
	El responsable del desarrollo deberá obtener la evidencia documental mínima siguiente: documentación técnica Sistema o aplicativo; documentación del código de la talidad de los componentes del sistema; documentación de las bases de datos del sistema o aplicativo; manual de usuario y el manual técnico; instrucciones de configuración y operación del sistema o aplicativo y de la totalidad de sus componentes.
	El responsable del proyecto de desarrollo por fábrica de software deberá asegurarse que la fabrica siga la metodología definida por ella misma y comprometida en el contrato correspondiente y adicionalmente la que aplica la UTIC en cuanto el desarrollo entre a las fases de pruebas integrales de funcionalidad así como el proceso de transición, aprobación del usuario y entrega a las áreas de operación de la UTIC.
	Las UTIC son las únicas UR con la atribución para que podrán desarrollar mantenimiento al software, sistemas o aplicativos de la dependencia o entidad. Independientemente de que el mantenimiento se efectúe por los grupos de desarrollo de la UTIC o vía fábrica de software
	Las UTIC efectuarán mantenimiento a sistemas, aplicativos o componentes cuando: Se deban corregir defectos de funcionalidad o de construcción del código y rediseñar procedimientos.
	Las UTIC efectuarán mantenimiento a sistemas, aplicativos o componentes cuando: Se requiera la conversión de código, ya sea por cambios en los equipos de cómputo, sistemas informáticos o comunicaciones, para que puedan ser utilizados en un ambiente diverso.
	Las UTIC efectuarán mantenimiento a sistemas, aplicativos o componentes cuando: no exista y se requiera por interoperabilidad con otros sistemas.
	Las UTIC efectuarán mantenimiento a sistemas, aplicativos o componentes cuando: Existan cambios en las especificaciones del sistema por parte del usuario.
	A fin de mantener el nivel de calidad logrado en las soluciones tecnológicas desarrolladas en operación el Responsable del Proyecto deberá mantener contacto permanente con el usuario, a fin de obtener información que permita la actualización del sistema.
	La UTIC deberá asegurar la aplicación de las mejores prácticas en el desarrollo de mantenimientos para mantener el nivel de calidad de las soluciones tecnológicas desarrolladas.
	La UTIC, derivado de los mantenimientos que se apliquen a un software, sistema o aplicativo durante su ciclo de vida útil, deberá mantener un control de versiones, respaldos y documentación. Apegado a las mejores prácticas que la propia UTIC haya implementado.
	Las UTIC deberán proteger el software, sistemas y/o aplicativos desarrollado a efecto de: i) minimizar el riesgo de fugas de información que revelen información confidencial sobre la operación

	de dependencia o entidad, transacciones y/o cualquier dato que atente contra su seguridad y ii) asegurar que el código y los componentes del software, sistemas y/o aplicativos que sean desarrollados permanecen como propiedad intelectual de la institución.
	La UTIC deberá asegurarse de que el personal interno o externo que participe en el desarrollo de aplicaciones durante cualquiera de las etapas de estudio de factibilidad, análisis, diseño, programación, pruebas, capacitación, migración, puesta en marcha, mantenimiento y cualquiera otra actividad relacionada deberá firmar convenio de confidencialidad, dónde se compromete a guardar estricto secreto profesional sobre el software y su proceso de desarrollo, y donde acepta que el código y todos sus componentes son propiedad de la dependencia o entidad, por lo que no copiará ni reutilizará el código parcial o totalmente para ningún otro fin.
	Deberá implementar controles que impidan que el código y los componentes del software, sistemas y/o aplicativos y todos los elementos relacionados con el software se copien en medio alguno, sean enviados por correo electrónico, fax u otro medio, se impriman, o se publiquen en cualquier medio, para fines diferentes a los autorizados para las funciones de cada miembro del equipo de desarrollo, con base en el privilegio mínimo.
	Las UTIC deberán asegurar que en todo componente de software se incorporen controles de seguridad mínimos que protejan las transacciones y los datos, de acuerdo con su sensibilidad y criticidad. Con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de los datos y transacciones que realiza una aplicación, así como la funcionalidad que fue aprobada como versión para producción.
	Las UTIC deberán asegurar que en sus desarrollos se integren controles de validación de entrada y salida de datos, con base en los requerimientos del sistema y sensibilidad de la información.
	Las UTIC deberán asegurar que en sus desarrollos se integren controles durante el diseño e implementación que minimicen los riesgos de fallas en el procesamiento interno de la aplicación que pudieran afectar en su integridad.
	Las UTIC deberán asegurar que en sus desarrollos se integren controles criptográficos de acuerdo con la sensibilidad y criticidad de la información: confidencialidad: codificación para proteger la información confidencial o crítica, ya sea almacenada o transmitida; ii) integridad/autenticidad: firmas digitales o códigos de autenticación o crítica almacenada o trasmitida; iii) no repudio, técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.
	Las UTIC deberán asegurar que en sus desarrollos se integren registros de errores y revisarlos periódicamente para valorar riesgos en el funcionamiento.
	Las UTIC deberán asegurar que en sus desarrollos se integren bitácoras de uso del software, sistemas y aplicativos para identificar y/o evitar su uso inadecuado, incluyendo borrado o modificación.
	Las UTIC deberán asegurar que en sus desarrollos se integren controles de acceso, de acuerdo con la sensibilidad de la información, incluyendo la identificación, autenticación y autorización del usuario.
	Las UTIC deberán asegurar que en sus desarrollos se integren procedimientos de protección de la contraseña incluyendo características, frecuencia de actualización, encriptación, entre otros.
	Las UTIC deberán asegurar que en sus desarrollos se integren bitácoras de las operaciones de forma detallada (fecha, hora, autor) en bitácoras, incluyendo acceso, transacciones y modificaciones a la configuración, así como actualizaciones de versiones.
	Las UTIC deberán asegurar que en sus desarrollos se integren tiempos para el cierre de sesión inactiva.
	Las UTIC deberán asegurar que en sus desarrollos se integren mecanismos de respaldo y

	recuperación de datos.
	Las UTIC deberán asegurar que en sus desarrollos se integren valoraciones de riesgos de las aplicaciones, a través de pruebas de vulnerabilidades, pruebas de código, pruebas de intrusión, de manera periódica
	El personal de la UTIC que administre el desarrollo y mantenimiento de software, sistemas y/o aplicativos debe prohibir la utilización de datos Confidenciales o Reservados para realizar pruebas.
	El personal de la UTIC que administre el desarrollo y mantenimiento de software, sistemas y/o aplicativos debe destruir datos Confidenciales o Reservados que se consideren no vigentes en estricto apego a la normatividad vigente aplicable.
	Los ambientes de desarrollo y pruebas deben observar las siguientes condiciones: i) deben ser de uso exclusivo de analistas y/o programadores; ii). Deben contener un directorio de software base utilizado por el área de desarrollo para sus trabajos; iii) deben contener un directorio de desarrollo y pruebas donde residan el software, sistemas y/o aplicativos que están siendo desarrollados, mantenidos y los archivos de datos de prueba correspondientes; iv) deben contener un directorio de control para la correcta publicación o transferencia a los ambientes de producción, programas ejecutables que han sido desarrollados o modificados, y la transferencia de los programas en código fuente a las bibliotecas de programas fuentes; v) deben contener un directorio de archivos fuente donde se alojarán todos los programas fuente de la dependencia o entidad, que se encuentren en producción, misma que debe tener el máximo nivel de seguridad y control de acceso.
	El ambiente de producción debe observar las siguientes condiciones: debe contener los directorios que contengan archivos de datos, bases de datos, programas ejecutables o compilados, distribuidos por el software, sistemas y/o aplicativos en producción; debe contener un directorio de objetos ejecutables el cual contendrá todos los objetos ejecutables, que corresponden con programas fuentes debidamente autorizados y de acuerdo con las normas sobre desarrollo de aplicaciones; debe contener un directorio de datos de aplicación el cual contendrá los archivos físicos, bases de datos y las vistas lógicas asociadas y utilizadas por cada aplicación.
	Las medidas de seguridad que defina la UTIC para al software, sistemas y/o aplicaciones estarán en función de la clasificación de la información que generen, almacenen o procesen.
	La UTIC debe evaluar y aprobar la arquitectura de seguridad definida para durante las fases iniciales del proyecto de desarrollo o adquisición de un software, sistema o aplicativo así como los mecanismos de seguridad que formarán parte de la funcionalidad a desarrollar de manera que se asegure que la información estará protegida de acuerdo a su clasificación.
	Cualquier requerimiento de cambio en la funcionalidad o componentes del servicio, software, sistema o aplicativo a desarrollar que impacte la seguridad de la arquitectura o del componente a desarrollar deberá ser evaluada y aprobada por el personal responsable de la seguridad en la UTIC.
	El área de la UTIC responsable del proceso de liberación de sistemas o servicios informáticos deberá asegurar la separación de funciones entre los responsables de la implementación y el área de desarrollo.
	La dependencia o entidad dispondrá de un portal Institucional en Internet. La UTIC será a responsable de la administración y mantenimiento de la operación de éste.
	El área designada por la UTIC para proporcionar los servicios de Internet e Intranet así como todos aquellos asociados a éstos es el área responsable técnicamente para apoyar en la publicación y actualización de información en el sitio de Internet, a las áreas que lo soliciten, a través del área responsable de los servicios de Internet, intranet y servicios asociados.
	El área designada por la UTIC para proporcionar los servicios de Internet e Intranet así como todos aquellos asociados a éstos deberá asegurarse de proporcionar las herramientas y mecanismos así como capacitación a los usuarios institucionales responsables de la información que se publica en el Sitio Institucional.
	Las solicitudes de actualización o publicación de información de las UR deberá ser requerida a la

	UTIC, de conformidad con lo establecido por la UTIC.
	La UTIC será la responsable de revisar que los contenidos se apeguen a los intereses y lineamientos de la dependencia o entidad .
	La publicación de las páginas elaboradas por las diferentes Urs que conforman la dependencia o entidad, deberán apegarse a los lineamientos que emita la UTIC para la publicación en el portal de Internet e Intranet.
	La UTIC será la única entidad reconocida para llevar a cabo el análisis, diseño e instrumentación de estándares tecnológicos, procesamiento de datos e implementación de tecnologías de información relacionadas con Internet.
	La UTIC tiene la facultad de hacer respetar los estándares tecnológicos de publicación en el sitio Web de la dependencia o entidad, para mantener la coherencia de diseño y concepto del sitio de Internet.
	Ninguna UR podrá realizar modificaciones, configuraciones, instalaciones o liberaciones de Hardware o Software de procesamiento de datos y comunicaciones de datos, sin la autorización de la UTIC, en lo relacionado a las tecnologías de Internet o servicios de transferencia de archivos.
	La UTIC se reserva el derecho de retirar o inhabilitar servidores que ofrezcan servicios de nternet, transferencia de datos o almacenamiento que no haya autorizado y que opere en su infraestructura de datos o comunicaciones.
	La UTIC será la responsable de la administración tecnológica del sitio de Internet corporativo, servidores, infraestructura de comunicaciones y transferencia de contenidos al servidor Web, y de manera indirecta cuando se trate de tecnologías del Portal, Negocio a Negocio (B2B), Negocio a Usuario (B2C), Protocolo de aplicación Inalámbrica (WAP) u otras tecnologías en la que deba participar un administrador de infraestructura de terceros o servicios de terceros; O en los casos que la información sea generada como proceso de negocio.
	El usuario acepta que la información publicada podrá ser removida, eliminada o cambiada de su ubicación física en el sitio de Internet, previo aviso y de acuerdo con las especificaciones de su solicitud.
	En caso de existir aplicaciones dentro del portal, éstas deberán contar con herramientas de identificación y autenticación de usuarios definidos por la UTIC.
	La UTIC se compromete a que la publicación se encuentre disponible en su ubicación y forma correspondiente en un plazo no mayor a 4 días.
	La UTIC enviará a las áreas una notificación de que su publicación ya fue realizada, una vez publicada, en un plazo no mayor a 4 días.
	La permanencia de la información en el Portal de Internet e Intranet será de acuerdo al plazo estipulado en el oficio y/o solicitud, o en caso de no ser estipulado su permanencia en el portal será de un plazo no menor a un mes. La UTIC. Procederá a depurar la información.
	El desarrollo de aplicaciones en Internet, deberá apegarse a los estándares que para tal efecto se definen en las normas de desarrollo de sistemas.
	El servicio Institucional de Intranet, es el único medio oficial interno de publicación electrónica de información y cada publicación debe tener un responsable. La UTIC es el área responsable de administrar y operar los recursos para el servicio de Intranet.
	Toda la información que los usuarios de TIC generen para Internet, serán propiedad de la dependencia o entidad. La UTIC vigilará el uso y las condiciones de la misma, sin perjuicio de la propiedad de la información a favor de la dependencia o entidad.
	El usuario solicitará el servicio de Publicación de Información y/o Aplicaciones en el Portal de Internet e Intranet a través del personal facultado por la UTIC una vez que haya validado los requisitos de la información a publicar.
	El servicio Web sólo debe ser usado con el propósito de comunicación o consulta de asuntos relativos a la dependencia o entidad.

	Los usuarios del servicio Web deben adoptar absoluta seriedad en el manejo de información confidencial o reservada, por lo que no deberán publicar o distribuir algún tipo de software con licencia o cualquier tipo de información clasificada como confidencial o reservada propiedad de la dependencia o entidad .
	El servicio Web debe ser usado sin interferir con el rendimiento laboral del personal y sin degradar el rendimiento o desempeño de los recursos de acceso al servicio.
	Previo al inicio del desarrollo de cualquier solución tecnológica (sistema, aplicativo, componente), ya sea por desarrollo interno, o bajo contrato, se deberá contar con la autorización escrita del Titular de la UTIC o responsable facultado y el dictamen correspondiente.
	En todo desarrollo de software se deberá considerar: a). que satisfaga las necesidades de la dependencia o entidad agregando valor, esto es: incrementando la productividad, mitigando riesgos, ahorro de recursos, nuevos y mejores servicios al usuario, ; b). la capacidad y calidad del software, sistema o aplicativo para integrarse a otros sistemas existentes en operación; c). la interoperabilidad con otros sistemas de las dependencias o entidades, y el costo inicial y el costo de su implantación, mantenimiento y soporte a lo largo de su vida útil.
	Se deberá asegurar que, desde la conceptualización en el proceso de desarrollo, el software, sistemas o aplicativos que estén orientados a funcionarios de la dependencia o entidad, sean accedidos como mínimo mediante un hipervínculo a la intranet o al portal de la dependencia o entidad.
	Se deberá certificar que, desde la conceptualización en el proceso de desarrollo, el software, sistemas o aplicativos que estén orientados a ciudadanos, empresarios o cualquier entidad externa a la dependencia o entidad, sean accedidos como mínimo mediante un hipervínculo al Portal de la dependencia o entidad.
	Las áreas responsables que adquieran, desarrollen o proporcionen mantenimiento de software, sistemas y/o aplicativos deberán someter a todo modulo o componente desarrollado a pruebas unitarias, de integración, de funcionalidad, de volumen, de aceptación del usuario y de seguridad.
	Las áreas requirentes de la adquisición o desarrollo de software, sistemas y/o aplicaciones deberán proporcionar los elementos necesarios que apoyen el desarrollo del sistema (documentación, bases de datos, desarrollos previos, entre otros).
	Se deberá contar con un catálogo de software cuando menos con los siguientes datos: nombre del software de sistemas; descripción; descripción de los licenciamientos que cubren los derechos de su uso según corresponda; requerimientos de hardware y software comercial, propietario, libre o de código abierto, para su operación y uso; nombre y ubicación del responsable del software de sistemas; nombre del propietario del software de sistemas; y memoria técnica, incluyendo actualizaciones.
	Se efectuará una revisión periódica del catálogo de software, de sistemas y aplicativos; y lo pondrán a disposición de la UGD.
	Se debe definir e implementar las mediciones de eficiencia en el proceso de desarrollo de sistemas, de forma que éstas se trasladen a indicadores de desempeño.
	Se deberá asegurar las capacidades de reutilización de código de las soluciones tecnológicas , aplicativos, servicios web, componentes y demás código existente antes de iniciar un nuevo desarrollo,
	Para el caso de los desarrollos de software, sistemas y/o aplicativos por fábrica, las UTIC deberán asegurar, previo a la contratación, que el proveedor usará esta metodología.
	Se debe considerar la capacitación de todos aquellos que estén involucrados en el manejo de un software, sistema o aplicativo en desarrollo.
	Los ambientes de desarrollo, pruebas y producción deben estar protegidos a través de los controles de seguridad que permitan mantener independencia e integridad en el código, los datos y las transacciones.

	Los ambientes de desarrollo, pruebas y producción, deben estar separados, tanto a nivel físico como lógico.
	Las herramientas para el desarrollo de software deberán ser accesibles sólo para los miembros autorizados de desarrollo de sistemas.
	Las herramientas de desarrollo de software deben eliminarse de cualquier equipo de cómputo que no sea utilizado para el desarrollo de sistemas, o bien, deberá justificarse su uso mediante un análisis de riesgos, y un documento aprobado por el Oficial de Seguridad o su equivalente.
	Las herramientas de desarrollo no se deben instalar en los ambientes de producción o pruebas.
	El uso de información operacional, con propósito de pruebas en el desarrollo de sistemas no está permitido, si fuera necesario, debe estar autorizado por los dueños de los activos de información.
	Se deberá de incluir la especificación de los requerimientos de seguridad establecidos tanto en la política de seguridad como en las políticas de nivel medio relacionadas al desarrollo seguro de soluciones tecnológicas.
	Se deberán de realizar verificaciones y validaciones a los productos y soluciones tecnológicas de acuerdo a lo establecido en el proceso Establecimiento del sistema de gestión de procesos y calidad.
	Asistir al personal facultado, para que todo nuevo desarrollo o mantenimiento de un sistema cumpla con los requerimientos.
	Establecer los puntos mínimos a ser considerados en los términos de referencia de un sistema de información.
	Deberá haber una segregación entre los entornos de desarrollo, prueba y producción. Se deberá disponer de procedimientos para trasladar aplicaciones desde el entorno de desarrollo al de producción con autorización a cada paso.
	Verificar que se lleve a cabo la elaboración de procedimientos de atención de incidencias y de control de cambios a las soluciones tecnológicas en coordinación con el personal facultado por la UTIC y el responsable designado por el área usuaria correspondiente.
	Para todo proyecto de desarrollo de una solución tecnológica se deberá asegurar que antes de poner en producción el sistema, el responsable del sistema valide y acepte el funcionamiento del sistema.
	Proporcionar asesoría en materia de desarrollo soluciones tecnológicas a los usuarios que realicen la solicitud de apoyo de manera formal.
	Verificar en coordinación con el personal facultado por la UTIC y el responsable designado por el usuario correspondiente que todo nuevo desarrollo o mantenimiento de una solución tecnológica cumpla con los requerimientos especificados.
	La UTIC establecerá los instructivos para la conformación de las contraseñas seleccionadas por los usuarios para el uso de las soluciones tecnológicas a las que debe tener acceso. Es responsabilidad del personal facultado de la UTIC asistir a los usuarios en la definición y cumplimiento de las siguientes disposiciones:
	Elaborar en conjunto con el Usuario responsable de la solución tecnológica, los términos de referencia de la solución tecnológica a ser desarrollada o actualizada en el cual se describan los requisitos de negocio y el alcance que ha de satisfacer el sistema antes de que se inicie el trabajo del proyecto.
	Revisar que el software propuesto o utilizado para el desarrollo de una solución tecnológica cumpla con los requisitos estipulados.
	Verificar que en todo desarrollo de una solución tecnológica se prevea que el responsable del sistema y el encargado del desarrollo acuerden criterios de aceptación, manejo de modificaciones, roles de los usuarios, instalaciones, software y procedimientos.
	Verificar que todo nuevo desarrollo o mantenimiento de una solución tecnológica, cumpla con los requerimientos.

Todo desarrollo de una solución tecnológica deberá haberse terminado y aprobado antes de que éste pase a producción, además de contar con la documentación correspondiente.
Para modificaciones importantes de aplicaciones de alto riesgo, deberán realizar pruebas de aceptación en un entorno que sea representativo del entorno operativo.
Verificar que estén diseñadas para admitir una única fuente de acceso de Usuario y contraseñas.
Verificar que todas las soluciones tecnológicas nuevas cuenten con la documentación requerida en cada una de las etapas.
Todo nuevo desarrollo o mantenimiento de una solución tecnológica, deberá ser presentado al grupo de trabajo responsable del portafolio de proyectos o su equivalente de la dependencia o entidad, para su evaluación y aprobación.
Verificar que las soluciones tecnológicas que sean desarrolladas expresamente para la dependencia o entidad o que sean adaptados para su utilización en ésta, deberán contar con el código fuente o en su caso la licencia de uso.
El personal facultado por la UTIC orientará a los usuarios, vía la mesa de servicios, para la conformación de las contraseñas seleccionadas por ellos mismos para el uso de las soluciones tecnológicas a las que debe tener acceso. Es responsabilidad del Usuario que use o requiera el desarrollo de una solución tecnológica, dar cumplimiento a las siguientes disposiciones:
El Usuario no debe utilizar herramientas de hardware o software para eludir o comprometer la seguridad de ningún Sistema de Información.
El Usuario no debe compartir información de la dependencia o entidad, resultado de los Sistemas de Información a los que tenga acceso, con personas no autorizadas.
El Usuario tiene prohibido copiar, vender o circular sin autorización software o datos que estén protegidos por licencia o copyright.
El Usuario que deje la dependencia o entidad, no deberá llevar consigo ni divulgar la documentación relacionada con informáticos de la dependencia o entidad.
El buen uso de las soluciones tecnológicas es responsabilidad del Usuario.
El usuario que requiera el desarrollo de una solución tecnológica deberá designar un responsable por parte del usuario.
El usuario, en su caso, deberá contactarse con el responsable del sistema designado por la UR correspondiente, quién será el que determine las medidas de seguridad apropiadas y quién autorice las solicitudes de acceso al sistema
El Usuario verificará en conjunto con el área de la UTIC que lo atiende, que el software utilizado para el desarrollo de una solución tecnológica, cumpla con los requisitos estipulados en el Requerimiento de Sistemas.
El Usuario acordará los criterios de aceptación, manejo de modificaciones, roles, instalaciones, herramientas, software y procedimientos, con el responsable del desarrollo.
El Usuario deberá desarrollar procedimientos específicos que permitan asegurar que, para cada relación con un proveedor de servicios externos, se defina y acuerde un contrato antes de que se inicie el desarrollo de una solución tecnológica.
El Usuario presentará todo nuevo desarrollo de Sistemas de Información al grupo de trabajo responsable del portafolio de proyectos o su equivalente, para su evaluación y aprobación
El Usuario verificará que todo nuevo desarrollo o mantenimiento de un sistema, cumpla con los requerimientos establecidos.
Para todo problema asociado a la operación de los Sistemas de Información, el único punto de contacto es la mesa de servicios o su equivalente en la UTIC.

7.7.2.5 Documentación soporte del proceso

	No aplica

7.7.3. Calidad de soluciones tecnológicas

7.7.3.1. Objetivos del proceso

General.-

Asegurar que las soluciones tecnológicas desarrolladas o adquiridas cumplan con los requerimientos especificados, así como los procesos de desarrollo de estas últimas.

Específicos.-

1. Definir los criterios de verificación de las soluciones tecnológicas, para incluirlas en los requerimientos contractuales así como en los planes y programas del proyecto de implantación
2. Validar las soluciones tecnológicas, incluyendo selección de componentes y productos y estableciendo y manteniendo el ambiente de validación, procedimientos y criterios.
3. Asegurar que la solución tecnológica desarrollada o adquirida pueda implementarse en el ambiente operativo destinado.
4. Evaluar los resultados de las validaciones.

7.7.3.2 Descripción del proceso

7.7.3.2.1 Mapa general del proceso

Diagrama de flujo de información

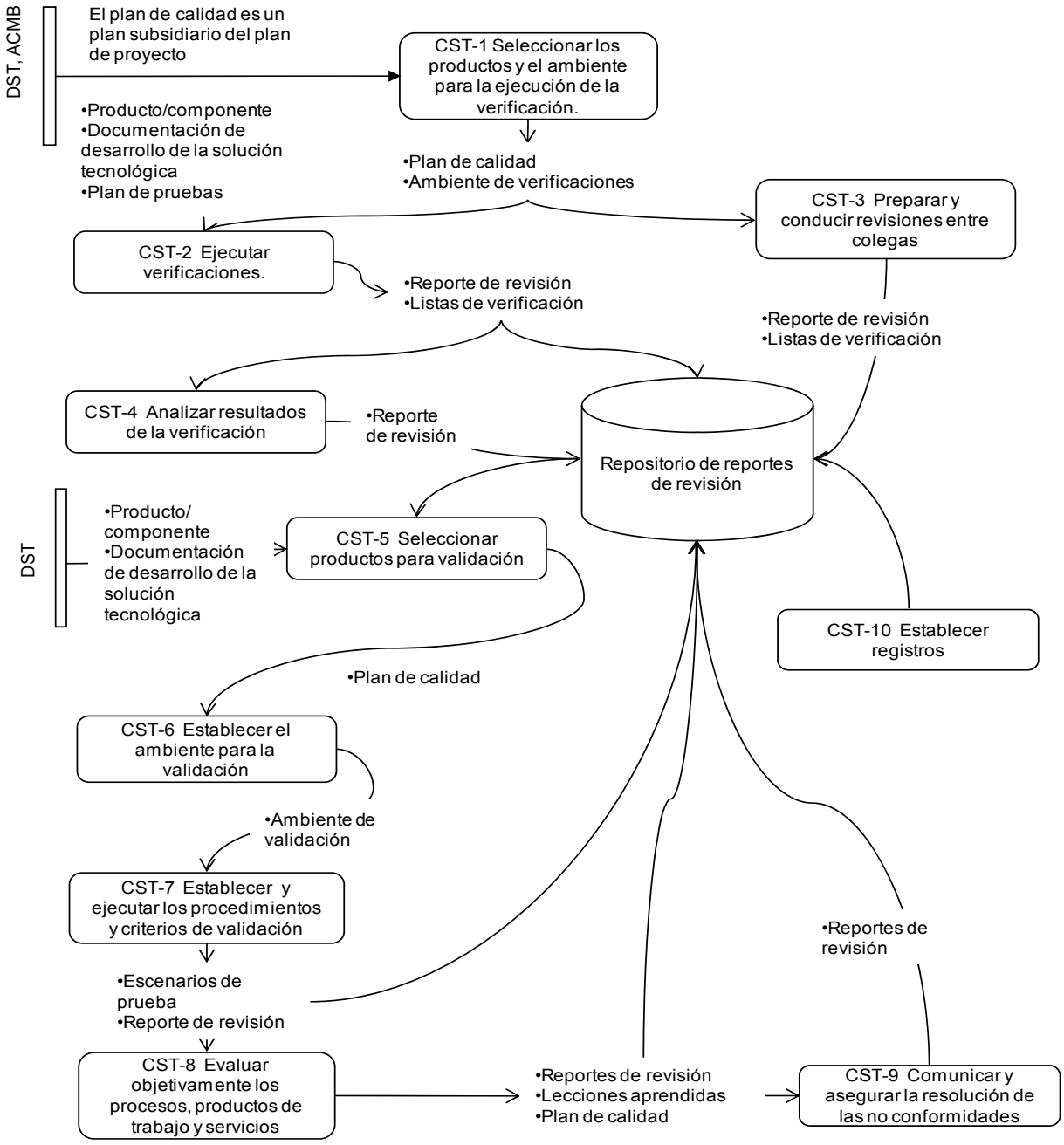
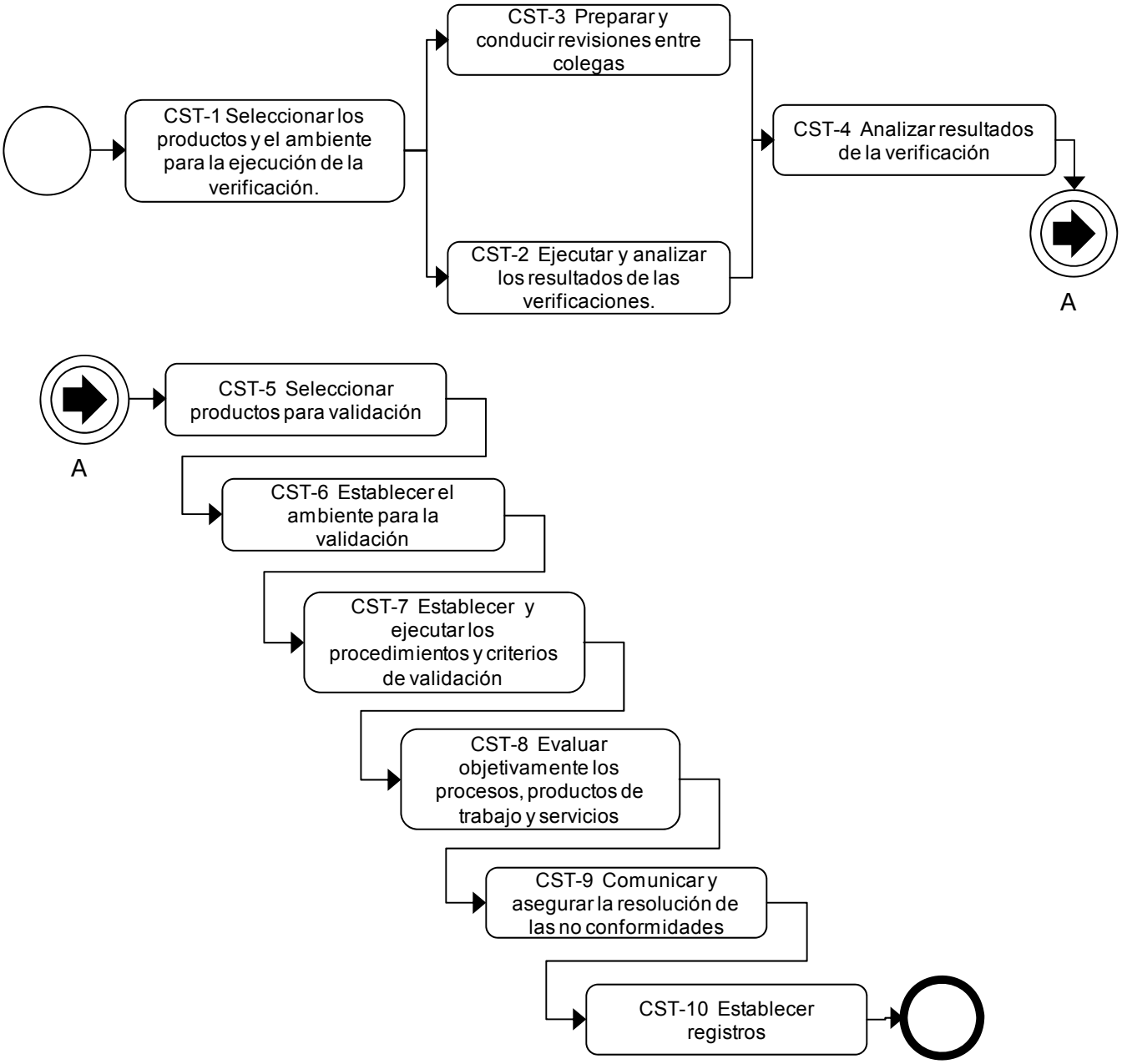


Diagrama de flujo de actividades



7.7.3.2.2 Descripción de las actividades del proceso

CST-1 Seleccionar los productos y el ambiente para la ejecución de la verificación

Descripción	Seleccionar los productos de trabajo de la solución tecnológica adquirida que se van a verificador y los métodos de verificación que a utilizar.
Factores Críticos	1. Identificar los productos de trabajo adquiridos a ser verificados. Los productos de trabajo son seleccionados basados en su contribución al cumplimiento de objetivos y requerimientos. Se establecen los requisitos para el ambiente que soportará la verificación. 2. Identificar los métodos de verificación disponibles y que serán usados para la verificación de cada producto de trabajo seleccionado. 3. Identificar los requerimientos del ambiente para la verificación. 4. Identificar los recursos para la verificación que están disponibles para reutilizar y modificar. 5. Identificar el equipo y herramientas de verificación. Durante la identificación del equipo de revisión se deberá garantizar que este sea independiente al equipo involucrado en el desarrollo de la solución tecnológica. 6. Establecer y mantener procedimientos y criterios de verificación para seleccionar productos de trabajo.
Relación de productos	• Plan de calidad • Ambiente de verificaciones

CST-2 Ejecutar verificaciones

Descripción	Ejecutar la verificación de los productos de trabajo seleccionados y analizar los resultados.
Factores Críticos	1. Ejecutar verificación de productos de trabajo seleccionados contra sus requerimientos. Las verificaciones a productos y/o productos de trabajo promueven una detección temprana de problemas y pueden resultar en la eliminación temprana de defectos. 2. Registrar los resultados de las actividades de verificación. 3. Analizar los resultados. 4. Identificar acciones a tomar que son resultado de verificaciones de productos de trabajo y darles seguimiento hasta el cierre de los hallazgos detectados. 5. Documentar la ejecución del método de verificación y las desviaciones de los métodos disponibles y otros procedimientos utilizados durante la ejecución.
Relación de productos	• Reporte de revisión • Listas de verificación

CST-3 Preparar y conducir revisiones entre colegas

Descripción	Preparar y conducir las revisiones entre colegas de los productos de trabajo seleccionados para identificar defectos y removerlos en una etapa temprana.
Factores Críticos	1. Determinar el tipo de revisión entre colegas a ser conducida. 2. Establecer y mantener criterios de entrada y salida para la revisión entre colegas. 3. Establecer y mantener listas de verificación para asegurar que los productos de trabajo son revisados consistentemente. Las listas de verificación se modifican según sea necesario para dirigir un tipo específico de revisión entre colegas para un producto de trabajo. 4. Planear las revisiones entre colegas. 5. Ejecutar las revisiones para asegurar que los productos de trabajo satisfacen los criterios de entrada para una revisión entre colegas antes de su distribución. 6. Distribuir los productos de trabajo a ser revisados y su información relacionada a los participantes con suficiente antelación para hacer posible una adecuada preparación para la revisión entre colegas. 7. Asignar roles para la revisión entre colegas según proceda. 8. Identificar y documentar defectos y otros hallazgos en los productos de trabajo, así como las acciones a tomar para las correcciones. 9. Identificar acciones a tomar (correctivas) y comunicar los defectos y hallazgos relevantes a los interesados. 10. Conducir una revisión entre colegas adicional si los criterios definidos indican la necesidad de ejecutarla. 11. Asegurar que los criterios de éxito para la revisión entre colegas se satisfacen. 12. Almacenar los datos para futuras referencias y análisis. 13. Proteger los datos de las revisiones entre colegas para asegurar que no sean usados de manera inapropiada.
Relación de productos	• Reporte de revisión • Listas de verificación

CST-4 Analizar resultados de la verificación

Descripción	Analizar los resultados de todas las actividades de verificación.
Factores Críticos	1. Comparar resultados actuales contra resultados esperados bajo el entorno de colaboración. 2. Los resultados son comparados para establecer criterios de verificaciones para determinar la aceptabilidad. 3. Identificar con base en los criterios de verificación establecidos los productos que no han cumplido con sus requerimientos o identificar problemas con los métodos, procedimientos, criterios y verificación de ambiente. 4. Analizar los datos de verificación de los defectos.

	5. Registrar todos los resultados del análisis en un reporte de revisión. 6. Utilizar los resultados de verificaciones para comparar mediciones actuales y de rendimiento para los parámetros técnicos de desempeño (ver el proceso de AD). 7. Proporcionar información de cómo los defectos se pueden resolver (incluyendo métodos de verificación, criterios y ambiente de verificación) y formalizarlas en un documento, estableciendo responsabilidades y tiempos en la resolución de los defectos.
Relación de productos	• Reporte de revisión

CST-5 Seleccionar productos para validación

Descripción	Seleccionar los productos y componentes de productos para ser validados y los métodos de validación que serán usados para cada uno.
Factores Críticos	1. Identificar los principios fundamentales, características y fases para la validación de la solución tecnológica durante todo el ciclo de vida de la elaboración. 2. Determinar cuáles son las categorías de las necesidades de usuario (operacional, mantenimiento, capacitación, o soporte) que serán validadas. 3. Los productos o componentes de productos deberán ser mantenibles y soportables en su propio ambiente operacional. Este factor crítico también se refiere al mantenimiento actual, capacitación y servicios de soporte que pueden ser liberados con el producto. 4. Seleccionar el producto o componentes de la solución tecnológica a ser validados. 5. Seleccionar los métodos para la validación del producto o componentes de la solución tecnológica que se adquiere, realizando las pruebas y valoración haciendo uso de herramientas de apoyo para: • La realización de pruebas de caja blanca y caja negra • La realización de pruebas funcionales • La realización de pruebas de rendimiento • La realización de pruebas de seguridad • Y todas aquellas pruebas que sean requeridas para validar la funcionalidad y operación en los ambientes productivos finales. 6. Revisar la validación seleccionada, restricciones y métodos con los interesados y unidades responsables más relevantes.
Relación de productos	• Plan de calidad

CST-6 Establecer el ambiente para la validación

Descripción	Establecer y mantener los requerimientos de ambiente para apoyar la validación.
Factores Críticos	1. Identificar los requerimientos para el ambiente de validación. Los requerimientos para el ambiente de validación son impulsados por el producto o servicio seleccionado, por el tipo de producto de trabajo y por el método de validación. 2. Identificar los productos suministrados por la unidad responsable.

	3. Identificar elementos reutilizables. 4. Identificar los recursos humanos, las plataformas y las herramientas para la realización de las diferentes pruebas establecidas. 5. Identificar herramientas para la administración de las pruebas. 6. Definir un ambiente colaborativo para las herramientas de validación y establecer los niveles de acceso necesarios para mantener la integridad, monitoreo y control de los resultados de las validaciones. 7. Identificar los recursos de validación que están disponibles para reutilización e integración de la solución. 8. Planear la disponibilidad de recursos humanos que participaran durante las validaciones.
Relación de productos	• Ambiente de validación

CST-7 Establecer y ejecutar los procedimientos y criterios de validación

Descripción	Establecer y mantener procedimientos y criterios para validación.
Factores Críticos	1. Revisar los requerimientos del producto para asegurar que los defectos que afectan la validación del producto o servicio adquirido son identificados y resueltos. 2. Documentar el ambiente, escenarios operacionales, procedimientos, entradas, salidas, y criterios para la validación de los productos o servicios adquiridos. 3. Favorecer la generación de una infraestructura de pruebas la cual garantice el re uso de activos utilizados en las validaciones. 4. Los procedimientos y criterios de validación deberán ser definidos para asegurar que los productos o componentes de la solución tecnológica cumplan con su propósito. 5. Al ser ejecutadas las actividades de validación deberá asegurarse que los datos resultantes son coleccionados y analizados de acuerdo a los métodos, procedimientos y criterios establecidos. 6. Evaluar el producto o servicio adquirido a medida que madura en el contexto de validación del ambiente para identificar defectos de validación. 7. Comparar los resultados actuales contra los resultados esperados, bajo un entorno de colaboración. 8. Identificar con base a los criterios de validación establecidos, aquellos productos y componentes de productos que no cumplen adecuadamente con su propósito en sus ambientes operativos, o identificar problemas con los métodos, criterios y/o ambientes. 9. Analizar los datos de validación de los defectos en el entorno de colaboración. 10. Registrar los resultados del análisis e identificar defectos. 11. Utilizar los resultados de la validación para comparar mediciones actuales y de rendimiento contra el uso previsto o necesidades operacionales. 12. Identificar las acciones a realizar para el cierre de los hallazgos en los productos de trabajo que no pasan la validación.

Relación de productos	• Escenarios de prueba • Reporte de revisión

CST-8: Evaluar objetivamente los procesos, productos de trabajo y servicios

Descripción	Se evalúa objetivamente la adherencia a los procesos desarrollados y sus productos y servicios asociados, de acuerdo a sus estándares y descripción de procesos.
Factores Críticos	1. Seleccionar los productos de trabajo que serán evaluados, basándose en un criterio de muestras de documentos si se utilizan muestras. 2. Establecer y mantener criterios de evaluación, bajo un entorno de colaboración. • Los criterios de evaluación de procesos, productos de trabajo y servicios deberán definirse basados en las necesidades de la dependencia o entidad, tales como: ¿que será evaluado?, ¿cuándo y/o con qué frecuencia los procesos y productos de trabajo serán evaluados?, ¿cómo será conducida la evaluación?, ¿quién debe involucrarse en la evaluación?, entre otros • En este tipo de evaluación se deberá contemplar que el personal a realizar estas actividades sea completamente independientes de la elaboración de los productos de trabajo. • Se deberá generar una infraestructura de pruebas la cual garantice el reuso de activos utilizados en las validaciones • Se deberán definir criterios de evaluación para evaluar los productos de trabajo, servicios y la cohesión de los procesos contra las descripciones de procesos, estándares y procedimientos 3. Evaluar los productos de trabajo antes de que sean entregados al usuario, de acuerdo al cronograma de trabajo corrspondiente, en hitos seleccionados durante su desarrollo; mientras se desarrollan de manera incremental (productos de trabajo y servicios). 4. Identificar hallazgos (no conformidades) durante las evaluaciones.
Relación de productos	• Reportes de revisión • Lecciones aprendidas • Plan de calidad

CST-9: Comunicar y asegurar la resolución de las no conformidades

Descripción	Comunicar los asuntos a los involucrados y asegurar la resolución de las no conformidades.
Factores Críticos	1. Resolver cada no conformidad con los participantes apropiados del equipo, cuando sea posible. • Entendiendo por no conformidades los problemas identificados en las evaluaciones que reflejan la falta de adherencia a los estándares, procesos o procedimientos. • Los estatus de las no conformidades deben proveer un indicador de las tendencias de calidad. 2. Documentar las no conformidades cuando no puedan ser resueltas dentro del proyecto.

	3. Escalar las no conformidades que no pueden ser resueltas dentro del proyecto a los niveles administrativos designados para recibirlos y actuar sobre ellas. 4. Analizar las no conformidades para ver si existen tendencias de calidad que puedan ser identificadas y corregidas. 5. Asegurar que los involucrados relevantes están enterados de los resultados de las evaluaciones y de las tendencias de calidad de una manera oportuna. 6. Realizar revisiones periódicas sobre las no conformidades y las tendencias que se tengan pendientes con los administradores designados para recibir y actuar sobre éstos. 7. Dar seguimiento a las no conformidades hasta su cierre.
Relación de productos	• Reportes de revisión

CST-10: Establecer registros

Descripción	Establecer y mantener los registros de actividades de aseguramiento de calidad.
Factores Críticos	1. Registrar las actividades de aseguramiento de calidad de procesos y de productos, con el suficiente detalle para que su estado y resultados sean conocidos. 2. Revisar periódicamente el estado y la historia y lecciones aprendidas resultado de las actividades de aseguramiento de calidad.
Relación de productos	• Repositorio de reportes de revisión

TIEMPO TOTAL DEL PROCESO: Variable

7.7.3.2.3 Descripción de roles

Rol	Responsabilidad
Administrador de calidad	Responsable de planear y coordinar las actividades de aseguramiento de la calidad. Confirma la participación de los involucrados en las revisiones y auditorias, asegurándose que ocurran de forma oportuna, y acorde al estándar requerido.
Revisor	Revisa que los productos y/o entregables generados tengan la calidad esperada, cumplan con los criterios de calidad definidos, y cubran los requerimientos del solicitante, antes de ser entregados; a su vez reporta las no conformidades detectadas y les da seguimiento hasta su cierre.
Ingeniero de pruebas	Responsable de ejecutar las prueba y dar seguimiento a los defectos encontrados hasta su cierre, así como llevar la rastreabilidad de los escenarios de prueba.

Auditor	Se encarga de generar el Programa de auditoria, darle seguimiento al mismo y comunicar los resultados a los interesados. Asigna al Auditor responsable de ejecutar las auditorias y da apoyo a éste en sus actividades. Es responsable de realizar las actividades relacionadas con la planeación y ejecución de la auditoria. Cuando exista un Equipo auditor, este es responsable de dirigirlo y se conoce como Líder del equipo auditor.
Grupo de aseguramiento de Calidad	Se encarga de conducir auditorias y revisiones sobre los proyectos a fin de reportar las no conformidades y darle seguimiento hasta su cierre.
Líder de calidad	Coordina al grupo de aseguramiento de calidad asignado a un proyecto.
Desarrollador	Es la persona que elabora el producto de trabajo o desarrolla un servicio que es revisado y auditado.
Colega	Persona o grupo de personas con el mismo rol y nivel de experiencia para llevar a cabo una revisión de un producto, producto de trabajo y/o componente de un producto.

7.7.3.2.4 Descripción de productos

Nombre	Descripción
Plan de calidad	Establece la estrategia y recursos a utilizar para la planeación y ejecución del aseguramiento de la calidad. Define los elementos a ser revisados, auditados y probados, los entregables a ser elaborados y los criterios de aceptación del producto o servicio adquirido. Algunos elementos que se detallan en este documento son: • Define al producto o servicio • Estrategia de calidad • Tipos de Prueba a ejecutar • Recursos disponibles • Requerimientos de ambientes • Estimaciones
Ambiente de verificaciones	Ambiente que contiene la configuración adecuada en los que residirá el producto de trabajo a verificar.
Reporte de revisión	Contiene el registro de los defectos y hallazgos encontrados durante las revisiones realizadas, tales como, revisiones entre colegas, evaluaciones y auditorias, así como se utiliza para dar seguimiento a los defectos hasta su cierre.
Escenarios de prueba	Contiene todos los escenarios pruebas, agrupándolos y mostrando la severidad y prioridad de cada uno, además de los puntos de verificación por cada escenario, así como el estatus final, una vez ejecutado.
Solicitud para ambiente de pruebas	La solicitud de ambiente se realiza según el medio definido en el proyecto. Algunos ejemplos son correo electrónico, solicitud o algún otro medio de comunicación formal.

Nombre	Descripción
Listas de verificación	Documento en el cual se establecen los criterios y puntos críticos a revisar en una auditoria, revisión o evaluación, para determinar el adecuado desempeño Y su apego al proceso definido.
Lecciones aprendidas	Repositorio donde se guardarán las lecciones aprendidas resultantes de la ejecución de los procedimientos.

7.7.3.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Índice defectos x validación	Incrementar la eficiencia operativa de la validación de software	Defectos encontrados en validación / horas de validación (incluyendo preparación y re-trabajos)	Eficacia	De gestión	Defectos/Hora	Líder de proyecto	Al cierre de la fase de liberación
Densidad defectos x validación	Reducir la densidad de defectos x validación	Defectos encontrados en validación / requerimientos	Eficacia	De gestión	Defectos/Requerimientos	Líder de proyecto	Al cierre de la fase de liberación
Índice de desempeño de pruebas	Gestionar de manera objetiva la eficiencia operativa del proceso de calidad	Porcentaje de desviación entre casos de prueba planeados y casos de prueba ejecutados	Eficacia	De gestión	((casos de prueba ejecutados - casos de prueba planeados a ejecutar) / casos de prueba planeados a ejecutar)	Líder de proyecto	A solicitud de la UTIC

7.7.3.4 Reglas del proceso

1.1	Para todos los casos los requerimientos de las unidades responsables y los requerimientos técnicos de la solución tecnológica deberán ser identificados, documentados y aprobados.
1.2	Se deberán establecer criterios de aceptación y procedimientos de verificación y validación que permitan verificar que la solución tecnológica no presenta defectos y funciona correctamente.
1.3	El responsable de la elaboración de la solución tecnológica es el responsable de la calidad de los productos, componentes y documentos asociados a la entrega de la solución tecnológica.
1.4	Se deberán realizar revisiones para asegurar la calidad en los productos y los procesos documentando los resultados, estas revisiones se deberán de llevar a cabo por equipos independiente a aquellos que ejecutan los procesos y generan los productos.
1.5	Se deberán tomar las acciones correctivas necesarias para cada uno de los defectos detectados en

	los procesos de verificación y validación, así como darles seguimiento hasta su atención total y definitiva.
1.6	Se deberán analizar los resultados de los diferentes tipos de revisiones en forma periódica, mantener su registro y comunicarlos institucionalmente.
1.7	Se deberá de asegurar la comunicación oportuna de las lecciones aprendidas resultantes del proceso de las revisiones a los productos y servicios de trabajo.
1.8	Se deberán de incluir las actividades necesarias para asegurar que se cubran los requerimientos especificados en la política de seguridad de la dependencia o entidad.
1.9	El plan de calidad deberá de incluir las actividades necesarias para asegurar la verificación y validación de los productos y procesos, así como la participación de los recursos humanos y herramientas necesarias para la ejecución de las actividades.
1.10	El Plan de calidad deberá de estar incluido o integrado con el Plan de proyecto asegurando la integración con otras entidades o interfaces con áreas o sistemas.
1.11	Todos los resultados obtenidos en las verificaciones y validaciones deberán de estar almacenadas y comunicadas, ver el proceso AD.

7.7.3.5	**Documentación soporte del proceso**
	No aplica

7.8 TRANSICIÓN Y ENTREGA

7.8.1. Administración de cambios

7.8.1.1 Objetivos del proceso

General.-

Lograr una integración eficiente, segura y oportuna de los cambios que modifican el ambiente operativo mediante la definición y establecimiento de los métodos, procedimientos y estándares necesarios.

Específicos.-

1. Asegurar que toda propuesta de cambio recibida incluya una justificación técnica y económica.
2. Validar y calendarizar la propuesta de cambio mediante revisión detallada de su justificación.
3. Asegurar que la información relacionada con los cambios se documente para su medición y comunicación.
4. Administrar adecuadamente los riesgos inherentes a los cambios.

7.8.1.2 Descripción del proceso

7.8.1.2.1 Mapa general del proceso

Diagrama de flujo de información

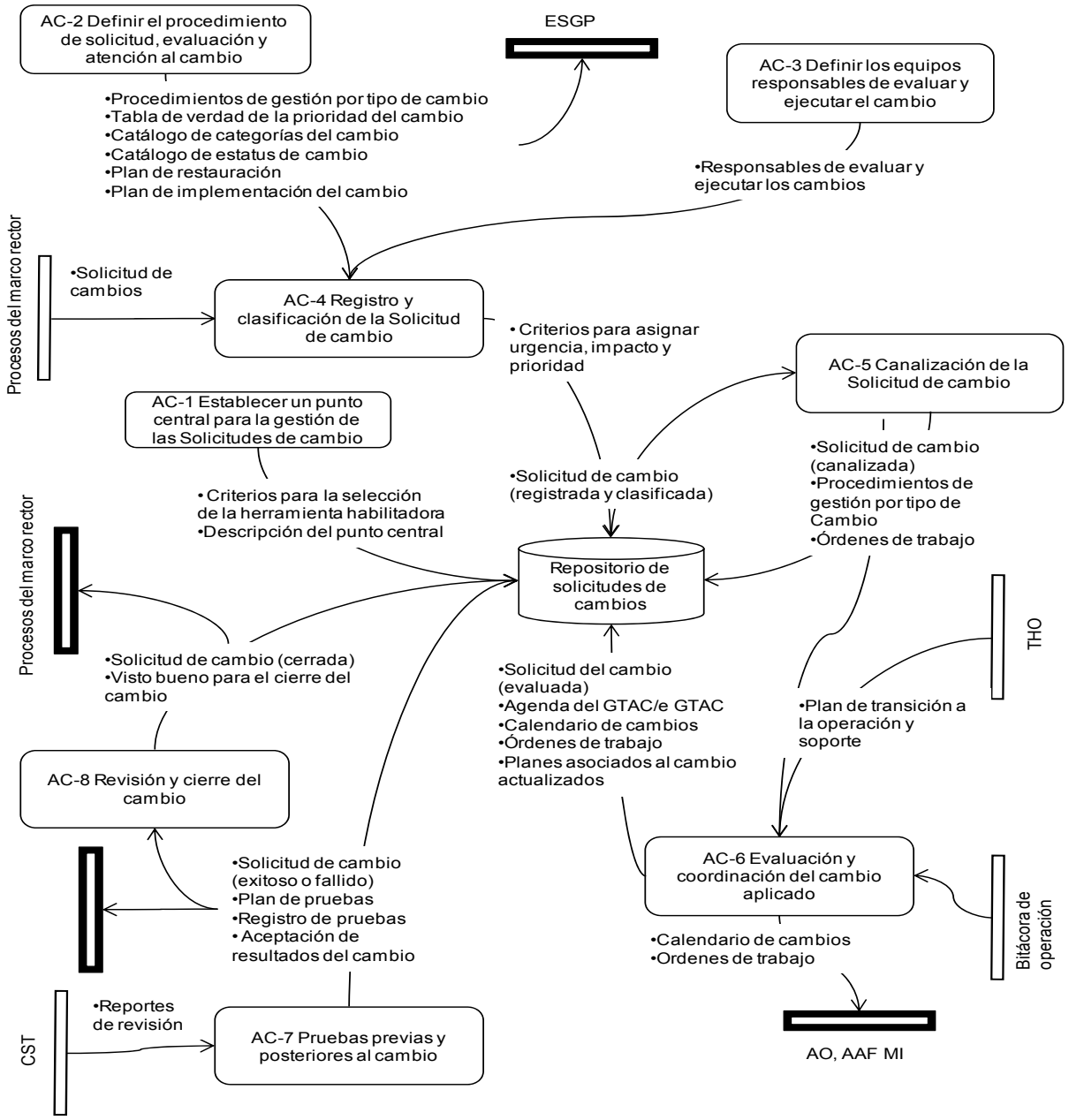
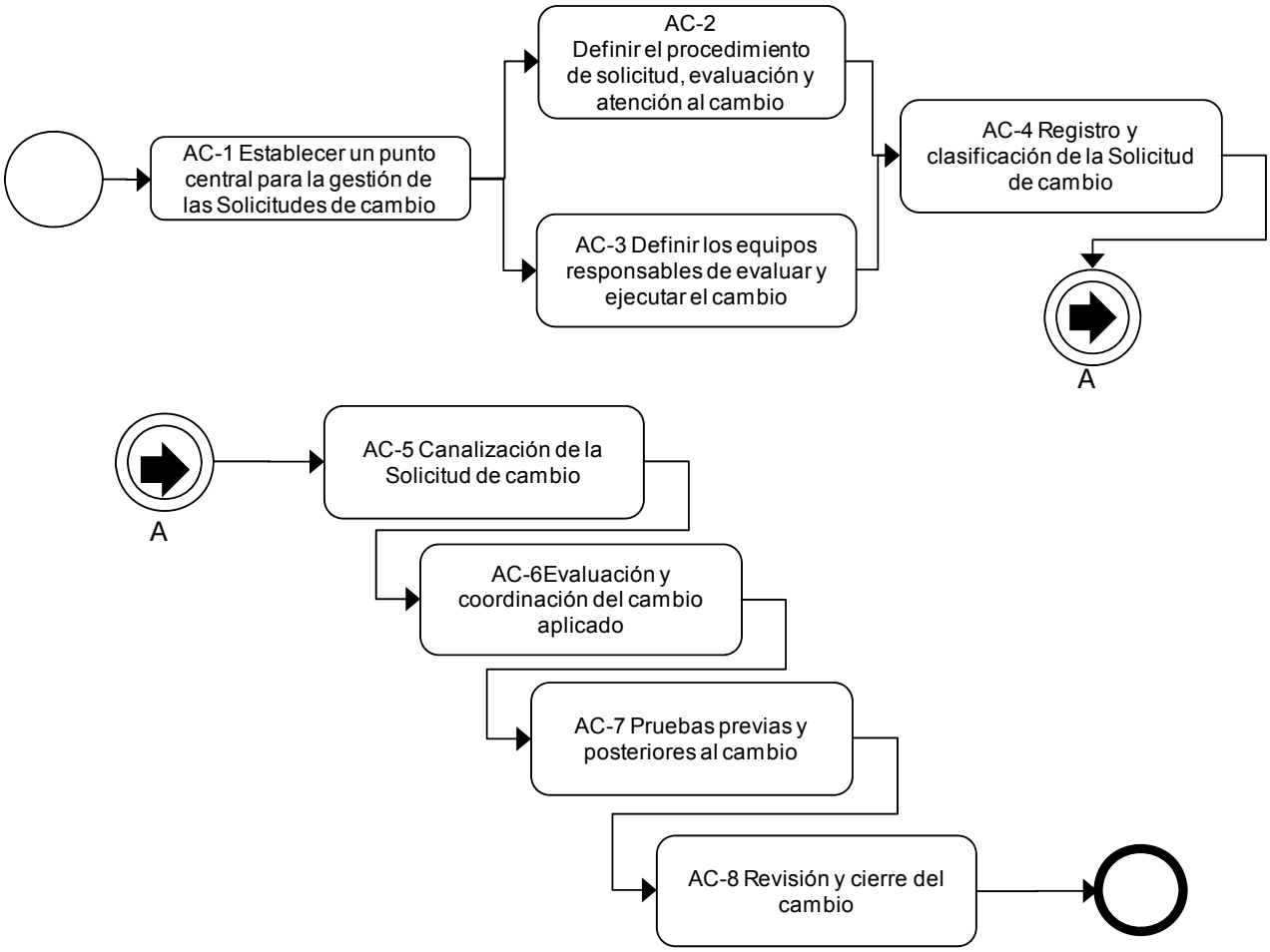


Diagrama de flujo de actividades



7.8.1.2.2 Descripción de las actividades del proceso

AC-1 Establecer un punto central para la gestión de las Solicitudes de cambio

Descripción	Es necesario establecer un punto central o único, a través del cual se administre de manera centralizada el ciclo de vida de las Solicitudes de cambio que permita su control adecuado. Esto con el fin de minimizar la probabilidad de conflictos entre cambios, que derive en una posible afectación al ambiente operativo de la dependencia o entidad.
Factores Críticos	1. Establecer el punto central para la Administración de cambios y realizar la difusión del mismo entre los interesados, incluidos aquellos que tendrán el rol de Solicitante del cambio. 2. De haberse decidido que el punto central para gestionar los cambios sea diferente a la mesa de servicios, deberá generarse la interfase de trabajo entre ambos para lograr consistencia y comunicación en las actividades de ambos procesos. 3. Definir y difundir los canales de comunicación oficiales para la administración de cambios (teléfono, correo electrónico, páginas y formatos Web) 4. Implementar las herramientas tecnológicas que permitan la recepción y gestión de la Solicitud de cambio. 5. Establecer la interfaz del punto central para cambios, con los procesos y funciones con los que se relacione la administración de cambios.
Relación de productos	• Criterios para la selección de la herramienta habilitadora • Descripción del punto central

AC-2 Definir el procedimiento de solicitud, evaluación y atención al cambio

Descripción	La Solicitud de cambio es el instrumento mediante el cual, se requiere la modificación de un elemento del entorno operativo actual, por lo que es necesario que dicho formato contenga la información mínima necesaria para que sea posible procesar el cambio a lo largo de su ciclo de vida. Debe entonces establecerse qué información se requiere integrar a la Solicitud de cambio para su gestión.
Factores Críticos	1. Definir los datos mínimos que se requieren del Solicitante del cambio tales como nombre y detalles de contacto. • Pedir al Solicitante del cambio que describa en la solicitud, el detalle del Cambio propuesto. • Solicitar la justificación de la Solicitud de cambio en términos de beneficios a la dependencia o entidad. 2. Establecer un control (lista o herramienta) para asegurar que en la Solicitud de cambio se identifiquen los riesgos potenciales que se derivan del cambio, incluyendo tanto riesgos de tipo técnico, como de negocio. 3. Establecer un identificador único por cada Solicitud de cambios para evitar la duplicidad de los mismos y facilitar su monitoreo. 4. En caso de tratarse de un cambio derivado de un incidente, problema o iniciativa, incluidas la de mejora, referir el identificador de esos otros registros. 5. Asegurar que el solicitante incluya la petición de una ventana de tiempo del cambio, en la que se considere el tiempo que demandará aplicar todas las actividades, cuando así aplique. 6. Definir con qué autorizaciones previas debe contar el Solicitante del cambio al hacer su

solicitud, cuando así aplique.

7. En caso de existir un repositorio o inventario de los elementos del ambiente productivo (activos, elementos de configuración, procesos, servicios, formatos, roles), solicitar que se listen los elementos que serán impactados directa o indirectamente por el cambio.
8. Establecer la documentación mínima que se requerirá para soportar la Solicitud de Cambio (Plan de implementación del cambio, Plan de restauración, Plan de pruebas, entre otros).
9. Definir qué documentación será la mínima requerida para solicitar un cambio de emergencia.
10. Determinar qué documentación sería opcional para ciertos tipos de cambio.
11. Solicitar cuando así aplique, el resultado de pruebas controladas del cambio realizadas previamente.
12. Definir los tipos de cambio que estarán disponibles para la clasificación de las Solicitudes de cambio
13. Deberán considerarse al menos los tres tipos referidos en el marco de mejores prácticas de ITIL:
    a. Cambio estándar (pre autorizado)
    b. Cambio normal
    c. Cambio de emergencia
14. Para cada tipo de cambio, se deberá desarrollar un procedimiento en particular que se aplicará sobre ese tipo de cambio.
15. Al clasificar un cambio, deberá elegirse el tipo de cambio que aplique.
    Establecer un mecanismo para diferenciar aquellos cambios que resultan de un incidente o problema, de los que tienen como motivo una mejora.
16. Definir durante el diseño del proceso de Administración de cambios, los estatus que reflejen los diferentes estados por los que puede pasar un cambio.
17. Los estatus del cambio deberán estar disponibles en la herramienta habilitadora (posteriormente descrita) del proceso para su uso y deberán poderse cambiar conforme se requiera.
18. Definir las reglas que aplicarán para el cambio de estatus de un registro de cambio en la herramienta habilitadora.
19. Conforme el cambio avance a través de su ciclo de vida, el estatus del registro deberá ser actualizado para reflejar su estado actual.
20. Determinar el impacto del cambio a través de la medición de su efecto en los procesos operativos de la dependencia o entidad.
21. El impacto del cambio no deberá deducirse considerando únicamente un enfoque cuantitativo del cambio.
22. Determinar la urgencia del cambio mediante la medición de cuánto tiempo tomará hasta que el cambio tenga un Impacto en la dependencia o entidad.
23. La prioridad del cambio se determina a partir de considerar ambos, el impacto y la urgencia del cambio mediante una tabla de verdad. Con la prioridad se determina el lugar del cambio en relación a otros pendientes.
24. El impacto, urgencia y por lo tanto la prioridad, pueden cambiar mientras el cambio avanza en su ciclo de vida.
25. Deberán considerarse al menos los cuatro tipos de prioridad referidos en el marco de mejores practicas de ITIL:
    - Baja
    - Normal
    - Alta
    - Urgente
26. Definir los niveles que se necesitarán para categorizar los cambios.

	27. Definir las categorías de cambio que se prevé puedan abarcar la mayor parte de los posibles tipos de cambio en cuanto a su naturaleza. 28. Las categorías de los cambios deben describir el rubro que será afectado, por ejemplo procesos, hardware, software, aplicaciones, etc. 29. Las subcategorías deberán estar relacionadas a la categoría del nivel anterior y refieren el detalle de ese nivel.
Relación de productos	• Procedimientos de gestión por tipo de cambio • Tabla de verdad de la prioridad del cambio • Catálogo de categorías del cambio • Catálogo de estatus de cambio • Plan de restauración • Plan de implementación del cambio

AC-3 Definir los equipos responsables de evaluar y ejecutar el cambio

Descripción	No obstante que cada cambio es diferente del resto en cuanto a naturaleza, complejidad y alcance, es posible acotar los equipos responsables de evaluar y ejecutar los cambios que se propongan. Una vez identificados los equipos, deben cargarse en la herramienta habilitadora para que sea posible la asignación de actividades a esos equipos.
Factores Críticos	1. Identificar a todos aquellos equipos de especialistas para la evaluación y ejecución de los cambios, a quienes se les podrán asignar la evaluación y ejecución de los cambios. 2. De existir una herramienta habilitadora para el proceso de administración de cambios, cargar a los equipos definidos en la herramienta habilitadora para la asignación de los cambios y la notificación de dicha asignación.
Relación de productos	• Responsables de evaluar y ejecutar los cambios

AC-4 Registro y clasificación de la solicitud de cambio

Descripción	Una vez que el Solicitante hace llegar su Solicitud de cambio, esta deberá ser registrada y clasificada en la herramienta habilitadora que se haya destinado para este fin. El Solicitante del cambio recibirá una notificación con el identificador único que distinguirá individualmente su solicitud, para su seguimiento. También, como resultado de la clasificación que se realice, se habrá determinado la naturaleza del cambio, su Impacto previsto, la urgencia y prioridad respecto a otros cambios y la ruta que seguirá para su evaluación.
Factores Críticos	• Recibir la Solicitud de cambio por los canales de comunicación establecidos para este fin. • Validar que la Solicitud de cambio se entregó en el formato que se haya definido para ese fin. • Las Solicitudes de cambios incompletos o imprácticas deberán ser rechazadas. • Cuando así aplique, validar que el Solicitante del cambio esté autorizado para requerir un cambio. • Preferentemente, se deberá contar con una herramienta habilitadora que permita capturar en un registro electrónico, la información provista en la solicitud de cambio. • Capturar y clasificar la solicitud de cambio con base en la información provista en el formato y la documentación de soporte adjunta. • Generar las órdenes de trabajo para la evaluación del cambio por los especialistas, cuando por el tipo de cambio así lo requiera.

Relación de productos	• Criterios para asignar urgencia, impacto y prioridad • Solicitud de cambio (registrada y clasificada)

AC-5 Canalización de la Solicitud de cambio

Descripción	Dependiendo del tipo de cambio, así como de su prioridad y categoría, la solicitud es dirigida a la siguiente actividad y roles que apliquen según el procedimiento que corresponda.
Factores Críticos	1. Con base en el tipo, prioridad y categoría, determinar que procedimiento aplica para el tratamiento de la solicitud. 2. Canalizar la solicitud a la actividad que corresponda según el procedimiento. 3. Documentar todas las actividades realizadas, en el registro del cambio. 4. Dar seguimiento al avance del cambio.
Relación de productos	• Solicitud de cambio (canalizada) • Procedimientos de gestión por tipo de Cambio • Órdenes de trabajo

AC-6 Evaluación y coordinación del cambio aplicado

Descripción	El procedimiento de evaluación del cambio depende de la clasificación con la que haya sido registrada la solicitud. Dependiendo del tipo de cambio, prioridad y categoría, podrá variar quién, qué y cómo se evalúa el cambio.
Factores Críticos	1. En general, para la evaluación de un cambio se considerarán las respuestas a los siguientes cuestionamientos: • ¿Quién solicitó el cambio? • ¿Cuál es la justificación del cambio? • ¿Qué beneficios se logran a partir del cambio? • ¿Qué riesgos están asociados al cambio? • ¿Qué recursos se requieren para realizar el cambio? • ¿Quiénes son responsables de la ejecución prueba e implementación del cambio? • ¿Cuáles es la relación de este cambio con otros previos? • ¿Se cumplieron los objetivos previstos? • ¿Cuál ha sido la percepción de los usuarios respecto al cambio? • ¿Se pusieron en marcha los planes de retorno en alguna fase del proceso? ¿Por qué? • La evaluación del cambio regularmente se lleva a cabo en dos ocasiones en diferentes momentos del ciclo de vida del cambio. Una primera evaluación generalmente la lleva a cabo el equipo de especialistas, mientras que la segunda es realizada por el grupo de trabajo asesor de cambios y/o grupo de trabajo asesor de cambios de emergencia y el Administrador de cambios. 2. Definir el riesgo implícito en el cambio mediante una matriz de categorización del riesgo. 3. Se debe determinar si la prioridad o categoría del cambio necesitan ser actualizados. 4. Con base en el resultado de la evaluación y de ser autorizado el cambio, modificar los planes asociados al cambio cuando así sea necesario. 5. Actualizar y compartir el calendario de cambios con los involucrados en el cambio. 6. Documentar todas las actividades realizadas en el registro del cambio. 7. De estar aprobado el cambio, generar las órdenes de trabajo para la ejecución del cambio. 8. Se coordinan las actividades para llevar a cabo el cambio por el equipo responsable de ejecutar el cambio.
Relación de	• Solicitud del cambio (evaluada)

productos	• Agenda del GTAC/e GTAC • Calendario de cambios • Órdenes de trabajo • Planes asociados al cambio actualizados

AC-7 Pruebas previas y posteriores al cambio

Descripción	Un cambio necesita ser probado antes y después de su aplicación, aún cuando se trate de cambios de emergencia. En el primer caso, las pruebas se realizan para validar a través de un ambiente controlado, que con el cambio se logran los resultados esperados sin que resulten afectaciones a la dependencia o entidad. Las pruebas posteriores al cambio, se efectúan para validar si el cambio cumplió o no con su objetivo, si arrojó los resultados esperados y si no derivó en un daño colateral en el ambiente operativo de la dependencia o entidad que implique incluso detener el cambio y regresar los elementos afectados a su estado original antes del cambio.
Factores Críticos	1. En los ambientes de prueba, deberían emular lo mejor posible el ambiente de producción. 2. Para los cambios de emergencia, adecuar la requisición de pruebas de tal forma que se realicen, aunque de manera limitada de acuerdo al tiempo y necesidad que plantee el escenario que se experimente en la operación. 3. Los resultados de las pruebas previas al cambio, podrían solicitarse como parte de la documentación que debe soportar la propuesta del cambio. 4. Las pruebas a realizar una vez que se haya implementado el cambio, deberán haber sido documentas y entregadas junto con la Solicitud de cambio. 5. El plan de pruebas y su ejecución son imperativos para cualquier tipo de cambio, incluido el de emergencia. 6. Todo cambio deberá incluir un plan de restauración a través del cual sea posible regresar el entorno a su estado original. 7. Documentar todas las actividades realizadas, en el registro del cambio.
Relación de productos	• Solicitud de cambio (exitoso o fallido) • Plan de pruebas • Registro de pruebas • Aceptación de resultados del cambio

AC-8 Revisión y cierre del cambio

Descripción	Cuando un cambio ha sido ejecutado, se deberán valorar y validar los resultados logrados. Para esto se determina si el cambio fue exitoso o falló, si se logró cumplir con el objetivo que se fijó para el cambio, si este derivó o no en incidentes o problemas en el ambiente operación y si tanto el solicitante como los interesados, incluyendo los representantes de la dependencia o entidad, están satisfechos con la ejecución y los resultados logrados.
Factores Críticos	Definir si la revisión post implementación del cambio se aplicará sobre la totalidad de los cambios terminados en el periodo o sobre una muestra. Determinar si las actividades realizadas en el cambio se hicieron conforme a lo planeado y no se experimentó alguna desviación importante que haya derivado en un riesgo para el ambiente operativo o el cambio mismo, o incluso haya resultado en la falla del cambio. Confirmar si el cambio logró su objetivo. Verificar con el representante de la dependencia o entidad y los usuarios, si surgieron o no incidentes o problemas a partir de la aplicación del cambio.

	En general, medir la satisfacción del Solicitante del cambio, del Usuario y de todos los involucrados respecto a cómo se ejecutó el cambio y los resultados logrados. Documentar todas las actividades realizadas, en el registro del cambio. La evaluación de desempeño del proceso, deberá realizarse mediante el proceso de Administración del desempeño de TIC.
Relación de productos	• Solicitud de cambio (cerrada) • Visto bueno para el cierre del cambio

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.8.1.2.3 Descripción de roles

Rol	Descripción
Administrador de cambios	Recibe, registra y clasifica el cambio, convoca al GTAC/eGTAC para la evaluación del mismo, lleva las reuniones de evaluación, coordina las actividades del proceso y decide la autorización o rechazo de la propuesta junto con el comité que aplique. Seguimiento del cambio y actualización del registro del mismo, a lo largo de su ciclo de vida.
Grupo asesor de cambios (GTAC)	Grupo de trabajo que evalúa, asesora y aconseja acerca de un cambio propuesto y que regularmente junto con el Administrador de cambios, decide la aprobación o no del cambio.
Grupo asesor de cambios de emergencia (eGTAC)	Grupo de trabajo conformado por los roles mínimos necesarios con la experiencia y autoridad suficiente para evaluar y decidir la procedencia de un cambio de emergencia.
Solicitante del Cambio	Solicitante del cambio mediante el formato definido para este fin, integrando a dicha solicitud toda la información y documentación que aplique y sea requisito para el tipo de cambio en cuestión. También valida el cierre del cambio después de realizar una verificación de su ejecución y resultados logrados. Los cambios pueden ser solicitados a partir de necesidades derivadas de la ejecución de los procesos del marco rector.
Equipo responsable de ejecutar el cambio	Equipo(s) de experto(s) dentro del ámbito de aplicación del cambio, responsables de evaluar y validar técnica o conceptualmente el cambio propuesto, para que sus observaciones sean consideradas por los roles que deciden la autorización del cambio. También son los responsables de la implementación de los cambios aprobados para su implementación dentro de la ventana de tiempo, costo y procedimientos definidos en los planes, así como de documentar las actividades realizadas y aplicar el procedimiento de restauración cuando un cambio falla en su implementación.

7.8.1.2.4 Descripción de productos

Producto	Descripción

Descripción del punto central	Definición de las actividades del proceso de cambio: • Objetivo del cambio • Beneficios • Áreas involucradas • Impactos: o Costos o Ingresos o Social
Solicitud de cambio	Formato para documentar el propósito y detalles del cambio propuesto que es sometido a consideración y valoración por parte los roles con la autoridad para decidir su procedencia o rechazo. Características: • Contiene los detalles de las propuesta del cambio • Nombre y detalles del contacto • Se le asigna un identificador único • Se anexan al formato, documentos de soporte
Plan de implementación del cambio	Plan donde se definen de forma detalla las actividades a ejecutar para la implementación del cambio, incluyendo tiempos y recursos.
Plan de restauración	Documento donde se especifican las acciones para regresar el entorno a su estado original en caso de que la implementación del cambio resulte fallido.
Plan de pruebas	Plan donde se describen las prueba a ejecutar para determinar el éxito o fracaso del cambio o del plan de restauración.
Registro de pruebas	Registro de los resultados y defectos localizados durante la ejecución de las pruebas, que pudieron haber sido realizadas previamente a la Solicitud del cambio.
Procedimiento de gestión por tipo de cambio	Conjunto de acciones a seguir específicas para cada tipo de cambio.
Catálogo de estatus del cambio	Documento donde se listan y describen los estatus que podrán utilizarse durante el ciclo de vida del cambio, y las reglas que aplican para pasar de uno a otro y por quién.
Tabla de verdad de la prioridad del cambio	Tabla para determinar la prioridad que tiene el cambio a través del impacto al negocio y el nivel de urgencia solicitado para su implantación.
Catálogo de categorías del cambio	Documento donde se definen los niveles que debe cubrir un cambio para poder ser categorizado, con base en los elementos que se afectarán.
Criterios de selección de la herramienta habilitadora para el proceso de cambios	Especificaciones para poder seleccionar una herramienta mediante la cual sea posible automatizar algunas o todas las actividades del proceso de cambios. Cada criterio describe las características y funcionalidades que se deben evaluar de acuerdo a las necesidades del negocio.

Agenda del GTAC/e GTAC	Documento donde se describen los temas a abordar durante las sesiones del GTAC o eGTAC.
Planes asociados al cambio actualizados	Son los planes originales de instalación, pruebas y regresión de un cambio, con las adecuaciones que hayan resultado de su evaluación.
Visto bueno para el cierre del cambio	Aprobación del cambio en vista del nivel de satisfacción del Solicitante del cambio y todos los involucrados.
Calendario de cambios	Calendario en donde se registran todo los cambios aprobados para ejecutarse y que se comparte con los interesados.
Criterios para asignar urgencia, impacto y prioridad	Documento en donde se describen las pautas para clasificar un cambio en cuanto a su urgencia, impacto y prioridad.
Catálogo de categorías del cambio	Lista ordenada de las categorías válidas y disponibles para clasificar una Solicitud de cambio con base en su ámbito de aplicación y naturaleza.
Criterios para asignar categorías	Documento en donde se describen las pautas para clasificar un cambio, esto con base en el Catálogo de categorías del cambio.
Repositorio de solicitudes de cambios	Sitio centralizado dedicado a almacenar las Solicitudes de cambio.
Orden de trabajo	Documento a través del cual se solicita la ejecución de actividades que generen una solución hacia una petición.
Aceptación de los resultados del cambio	Documento que formaliza la aceptación de los resultados del cambio.
Responsables de evaluar y ejecutar el cambio	Lista de personas con el perfil adecuado para evaluar y ejecutar un cambio solicitado de acuerdo a su impacto y urgencia.

7.8.1.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Indicador de órdenes de cambio	Cuantificar los cambios solicitados en el periodo	Medir la cantidad de órdenes de cambio solicitadas para los requerimientos del periodo	Eficiencia	De gestión	Valor acumulado de las órdenes de cambio del periodo	Líder de proyecto	Mensual

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Eficiencia en el proceso de cambios	Incrementar la proporción de los cambios exitosos	Medir la proporción de cambios exitosos con respecto al total	Eficiencia	De gestión	Câmbios exitosos / total de cambios	Líder de proyecto	Mensual

7.8.1.4	Reglas del proceso
1.1	El titular de la UTIC designará al área responsable del proceso de Administración de cambios.
1.2	Todo cambio que esté dentro del alcance definido para el proceso, deberá ser gestionado mediante el proceso de Administración de cambios.
1.3	Los participantes del proceso de Administración de cambios cumplirán con las disposiciones establecidas en dicho proceso.
1.4	Todo cambio deberá ser justificado, registrado, clasificado, monitoreado, evaluado, priorizado, planeado, probado y documentado, así como revisado tras su implementación.
1.5	Para la evaluación y autorización del cambio, se deberá de involucrar siempre por lo menos a un representante de la dependencia o entidad con la visión y autoridad para ver por los intereses de la dependencia o entidad.
1.6	Los cambios de emergencia se reservan exclusivamente a aquellos que responden a un Incidente “crítico o inesperado” que produce interrupciones al servicio o exista algún riesgo de que el usuario no pueda realizar sus actividades y deberá contar con la documentación asociada a posteriori.
1.7	Todas las actividades involucradas en el proceso de cambios deberán ser asignadas a algún rol, mismo que tendrá la responsabilidad y autoridad para realizarlas.
1.8	Los roles y responsabilidades, deberán definirse mediante el proceso de establecimiento de estructura de gobierno de TI.
1.9	Se deberá asignar un responsable del proceso de administración de cambios.
1.10	Se deberá asegurar que los controles y niveles de acceso que se establezcan eviten que personal no autorizado realice cambios en el ambiente productivo.
1.11	Se deberán diseñar, generar y evaluar regularmente métricas de desempeño a través de las cuales se pueda identificar la efectividad y eficiencia del proceso, con fines de verificación y mejora.
1.12	Los cambios que fallen durante su ejecución, deberán ser documentados y cerrados para dar inicio a una nueva Solicitud de cambio cuando se decida intentar de nuevo el cambio.
1.13	Las políticas de seguridad de la información que aplican para la dependencia o entidad, son extensivas al proceso de Administración de cambios.
1.14	La evaluación de desempeño del proceso, deberá realizarse mediante el proceso de Administración del desempeño de TIC.
1.15	Todo cambio deberá contar con un plan de regreso que permita la recuperación de la última configuración estable antes del inicio de la ejecución del cambio.
1.16	Se deberá asegurar que la totalidad de las solicitudes de cambio que se ingresen al proceso para su ejecución reúnan los requisitos mínimos necesarios para asegurar su control.

7.8.1.5	Documentación soporte del proceso
	No aplica

7.8.2. Liberación y entrega

7.8.2.1 Objetivos del proceso

General.-

Garantizar que la solución tecnológica o servicio que se entregue para su puesta de operación, cumpla con los requerimientos técnicos establecidos y con los necesarios para su puesta en operación.

Específicos.-

1. Asegurar que se elaboren planes de liberación y entrega aprobados por las partes involucradas.
2. Garantizar que el paquete de liberación de una solución tecnológica o servicio sea construido, instalado, probado y desplegado eficientemente en el ambiente de implementación de manera oportuna y exitosa.
3. Asegurar que los paquetes de liberación puedan ser rastreados, verificados, desinstalados y respaldados ágilmente para responder oportunamente a cambios o eventos inesperados.
4. Asegurar que el paquete de liberación de la solución tecnológica o servicio que se entregue para su puesta en operación así como sus elementos habilitadores entreguen los requerimientos de servicio comprometidos.
5. Asegurar que los paquetes de liberación y los componentes que los constituyen sean registrados total y correctamente en CMDB para que los involucrados garanticen el mantenimiento, la continuidad y la disponibilidad del servicio.

7.8.2.2 Descripción del proceso

7.8.2.2.1 Mapa general del proceso

Diagrama de flujo de información

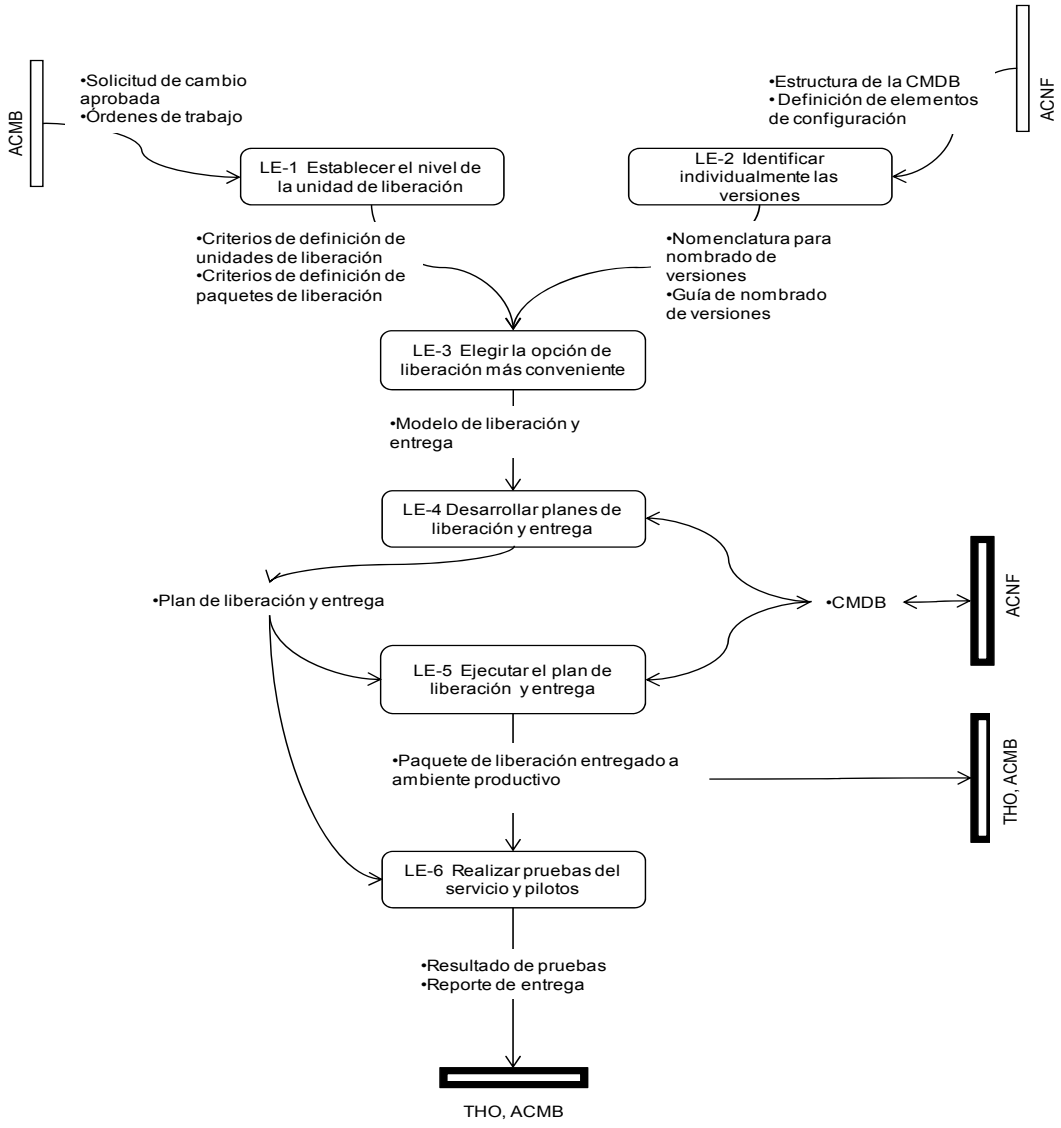
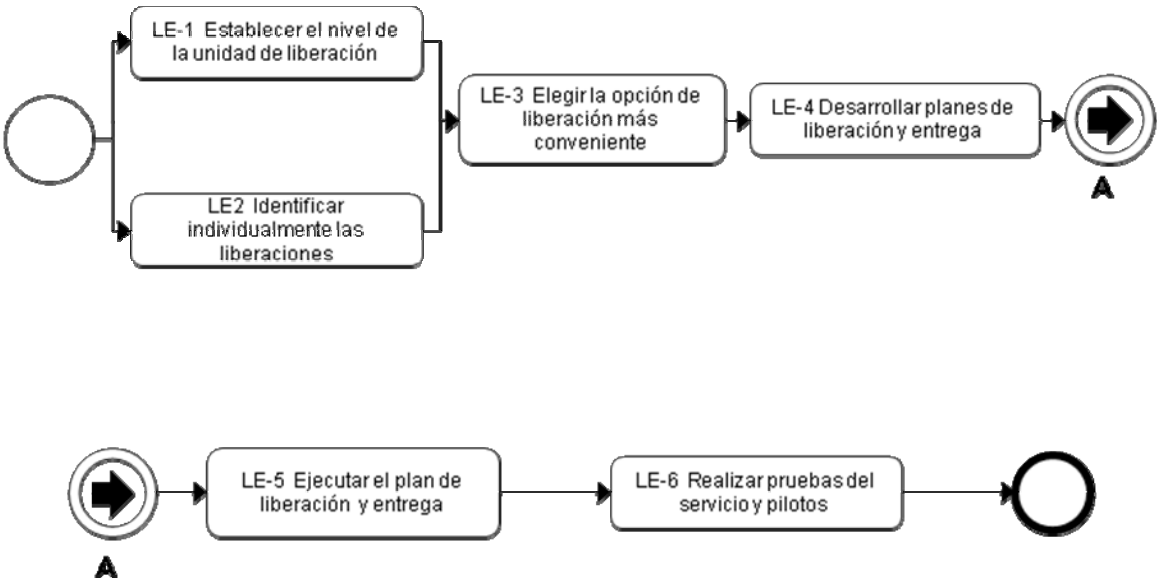


Diagrama de flujo de actividades



7.8.2.2.2 Descripción de las actividades del proceso

LE-1 Establecer el nivel de la unidad de liberación

Descripción	Decidir el nivel más apropiado que se manejará como unidad de liberación, el cual depende de la conveniencia y necesidad de la dependencia o entidad, así como los recursos que se puedan destinar para su administración. La unidad de liberación puede variar dependiendo de los tipos o elementos de los activos de servicio o componentes, tales como hardware y software.
Factores Críticos	1. Identificar, definir y considerar los tipos de unidades de liberación. 2. Decidir el nivel de detalle o granularidad de la unidad, considerando que la complejidad y efectividad de las actualizaciones subsecuentes, estarán directamente relacionadas con el nivel que se decida. 3. Considerar el costo y facilidad de liberar, actualizar y retirar la unidad de liberación en relación a su tamaño y complejidad de la unidad y los elementos con los que se relaciona. 4. La cantidad de recursos y tiempo necesario para construir, distribuir y probar la unidad de liberación, dependerá del tipo, tamaño y complejidad de la unidad y los elementos con los que se relaciona. 5. Asegurar que se puedan construir y probar en paralelo e integrar en un solo paquete de liberación. 6. Decidir tomando en cuenta la complejidad de las interfases que existirán entre la unidad propuesta, otras unidades, el paquete de liberación, los servicios de TIC y la infraestructura. 7. Asegurar que el paquete de liberación consista de activos y componentes que son compatibles entre sí. 8. Asegurar que el paquete de liberación puede construirse, instalarse y probarse. 9. Verificar dependencias entre las unidades que conforman el paquete, así como el paquete en cuestión y otros paquetes de liberación. 10. El paquete de liberación debe ser diseñado de tal forma que algunas unidades de liberación puedan ser removidas si son causantes de fallas durante su prueba u operación.
Relación de productos	• Criterios de definición de unidades de liberación • Criterios de definición de paquetes de liberación

LE-2 Identificar individualmente las versiones

Descripción	Identificar individualmente y de manera única las versiones. La identificación debe incluir una referencia hacia el elemento de configuración que representa, así como un número de versión que normalmente se compone de varias partes que indican el nivel e importancia de esa versión en lo particular.
Factores Críticos	1. Establecer reglas para la identificación de las unidades y paquetes de liberación. 2. El identificador de la versión deberá incluir una referencia al elemento de configuración que representa y el número de versión. 3. Considerar el uso de un sistema para administrar las versiones.
Relación de productos	• Nomenclatura para nombrado de versiones • Guía de nombrado de versiones

LE-3 Elegir la opción de liberación más conveniente

Descripción	Elegir el método más adecuado de liberación, considerando las ventajas así como los riesgos, y dependiendo del tipo, volumen, número de ubicaciones y complejidad de la liberación que se vaya a realizar. Para el despliegue del paquete de liberación, pueden considerarse varias opciones en cuanto a la estrategia a seguir.
Factores Críticos	1. El método de liberación elegido debe ser justificado, acordado y comunicado a los representantes de la dependencia o entidad y áreas especialistas interesadas. 2. Considerar la infraestructura y recursos disponibles; cada método de liberación exigirá recursos, procedimientos, riesgos y complejidad diferentes en distintos tiempos de la liberación. 3. Considerar si es posible técnicamente o conveniente para la dependencia o entidad, que dos o más versiones del producto coexistan por algún tiempo en el ambiente operativo. 4. Considerar el uso de varios métodos de despliegue para maximizar los beneficios de cada uno y minimizar sus debilidades. 5. Usar una estrategia de liberación de tipo masivo solo cuando el riesgo y recursos demandados son bajos y cuando sea rutinario, o cuando la liberación es emergente. 6. Usar un método por fases cuando el riesgo sea admisible y se necesite comprobar antes de liberar masivamente., cuando necesite afinarse el procedimiento. 7. Usar una estrategia de liberación obligatoria cuando necesite forzarse el pase a producción de la liberación, por ejemplo en caso de una actualización importante o urgente. 8. Usar una estrategia de liberación de acceso voluntario cuando se puedan centralizar el almacenamiento de la liberación y se quiera dar la opción del momento del despliegue al usuario que lo recibe. 9. Usar un método automático permite generalmente lograr repetibilidad y consistencia, verificar previamente la compatibilidad de elemento destino para recibir la liberación, seleccionar la población destino específico e incluso automatizar mediante calendario, hacer el despliegue sin o con el mínimo de intervención humana. Sin embargo, considerar que el alcance de este método se limita a aquellos ambientes a los que llegue la tecnología. 10. Considerar la tolerancia e impacto de errores en la dependencia o entidad respecto a la liberación, cuando se considere un método de liberación manual.
Relación de productos	• Modelo de liberación y entrega •

LE-4 Desarrollar planes de liberación y entrega

Descripción	Desarrollar el plan de liberación y entrega que funciona como un conjunto de guías para la liberación en producción. El plan referido, se compone a su vez de otros planes tales como plan para construir y probar previo a liberar en producción, definición de criterio de pase o falla de la liberación, planeación de pilotos, del despliegue, logística y entrega.
Factores	1. El o los planes deberán describir qué porciones de la funcionalidad del sistema será

Críticos	desplegada en qué liberaciones. 2. Los planes de liberación deberán ser validados contra los planes que tenga la dependencia o entidad, con los que pudiera tener un conflicto o debiera coordinarse. 3. Los planes deberán acordarse y compartirse con la dependencia o entidad de tal forma que esta pueda planear sus actividades al considerar los planes. 4. La ejecución de las actividades de los planes que pudieran afectar el ambiente productivo de la dependencia o entidad, deberán ser autorizados mediante el proceso de Cambios. 5. Deberán describirse el contenido de las liberaciones y la relación entre las diferentes etapas de liberación cuando así aplique. 6. Al definir el piloto, determinar su alcance en cuanto a tiempo de duración, participantes, recursos de soporte, etc. 7. Para el o los pilotos, establecer la diversidad, inclusiones y excepciones en cuanto a los participantes.
Relación de productos	• Plan de liberación y entrega • CMDB actualizada

LE-5 Ejecutar el plan de liberación y entrega

Descripción	Ejecución de las actividades del plan de liberación y entrega que comprenden la construcción del paquete de liberación, las pruebas, entrega, soporte temprano y cierre de la entrega.
Factores Críticos	Para la construcción: 1. Determinar el ambiente que se necesita para construir las liberaciones. 2. Definir los procedimientos, metodologías, herramientas y listas de verificación que deberían aplicarse para asegurar que el paquete de liberación sea construido de manera estándar, controlada y replicable. 3. Hacer uso de modelos y metodologías especializadas para la gestión de las actividades de construcción. 4. Asegurar que las actividades de construcción, así como el ambiente, cumplen con las reglas y regulaciones que apliquen, incluyendo las de seguridad de la información. 5. Los avances en la construcción y pruebas deberán registrarse. 6. Prueba de los elementos que compondrán la liberación 7. Empaquetar las liberaciones considerando el modelo y definición de los paquetes y unidades de liberación. 8. Planear las actividades de transición a la operación: transferencia de responsabilidad sobre recursos e instalaciones. 9. Establecer las actividades para el pase de la documentación y la experiencia a la operación. Esto mediante el proceso de Administración del Conocimiento. 10. Transferir los compromisos con motivo de contratos, licencias, fondos y pagos. 11. Asegurar la disponibilidad de los recursos a emplear, principalmente lo que respecta a capital humano. 12. Identificar y en su caso solicitar la autorización de operar en dos ambientes cuando se trate de una liberación por fases. 13. Planear la liberación de recursos en préstamo. 14. Documentación de la construcción y liberación Para las pruebas:

	1. Determinar el ambiente que se necesita para probar las liberaciones, procurando sea lo más similar posible al ambiente productivo sobre el que se realizará la liberación. 2. Asegurar que las actividades de prueba, así como el ambiente, cumplen con las reglas y regulaciones, incluyendo las de seguridad de la información. 3. Establecer controles y procedimientos para medir el impacto de la liberación en el ambiente, una vez que se haya desplegado. 4. Integrar actividades mediante las cuales se verifique que tanto el ambiente, como los servicios y usuarios afectados por la liberación, estén listos para recibir la liberación. 5. Lograr un balance entre los recursos a usar en las pruebas y los beneficios que se derivarán de ellas. Soporte temprano 6. Establecer un plan para el soporte temprano de la operación con los recursos y experiencias generados durante la construcción y la liberación. 7. Delimitar el alcance, naturaleza y duración del soporte temprano
Relación de productos	• Paquete de liberación entregado a ambiente productivo

LE-6 Realizar pruebas del servicio y pilotos

Descripción	Realizar pilotos que permitan verificar que el servicio y ambiente sobre el que se realiza la liberación y la entrega final, recibe de facto los beneficios esperados que originaron el cambio y la liberación, con un impacto limitado en caso de surgir alguna situación negativa inesperada. El piloto debe realizarse además con el fin de identificar áreas de mejora que necesitarán ajustarse previo a la liberación general y la entrega, así como para comenzar a construir la confianza del patrocinador y usuarios acerca del sistema a liberarse.
Factores Críticos	1. Verificar que la integridad del o los paquetes de liberación se haya mantenido durante las actividades de liberación y se registre en el repositorio de configuraciones. 2. Validar que una vez liberado el paquete, el servicio en el que participa cumple con los niveles de servicio. 3. Identificar si hay impacto no previsto en el ambiente que se manifieste en forma de Incidentes o Problemas. 4. Verificar que el servicio se puede usar como se esperaba. 5. Probar los servicios y/o componentes dependientes o afectados directa e indirectamente por la liberación. 6. Lograr patrocinio para el o los pilotos, considerando que pueden demandar tiempo y productividad de los usuarios 7. Reportar el progreso y resultados de las pruebas sobre las liberaciones. 8. Verificar y reportar acerca de que la liberación se haya cumplido dentro del tiempo y costo previstos. 9. Confirmar que el monto de incidentes y problemas que pudieran derivarse de la liberación sean aceptables por la dependencia o entidad y los usuarios.
Relación de productos	• Resultado de pruebas • Reporte de entrega

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.8.2.2.3 Descripción de roles

Rol	Descripción
Gestor de Implementación y Versión	Responsable de la planeación, el diseño, la creación, la configuración, y las pruebas de todo el software y hardware utilizado para crear el paquete de implementación para la entrega del, o los cambios que se le harán, al servicio designado.
Gestor de construcción y empaquetamiento de la Implementación	Establece la configuración final de la implementación (por ejemplo: conocimiento, información, hardware, software, e infraestructura); construye el paquete final de entrega de la implementación, y prueba la entrega final.
Administrador de liberación y entrega	Responsable de la eficiencia y despliegue seguro de los cambios aprobados de solución tecnológica o hardware en el ambiente productivo.

7.8.2.2.4 Descripción de productos

Producto	Descripción
Criterios de definición de unidades de implementación	Documento en donde se describen las pautas para decidir acerca la naturaleza, tamaño y arquitectura de la unidad de liberación.
Criterios de definición de paquetes de liberación	Documento en donde se describen las pautas para decidir acerca la naturaleza, tamaño y arquitectura del paquete de liberación.
Nomenclatura para nombrado de versiones	Documento donde se define y describe la nomenclatura que deberá cumplirse para la identificación y nombrado de las versiones.
Guía de nombrado de versiones	Guía en la que se describe el procedimiento para el nombrado de las versiones.
Criterios de selección del método de liberación	Documento en donde se describen las pautas a considerar para decidir el método de liberación que más convenga a los intereses de la dependencia o entidad.
Modelo de liberación y entrega	Modelo en donde se establece el alcance, los procesos, procedimientos y recursos a utilizar en las actividades de liberación, y también define el entorno, estructura y roles implícitos.
Plan de liberación y entrega	Guía con las actividades que se deberán ejecutar exitosamente la liberación en el ambiente de producción, incluye las actividades de pruebas previas y posteriores a la liberación, criterios de evaluación, un plan financiero y comercial.

Producto	Descripción
Reporte de validación de la liberación	Documento con los resultados de la validación de los requerimientos en el ambiente de producción, este reporte se realiza después de la liberación en producción, indicando en la evaluación si los cambios realizados permiten lograr los objetivos esperados.
Plan de construcción	Plan en donde se describen las actividades, tareas, roles y fases para la construcción de las unidades y paquete de liberación.
Plan de pruebas	Plan en donde se describen las actividades, tareas, roles y fases para probar las unidades y paquete de liberación, así como el servicio y ambiente donde se aplicaron.
Resultado de pruebas	Reporte donde se describen los resultados de las pruebas realizadas posteriormente a las liberaciones.
Plan de piloto	Plan en donde se describen las actividades, tareas, roles y fases para el despliegue de un piloto con fines de validación de la calidad de la liberación.
Plan de entrega	Plan en donde se describen las actividades, tareas, roles y fases para transferir la construcción y entrega de los servicios, al ámbito de operaciones.
Reporte de entrega	Reporte donde se documentan las actividades de entrega realizadas posteriormente a la liberación, incluyendo la transferencia de recursos, responsabilidades y compromisos.
Unidad de liberación	Componentes de un Servicio de TIC que normalmente son implementados juntos. Una Unidad de implementación habitualmente incluye suficientes componentes para realizar una función útil. Por ejemplo, una Unidad de implementación podría ser una computadora de escritorio, incluyendo hardware, software, licencias, documentación, entre otros. Una Unidad de implementación distinta podría ser la Aplicación de Nóminas, incluyendo los procedimientos de operaciones de TI y la documentación del usuario.
Plan de soporte temprano	Plan con la descripción de los recursos, problemas y soluciones que se generaron durante la construcción y liberación.

7.8.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Variación de desempeño requerido por usuarios	Evaluar las desviaciones en desempeño	Evaluar los requerimientos del usuario para comparar con el desempeño obtenido en la liberación	Eficacia	De gestión	Desempeño logrado/desempeño objetivo	Administrador de liberaciones	mensualmente

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Tiempo de liberación	Evaluar el tiempo de cumplimiento de desarrollo del servicio	Es la duración de la liberación de un producto o servicio	Eficiencia	De gestión	Tiempo de liberación/tiempo planeado	Administrador de liberaciones	mensual
Satisfacción del usuario	Evaluar la satisfacción del cumplimiento de requerimientos	Encuesta de satisfacción del usuario para evaluar el cumplimiento de requerimientos de liberación	Calidad	De gestión	Resultado de la encuesta	Administrador de liberaciones	mensual

7.8.2.4 Reglas del proceso

1.1	Toda liberación de soluciones tecnológicas o hardware deberá ser gestionada mediante el proceso de Administración de Cambios, sin excepción.
1.2	Toda liberación e implementación de soluciones tecnológicas o hardware, deberá ser finalmente registrada en la Base de Datos de Configuraciones (CMDB)
1.3	Los procedimientos y reglas que apliquen para el proceso, deberán definirse, documentarse y aprobarse por la administración del ambiente productivo, quien se asegurará que estos sean comunicados a través de la dependencia o entidad y a todos los proveedores relevantes en el proceso
1.4	Los procedimientos y reglas que apliquen para el proceso, deberán estar alineados al marco de gobierno que impere en la administración de servicios y en la dependencia o entidad.
1.5	Toda no conformidad con alguna política del proceso, debe ser investigada, documentada, reportada y corregida.
1.6	El proceso de liberación y entrega deberá alinearse con los procesos y sistemas de la dependencia o entidad con el fin de mejorar la eficiencia y efectividad.
1.7	El proceso de liberación y entrega deberá regirse por un enfoque de uso de la información, procedimientos y las soluciones tecnológicas ya existentes.
1.8	Procedimientos automáticos repetitivos deberán ser desarrollados para incrementar la eficiencia y eficacia de las actividades clave del proceso tales como distribución e instalación.
1.9	Las políticas de seguridad de la información que aplican para la dependencia o entidad, son extensivas al proceso de liberación y entrega.
1.10	La evaluación de desempeño del proceso de liberación y entrega deberá realizarse dentro del proceso de Administración del desempeño de TIC.
1.11	Los roles y responsabilidades del proceso de liberación y entrega, deberán definirse mediante el proceso de estructura de gobierno de TIC.
1.12	La UTIC deberá asegurar que las actividades realizadas antes y durante la fase de puesta en producción cuenten con los controles de seguridad necesarios y suficientes que protejan el código que se va a liberar así como el ambiente que asegurará la funcionalidad al entregar al usuario.
1.13	La UTIC deberá realizar pruebas del software, sistema o aplicativo a liberar, incluyendo pruebas individuales, de estrés, de volumen, integrales, de regresión, antes de liberar una versión a producción
1.14	La UTIC deberá garantizar la puesta en producción de la versión final de las soluciones

	tecnológicas evitando el uso de datos de prueba en producción así como la exposición del código de lectura o escritura a los usuarios y, de ser el caso, hacia Internet
1.15	La UTIC deberá asegurar y mantener evidencia de la realización de pruebas de seguridad, probar los parches de seguridad en los servidores y componentes involucrados, los controles de acceso incluyendo identificación, autenticación y autorización al software, sistema o aplicativo a liberar, los controles de encriptación y de almacenamiento seguro, y cualquier otro control de seguridad que requiera el software, sistema o aplicativo a liberar o la propia plataforma de proceso del centro de datos.
1.16	La UTIC deberá asegurar y mantener evidencia de la realización de pruebas a las configuraciones del sistema incluyendo sistema operativo, bases de datos y cualquier componente que interactúe con el software a liberar.
1.17	La UTIC deberá asegurar y mantener evidencia de la realización de que, en caso de que se usen datos de producción en el ambiente de pruebas, estos mantengan confidencialidad y sean destruidos una vez concluidas las pruebas.
1.18	La UTIC deberá asegurar y mantener evidencia de la realización de eliminación de forma definitiva de todos los datos de pruebas, cuentas creadas, contraseñas, y cualquier otra información de prueba antes de liberar una versión del software, sistema o aplicativo a liberar.
1.19	La UTIC deberá asegurar y mantener evidencia de la realización de la verificación del código antes de ser liberado a través de herramientas especializadas para identificar potenciales vulnerabilidades (de volumen, de concurrencia y estrés, de acceso a base de datos, de comunicaciones, del tubo de Internet).
1.19	La UTIC deberá asegurar y mantener evidencia de la aprobación de liberación dónde participen las áreas usuarias, particularmente aquellas que se califiquen como las dueñas del proceso que soporta el software, sistema o aplicativo a liberar, o los usuarios requirentes, el responsable del equipo de desarrollo, y el responsable del centro de datos.
1.20	La UTIC deberá asegurar y mantener evidencia de haber etiquetado, respaldado y resguardar todos los componentes del software, sistema o aplicativo a liberar, esto es, la versión definitiva que se libera, aplicando las mejores platicas a su alcance.
1.21	La UTIC deberá garantizar que los ambientes de desarrollo, pruebas y producción, deben estar separados, tanto a nivel físico como lógico. De no ser posible la separación física de ambientes, se deben llevar a cabo separaciones lógicas de redes, directorios y archivos.
1.22	La UTIC deberá garantizar que las herramientas para el desarrollo de software estén accesibles sólo para los miembros autorizados de desarrollo de sistemas.
1.23	Las herramientas de desarrollo de software deben eliminarse de cualquier equipo de cómputo que no sea utilizado para el desarrollo de las soluciones tecnológicas, o bien, deberá justificarse su uso mediante un análisis de riesgos, y un documento aprobado por el responsable del proceso de Administración de cambios, esta actividad debe ser efectuada por los miembros del equipo de desarrollo y es responsabilidad del responsable de cada proyecto de desarrollo asegurarse de su cumplimiento.
1.24	El uso de información operacional del negocio, para el uso de pruebas en el desarrollo de las soluciones tecnológicas no está permitido, si fuera necesario, debe estar autorizado por los dueños de los activos de información y con conocimiento del grupo de desarrollo de las soluciones tecnológicas y del responsable del proceso de Administración de cambios, esta actividad debe ser efectuada por los miembros del equipo de desarrollo y es responsabilidad del responsable de cada proyecto de desarrollo asegurarse de su cumplimiento.
1.25	El código de las soluciones tecnológicas no deberá copiarse a los ambientes de pruebas o producción, esta actividad debe ser efectuada por los miembros del equipo de desarrollo y es responsabilidad del responsable de cada proyecto de desarrollo asegurarse de su cumplimiento.
1.26	Las pruebas efectuadas en el transcurso del desarrollo de las soluciones tecnológicas, serán

archivadas durante la vida operacional de la versión del software, para la que fueron utilizados.

7.8.2.5. Documentación soporte del proceso

No aplica

7.8.3. Transición y habilitación de la operación

7.8.3.1 Objetivos del proceso

General.-

Poner en operación una solución tecnológica liberada para que los usuarios utilicen el producto o servicio mediante la planeación y ejecución de un plan de transición y puesta en operación.

Específicos.-

1. Asegurar que se elaboren y comuniquen los planes de transición a puesta en operación de la solución tecnológica y que en los mismos estén integrados los requerimientos originales de diseño del servicio y operación.
2. Identificar y realizar los ajustes necesarios en la solución tecnológica o el elemento de TIC, previo a la liberación a operación.
3. Coordinar la ejecución del plan para asegurar la integridad del ambiente de operación en el que residirá el la solución tecnológica.
4. Asegurar la transición de la solución tecnológica de TIC a la operación en el tiempo y costo previstos y con la calidad esperada.
5. Transferir la información y conocimiento necesarios para operar la solución tecnológica puesta en operación.

7.8.3.2 Descripción del proceso

7.8.3.2.1 Mapa general del proceso

Diagrama de flujo de información

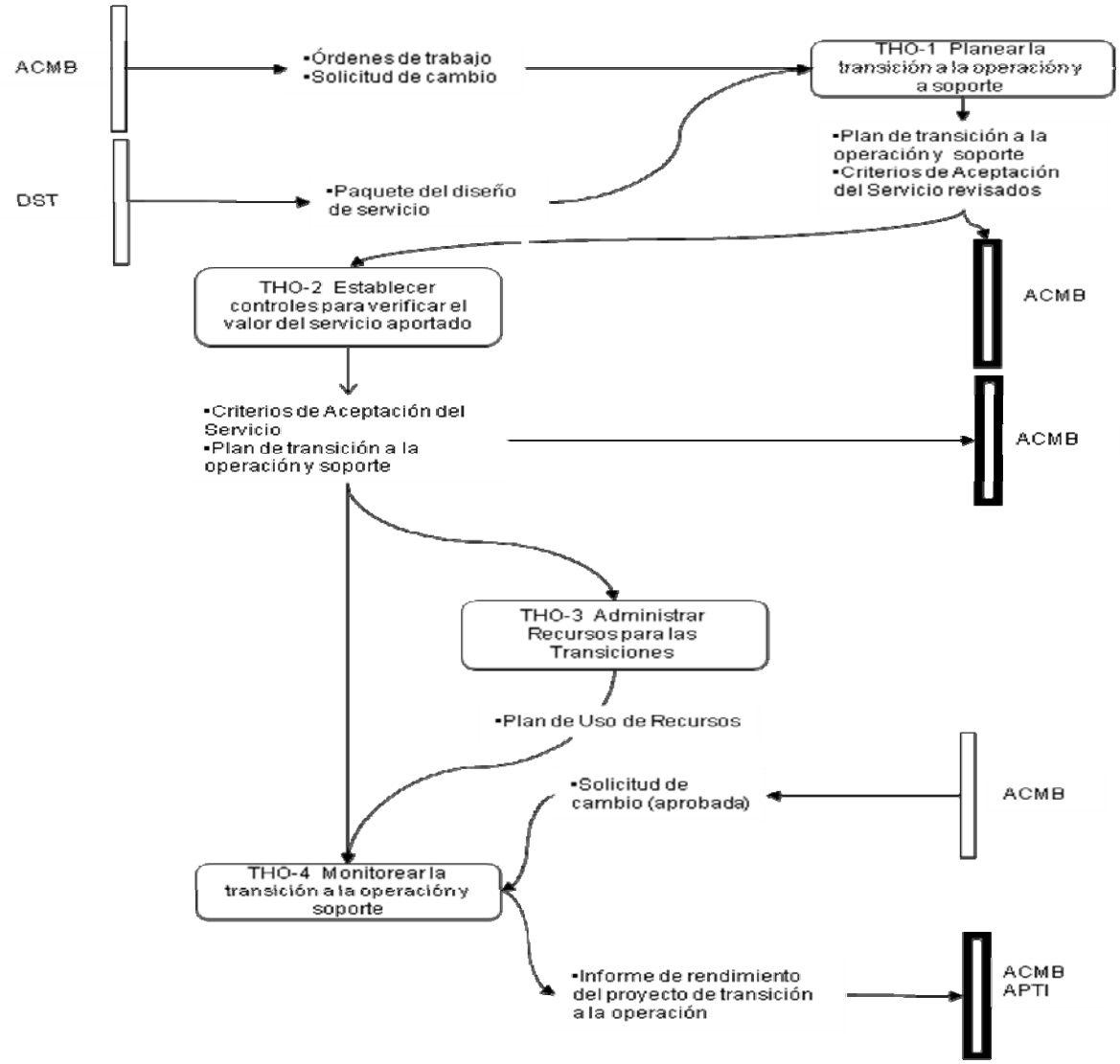
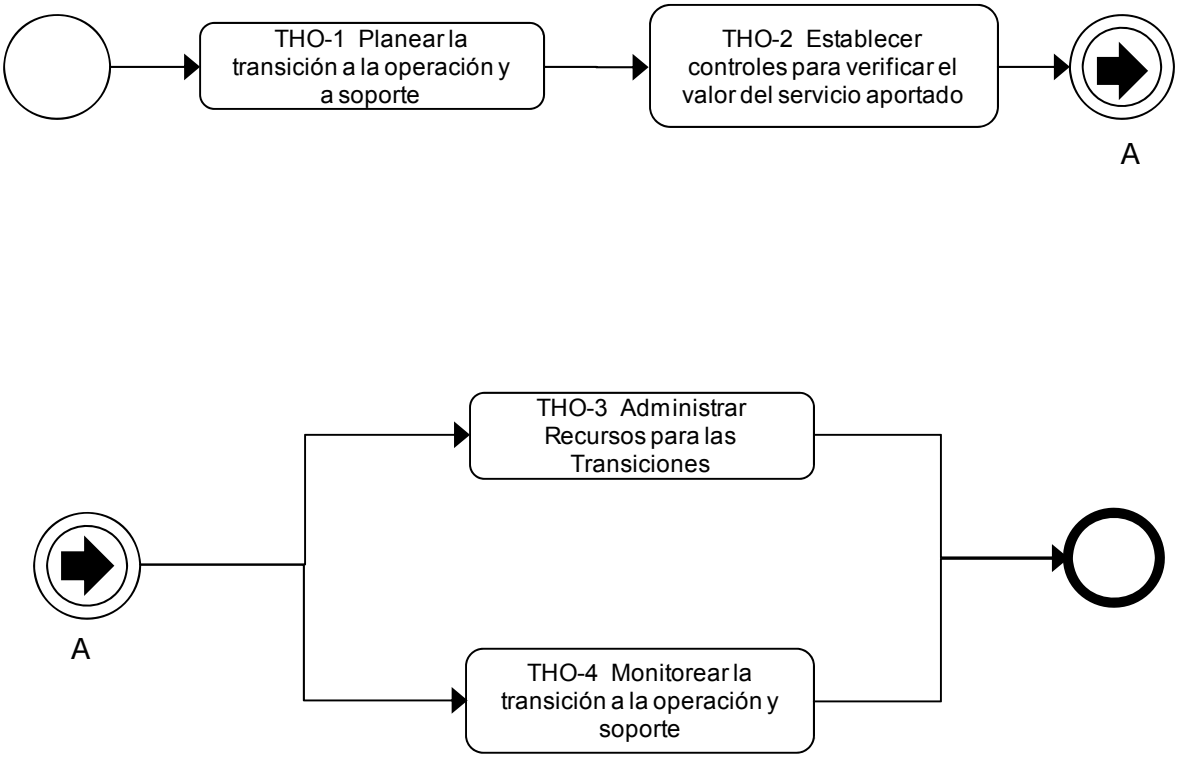


Diagrama de flujo de actividades



7.8.3.2.2 Descripción de las actividades del proceso

THO-1 Planear la transición a la operación y soporte

Descripción	Integrar al plan del proyecto de transición, actividades para lograr la introducción, la habilitación operativa y mantenimiento de los productos entregados al área responsable de operar y soportar el servicio. Las actividades para transición hacia la operación y el soporte, deben incluir las validaciones (con apego a lo indicado en el proceso sistema de gestión de procesos y mejora continua), la transferencia de responsabilidades a la operación, la realización del entrenamiento, así como la obtención y disposición de los recursos, incluyendo las entradas de otras etapas y procesos, fondos y patrocinio, acceso a repositorios de información y ambientes de pruebas, y lo necesario para realizar la transferencia exitosa del servicio o elemento.
Factores Críticos	1. Planear la capacidad y recursos apropiados para la construcción, liberación, validación, implementación, establecimiento y operación del servicio nuevo o modificado en producción 2. Asegurar que se consideran integralmente los aspectos entregados por el Proceso diseño de servicios de TIC, así como lo acordado en la línea base de los criterios de aceptación del servicio, para iniciar la transición. 3. Asegurar que se tiene documentada y formalizada, la autorización para iniciar la transición del servicio 4. Identificar, comunicar y controlar los riesgos de fracaso e interrupción en las actividades de transición. • Planificar los cambios necesarios de una manera que asegure la integridad de los activos a medida que evolucionan dentro de la transición. 5. Asegurar que todos los asuntos de transición, operación, riesgos y las desviaciones son reportados a los interesados, para tomar las decisiones adecuadas. 6. Coordinar las actividades necesarias relacionadas con los proyectos y proveedores, por medio de los Procesos de administración de proyectos de TIC y administración de proveedores. 1. Definir procedimientos estándar para la implementación y estabilización de la operación que asegure que la transición es correcta y el servicio entregado se puede usar conforme lo requirió la dependencia o entidad
Relación de productos	• Plan de transición a la operación y soporte • Criterios de Aceptación del Servicio revisados

THO-2 Establecer controles para verificar el valor del servicio aportado

Descripción	Establecer controles y disciplinas adecuados para identificar que la transición (cambio), del servicio nuevo o modificado, efectivamente provee el valor que la organización requiere y bajo los términos establecidos. Algunos controles deben involucrar directamente al usuario y su personal, como en las pruebas de aceptación del usuario de la entrega y medición de los resultados en comparación con los SLA esperados. Algunos de estos controles pueden ser aplicados por entidades que no participen en el proyecto, como los derivados de Auditorías o Evaluaciones Externas
Factores Críticos	1. Asegurar que se tiene la comprensión completa de los Requerimientos de Nivel de Servicio y los Criterios de Aceptación del Servicio, así como los puntos o hitos de control dentro del plan de transición del servicio.

	2. Identificar con certeza, partiendo de las especificaciones de diseño, la necesidad de adquirir elementos de configuración y componentes para realizar pruebas con el grado de calidad requerido para realizar la transición. 3. Verificar que cada interesado, tiene plena conciencia y documentación suficiente, sobre su rol y responsabilidad en cada fase de la transición, particularmente durante las Pruebas de Aceptación de Usuario UAT 4. Asegurar que existe un mecanismo formal de comunicación sobre los resultados de las Pruebas de Aceptación de Usuario, que permitan autorizar y transferir transición al Proceso de Administración de Liberación y Entrega
Relación de productos	• Criterios de Aceptación del Servicio • Plan de transición a la operación y soporte

THO-3 Administrar recursos para la transición

Descripción	Monitorear y asegurar que la transición del servicio nuevo o modificado se haga con apego al plan de transición y soporte acordado. El monitoreo establece, mediante los controles e hitos, si cada transición (cambio) se está realizando conforme al plan de transición y soporte autorizado.
Factores Críticos	1. Controlar el progreso de cada transición, a los hitos o puntos de referencia, así como la recepción y actualizaciones de forma periódica. 2. Asegurar, en su caso, que se actualizan los Requerimientos de Nivel de Servicio, como resultado de las actividades de corrección a las desviaciones detectadas en el monitoreo (en caso de ser necesario). 3. Dar seguimiento y control, en su caso, al proyecto de transición, de acuerdo con los lineamientos del plan generado. 4. Buscar progresivamente la estandarización de prácticas y la automatización de procesos que hayan probado su efectividad y eficiencia
Relación de productos	• Plan de Uso de Recursos

THO-4 Monitorear la transición a la operación y soporte

Descripción	Monitorear y asegurar que la transición del servicio nuevo o modificado se haga con apego al plan de transición y soporte acordado. El monitoreo establece, mediante los controles e hitos definidos en THO-3, si cada transición (cambio) se está realizando conforme al plan autorizado.
Factores Críticos	1. Controlar el progreso de cada transición, a los hitos o puntos de referencia, así como la recepción y actualizaciones de forma periódica. 2. Asegurar, en su caso, que se actualizan los Requerimientos de Nivel de Servicio, como resultado de las actividades de corrección a las desviaciones detectadas en el monitoreo. 3. Dar seguimiento y control, en su caso, al proyecto de transición, de acuerdo con los lineamientos del plan generado.

Relación de productos	• Informe de rendimiento del proyecto de transición a la operación

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.8.3.2.3 Descripción de roles

Rol	Descripción
Administrador de la transición del servicio	Gestión y control del día a día sobre los equipos de trabajo y sus actividades mediante la planeación de la transición, coordinación de las funciones, presupuestos, contabilidad, trato con el usuario respecto a la transición, aseguramiento del cumplimiento del proceso y logro de los resultados esperados.
Administrador del Conocimiento del Servicio	Diseño, entrega y mantenimiento de la estrategia, procesos y procedimientos de Administración del Conocimiento. Es el arquitecto para la identificación y control del conocimiento, su captura, mantenimiento y distribución.

7.8.3.2.4 Descripción de productos

Producto	Descripción
Plan de transición a la operación y soporte	El Plan establece las actividades, responsabilidades y recursos necesarios para realizar una transición efectiva del elemento o servicio desarrollado de tal forma que se cuenten con los elementos necesarios y suficientes para su puesta en operación así como para brindar el soporte necesario ya sea de manera directa y/o a través de un tercero.
Procedimiento de Transición	Es el conjunto de actividades del Proceso de Transición y Habilitación a la Operación.
Criterios de Aceptación del Servicio (actualizados)	Son los atributos que restringen los diversos aspectos de un servicio, que deben ser satisfechos, para considerar que el Servicio cumple con lo requerido en cada fase de su ciclo de vida. En la transición es fundamental la claridad de estos criterios, para autorizar la entrada en operación del servicio. El usuario debe establecerlos con toda precisión, se encuentran documentados en el paquete de diseño de servicios.
Requerimientos de Nivel de Servicio	Son la recopilación de necesidades, expectativas y restricciones del usuario, con relación a un aspecto del Servicio TIC y tiene como base los objetivos de la Organización, son necesarios para negociar las Metas de Niveles de Servicio. Se encuentran documentados en el paquete de diseño de servicios.
Recomendaciones y observaciones tempranas	Es el conjunto de alertas, requerimientos, riesgos, costos y cambios, que de manera anticipada –durante las fases tempranas del ciclo de vida de servicios- identifica la Administración de Transición y que ayudan para prevenir retrasos y costos adicionales durante la transición

Producto	Descripción
Plan de Uso de Recursos	Es el documento estructurado, normalmente asociado a un repositorio, que muestra la asignación actual y futura de recursos, conforme sus capacidades para apoyar en el éxito de las transiciones. Se usa para maximizar la experiencia, competencia y habilidades de los recursos. Puede incluir componentes que automaticen ciertas capacidades de transición, como la distribución de servicio y otras establecidas en el proceso de liberación y entrega.
Informe de rendimiento del proyecto de transición a la operación	Reporte de avance de las actividades de transición (Ver proceso de Administración de Proyectos)

7.8.3.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Variación de desempeño requerido por usuarios	Evaluar las desviaciones en desempeño	Evaluar los requerimientos del usuario para comparar con el desempeño obtenido en la liberación	Eficiencia	De gestión	Desempeño logrado/Desempeño objetivo	Administrador de liberaciones	Por evento
Satisfacción del usuario	Evaluar la satisfacción del cumplimiento de requerimientos	Encuesta de satisfacción del usuario para evaluar el cumplimiento de requerimientos de liberación	Calidad	De gestión	Resultado de la encuesta	Administrador de liberaciones	Por evento

7.8.3.4 Reglas del proceso

1.1	La información que sea recopilada para su uso durante la transición y que se entrega a la operación, debe tener como fuente directa la entidad original que la generó
1.2	Toda información que sea transferida a la operación y soporte, deberá antes ser validada para asegurar su calidad y efectividad
1.3	Todos los cambios que se generen a partir del proyecto de transición, deberán hacerse mediante el proceso de Administración de Cambios
1.4	La adición, remoción o modificación de elementos de configuración relacionados con las actividades de transición, deberán ser reportados al proceso de Administración de la Configuración
1.5	Las políticas de seguridad de la información que aplican para la organización, son extensivas al proceso de transición y habilitación de la operación.

1.6	La evaluación de desempeño del proceso, deberá realizarse mediante el proceso de Administración del desempeño de TIC
1.7	Los roles y responsabilidades, deberán definirse mediante el proceso de Establecimiento de estructura de gobierno de TIC

7.8.3.5	Documentación soporte del proceso

No aplica

7.8.4. Administración de la configuración

7.8.4.1 Objetivos del proceso

General.-

Mantener y tener disponible la información funcional y técnica relativa a las soluciones tecnológicas, los entornos de pruebas, de calidad, de pre operación y de operación para eficientar la ejecución de los procesos cuya operación requiera acceder a los datos de configuraciones, versiones y características de los servicios.

Específicos.-

1. Identificar, registrar, controlar, auditar y verificar los datos de las soluciones tecnológicas, los entornos de pruebas, de calidad, de pre operación y de operación, incluyendo sus atributos, relaciones con otros elementos, versiones, memorias técnicas de desarrollo y documentación relacionada.
2. Asegurar que la información provista a través de la base de datos de configuraciones (CMDB) se mantenga actualizada y accesible a los usuarios involucrados, asociándoles permisos acorde a su función y los procesos en que intervienen.
3.

7.8.4.2 Descripción del proceso

7.8.4.2.1 Mapa general del proceso

Diagrama de flujo de información

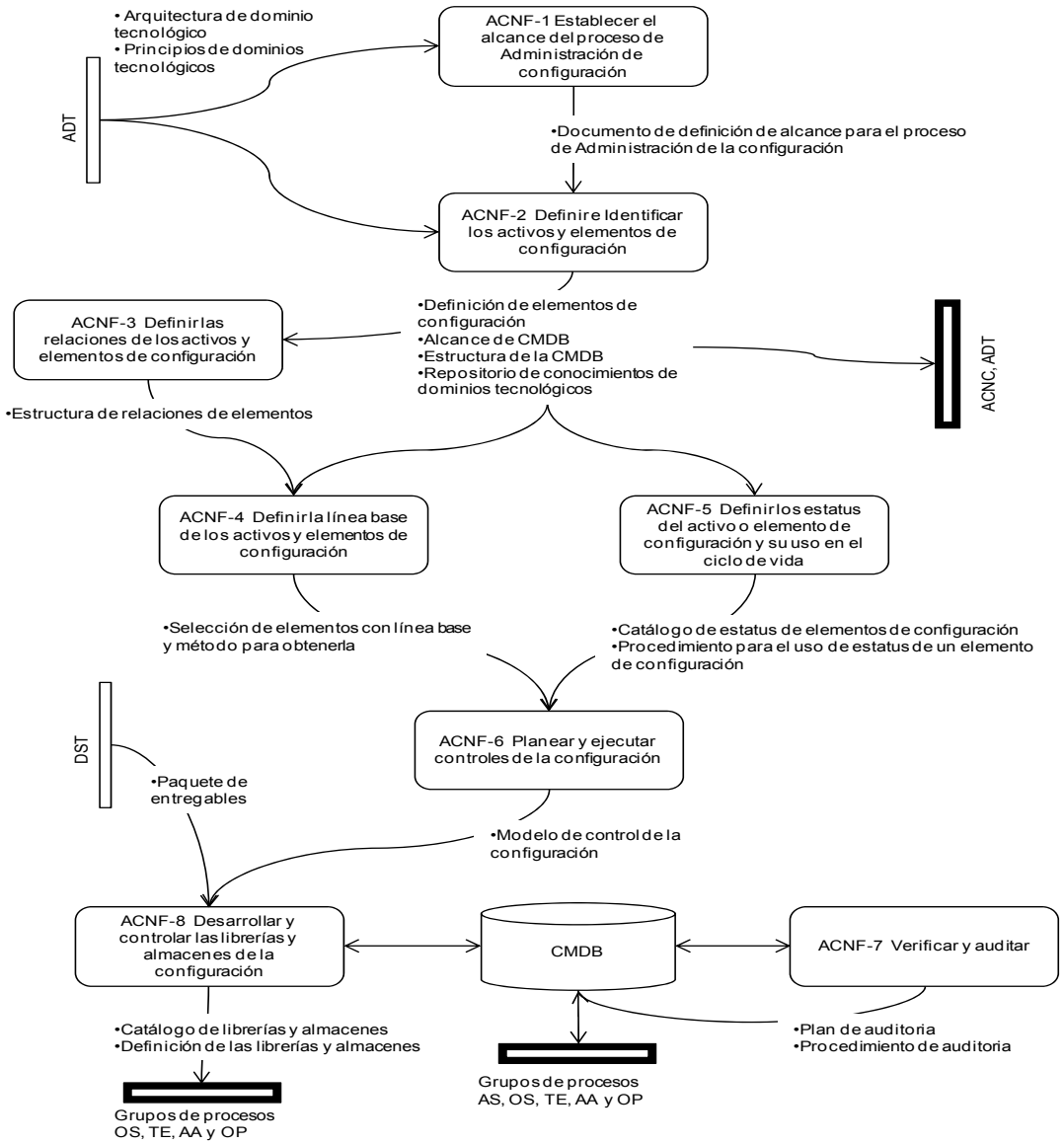
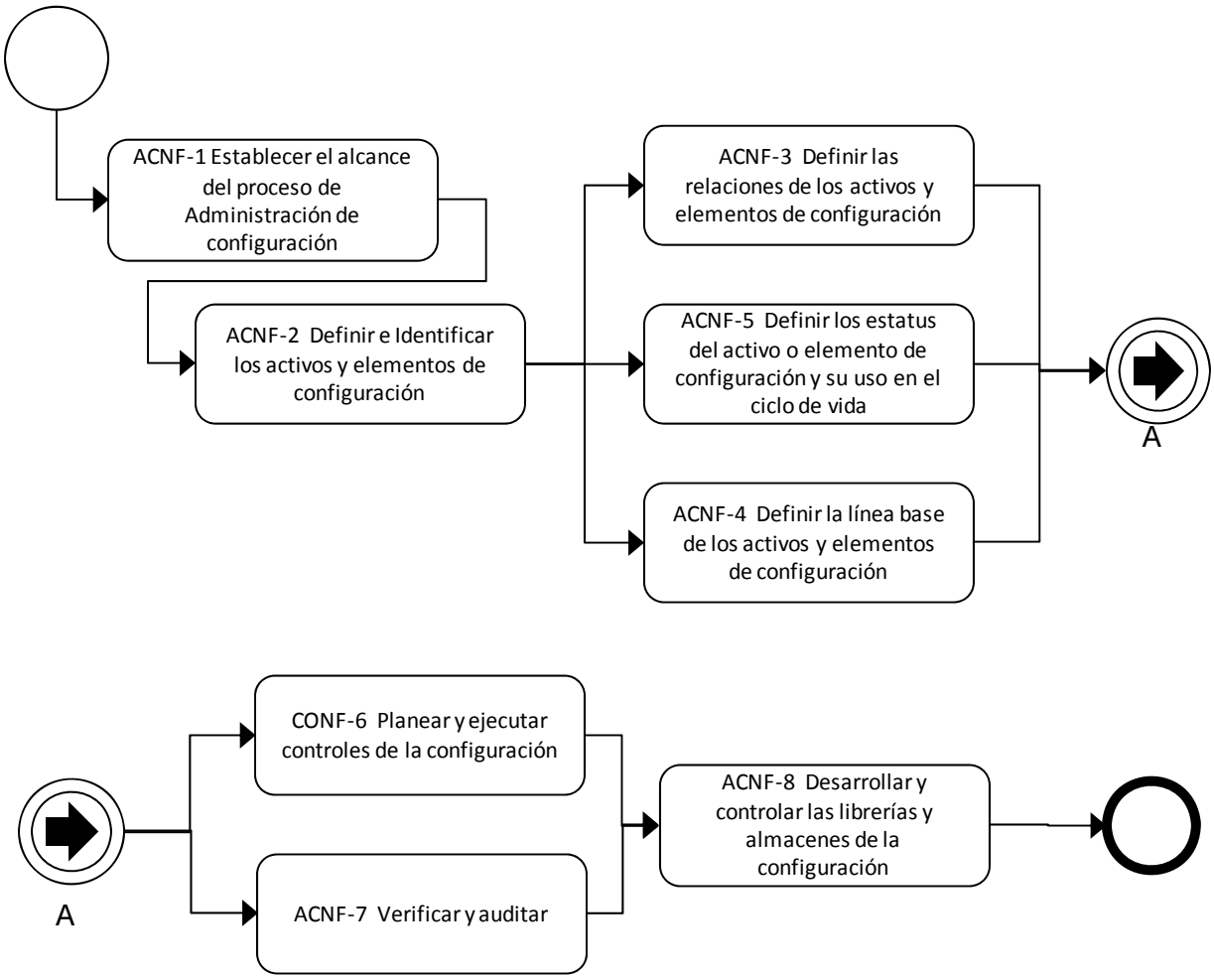


Diagrama de flujo de actividades



7.8.4.2.2 Descripción de las actividades del proceso

ACNF-1 Establecer el alcance del proceso de Administración de configuración

Descripción	Implementar y operar el proceso de Administración de Configuraciones, implica disponer de recursos que son, en gran medida, proporcionales a la cantidad y complejidad de los activos y elementos que se administrarán. La falta de claridad y deficiente planeación en el alcance del proceso, podría derivar en el mal uso de los recursos, así como que los resultados y valor del proceso no sean los que necesita la dependencia o entidad.
Factores Críticos	1. Determinar qué activos y elementos del ambiente actual y futuro, serán administrados por el proceso de Configuraciones con base en las necesidades de la dependencia o entidad y considerando los recursos disponibles tales como personal, tiempo, fondos, tecnología, cultura organizacional, madurez de los procesos que proveerán y los que utilizarán la información recopilada, entre otros. 2. Establecer un plan de alcance por fases considerando además de la criticidad de los activos y elementos a gestionar, sus tipos, los servicios actuales y futuros, así como el número de localidades, infraestructura y característica de las mismas. 3. Definir los objetivos específicos que se pretenden lograr a través del proceso de Administración de configuración, así como los procedimientos que regirán al proceso y su base de datos de la configuración (CMDB) 4. Seleccionar los elementos de configuración para los que se les constituirá una línea base (baseline). 5. Decidir si se incluyen dentro del alcance del proceso, ciertos activos y elementos de configuración que pertenecen a proveedores externos. Considerar la criticidad y participación de esos activos y elementos en los servicios que se proveen, para tomar esta decisión.
Relación de productos	• Documento de definición de alcance para el proceso de Administración de la configuración

ACNF-2 Definir e Identificar los activos y elementos de configuración

Descripción	Definir e identificar los activos y elementos de configuración, así como sus estructuras, que se administrarán a través del proceso. La extensión en cuanto a las propiedades, relaciones y nivel de detalle deben definirse en un principio, y a partir de estas se planean y deciden los procedimientos, tecnología, roles y recursos que los soportarán en las etapas subsecuentes.
Factores Críticos	1. Definir los atributos de los activos y elementos de configuración. Estos pueden ser: identificador, nombre, descripción, componentes, ubicación, línea base, estatus, versión, rol responsable e histórico, así como los criterios de relaciones con otros elementos, las clases y categorías que estarán disponibles para clasificar y controlar los elementos. Establecer las propiedades mínimas que conformarán la línea base de cada elemento y activo seleccionado para este procedimiento. 2. La identificación de los activos y elementos de Configuración se realiza no solo al inicio cuando se llena por primera vez el repositorio de configuraciones, sino en adelante para integrar nuevos elementos de configuración. Establecer una convención de nombres (nomenclatura) para los elementos: referir en su nombre la versión, clase, grupo, tipo, al tiempo que debe ser corto e ilustrativo. 3. Cerciorarse que las nomenclaturas, datos y su estructura, así como los procedimientos de recopilación, actualización y despliegue de información, cumplan con las disposiciones establecidas en las leyes, políticas y reglas gubernamentales y de la

	dependencia o entidad, vigentes, incluidas aquellas que se refieren a la seguridad de la información. 4. Rehusar en la medida de lo posible las definiciones, estructuras y códigos que pudieran ya existir en la dependencia o entidad. Utilizar cuando sea posible, herramientas tecnológicas para la identificación y actualización de elementos de configuración, que aplica mayormente para hardware y software. 5. Decidir el procedimiento y formato de etiquetado de los elementos físicos. 6. Comprobar que los procedimientos establecidos, no violen la normatividad existente. 7. Desarrollar un modelo lógico de configuración, en el que se describen las relaciones y posición de un elemento de configuración en cada estructura definida. 8. Partir de un modelo de configuración que vaya de lo general a lo particular, esto es desde el elemento de configuración padre, hasta los componentes del elemento de configuración descendiente.
Relación de productos	• Definición de elementos de configuración • Alcance de CMDB • Estructura de la CMDB • Repositorio de conocimientos de dominios tecnológicos

ACNF-3 Definir las relaciones de los activos y elementos de configuración

Descripción	Ubicar las relaciones entre todos esos elementos tangibles e intangibles para lograr un mapa conceptual del ambiente y esta información apoye la toma de decisiones. Definir las relaciones válidas y las reglas que regirán las tareas alrededor de la toma de decisiones.
Factores Críticos	1. Definir y estructurar las relaciones entre los elementos de configuración no solo entre elementos, sino también con elementos de otros procesos y sistemas tales como Acuerdos de Niveles de Servicio, roles, documentación, registros de Incidentes, Problemas, Cambios, Liberaciones, entre otros. 2. Definir las dependencias y jerarquías entre los elementos (relaciones padre-hijo), así como entre los elementos y sus componentes. 3. Determinar qué tipo de relaciones son válidas desde el punto de vista de bases de datos: uno a uno, uno a todos, todos a uno.
Relación de productos	• Estructura de relaciones de elementos

ACNF-4 Definir la línea base de los activos y elementos de configuración

Descripción	Identificar aquellos elementos para los que se fijarán y rastrearán líneas base. Definir líneas base permite establecer la configuración oficial y autorizada de un elemento de configuración, misma que servirá como punto de referencia para controlar el ambiente operativo, así como para tener una base de copia de configuración y de comparación en caso de necesitarse replicar u auditar ese elemento.
Factores Críticos	1. Definir Líneas base. • Considerar que el alcance inicial de los elementos de configuración a los que se le fijarán Líneas Base puede limitarse inicialmente solo aquellos más críticos en los servicios provistos. Posteriormente dicho alcance podría incrementarse se necesite, se madure el proceso y se disponga de recursos. • Para identificar una Línea Base, mediante un identificador, no usar nombres que denoten una etapa o momento, sino versiones. • Al acordar y establecer un punto inicial de Línea Base, este deberá se previamente acordado con los interesados e impactados por esa Línea Base, y deberá validarse contra las necesidades de la dependencia o entidad.

	• La Línea Base de un elemento puede variar y adaptarse conforme se necesite. Sin embargo cualquier cambio deberá ser previamente autorizado y deberá ser gestionado mediante el proceso de Administración de cambios. 2. Establecer procedimientos que regulen las actualizaciones o cambios a las Líneas base. 3. Mantener el histórico de todos las Líneas base. • Pueden existir diferentes líneas base que correspondan a diferentes etapas del elemento al que pertenece. • Considerar que un elemento de configuración puede tener más de una Línea Base vigente.
Relación de productos	• Selección de elementos con línea base y método para obtenerla

ACNF-5 Definir los estatus del activo o elemento de configuración y su uso en el ciclo de vida

Descripción	Definir los estatus que podrán usarse para identificar de manera exacta y clara el estado del elemento al momento de la consulta.
Factores Críticos	1. Todo elemento de configuración debe referir de manera correcta y actualizada el estado actual del elemento. 2. El cambio de estatus de un activo o elemento deberá estar autorizado y deberá llevarse a cabo de acuerdo al los procesos de Administración de Cambios. 3. Definir el procedimiento, roles y autorizaciones que se requerirán para que un activo o elemento pase de un estado a otro. 4. Justificar y documentar todo cambio de estatus. 5. Asegurar que ningún dato de un activo o elemento de configuración retirado, deberá ser borrado. En su lugar, establecer estatus que indiquen dicho estatus y que inhabilite su uso en el sistema como un elemento disponible para ser usado y relacionado con elementos activos. 6. Establecer estatus descriptivos y cortos. Ejemplos de algunos de estos estatus son: • En desarrollo • Borrador • Aprobado • Activo • Suspendido • Retirado
Relación de productos	• Catálogo de estatus de elementos de configuración • Procedimiento para el uso de estatus de un elemento de configuración

CONF-6 Planear y ejecutar controles de la configuración

Descripción	Controlar la información que es recopilada y provista por el proceso de Administración de la Configuración, es de suma importancia por constituir una de las fuentes para la toma de decisiones en otros procesos de la dependencia o entidad.
Factores Críticos	1. Generar un modelo de control de la configuración. 2. Desarrollar un plan de control para cada herramienta que participe en el proceso de tal forma que se les alineé con el modelo de control de Configuración. 3. Asegurar que solo aquellos elementos de configuración autorizados e identificados, sean registrados en la Base de Datos de la Configuración (CMDB) a través de un ciclo de vida. 4. Asegurar que cualquier modificación de un elemento de configuración y la consecuente actualización de su información en la CMDB, sea realizada a través del proceso de

	administración de cambios. 5. Proveer la información a detalle necesaria y de manera inmediata al proceso de Configuraciones, acerca de un cambio ejecutado sobre un elemento de configuración.
Relación de productos	• Modelo de control de la configuración

ACNF-7 Verificar y auditar

Descripción	Confirmar que, tras la implementación del proceso, la realización de un cambio mayor en el ambiente, o simplemente como la ejecución de una buena práctica, la información provista por el proceso sea correcta.
Factores Críticos	1. Asegurar que las actividades de auditoría se lleven de acuerdo al proceso de gestión de procesos y calidad. 2. Verificar que toda integración o actualización de información relacionada a un elemento de configuración, se llevó a cabo según los procedimientos establecidos en el proceso. 3. Establecer auditorias regulares para verificar que la información de la base de datos de la configuración (CMDB) está correcta respecto al ambiente físico real de la dependencia o entidad. Algunos de los aspectos que se verán involucrados en la verificación pueden ser: • Verificar que los elementos de configuración que física o lógicamente existen en el ambiente operativo de la dependencia o entidad, y en el alcance del proceso de Configuraciones, se encuentren registrados en el sistema de gestión de información. • Confirmar que las líneas bases están siendo respectadas según se establecieron. • Comprobar que la documentación de liberaciones y de configuración esté presente antes de llevarse a cabo una Liberación mediante el proceso de liberación y entrega. • Determinar si el estatus de los elementos de la configuración en la base de datos de la configuración (CMDB) coinciden con los estados físicos que tienen en el ambiente productivo. • Confirmar que en el ambiente productivo, solo se están usando elementos de configuración autorizados y registrados en la CMDB. 4. Cualquier herramienta, equipo de prueba, dispositivos y cualquier otro elemento no registrado debe ser eliminado, o registrado a través del proceso de cambios. 5. Investigar los hallazgos relacionados a elementos no registrados y no autorizados, y considerar acciones correctivas para tratar posibles fallas en procedimientos y el comportamiento del personal. 6. Registrar y reportar todas las excepciones encontradas.
Relación de productos	• Plan de auditoria • Procedimiento de auditoria

ACNF-8 Desarrollar y controlar las librerías y almacenes de la configuración

Descripción	Controlar los elementos que son utilizados para la entrega de servicios. Una parte de esos activos se encuentran resguardados en repositorios físicos y lógicos, referidos como librerías y almacenes, mediante los cuales se ponen disponibles para su uso en el ambiente operativo.
Factores Críticos	1. Integrar o en su defecto desarrollar los repositorios lógicos y físicos de configuraciones tales como la Librería Segura, Librería Definitiva de Medios, Almacén Seguro, Repuestos definitivos y demás repositorios que se precisen, al Sistema de Administración de la Configuración. 2. Desarrollar procedimientos para la actualización en el sistema de administración de la configuración, de la información que se derive de los repositorios.

	3. Establecer las regulaciones para el acceso a la información, diferenciando los privilegios que por rol sean definidos. 4. Implementar controles para la seguridad de los repositorios lógicos y físicos, mismos que deberán estar sujetos a las políticas y regulaciones de seguridad organizacionales y de gobierno vigentes.
Relación de productos	• Paquete de entregables • Catálogo de librerías y almacenes • Definición de las librerías y almacenes

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.8.4.2.3 Descripción de roles

Rol	Descripción
Administrador de Activos de Servicio	• Alinear las actividades del proceso a los intereses de la dependencia o entidad • Gestiona el plan de administración de Activos • Acuerda convenciones de identificación • Acuerda las interfases con otros procesos • Responsable de la base de datos de activos • Gestiona los reportes relacionados a activos • Audita las actividades del proceso • Evalúa las soluciones tecnológicas de gestión de activos • Establece el alcance del proceso de administración de activos • Reclutamiento y capacitación del personal involucrado en el proceso. • Evalúa las herramientas de activos • Identifica y da seguimiento a mejoras del proceso.
Administrador de la Configuración	• Alinear las actividades del proceso a los intereses de la dependencia o entidad. • Evalúa las soluciones tecnológicas de gestión de configuración. • Acuerda las interfases con otros procesos. • Establece el alcance del proceso de administración de la configuración. • Reclutamiento y capacitación del personal involucrado en el proceso. • Evalúa las herramientas de configuraciones • Acuerda acerca de la identificación y rastreo de los elementos de configuración. • Responsable del sistema de administración de la configuración (CMS). • Asegura la disponibilidad de recursos para mejoras. • Responsable de la base de datos de la configuración • Gestiona los reportes relacionados a configuraciones • Audita las actividades del proceso • Evalúa las soluciones tecnológicas de gestión de configuraciones. • Identifica y da seguimiento a mejoras del proceso.

Analista de Configuración	• Desarrolla estándares de activos y configuraciones • Capacitación del personal involucrado • Soporte del desarrollo y despliegue de configuraciones. • Desarrolla procedimientos. • Acuerda nomenclaturas de nombres. • Colabora en las evaluaciones de impacto con motivo de cambios. • Participa en auditorías. • Crea librerías. • Recibe productos de terceros • Da mantenimiento a los estatus de los elementos de configuración.
Administrador/Bibliotecario de la Configuración	• Controla la recepción, identificación, resguardo y retiro de los elementos de configuración soportados. • Provee información acerca de los estatus de los elementos de configuración.
Administrador de herramientas / CMS	• Evalúa las herramientas de activos y de configuración y hace recomendaciones sobre estas. • Evalúa el desempeño de las soluciones tecnológicas de activos y configuraciones. • Aplica los estándares definidos para activos y configuraciones.

7.8.4.2.4 Descripción de productos

Producto	Descripción
Documento de definición de alcance para el proceso de Administración de la Configuración	Documento con los objetivos específicos que se pretenden alcanzar por fases considerando activos, elementos de configuración y servicios.
Definición de elementos de configuración	Especificación de la estructura y atributos de los activos y elementos de configuración a administrar dentro del proceso. Se detallan las propiedades mínimas de los elementos de configuración al inicio y durante la ejecución del proceso de Administración de la Configuración.
Alcance de CMDB	Documento en donde se delimita el alcance de los elementos de configuración que estarán en el alcance para su inclusión y gestión mediante la CMDB.
Estructura de la CMDB	Refiere la estrategia y arquitectura que será base la construir, organizar y gestionar la información en la CMDB.
Estructura de relaciones de elementos	Documento con la estructura de configuración, dependencias, jerarquías y relaciones entre los elementos de procesos, sistemas, servicios, etc. Todos los activos tangibles e intangibles en la Base de Datos de Configuraciones.
Selección de elementos con Línea Base y método para obtenerla	Documento en donde se describen los elementos de configuración que estarán sujetos a un esquema de Líneas Base, así como la estrategia y procedimiento para establecer, actualizar y controlar las Líneas Base que se establezcan.
Catálogo de Estatus de elementos de configuración	Estatus definidos que identifican y describen el estado de un elemento. Estos estatus son cortos pero descriptivos.

Producto	Descripción
Procedimiento para el uso de estatus de un elementos de configuración	Especificaciones para asignar un estatus y generar el cambio de uno a otro.
Modelo de control de la configuración	Modelo para identificar y regular cómo diferentes procedimientos pueden modificar un elemento de configuración.
Plan de auditoria	De acuerdo al sistema de gestión de procesos y mejora continua.
Procedimiento de auditoria	De acuerdo al sistema de gestión de procesos y mejora continua.
Catálogo de librerías y almacenes	Documento donde se describen los activos que la dependencia o entidad resguarda en repositorios: librerías y almacenes. El objetivo de formar un catalogo es que toda la dependencia o entidad pueda tener acceso a la información.
Definición de las librerías y almacenes	Documentos mediante los cuales se definen las librerías y almacenes que serán implementados en el ambiente de configuraciones.
Criterios de selección de la herramienta habilitadora para el proceso de configuraciones	Especificaciones para poder seleccionar una herramienta que pueda automatizar el proceso de Administración de la configuración. Cada criterio describe las características y funcionalidades que se deben evaluar de acuerdo a las necesidades de la dependencia o entidad.
CMDB **Base de datos de la configuración**	Herramienta para el manejo de una base de datos, que debe proveer, entre otros los aspectos siguientes:: • Proveer el identificador único que se asignará a cada activo y elemento de configuración. Esto con base en la nomenclatura que por proceso se establezca. • La herramienta deberá soportar la gestión de todos los activos y elementos que se van a administrar, considerando que para cada uno la cantidad y tipo de datos puede variar en cantidad y complejidad, según se haya establecido en la definición de los activos y elementos de configuración. Considerar los atributos, relaciones, líneas base, clasificaciones, estatus, tipos y demás datos relacionados a los elementos y activos. • Las herramientas que se utilicen en los procesos usuarios y proveedores de información, así como aquel que funcione como el eje principal del proceso de Configuraciones, deberán poder integrarse entre ellas o en su defecto, permitirán establecer interfaces de comunicación para el intercambio de información para la recopilación, auditoria, actualización y entrega de la información del ambiente como un solo sistema. • Posibilitar la referencia y liga de los activos y elementos de configuración, así como de sus componentes, con los Incidentes, Problemas, Cambios, Proveedores, Solicitudes de Servicio y demás registros que usen o provean información. • La herramienta debería posibilitar la creación y gestión de múltiples Bases de Datos de Configuraciones (CMDB) si así lo necesitara la dependencia o entidad. • La herramienta deberá soportar el ciclo de vida de los activos y elementos de la configuración, incluyendo el rastreo de sus modificaciones y versiones. • La herramienta deberá permitir establecer y explorar las relaciones entre

Producto	Descripción
	elementos de software y hardware • La herramienta deberá permitir diferentes vistas de la información. • Se requieren funcionalidades para explorar el ambiente con fines de descubrimiento y auditoria, así como para identificar el estado actual de los activos y elementos, todo esto con base en criterios parametrizables. Estas funcionalidades aplican mayormente para elementos de tipo hardware y software.
Repositorio de conocimientos de dominios tecnológicos	Repositorio con los datos e información que sustenta al conocimiento de un dominio, incluye: el conjunto de principios, modelos, normas y estándares del dominio.

7.8.4.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Registro de elementos de configuración en base de datos	Asegurar el registro de todos los componentes de la configuración	Asegurar que todos los componentes de configuración autorizados e identificados se registren en la CMDB	Eficiencia	De gestión	Elementos de configuración registrados/Elementos de configuración	Lo definirá la UTIC	Por evento
Observaciones en auditorias de la base de datos de la configuración (CMDB)	Reducir las observaciones en auditorías	Identificar las observaciones realizadas en auditorias a la CMDB	Eficiencia	De gestión	Número de observaciones en auditorias a la CMDB	Lo definirá la UTIC	Por evento
Satisfacción del usuario	Evaluar la satisfacción del usuario para evaluar el servicio	Encuesta de satisfacción del usuario para evaluar el servicio	Calidad	De gestión	Promedio del resultado de las encuestas	Lo definirá la UTIC	

7.8.4.4 Reglas del proceso

1.1	Los productos que entrega el proceso de Administración de la configuración son la fuente única y oficial de información acerca de los elementos y activos del ambiente operativo de la dependencia o entidad.
1.2	La información contenida en la base de datos de configuraciones (CMDB) es confidencial y propiedad de la dependencia o entidad para su uso interno por usuarios autorizados por el titular de la UTIC y el responsable de la CMDB.
1.3	Las actividades implícitas en el proceso de configuraciones, principalmente aquellas relacionadas con la modificación de la información contenida en la CMDB, están reservadas únicamente para el

	personal que participa en el proceso de configuraciones mediante un rol asignado con esos privilegios.
1.4	Los roles y responsabilidades del proceso de Administración de la Configuración deberán definirse mediante el proceso de estructura de gobierno de TI.
1.5	Las políticas de seguridad de la información que aplican para la dependencia o entidad, son extensivas al proceso de administración de la configuración.
1.6	Las actividades respecto a la administración de los activos deberá observar también las leyes gubernamentales que a este respecto apliquen.
1.7	Cualquier proceso o actividad que modifique cualquier elemento o activo del ambiente operativo en el alcance del proceso, estará obligado a comunicar dichos cambios al proceso de configuraciones.
1.8	Cualquier consulta de información a la CMDB se hará mediante los procedimientos definidos por el proceso de configuraciones para este fin.
1.9	La información de los elementos y activos contenida en la CMDB deberá ser verificada de manera periódica contra los elementos que componen el ambiente operativo de la dependencia o entidad, esto con fines de seguridad de la información, de continuidad de la operación y auditoria.
1.10	La información de los elementos y activos del ambiente productivo que pertenezcan a proveedores pero estén en el alcance del proceso de configuraciones, son sujetos de las políticas y procedimientos definidos en el proceso de administración de la configuración.
1.11	Todo elemento o activo del ambiente productivo y gestionado mediante el proceso de configuraciones, deberá estar relacionado a un servicio que se proporcione la dependencia o entidad.
1.12	Toda modificación a la estructura de la CMDB, a las políticas, definición de roles, actividades y procedimientos, deberá gestionarse mediante el proceso de administración de cambios.
1.13	Cuando un elemento o activo del ambiente productivo sea retirado del entorno físico de la dependencia o entidad, su información reflejada en la CMDB no deberá ser borrada y en su lugar, se pasará a un estatus de inactividad.
1.14	La información contenida en la CMDB deberá hacerse disponible para consulta a los procesos autorizados para hacerlo.
1.15	La evaluación de desempeño del proceso, deberá realizarse mediante el proceso de administración del desempeño de TIC.
1.16	Deberá existir, bajo los mismos mecanismos de seguridad y control que la CMDB de producción, una CMDB para los ambientes de desarrollo, pruebas y preproducción.

7.8.4.5. Documentación soporte del proceso

	No aplica

7.9 OPERACIÓN DE SERVICIOS

7.9.1 Operación de la mesa de servicios

7.9.1.1 Objetivos del proceso

General.-

Construir el punto único de contacto para que los usuarios de los servicios hagan llegar sus solicitudes de soporte, recibirlas, registrarlas, clasificarlas, categorizarlas, atenderlas y documentarlas.

Específicos.-

1. Gestionar el ciclo de vida de los incidentes, requerimientos de servicio, solicitudes de cambio, problemas y demás solicitudes.
2. Generar y distribuir la información de los procesos realizados por la mesa de servicio, para la toma de decisiones.
3. Solucionar el mayor número de solicitudes de soporte en los primeros niveles de soporte para reducir su tiempo y costo.
4. Medir la satisfacción del usuario final con respecto al uso de los servicios provistos y difundir los resultados.

7.9.1.2. Descripción del proceso

7.9.1.2.1 Mapa general del proceso

Diagrama de flujo de información (1/2)

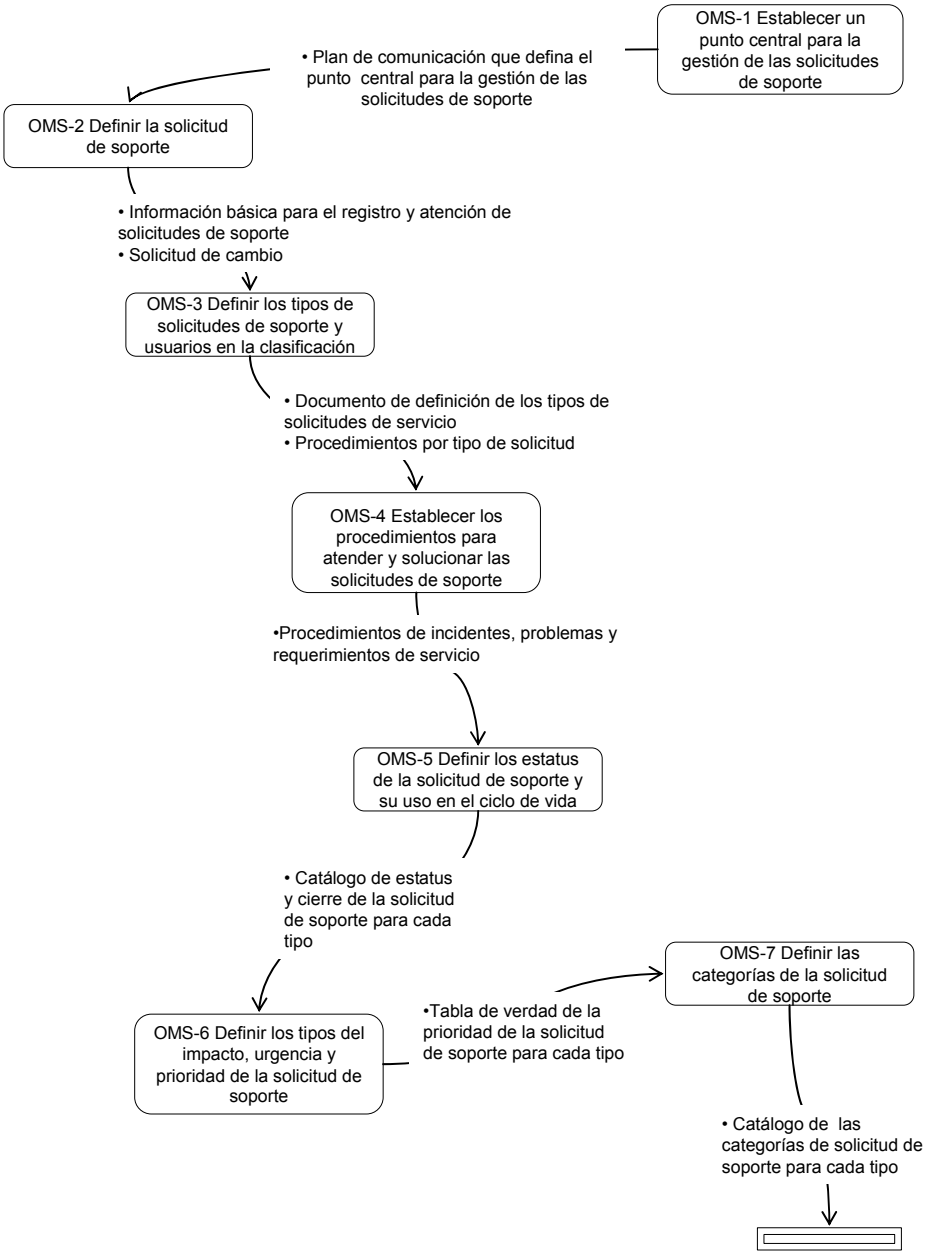


Diagrama de flujo de información (2/2)

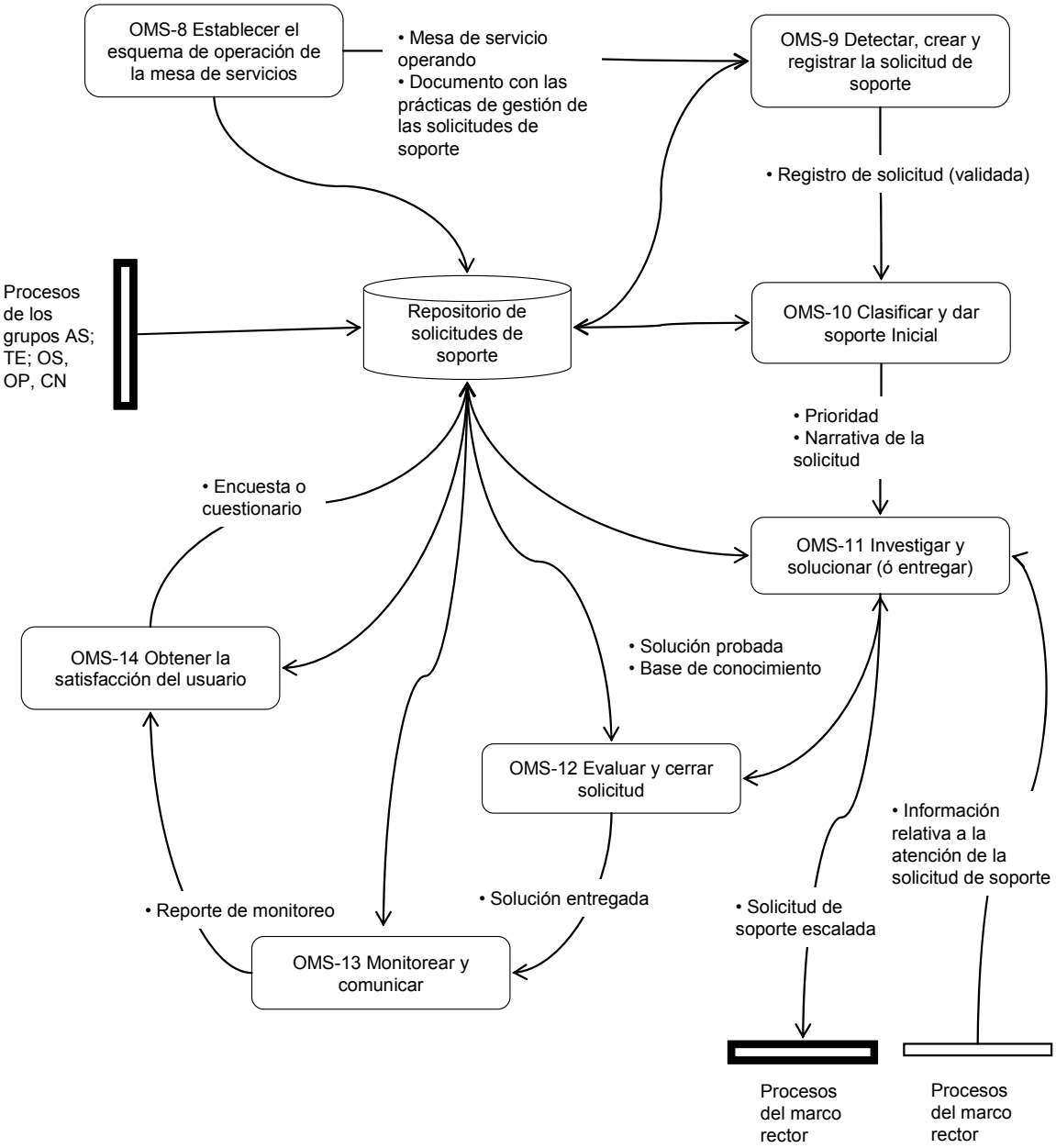


Diagrama de flujo de actividades (1/2)

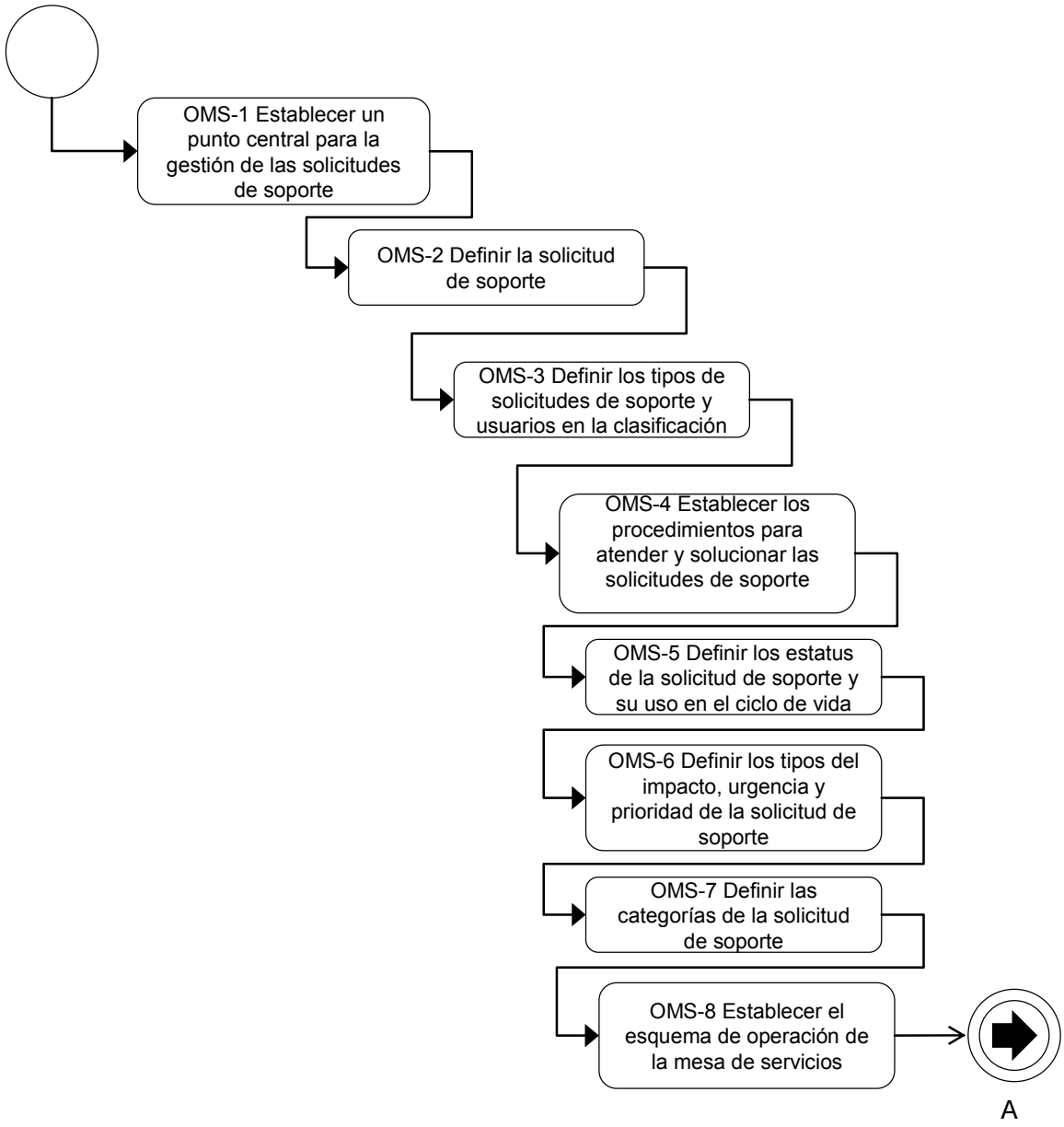
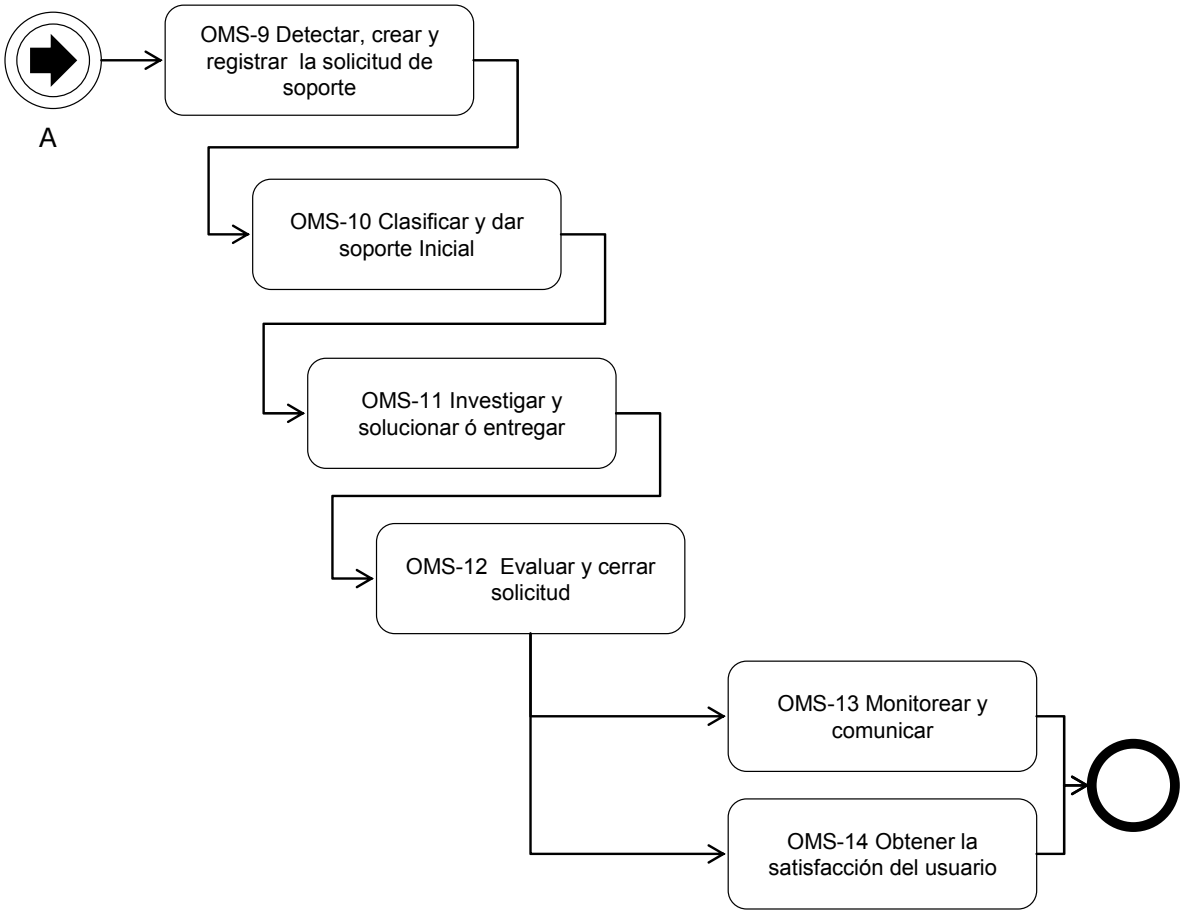


Diagrama de flujo de actividades (2/2)



7.9.1.2.2 Descripción de las actividades del proceso

OMS-1 Establecer un punto central focal para la gestión de las solicitudes de soporte

Descripción	Establecer un punto central único a través del cual, se administre de manera centralizada el ciclo de vida de las solicitudes de soporte que permita su control adecuado, esto con el fin de facilitar el ciclo de vida de las solicitudes y la evaluación del servicio de soporte que se presta a la dependencia o entidad
Factores Críticos	1. Establecer el punto central para la recepción y gestión de las solicitudes de soporte y realizar la difusión del mismo entre los involucrados, siendo los usuarios de los servicios, los de mayor prioridad. 2. Definir y difundir los canales de comunicación oficiales para la recepción y gestión de las solicitudes de soporte (teléfono, correo electrónico, páginas, formatos Web, entre otros). 3. Implementar las herramientas tecnológicas que permitan la recepción y el ciclo de vida de las solicitudes de la solicitud de soporte.
Relación de productos	• Plan de comunicación que defina el punto central para la gestión de las solicitudes

OMS-2 Definir la solicitud de soporte

Descripción	La solicitud de soporte es el instrumento mediante el cual el usuario de los servicios requiere el apoyo del o los proveedores de esos servicios, para satisfacer una necesidad de apoyo en forma de solución o aprovisionamiento. La solicitud deberá contener la información mínima necesaria para que sea posible procesarla, por lo que es necesario precisar la información que se requiere del solicitante
Factores Críticos	1. Definir los datos mínimos que se requieren del usuario tales como nombre y detalles de contacto. 2. Para el caso de requerimientos de servicio, definir con qué autorizaciones previas debe contar el usuario para hacer la solicitud. 3. En caso de que la solicitud de soporte se refiera a una solicitud de cambio y este tipo de solicitudes estén en el alcance de la mesa de servicios, comprobar que se cumplen con los requisitos establecidos por el proceso de administración de cambios. 4. Solicitar información a las áreas operativas sobre la información mínima suficiente para poder diagnosticar adecuadamente un incidente, requerimiento, problema o cambio. 5. Identificar elementos coincidentes de la información proporcionada por las áreas operativas. 6. Identificar información crítica y particular para que un área operativa en particular, atienda la solicitud. 7. Realizar los ajustes necesarios para estandarizar la recopilación de información.
Relación de productos	• Información básica para el registro y atención de solicitudes de soporte • Solicitud de cambio

OMS-3 Definir los tipos de solicitudes de soporte y usuarios en la clasificación

Descripción	Las solicitudes de soporte son procesadas de acuerdo al tipo de solicitud de que se trate tales como apoyo técnico, requerimientos, solicitudes de cambio, entre otros. Es con base en la categorización del tipo de solicitud de soporte, que se determina el procedimiento que aplicará, y es en función de ese procedimiento que variará el tiempo de su ciclo de vida, el equipo de

	especialistas responsables de solucionarlo e incluso las autorizaciones que se requerirán cuando así aplique.
Factores Críticos	1. Definir los tipos de solicitudes que estarán disponibles en la clasificación del caso. Podrán considerarse los siguientes tipos: • Incidente • Requerimiento de servicios • Solicitud de Cambio • Problema 2. Para cada tipo de solicitud, se deberá desarrollar un procedimiento en particular que se aplicará sobre ese tipo de solicitud. 3. Al clasificar una solicitud en un registro, deberá elegirse el tipo de solicitud que aplique.
Relación de productos	• Documento de definición de los tipos de solicitudes de servicio • Procedimientos por tipo de solicitud

OMS-4 Establecer los procedimientos para atender y solucionar las solicitudes de soporte

Descripción	Los procedimientos específicos para atender y solucionar las solicitudes de soporte deben definirse para darles el tratamiento adecuado. Deberán entonces definirse procedimientos para atender incidentes, requerimientos de servicios, problemas y cambios que permitan lograr que el impacto negativo o la oportunidad implícita en cada uno, sean minimizados y capitalizados respectivamente, en beneficio de la dependencia o entidad.
Factores Críticos	1. Definir el procedimiento para la atención de Incidentes. • Definir el alcance del proceso en cuanto a la naturaleza de los Incidentes. • Definir la clasificación y categorización de los Incidentes. • Definir el ciclo de vida de los Incidentes. • Establecer procedimientos para la investigación y diagnóstico de los Incidentes. • Establecer procedimientos para la solución de los Incidentes y restauración del servicio. • Generar las interfaces con el resto de procesos de la dependencia o entidad tales como problemas, requerimientos de servicio, configuraciones, cambios, SLA, entre otros. • Definir los códigos de cierre. • Generar y disponer de repositorios de conocimiento para la solución de Incidentes. • Establecer procedimientos de escalamiento jerárquico y funcional. 2. Definir el procedimiento para la atención de requerimientos de servicio. • Definir el alcance del proceso en cuanto a la naturaleza de los requerimientos de servicio. • Definir la clasificación y categorización de los requerimientos de servicio. • Definir el ciclo de vida de los requerimientos de servicio. • Establecer procedimientos para la realización de los requerimientos de servicio. • Generar las interfaces con el resto de procesos de la dependencia o entidad tales como configuraciones, cambios, SLA, entre otros. • Definir los códigos de cierre. • Generar y disponer de documentación guía para la atención de las solicitudes. • Establecer procedimientos de escalamiento jerárquico y funcional. • Definir una matriz de de autorización de requerimientos 3. Definir el procedimiento para la atención de solicitudes de cambio. • Considerar lo ya definido en el proceso de administración de cambios. 4. Definir el procedimiento para la atención de problemas. • Definir los criterios para identificar y escalar los problemas.

	• Definir la clasificación y categorización de los Problemas. • Definir el ciclo de vida de los Problemas. • Establecer procedimientos para la investigación y diagnóstico de los Problemas, con base en metodologías probadas para la identificación de causas raíz. • Establecer procedimientos para la solución de los problemas y restauración del servicio. • Generar las interfaces con el resto de procesos de la dependencia o entidad tales como Incidentes, configuraciones y cambios. • Generar y compartir la base de datos de errores conocidos con el proceso de Incidentes. 5. Asegurar que todos los usuarios de las soluciones tecnológicas , servicios y bienes de TIC conozcan las responsabilidades inherentes a su uso, solicitud y resguardo, otorgados mediante la entrega de nombres de usuario y contraseñas, así como por el equipamiento propio del cargo.
Relación de productos	• Procedimientos de incidentes, problemas y requerimientos de servicio

OMS-5 Definir los estatus de la solicitud de soporte y su uso en el ciclo de vida

Descripción	El Estatus de una solicitud de soporte refleja la etapa actual en la que se encuentra la solicitud respecto de su ciclo de vida. Es necesario entonces definir los estatus que se usarán para registrar y visualizar el avance actual de la solicitud.
Factores Críticos	1. Se definirán los estatus que reflejen los diferentes estados por los que puede pasar un registro durante su ciclo de vida 2. Los estatus de la solicitud deberán estar disponibles en la herramienta habilitadora del proceso para su uso y deberán poderse cambiar conforme se requiera. 3. Definir las reglas que aplicarán para el cambio de estatus de un registro de la solicitud en la herramienta habilitadora.
Relación de productos	• Catálogo de estatus y cierre de la solicitud de soporte para cada tipo

OMS-6 Definir los tipos de impacto, urgencia y prioridad de la solicitud de soporte

Descripción	Una solicitud de soporte necesita ser evaluada en cuanto al impacto y urgencia que tiene en los procesos, y así determinar el lugar que ocupará esa solicitud respecto a otras que se han solicitado, lo que se conoce como la prioridad de la solicitud. Por lo tanto es preciso definir las características de la solicitud deberán ser consideradas para determinar su impacto y urgencia.
Factores Críticos	1. Determinar el impacto de la solicitud a través de la medición de su efecto en los procesos de la dependencia o entidad. En general, los incidentes y problemas tienden a variar considerablemente su impacto de mediano a alto, mientras que los requerimientos de servicio deberían ser en su mayoría de impacto moderado a bajo. 2. El impacto de la solicitud no deberá deducirse considerando únicamente un enfoque cuantitativo. 3. Determinar la urgencia de la solicitud estableciendo la medición del tiempo que tomará hasta que tenga un Impacto en la dependencia o entidad. 4. La prioridad de la solicitud se determina a partir de considerar ambos, el impacto y la urgencia mediante una tabla de verdad. Con la prioridad se determina el lugar de esa solicitud en específico en relación a otras que estén pendientes. 5. El Impacto, Urgencia y por lo tanto la Prioridad, pueden cambiar conforme avance la solicitud en su ciclo de vida.
Relación de	• Tabla de verdad de la prioridad de la solicitud de soporte para cada tipo

productos	

OMS-7 Definir las categorías de la solicitud de soporte

Descripción	Se deberán definir las categorías de la solicitud de soporte que estarán disponibles como parte de la actividad de clasificación de la solicitud. La categoría de una solicitud define la naturaleza o campo de acción de las mismas y facilita la identificación de puntos que deben mejorarse en la provisión del servicio.
Factores Críticos	1. Definir los niveles que se necesitarán para categorizar las solicitudes de soporte. 2. Definir la categoría de las solicitudes, que contemplen todos los tipos de las mismas en cuanto a su naturaleza. 3. Las categorías de las solicitudes deben describir el rubro que será afectado, por ejemplo procesos, documentación, hardware, software, aplicaciones, entre otros. 4. Las categorías deben establecerse en una estructura de árbol con ramificaciones.
Relación de productos	• Catálogo de las categorías de solicitud de soporte para cada tipo

OMS-8 Establecer el esquema de operación de la mesa de servicios

Descripción	Considerar la forma en la que la mesa de servicios estará estructurada tanto jerárquicamente como en lo referente a las herramientas y personal que la integrarán,
Factores Críticos	1. Definir la cantidad de personal que se requerirá para la integración de la mesa de servicio con base en el número usuarios a atender, el volumen anticipado de solicitudes, el horario de operación de la dependencia o entidad y su distribución. 2. Definir el perfil del personal que se requerirá para la integrar la mesa de servicio considerando la complejidad y especialización del ambiente operativo, los SLA comprometidos, los recursos tales como tiempo y costos disponibles. 3. Definir la forma en la que la mesa de servicio interactúa con los administradores de otros procesos. 4. Definir las prácticas de gestión de las solicitudes en todo el ciclo de vida 5. Enfatizar y promover a la mesa de servicios como único punto de contacto 6. Contar con todos los procedimientos de atención de Solicitudes documentados y comprendidos. 7. Contar con todos los catálogos y las clasificaciones adecuadas, aprobadas y conocidas por el personal de la mesa de servicio. 8. Establecer una herramienta habilitadora de las funcionalidades de registro, correlación, flujo de trabajo, manejo de alertas y seguridad, que permita que en su conjunto, los procesos asociados a la mesa de servicio, se realicen de forma ágil y eficiente en un repositorio de datos. 9. Establecer mecanismos de comunicación ágiles para la interrelación entre la Mesa de servicios y los usuarios.
Relación de productos	• Mesa de servicio operando • Documento con las prácticas de gestión de las solicitudes de soporte • Repositorio de solicitudes de soporte

OMS-09 Detectar, crear y registrar solicitud de soporte

Descripción	Como parte operacional, las solicitudes deben ser, o bien detectadas y registradas, o bien creadas y registradas.
Factores Críticos	1. Los usuarios son responsables de crear y detectar las solicitudes, bajo los esquemas previamente definidos

	2. La mesa de servicio recibe continuamente dichas solicitudes y las registra o dependiendo de la herramienta habilitadora. 3. Asegurar del correcto registro de cada solicitud. Esta revisión de cada solicitud puede ser suficiente, requerir información adicional o incluso que el usuario vuelva a elaborarla.
Relación de productos	• Repositorio de solicitudes de soporte • Registro de solicitud (validada)

OMS-10 Clasificar y dar soporte inicial

Descripción	Una vez registrada la solicitud, la mesa de servicios debe realizar una clasificación inicial, y en base en ella y en la información de la solicitud, determinar, en primer lugar, el tipo de solicitud, en segundo lugar, establecer una prioridad, y finalmente debe tratar de dar el soporte inicial, para con ello concretar y acotar los términos y requerimientos de la solicitud.
Factores Críticos	1. Haber establecido catálogos con pocos niveles de profundidad, para facilitar la gestión 2. Haber establecido categorías adecuadas y homogéneas y claras, que realmente reflejen las variantes de las solicitudes tanto por tipo como por detalle y granularidad, buscando el equilibrio entre lo general y lo detallado 3. Contar con personal suficiente y adecuadamente entrenado y con el perfil requerido para laborar en la mesa de servicios 4. Contar con una herramienta habilitadora que facilite y agilice las actividades de esta práctica.
Relación de productos	• Repositorio de solicitudes de soporte • Prioridad • Narrativa de la solicitud

OMS-11 Investigar y solucionar (ó entregar)

Descripción	Cuando la solicitud se ha categorizado y priorizado, debe investigarse la mejor forma de dar el soporte. La investigación se realiza sobre diversas fuentes, usando procedimientos y estándares. Entonces se realizará la solución de la solicitud. Estas tareas son iterativas: se realizan tantas veces sea necesario. Debe asegurarse el apego a los tiempos establecidos, para realizar los escalamientos funcionales y/o jerárquicos, involucrando a niveles más expertos para la solución.
Factores Críticos	1. Contar con los procedimientos y modelos de proceso formalmente liberados y en operación, para asegurar la eficiencia en las actividades 2. Dentro del perfil del personal, debe considerarse la capacidad de organizarse y establecer actividades con sus iguales, con miras a agilizar la investigación y diagnóstico. 3. Contar con fuentes de información organizadas y con contenido de calidad, que ayuden a identificar y establecer las mejores soluciones con prontitud y certeza.
Relación de productos	• Solución probada • Base de conocimiento • Información relativa a la atención de la solicitud de soporte • Solicitud de soporte escalada

OMS-12 Evaluar y cerrar solicitud

Descripción	Una vez atendida la solicitud de soporte, el personal que lo entrega debe evaluar si todo se ha resuelto por completo y lo debe marcar como concluido. Sin embargo, es el usuario quien finalmente determina, a su satisfacción, si puede proceder a cerrar la Solicitud establecida previamente.

Factores Críticos	1. Asegurar que el personal que resuelva una solicitud de soporte realiza la evaluación del resultado de la entrega, y que verifica que el servicio opere dentro de los límites establecidos y acordados. 2. Asegurar que todas las actividades realizadas son registradas con precisión y consistencia, para construir mejores fuentes de información y construir una parte importante de la administración del conocimiento. 3. Establecer claramente los criterios para el cierre de cada tipo de solicitud de soporte 4. Asegurar que se cuenta con un procedimiento y mecanismo para registrar la evaluación proporcionada por el usuario
Relación de productos	• Solución entregada

OMS-13 Monitorear y comunicar

Descripción	Deberá asegurar el cumplimiento de las prácticas, para monitorear, dar seguimiento y comunicar sobre los estados, relacionados con el ciclo de vida de cada una de las solicitudes de soporte. Estas prácticas son indispensables para alinear y enfocar los esfuerzos para cumplir con los acuerdos establecidos, y mantener la comunicación constante y necesaria con todos los usuarios.
Factores Críticos	1. Desarrollar procedimientos de monitoreo, seguimiento y comunicación asimismo asegurar que son ejecutados durante el ciclo de vida de la solicitud de soporte. 2. Hacer conciencia sobre la criticidad de la práctica, en el sentido más amplio posible, para enfatizar la oportunidad y constancia con que debe realizarse 3. Contar con una herramienta habilitadora que sea capaz de resumir y reportar constantemente los cambios en los estados de las solicitudes, las alertas relacionadas con la evolución de la misma y que permitan rastrear y dar seguimiento a cada Solicitud de soporte
Relación de productos	• Reporte de monitoreo

OMS-14 Obtener la satisfacción del Usuario

Descripción	Determinar la satisfacción del usuario a través de la explotación de los indicadores de desempeño establecidos para cada proceso, además de conducir encuestas o cuestionarios de forma periódica para identificar áreas de oportunidad y mejorar la atención.
Factores Críticos	1. Haber diseñado encuestas o cuestionarios con el suficiente grado de imparcialidad para obtener los resultados más confiables posibles. 2. Establecer claramente los objetivos, metas y propósitos de las encuestas y cuestionario asociados, y difundirlos efectivamente tanto a la Unidad TIC como a los usuarios. 3. Determinar y escoger la muestra representativa dentro de los usuarios, para elaborar las encuestas y/o cuestionarios.
Relación de productos	• Encuesta o cuestionario • Repositorio de solicitudes de soporte

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.9.1.2.3. Descripción de roles

Rol	Descripción
Administrador de mesa de servicios	Coordinar las operaciones de la mesa de servicios. Administrar al personal de la mesa de servicios. Recopilar información de desempeño de la mesa de servicios. Proporcionar información de toma de decisiones a la dependencia o entidad. Escalar los incidentes / requerimientos a los niveles funcionales o jerárquicos que sean necesarios. Validar que la mesa de servicio apoye al cumplimiento de los SLA acordados con los clientes.
Administrador de incidentes	Impulsar la eficiencia y la eficacia para la atención de Incidentes. Coordinarse con el administrador de la mesa de servicios para atender los incidentes en tiempo y forma. Monitorear la efectividad de la administración de incidentes y hacer recomendaciones de mejora. Desarrollar y mantener sistemas de administración de incidentes. Monitorear el estado y el avance hacia la resolución de todos los incidentes abiertos. Mantener a los usuarios informados sobre el progreso de los incidentes. Apoyar al administrador de mesa de servicio para escalar el incidente, si es necesario.
Administrador de requerimientos	Impulsar la eficiencia y la eficacia en la atención de requerimientos de servicio. Coordinar con el administrador de la mesa de servicios para atender los requerimientos de servicio en tiempo y forma. Monitorear la efectividad del proceso y hacer recomendaciones de mejora. Desarrollar y mantener sistemas de administración de requerimiento de servicios. Monitorear el estado y el avance hacia la resolución de todos los requerimientos de servicios. Mantener a los usuarios informados sobre el progreso de sus solicitudes. Apoyar al administrador de mesa de servicio para escalar la solicitud.
Personal de la mesa de servicios	Responsable de la gestión de las solicitudes de soporte desde su recepción, hasta su cierre. Responsable de llevar la relación con los usuarios a nombre de los proveedores de los servicios. Dueño del ciclo de vida de los Incidentes y requerimientos de servicios. Escalar jerárquicamente solicitudes de soporte en riesgo de caer fuera de los SLA. Generar los reportes de desempeño de los procesos gestionados. Atención a primer nivel de las solicitudes de servicio con fines de solución. Escalar funcionalmente aquellas solicitudes que necesiten ser atendidas y solucionadas por los equipos de especialistas. Dar seguimiento constante de la solicitud de soporte hasta su cierre y mantener informado del avance al usuario que la reportó.

Equipos responsables de atender y solucionar las Solicitudes	Responsable de la atención, actualización, documentación y solución de las Solicitudes de soporte que se le han asignado, dentro de los niveles de servicio comprometidos. Responsable de llevar la relación con los proveedores externos involucrados en la provisión de sus propios servicios. Escalar funcionalmente aquellas solicitudes para las que se requiera el apoyo de un proveedor externo. Notificar a la mesa de servicios cualquier asunto relacionado a la solicitud de soporte que atiende, incluidas solicitudes de reasignación.

7.9.1.2.4. Descripción de productos

Producto	Descripción
Información básica para el registro y atención de solicitudes de soporte	Listado y descripción de los datos mínimos que son requeridos para registrar y gestionar cada tipo de solicitud de soporte. Esto incluye los datos del usuario y del tipo de apoyo que solicita
Documento de definición de los tipos de Solicitudes de Servicio	Documento en el que se listan y describen los tipo de solicitudes de soporte que estarán en el alcance de la gestión de la mesa de servicios. Los tipos definen no solo las solicitudes posibles, sino sus características y particularidades: • Incidentes • Requerimientos de servicios • Problemas • Solicitudes de Cambio
Catálogo de estatus y cierre de la solicitud de soporte para cada tipo	Tabla en donde se definen los códigos de estatus válidos para cada tipo de solicitud de soporte en el alcance de los procesos involucrados
Tabla de verdad de la prioridad de la solicitud de soporte para cada tipo	Tabla para determinar la prioridad que tiene la solicitud de soporte, a través del impacto a la dependencia o entidad y el nivel de urgencia solicitado para su implantación
Catálogo de las categorías de solicitud de soporte para cada tipo	Documento donde se definen los niveles que debe cubrir una solicitud de soporte para poder ser categorizado, con base en los elementos que se afectan
Plan de implementación y operación de la mesa de servicio	Documento que incluye el calendario de trabajo para la implementación de la mesa de servicio, las herramientas, personal, procesos y procedimientos requeridos para su correcta operación. Algunos puntos que deben de ser considerados en este documento son: a) Calendario de trabajo b) Recursos humanos y tecnológicos requeridos para su implementación c) Procesos y procedimientos de operación
Documento con las	Documento que incluye las mejores prácticas que se deben de implementar en la mesa de

Producto	Descripción
prácticas de gestión de las solicitudes de soporte	servicio para la gestión de las llamadas en todo el ciclo de vida: a) Etiqueta de inicio b) Procedimientos de atención c) Etiqueta de salida
Narrativa de solicitud	Es la información proporcionada a personal de mesa de servicio que describe el incidente o falla, y la cual es registrada en la herramienta para su interpretación por el área que dará atención al servicio.
Solicitud de cambio	Es una petición formal, para cambiar el estado de un componente, ya sea para recibir soporte, para solucionar un problema o para mejorar algún servicio. En el ámbito de la mesa de servicios s, son las que pueden realizarse por medio de la gestión de la mesa de servicios.
Repositorio de solicitudes de soporte	Son el conjunto de datos relacionados con la solicitud, capturados en una plantilla, ya sea en papel y comúnmente en la herramienta habilitadora. Este registro va modificándose, conforme avanza la solicitud en su ciclo de vida.
Solución entregada	Es el producto, soporte, ayuda o entrega de un servicio o componente de servicio, dado formalmente como respuesta a una Solicitud de soporte.
Base de conocimiento	Repositorio de conocimiento (información y datos en sus distintas manifestaciones incluyendo: modelos, patrones, estándares, plantillas y otros artefactos)
Encuesta o cuestionario	Es un documento diseñado para conocer la percepción real del usuario, sobre los servicios de la mesa de servicio.

7.9.1.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Número de solicitudes e incidentes atendidos	Medir la cantidad de solicitudes atendidas	Medir la cantidad de solicitudes atendidas	Cobertura	De gestión	Número de solicitudes e incidentes atendidos		Mensual
Incidentes y solicitudes atendidas en el tiempo comprometido	Incrementar las solicitudes atendidas dentro del tiempo comprometido	Medir la proporción de solicitudes atendidas dentro del tiempo comprometido	Eficiencia	De gestión	Solicitudes atendidas en tiempo/solicitudes atendidas		Mensual
Satisfacción del usuario	Evaluar la satisfacción del usuario para evaluar el servicio	Encuesta de satisfacción del usuario para evaluar el servicio	Calidad	De gestión	Promedio del resultado de las encuestas		Mensual

7.9.1.4	Reglas del proceso

1.1	La mesa de servicios es el punto único de contacto (SPOC) entre los usuarios de los servicios y los proveedores de los mismos.
1.2	Toda solicitud de soporte que esté dentro del alcance de los procesos de Incidentes y requerimientos de servicio, así como cualquier otro tipo de solicitud que se defina dentro del alcance tal como solicitudes de cambio, deberán tener como punto de entrada la mesa de servicios.
1.3	La mesa de servicios es responsable del ciclo de vida de las solicitudes de soporte que hagan los usuarios de los servicios, sean estos Incidentes, requerimientos de servicios u otro tipo de solicitudes en el alcance de esta función.
1.4	Toda solicitud de soporte, sin excepción, deberá ser registrada y clasificada y deberá generarse un identificador único que se le proporcionará al usuario.
1.5	La información que se genere a partir de la mesa de servicios es confidencial para uso exclusivo de la dependencia o entidad.
1.6	Se debe difundir la información de los procesos gestionados por la mesa de servicios (Incidentes, solicitudes, problemas, cambios, configuraciones, entre otros.).
1.7	Los roles y responsabilidades de este proceso deberán definirse mediante el proceso de Establecimiento de la estructura de gobierno de TI.
1.8	El área responsable de la mesa de servicios deberá comunicar a los usuarios, y tener evidencia de haberlo hecho, las disposiciones que le apliquen de acuerdo a los servicios que le habilite en ya sea en su equipo de escritorio o portátil, o por medio de los accesos a Internet, intranet, servicios de colaboración, accesos a sistemas o aplicativos y cualquier otro servicio de TIC.

	Reglas aplicables a los procedimientos que se rijan por este proceso
	La evaluación de desempeño del proceso, deberá realizarse mediante el proceso de administración del desempeño de TIC.
	Los roles y responsabilidades, deberán definirse mediante el proceso de estructura de gobierno de TI.
	Cada dependencia o entidad de la APF deberá contar con una mesa de servicios para la atención de reportes de falla y solicitudes de servicios de alcance Institucional.
	La UTIC deberá implementar la infraestructura necesaria para que la mesa de servicios atienda las solicitudes, requerimientos y reportes de fallas que reciba canalizándola a las áreas de solución respectivas.
	La UTIC deberá definir la implementación del sistema automatizado de gestión de mesa de servicios para la dependencia o entidad de conformidad a las presentes disposiciones.
	La UTIC será la responsable de supervisar, monitorear, controlar y evaluar las actividades desarrolladas por la mesa de servicios.
	La UTIC deberá definir los indicadores para evaluar el servicio de la mesa de servicios a fin de mantener el nivel de servicio acordado con las UR y un proceso de mejora continua.
	La UTIC deberá asignar un área responsable de la operación y buen funcionamiento de la mesa de servicios de alcance institucional.
	El área responsable de la mesa de servicios deberá registrar en la mesa de servicios los servicios de mantenimiento contratados, o los servicios de mantenimiento por garantía en equipos de reciente adquisición; como parte de la instrumentación de la mesa de servicio
	El área responsable de la mesa de servicios definirá los tiempos de atención y de solución que se comprometan con los usuarios; éstos deberán ser aprobados por el titular de la UTIC y las áreas

	de que atenderán las solicitudes que reciba la mesa de servicios o, en caso de tratarse de un servicio de un tercero, los niveles de servicio que correspondan para cada tipo de requerimiento o falla que se identifique.
	El área responsable de la mesa de servicios deberá realizar un análisis de prioridades y acordar con las UR los tiempos de atención para cada tipo de solicitud; para el caso de las UR que por su naturaleza requieran de una atención inmediata, la mesa de servicios con el soporte de las áreas de solución de la UTIC y los proveedores involucrados, implementará el proceso de atención necesario para cumplir con acuerdo comprometido.
	El área responsable de la mesa de servicios deberá mantener una difusión a la totalidad de los usuarios, de manera constante, de las disposiciones relacionadas con la utilización de la mesa de servicios y los servicios que proporciona.
	El área responsable de la mesa de servicios deberá canalizar las solicitudes y reportes que reciba de los usuarios y será la responsable del seguimiento de los reportes ante las áreas técnicas especializadas, o con los proveedores externos
	El área responsable de la mesa de servicios deberá comunicar a los usuarios, y tener evidencia de haberlo hecho, las disposiciones que le apliquen de acuerdo a los servicios que le habilite en ya sea en su equipo de escritorio o portátil, o por medio de los accesos a Internet, intranet, servicios de colaboración, accesos a sistemas o aplicativos y cualquier otro servicio de TIC.
	El área responsable de la mesa de servicios deberá poner a disposición de los usuarios un medio para que éstos puedan rastrear el proceso de atención de su solicitud o reporte.
	El área responsable de la mesa de servicios será la responsable de recibir las solicitudes que impliquen los servicios mantenimiento de los equipos de cómputo personal portátil o de escritorio, de acuerdo a las necesidades de los usuarios. Independientemente de que éstos se encuentren bajo contrato de mantenimiento, en garantía o sin contrato que los cubra.
	El área responsable de la mesa de servicios deberá recibir las solicitudes y reportes de equipos que impliquen los servicios de mantenimiento correctivo, tanto de equipos de cómputo personal portátil o de escritorio como de los dispositivos de respaldo de energía y equipos de comunicaciones que tengan asignados los usuarios o de los que hagan uso e identifiquen su falla.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios cuando requieran el alta, baja y/o cambio de cuentas de usuario para acceso a la red, sistemas operativos, bases de datos o aplicaciones institucionales.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios cuando se presenten problemas en los equipos de cómputo y/o periféricos asignados, software instalado o aplicaciones, o en los servicios que le son proporcionados.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios cuando requieran capacitación en materia de TIC o tengan inquietudes sobre el correcto uso de los recursos y/o servicios autorizados para ser canalizados al área correspondiente.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios cuando requieran capacitación o apoyo en la implementación de las disposiciones para el aseguramiento de su entorno de trabajo.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios cuando sospechen que su equipo se encuentra infectado por algún virus informático.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios requieran la instalación de un nuevo software o hardware institucional.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios cuando requieran trasladar o dar de baja un equipo de cómputo y/o sus periféricos.
	Los usuarios deberán solicitar servicios o efectuarán un reporte de falla a la mesa de servicios requieran del acceso al servicio de Internet a través de un enlace dial-up.

Los usuarios deberán reportar a través de la mesa de servicios cualquier afectación que identifiquen en los enlaces de comunicaciones, deberán ser reportadas a la mesa de servicios desde la ubicación dónde ocurra dicho evento, ya sea oficinas centrales o foráneas de la dependencia o entidad.
Los usuarios deberán reportar a través de la mesa de servicios cualquier afectación o mal funcionamiento de las soluciones tecnológicas y servicios de colaboración, Internet e intranet que identifiquen.
Es obligación del usuario utilizar el servicio de Internet, intranet y servicios asociados a éstos única y exclusivamente para fines relacionados con las funciones y atribuciones que tiene conferidas.
El Usuario deberá solicitar el acceso al servicio de Internet, a través de la mesa de servicios, la mesa de servicios informará de los requisitos que debe cubrir para otorgársele el servicio.
Los usuarios recibirán un nombre de usuario y contraseña para poder acceder a los servicios Internet, intranet y servicios asociados a éstos
Los usuarios que requieran algún cambio en su nombre de usuario y contraseña movimiento de cargo, separación, jubilación o término de contrato están obligados a informar a la mesa de servicios para que ésta gestione los cambios correspondientes con el área responsable de los servicios en la UTIC.
El usuario tiene prohibido instalar y/o utilizar programas que no correspondan a los definidos institucionalmente para la configuración del acceso a los servicios de Internet, Intranet y servicios asociados que le hayan sido instalados por el personal de la UTIC.
Por seguridad de la información institucional que reside en su equipo personal y/o en las soluciones tecnológicas institucionales disponibles vía Internet o Intranet no deberá compartir su nombre de usuario y contraseña para acceder a estos servicios, ya que éstas son de carácter personal e intransferible.
El mal uso del nombre de usuario y contraseña para acceso a los servicios de Internet, Intranet y servicios asociados será responsabilidad de la persona a la que se le asignó el nombre de usuario y contraseña.
La información que el usuario obtenga por medio del uso de los servicios de Internet, intranet y otros servicios asociados, incluyendo su uso y contenido, es responsabilidad del usuario, por lo que está prohibido obtener información con fines de lucro y con contenidos religiosos, pornográficos, musicales, de entretenimiento, políticos o cuyo contenido sea ofensivo o contrario a lo establecido dentro del código de conducta de la dependencia o entidad.
El usuario que requiera la conexión a sitios de Internet, con configuraciones diferentes a las que usualmente instaladas deberá solicitar su requerimiento vía la mesa de servicio.
El usuario tiene prohibido modificar los parámetros de configuración en el navegador de Internet.
Los accesos hacia Internet por parte del usuario podrán ser controlados por parte de la UTIC, quedando bajo la responsabilidad estricta del usuario dichos accesos.
El usuario tiene prohibido descargar archivos con extensiones diferentes a las que la mesa de servicios establezca como extensiones seguras de manera que no se ponga en riesgo la integridad de la red de datos de la dependencia o entidad.
El usuario que por razones excepcionales requiera utilizar aplicaciones de Internet que ocupan configuraciones especiales, solicitará al área responsable de UTIC o su equivalente, el apoyo para que les facilite una salida a través de una conexión segura, previa autorización de la UTIC.
No se permitirá el uso de módem (conexión Dial-up) para acceder a Internet, salvo en aquellos casos en que se autorice expresamente por el vía la mesa de servicios por el área responsable de los servicios de Internet, Intranet y servicios asociados en la UTIC.

El usuario tiene prohibido usar cámaras de video y comunicación de audio (transmisión de voz vía micrófono) al hacer uso de los servicios de Internet, Intranet y servicios asociados. En caso de requerir la habilitación de este tipo de comunicación, se deberá considerar como una solicitud de videoconferencia, el usuario deberá hacer una solicitud vía la mesa de servicios.
El usuario tiene prohibido intentar cualquier tipo de ataque en cualquier forma, escaneo, lectura de información interna o penetración de sistemas de cómputo o redes a través de los servicios de Internet, Intranet y servicios asociados que le son otorgados con carácter de oficial.
El usuario tiene prohibido la utilización de papel tapiz y protectores de pantalla con imágenes descargadas de Internet, que sustituyan a los que se difundan o instalen institucionalmente.
El usuario tiene prohibido descargar archivos ejecutables de Internet a menos que sea derivado de alguna de las funciones que le son conferidas por el cargo que ocupa.
Para el caso de relaciones con proveedores de servicios externos el Usuario deberá, apegarse a las condiciones de seguridad, confidencialidad y cumplimiento de las disposiciones en el presente manual.
La UTIC deberá Implementar herramientas de software para analizar todos los mensajes de entrada o salida del correo electrónico para, detectar virus informáticos o contenidos maliciosos.
Los usuarios de los servicios y la infraestructura de TIC deben verificar que su equipo de cómputo tenga instalado el antivirus institucional definido por la UTIC, y tienen la obligación de mantenerlo habilitado permanentemente, en caso de requerir deshabilitarlo deberán solicitar autorización vía la mesa de servicios.
Los usuarios de los servicios y la infraestructura de TIC deben verificar que los archivos obtenidos de manera externa a través de cualquier medio, independientemente de la fuente que envíe el o los archivos, estén libres de virus informáticos antes de ser almacenados o procesados en su equipo de cómputo.
Los usuarios de los servicios y la infraestructura de TIC deberán asegurarse de que, en los casos en que el antivirus institucional identifique que un archivo recibido se encuentra infectado por virus informáticos, emitan un reporte de inmediato a la mesa de servicios indicando el área emisora del o los archivos infectados y esperar instrucciones de la UTIC a través de la mesa de servicios
En relación con el lenguaje que el usuario utilice en el cuerpo de los correos electrónicos, éste deberá apegarse a los códigos de conducta de la dependencia y entidad, al código de ética de los servidores públicos de la administración pública federal así como a las disposiciones emitidas por el IFAI, el AGN, así como a la LFTAIPG que apliquen.
Complementariamente al punto anterior, está prohibido para el usuario del correo electrónico el envío de mensajes cuyo contenido sea nocivo o que atente contra las buenas costumbres y la moral: la pornografía, contenidos obscenos, radicales, juegos, chistes, vídeo y audio entre otros, así como cualquier otro que no tenga relación con las actividades laborales encomendadas al usuario por la dependencia o entidad.
El contenido del buzón de correo electrónico será responsabilidad del usuario al cual se le asignó la cuenta de usuario y contraseña.
En caso de que el usuario de la cuenta de correo y contraseña sospeche que su clave ha sido descubierta deberá dar aviso de inmediato vía los servicios de la mesa de servicio, a fin de que su contraseña sea cambiada.
El área responsable del Correo Electrónico podrá limitar total o parcialmente el acceso a una cuenta de correo determinada, así como cancelar, suspender, bloquear, respaldar o eliminar cuentas, si tuviese conocimiento efectivo de que la actividad o la información almacenada es ilícita o lesiona bienes o derechos de la dependencia o entidad; con independencia de las sanciones a que dieran lugar los hechos.
El área responsable del Correo Electrónico podrá establecer los filtros necesarios a fin de evitar que a través de este servicio puedan difundirse contenidos ilícitos o nocivos para la dependencia o

entidad.
En relación con la confidencialidad del contenido del buzón de los usuarios éstos deberán apegarse a las disposiciones emitidas al respecto por el IFAI, el AGN, así como a la LFTAIPG.
El área responsable del correo Electrónico deberá definir la configuración del formato de salida de los usuarios: No deberá integrarse un fondo, el tipo de la fuente la podrá seleccionar el usuario; deberá contar con un pie de despedida que incluya la siguiente información: nombre del funcionario publico, cargo que ocupa; área de adscripción; nombre de la dependencia o entidad; dirección y ubicación; teléfono y, deberá contener la siguiente leyenda al pie de la página: “La presente información se transmite mediante sistemas y equipos del Estado y se encuentra protegida por mecanismos de seguridad, su revelación, modificación ó reproducción por cualquier medio constituye un delito en términos de lo previsto por los artículos 210 y 211·bis 2 del Código Penal Federal, si Usted no es el destinatario de esta información o la recibió por error deberá borrarla de su sistema y avisar a quien la envió”.
El área responsable del correo electrónico deberá asegurar que se incluya en el cuerpo del correo texto o imágenes derivadas de cualquier otra disposición que se emita en este servicio para la APF.
El uso del servicio de correo electrónico sólo debe ser utilizado para los propósitos de comunicación de asuntos relativos a la dependencia o entidad.
Sólo se considera cuenta de correo electrónico institucional aquella asignada por el área responsable del Correo Electrónico por lo que no se dará soporte al usuario para ningún otro tipo de cuentas de correo y sus correspondientes buzones, quedando bajo la estricta responsabilidad del usuario.
Los usuarios no deberán manejar, con los recursos de red, colaboración y equipo personal que les fueron asignados, ninguna otra cuenta de correo ni sus correspondientes buzones, salvo la asignada para cumplimiento de sus funciones
Las cuentas de correo electrónico y contraseñas asignadas a cada usuario son personales e intransferibles.
En caso de olvido o pérdida de la contraseña, el usuario deberá dar aviso a través de la mesa de servicio para la restauración del uso vía una nueva contraseña.
El Usuario tiene prohibido la alteración de la configuración de cuentas de correo configuradas en el equipo que le haya sido asignado para el desempeño de sus funciones.
El área responsable del Correo Electrónico deberá establecer y difundir vía la mesa de Ayuda, las características para la selección de una contraseña por parte del usuario del correo electrónico.
No se deberá usar la infraestructura de correo electrónico para cualquier práctica tendiente a utilizar, distribuir y/o duplicar información o programas que no sean consistentes con las licencias de uso correspondientes o no este expresamente aprobado por su autor.
Cuando el usuario esté fuera de la oficina por un periodo largo de tiempo y sin atender el correo, deberá utilizar las notificaciones de correo para comunicar esta situación a los remitentes e indicar, de ser necesario, un contacto alterno previa autorización escrita de su inmediato superior.
El usuario no deberá abrir archivos de datos adjuntos que provengan de un origen desconocido, los cuales podrían dañar el equipo del usuario o su información.
Siempre que se reciban archivos vinculados a mensajes de correo deberán escanearse con el antivirus institucional definido por la UTIC con el fin de evitar “virus” o cualquier otra amenaza.

7.9.1.5 Documentación soporte del proceso

No aplica

7.9.2. Administración de servicios de terceros

7.9.2.1. Objetivo general del proceso

General.-

Definir los lineamientos para desarrollar revisiones técnicas y auditorias al proceso del proveedor, así como pruebas técnicas del servicio con el fin de evaluar los niveles de servicio y su cumplimiento conforme a los términos acordados.

Específicos.-

1. Asegurar la calidad del servicio prestado por terceros mediante la evaluación del cumplimiento de los requerimientos técnicos, operativos, contractuales, SLA establecidos y procesos acordados.
2. Planear, ejecutar y dar seguimiento a revisiones técnicas durante el desarrollo de los servicios.
3. Auditar los procesos del proveedor para desarrollar un servicio, asegurando el cumplimiento de los niveles establecidos en los acuerdos contractuales.

7.9.2.2 Descripción del proceso

7.9.2.2.1 Mapa general del proceso

Diagrama de flujo de información

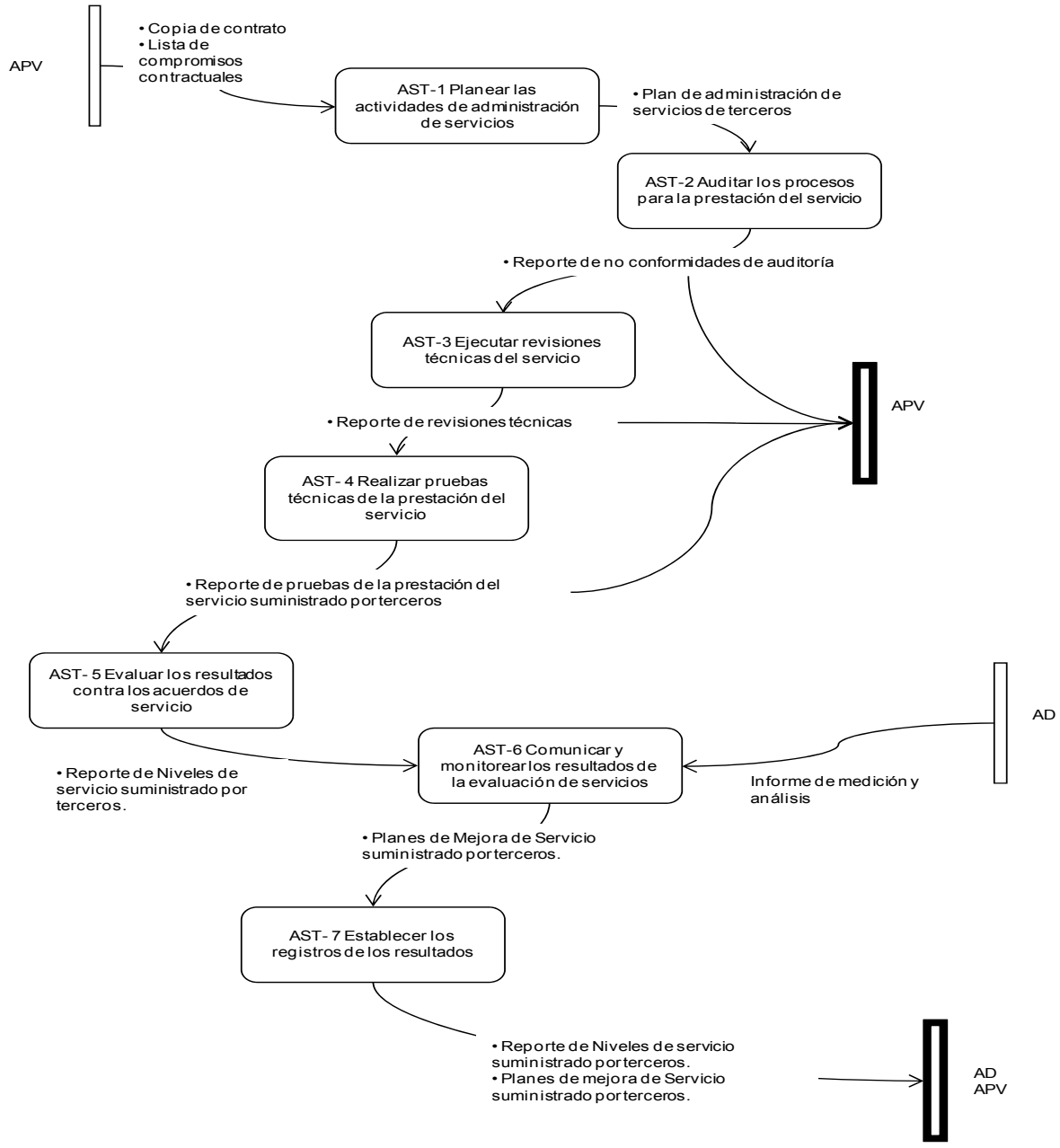
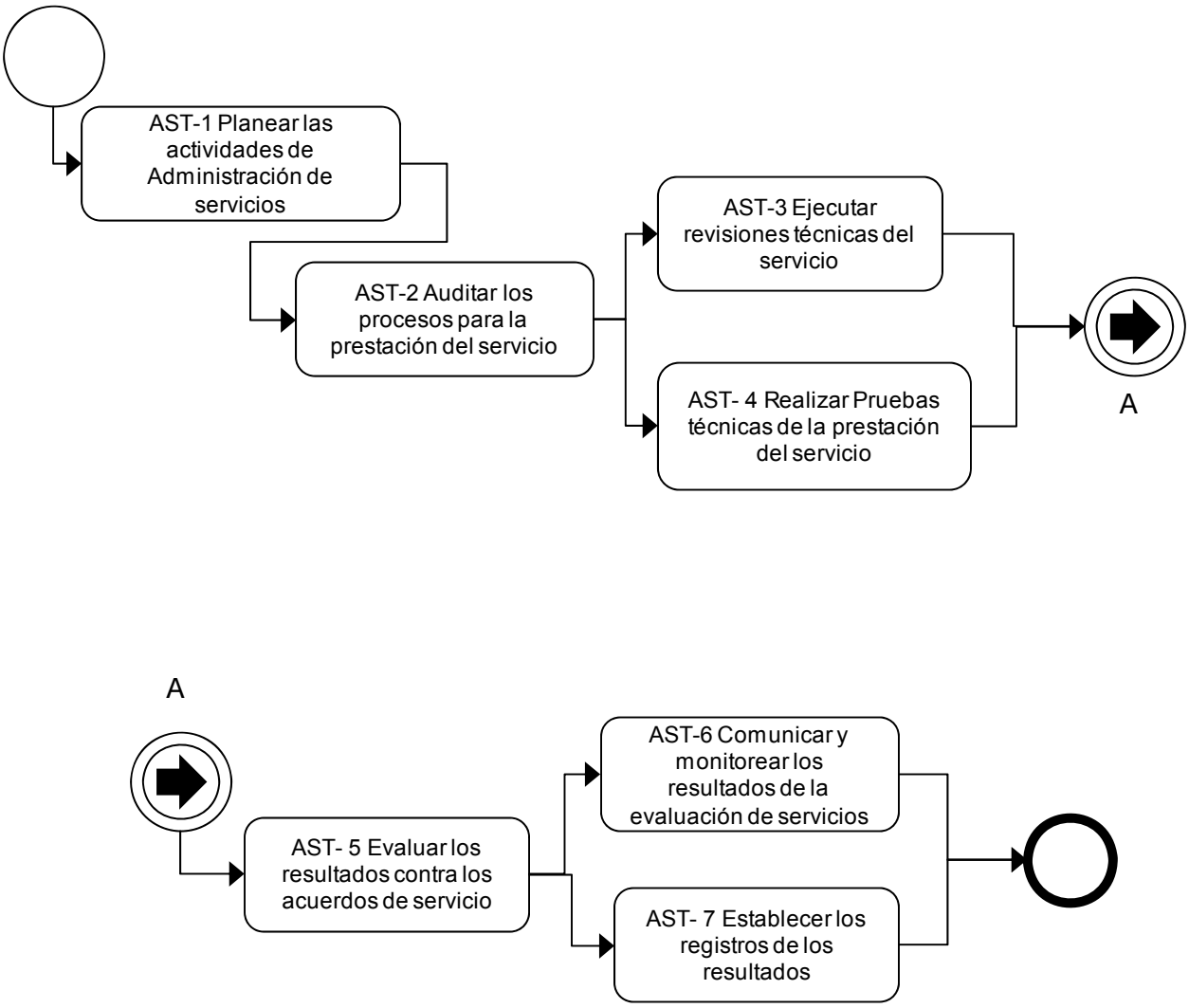


Diagrama de flujo de actividades



7.9.2.2.2. Descripción de las actividades del proceso

AST-1 Planear las actividades de administración de servicios

Descripción	Planear las actividades y recursos necesarios para ejecutar la administración de servicios a terceros.
Factores Críticos	1. Identificar las actividades de evaluación de servicios de terceros que deberán de ser ejecutadas para el aseguramiento del cumplimiento del contrato establecido. 2. Contemplar las revisiones técnicas del servicio, en las que se evalúan los componentes del sistema para la prestación del servicio a ser evaluados y asegurar que tienen la suficiente capacidad, escalabilidad y modularidad para la prestación del servicio. 3. Auditorias a procesos, en las que se evalúa el desarrollo del servicio conforme a los procesos establecidos 4. Pruebas técnicas para asegurar que los resultados de la prestación del servicio son consistentes con los acuerdos contractuales establecidos y a los reportes entregados. 5. Identificar los recursos necesarios para la ejecución de las actividades de evaluación de niveles de servicios. 6. Generar un cronograma en donde se gestionen las actividades y los recursos materiales y humanos necesarios para realizar las actividades de administración de servicios de terceros, para el aseguramiento del cumplimiento de SLA.
Relación de productos	• Plan de administración de servicios de terceros

AST-2 Auditar los procesos para la prestación del servicio

Descripción	Evaluar el apego a los procesos, durante el desarrollo del servicio, conforme a lo establecido en los acuerdos contractuales.
Factores Críticos	1. Establecer los procesos del proveedor y servicios que serán auditados. 2. Identificar los criterios a utilizar para le ejecución de la auditoria a los procesos y servicios, dichos criterios deberán contemplar: • Procesos establecidos a evaluar. • Requerimientos técnicos y operativos del servicio. • Acuerdos contractuales establecidos. 3. Evaluar objetivamente los procesos y productos; revisando los procesos ejecutados en la prestación del servicio contra las descripciones técnicas y operativas aplicables de los procesos; así como los productos desarrollados contra las características técnicas definidas para los mismos. 4. Las actividades y los productos resultantes conforme a los lineamientos establecidos en los procesos. 5. Registrar los hallazgos o desviaciones identificadas con respecto al cumplimiento de los procesos. 6. Comunicar al proveedor y al responsable de la administración del contrato, las no conformidades o desviaciones identificadas. 7. Establecer los planes de acción correspondientes a la solución de los hallazgos o desviaciones detectadas. 8. Dar seguimiento a la ejecución de los planes de acción definidos por el proveedor y asegurar el cierre de los hallazgos o desviaciones resultantes. 9. Establecer registros de los resultados de las auditorias y del resultado de las actividades de monitoreo ejecutadas.

Relación de productos	• Reporte de no conformidades de auditoría

AST-3 Ejecutar revisiones técnicas del servicio

Descripción	Seleccionar componentes del servicio para evaluar los aspectos técnicos y operativos establecidos para desarrollo del servicio, con el objetivo de asegurar que el servicio cuente con la funcionalidad y las capacidades necesarias para cubrir con los requerimientos establecidos en el contrato
Factores Críticos	1. Identificar los componentes del servicio a ser revisados. 2. Establecer los criterios para ejecutar las revisiones técnicas. • Para el establecimiento de los criterios a seguir en las revisiones técnicas, se tienen que tomar en cuenta los requerimientos técnicos y operativos del servicio, requerimientos contractuales y niveles de servicio establecidos en el contrato. • Estos criterios deben tener como objetivo la revisión de los componentes definidos para la prestación del servicio. 3. Establecer y mantener las condiciones y el ambiente requerido para la ejecución de las revisiones técnicas a la prestación del servicio. 4. Registrar los resultados de las revisiones desarrolladas al (los) componente(s) del servicio.
Relación de productos	• Reporte de revisiones técnicas

AST- 4 Realizar pruebas técnicas de la prestación del servicio

Descripción	Asegurar que los servicios seleccionados cumplen con los requerimientos.
Factores Críticos	1. Definir los servicios y procesos a ser probados, conforme a lo establecido en el contrato. 2. Definir los SLA que regirán las pruebas operativas de equipo y sistema a ejecutar y los criterios aplicables conforme a los requerimientos técnicos y operativos del servicio y requerimientos contractuales definidos. 3. Establecer los procedimientos a ejecutar para evaluar los.SLA 4. Establecer los ambientes requeridos para la ejecución de las pruebas. 5. Establecer los recursos, así como las características técnicas para la ejecución de las pruebas. 6. Asegurar que se tienen los recursos financieros materiales humanos, y otros como el ambiente, necesarios para la ejecución de las pruebas. 7. Ejecutar las pruebas conforme a los procesos y criterios definidos para este efecto. 8. Establecer un registro de los resultados obtenidos de las pruebas. 9. Analizar la información resultante de las pruebas y evaluarlas conforme a los acuerdos contractuales de servicio establecidos.
Relación de productos	• Reporte de pruebas de la prestación del servicio suministrado por terceros

AST- 5 Evaluar los resultados contra los acuerdos de servicio

Descripción	Revisar los resultados de las auditorias y revisiones de la ejecución de los servicios contra los niveles de servicio establecidos contractualmente.
Factores Críticos	1. Colectar los reportes y la información relacionada para evaluar el desempeño de los servicios del proveedor dentro de los requerimientos funcionales y de capacidad ofertados. 2. Evaluar los resultados obtenidos con respecto a lo establecido en los acuerdos contractuales; esta evaluación deberá de conducirse tomando en cuenta: o Requerimientos funcionales y operativos del servicio. o Requerimientos contractuales.

	o Niveles de servicio establecidos. 3. Registrar los resultados obtenidos de la medición del desempeño y compararlos con lo establecido en los acuerdos contractuales.
Relación de productos	• Reporte de Niveles de servicio suministrado por terceros.

AST-6 Comunicar y monitorear los resultados de la evaluación de servicios

Descripción	Dar a conocer los resultados de la evaluación del servicio para establecer los planes de acción para alinear las actividades de prestación de dicho servicio, conforme a los acuerdos contractuales establecidos.
Factores Críticos	1. Recopilar y consolidar los resultados de las actividades de administración de servicios suministrados por terceros. 2. Comunicar los resultados de la evaluación, conforme a los medios establecidos; esta comunicación deberá de darse a través de métodos formales y hacerse del conocimiento de todos los involucrados relevantes. 3. Registrar los acuerdos contractuales a los que se compromete el proveedor, para lograr mejorar los niveles de servicio establecidos y cumplir con lo definido en el contrato de servicio. 4. Establecer las fechas compromiso para el cumplimiento de los acuerdos contractuales establecidos. 5. Monitorear el cumplimiento de los acuerdos contractuales establecidos para el cumplimiento de los niveles de servicio y corregir las desviaciones identificadas.
Relación de productos	• Planes de Mejora de Servicio suministrado por terceros.

AST- 7 Establecer los registros de los resultados

Descripción	Recopilar los resultados de las evaluaciones de niveles de servicio suministrado por terceros.
Factores Críticos	1. Recopilar y consolidar los resultados de las evaluaciones realizadas a los niveles de servicio, los compromisos y el cumplimiento de los acuerdos establecidos. 2. Proveer la información necesaria a la administración para la gestión del contrato de servicios. 3. Proveer información de los resultados de cumplimiento de acuerdos contractuales del servicio de los proveedores.
Relación de productos	• Reporte de Niveles de servicio suministrado por terceros. • Planes de mejora de Servicio suministrado por terceros.

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.9.2.2.3. Descripción de roles

Rol	Descripción
Proveedor	Es el responsable de prestar un servicio de acuerdo a un contrato establecido, el cual deberá establecer los lineamientos que regirán la prestación del servicio de acuerdo a los requerimientos técnicos y operativos del cliente y los niveles de cumplimiento del contrato de referencia.

Auditor	Responsable de evaluar las actividades y productos de trabajo desarrollados de los procesos, verificando su apego a los lineamientos establecidos, conforme a lo definido en el contrato de servicios.
Revisor	Responsable de realizar la evaluación técnica y operativa de los componentes del sistema desarrollado para la prestación del servicio. Es su responsabilidad asegurar que el componente evaluado, cumple con todas las características técnicas para poder realizar la prestación del servicio, conforme a los requerimientos establecidos contractualmente.
Responsable de la prestación de servicios	Es el responsable de coordinar las actividades y recursos necesarios para realizar los trabajos de auditoría y revisiones técnicas de los componentes del sistema para la prestación del servicio y de esta prestación con respecto a los lineamientos establecidos de manera contractual. Dentro de sus responsabilidades se encuentra la planeación de las actividades antes referidas, el establecimiento de los criterios correspondientes, así como la comunicación y recopilación los resultados de la evaluación de los SLA.
Asegurador de calidad	Es el responsable de ejecutar las pruebas al sistema, equipos y procesos que lo conforman, establecidos para la prestación del servicio, así como realizar la evaluación de los niveles de servicio correspondientes, de acuerdo a los criterios contractuales establecidos, así como comunicar, registrar, consolidar y dar seguimiento a las acciones correctivas que serán registradas para efectuar la toma de decisiones que permita la mejora continua de la prestación del servicio referido.
Áreas usuarias	La dependencia o entidad, las personas y subprocesos productivos, a los que se les deberá cubrir sus necesidades operativas con él o los servicios suministrados, y que son los beneficiados de la prestación del servicio

7.9.2.2.4. Descripción de productos

Producto	Descripción
Plan de Administración de servicios de terceros.	En este producto de trabajo se describen las actividades a realizar para monitorear las actividades de revisión y auditoria a la prestación del servicio, así como los recursos necesarios para ejecutar las actividades y su distribución con base en los siguientes puntos: • En este documento se establece el calendario y las responsabilidades establecidas para la ejecución de las revisiones. • Se deberán de registrar los criterios de evaluación y de revisión para los productos y servicios suministrados por terceros. • Se mencionan procesos a ser auditados. • Se relacionan productos / servicios a ser revisados técnicamente. • Se describen procedimientos para ejecutar las revisiones técnicas de la prestación del servicio.
Reporte de no conformidades de auditoría	En este documento se registran las desviaciones o no conformidades detectadas, respecto a las actividades realizadas, cotejadas contra lo establecido en los procesos y considera: • Desviaciones detectadas.

Producto	Descripción
	• Proceso/producto o servicio no cumplido. • Plan de acción. • Fecha compromiso. • Responsable de aplicación de plan de acción. • Responsable de la ejecución de la auditoria. • Seguimiento al cierre de las no conformidades. • Estatus de las no conformidades.
Reporte de revisiones técnicas	En este producto resultante de la revisión técnica, el cual emite el revisor, se registra lo siguiente: • Criterios utilizados para las revisiones técnicas a los componentes y proceso del servicio. • Información del componente/ proceso revisado. • Desviaciones o no conformidades identificadas. • Repercusiones en los acuerdos contractuales establecidos. • Acciones de corrección recomendadas por el revisor. • Planes de acción propuestos. • Acciones inmediatas.
Reporte de pruebas de la prestación del servicio	En este producto se mantiene el registro de los resultados de las pruebas para evaluar el cumplimiento de los acuerdos contractuales del servicio, en el se debe considerar lo siguiente: • Objetivo de las pruebas. • Ambiente requerido y utilizado para la ejecución de las pruebas. • Recursos involucrados para le ejecución de las pruebas. • Procedimientos de evaluación. • Escenarios probados. • SLA establecidos a ser comprobados. • SLA resultantes. • Desviaciones o no conformidades identificadas. • Estatus de las pruebas.
Reporte de Niveles de servicio suministrado por terceros	Documento en el que se recopilan los resultados de las evaluaciones del cumplimiento de los SLA suministrados por terceros • SLA establecidos. • SLA obtenidos. • Criterios utilizados. • Desviaciones o no conformidades detectadas • Planes de acción propuestos. • Estatus de las desviaciones o no conformidades.
Planes de mejora de servicio suministrados por terceros	Documento en donde el proveedor define los compromisos que asume con respecto al incumplimiento de los SLA y las no conformidades detectadas, en el cual se describen las acciones correctivas a aplicar para dar cumplimiento a los acuerdos contractuales establecidos. • Desviación o no conformidad. • Plan de acción. • Responsable. • Fecha compromiso.

7.9.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Niveles de servicio	Disminuir las desviaciones en el nivel de servicio	Medir los niveles de servicio recibidos contra contratados	Eficiencia	De gestión	nivel de servicio recibido / nivel de servicio contratado	Lo definirá la UTIC	
Observaciones en auditorias de la prestación de servicios	Reducir las observaciones en auditorias	Identificar las observaciones realizadas en auditorias a los servicios	Eficiencia	De gestión	Número de observaciones en auditorias a los servicios	Lo definirá la UTIC	

7.9.2.4 Reglas del proceso

1.1	Las revisiones técnicas y auditorías se deben ejecutar con el objetivo de identificar el cumplimiento con los requerimientos técnicos y operativos del servicio, requerimientos contractuales, SLA, , procedimientos y prácticas en el desarrollo del servicio suministrado, conforme a los niveles y lineamientos establecidos para este efecto en el contrato correspondiente.
1.2	Los resultados de las revisiones y auditorias, así como las fechas compromiso, deben comunicarse al órgano de control responsable de la adquisición, para ejecutar las acciones que correspondan de acuerdo a lo establecido en la adquisición o contratación del servicio correspondiente.
1.3	En el contrato con terceros deben quedar asentados los procesos del proveedor que serán auditados y los criterios aplicables.
1.4	Las actividades de seguimiento al cierre de las no conformidades detectadas, deben ejecutarse formalmente y su resultado debe informarse a los involucrados.
1.5	Se desarrollarán actividades de verificación a los servicios, de acuerdo a los SLA establecidos de manera planificada ó imprevista, conforme a las necesidades de la dependencia o entidad.
1.6	Cualquier cambio a los SLA prestado por terceros, debe evaluarse y acordarse por las partes involucradas, con objeto de preparar la resolución correspondiente y así proceder con la solicitud de cambio a las condiciones originales del servicio, la cual deberá justificar cualquier afectación a los criterios de evaluación establecidos por los auditores y revisores. La solicitud referida debe hacerse del conocimiento del prestador del servicio, administrador y áreas usuarias, mediante los medios formales u oficiales.
1.7	En las revisiones y auditorías deben considerarse los aspectos de seguridad para que el servicio proporcionado por terceros y el intercambio de información entre éstos y la dependencia o entidad aseguren los requerimientos de seguridad que deben ser cumplidos.

7.9.2.5 Documentación soporte del proceso

No aplica

7.9.3. Administración de niveles de servicio

7.9.3.1. Objetivos del proceso

General.-

Definir, comunicar y cumplir con los niveles de servicio comprometidos.

Específicos.

1. Asegurar que se definan los SLA, OLA y UC para los servicios existentes en el catálogo de servicios.
2. Asegurar que los SLA, OLA y UC permitan cumplir con los estándares de servicio de la dependencia o entidad.
3. Asegurar la existencia de compromisos SLA, OLA y UC medibles y acordes a la capacidad tecnológica instalada.
4. Asegurar que la UTIC, usuarios y proveedores del servicio de TIC conozcan los niveles de servicio que serán entregados.
5. Asegurar que se cumplan los niveles de servicio definidos.

7.9.3.2 Descripción del proceso

7.9.3.2.1 Mapa general del proceso

Diagrama de flujo de información

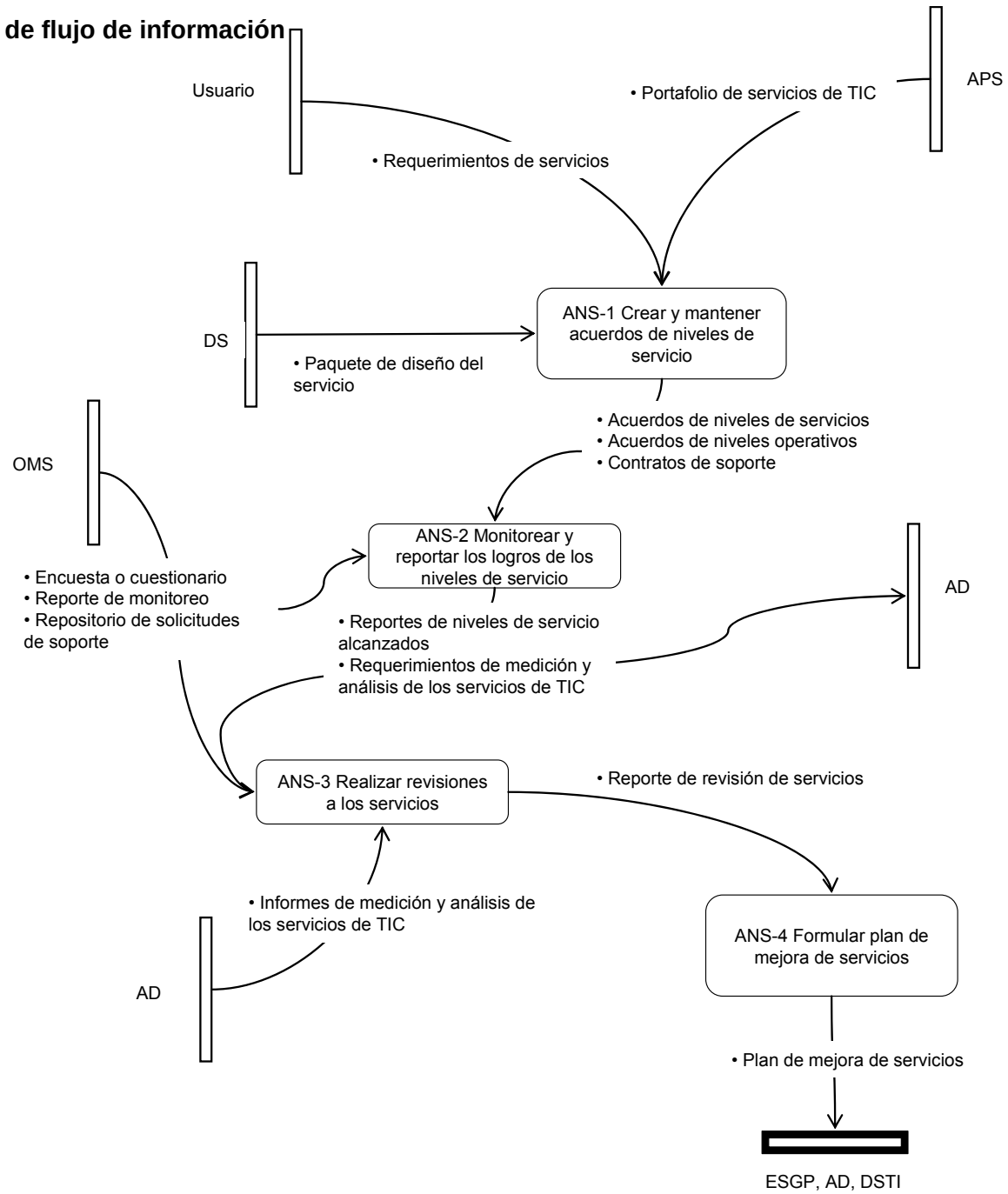
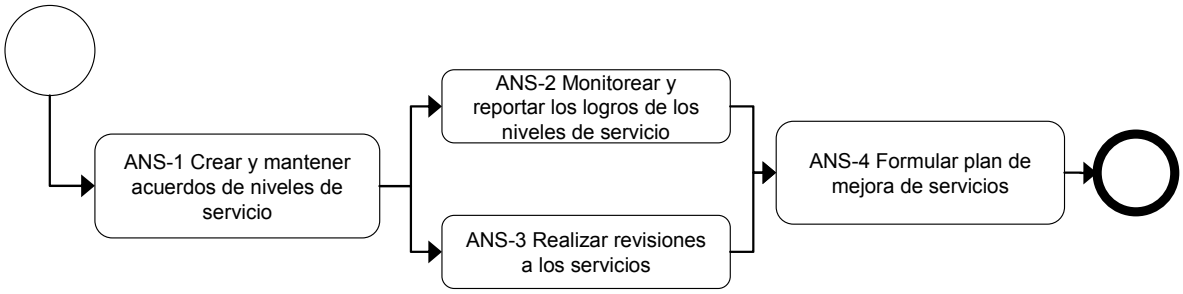


Diagrama de flujo de actividades



7.9.3.2.2 Descripción de las actividades del proceso

ANS-1 Crear y mantener acuerdos de niveles de servicio

Descripción	Definir los SLA basados en el catálogo de servicios de las TIC acordes a los requerimientos de la operación y las necesidades de los usuarios de cada uno de los servicios definidos
Factores Críticos	1. Alinear los SLA a los objetivos estratégicos de la dependencia o entidad y a la capacidad de entrega de servicio y los planes de disponibilidad y operación. 2. Disponer de una relación de los componentes de los costos de los servicios para su entrega, la cual puede ser interna, externa o una combinación. 3. Incluir una descripción de los servicios y tiempos de respuesta en la documentación de los SLA. 4. Asegurar que todos los SLA puedan ser monitoreados y medidos. 5. Acordar los SLA con todos los interesados incluyendo al usuario antes que el contenido pueda ser aprobado. 6. Actualizar y mantener los SLA, de acuerdo a las necesidades de la dependencia o entidad bajo un control de cambios. 7. Establecer los OLA con los proveedores de servicio internos y UR con los proveedores de servicio externos, para asegurar apropiadamente el logro de los SLA establecidos con el usuario.
Relación De productos	• Acuerdos de niveles de servicios • Acuerdos de niveles operativos • Contratos de soporte

ANS-2 Monitorear y reportar los logros de los niveles de servicio

Descripción	Elaborar reportes de resultados sobre el grado de cumplimiento de los SLA, esta actividad sigue las directrices del proceso de Administración del Desempeño de TIC.
Factores Críticos	1. Analizar los SLA para determinar las necesidades de métricas basándose en los indicadores de SLA. Incluir retroalimentación de los clientes y/o usuarios. • Especificar los procedimientos de recolección y almacenamiento así como el procedimiento de análisis. • Determinar los reportes e informes que serán usados para comunicar los resultados. • Recolectar y revisar los datos de medición. • Elaborar informes de medición y análisis.
Relación de productos	• Reportes de niveles de servicio alcanzados • Requerimientos de medición y análisis de los servicios de TIC

ANS-3 Realizar revisiones a los servicios

Descripción	Utilizar los reportes de logro de niveles de servicio para identificar y revelar áreas de oportunidad actual o potencial entre los niveles de servicios entregados y los requeridos.
Factores Críticos	1. Revisar y comparar los SLA y los resultados actuales de entrega de servicio, en sesiones formales de revisión. 2. Definir penalizaciones y establecer responsabilidades como consecuencia del no cumplimiento de los niveles de servicio (de ser apropiado). 3. Recopilar y considerar los hallazgos y tendencias identificados en el análisis, al momento de definir los dos tipos de acciones: reevaluación de actuales niveles de servicio y mantenimiento de los niveles de servicio.
Relación de productos	• Reporte de revisión de servicios

ANS-4 Formular plan de mejora de servicios

Descripción	Recomendar mejoras a los SLA consecuencia de las insatisfacciones del cliente o no cumplimiento de acuerdos establecidos.
Factores Críticos	1. Establecer el plan de mejora de servicios, considerando lo siguiente: • La evaluación de los resultados de los niveles de servicio, la retroalimentación de los usuarios y las unidades de entrega de servicio son parte de las entradas para la formulación del plan de mejora de servicios. • Las mejoras pueden tener foco en modificar los objetivos de los servicios, considerando ajustes a la entrega, monitoreo y al mismo SLA. • Antes de finalizar el plan de mejora, es necesario recopilar más retroalimentación de parte de las áreas técnicas y especialistas y esta debe convertirse en parte del plan con el fin de alinear las acciones con las capacidades de la operación. 2. Monitorear y mantener de forma regular y formal el plan de mejora de servicios.
Relación de productos	• Plan de mejora de servicios

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.9.3.2.3 Descripción de roles

Rol	Descripción
Gestor de niveles de servicios	Asegurar que los niveles de servicio sean identificados, acordados y documentados en SLA, así como monitorear y revisar con el cliente el desempeño alcanzado por el servicio entregado.
Proveedor	Es el responsable de prestar un servicio de acuerdo a un contrato establecido, el cual deberá establecer los lineamientos que regirán la prestación del servicio de acuerdo a los requerimientos técnicos y operativos del cliente y los niveles de cumplimiento del contrato de referencia.

Auditor	Responsable de evaluar las actividades y productos de trabajo desarrollados de los procesos, verificando su apego a los lineamientos establecidos, conforme a lo definido en el contrato de servicios.
Revisor	Responsable de realizar la evaluación técnica y operativa de los componentes del sistema desarrollado para la prestación del servicio. Es su responsabilidad asegurar que el componente evaluado, cumple con todas las características técnicas para poder realizar la prestación del servicio, conforme a los requerimientos establecidos contractualmente.
Asegurador de calidad	Es el responsable de ejecutar las pruebas al sistema, equipos y procesos que lo conforman, establecidos para la prestación del servicio, así como realizar la evaluación de los niveles de servicio correspondientes, de acuerdo a los criterios contractuales establecidos, así como comunicar, registrar, consolidar y dar seguimiento a las acciones correctivas que serán registradas para efectuar la toma de decisiones que permita la mejora continua de la prestación del servicio referido.
Áreas usuarias	Las personas, organizaciones y subprocesos productivos, a los cuales deben cubrirse sus necesidades operativas con el o los servicios suministrados y que son los beneficiados con la prestación del servicio.

7.9.3.2.4 Descripción de productos

Producto	Descripción
Acuerdo de niveles de servicio **SLA**	Es conveniente estructurar los SLA más complejos en diversos documentos de tal forma que cada grupo involucrado reciba exclusivamente la información correspondiente al nivel en que se integra, ya sea en el lado del usuario como del proveedor. La elaboración de un SLA requiere tomar en cuenta aspectos no tecnológicos, entre los que se encuentran, la naturaleza de la dependencia o entidad, aspectos organizativos del proveedor y usuario así como aspectos culturales locales. Algunos puntos que deben de ser considerados en este documento son: a) En un lenguaje no técnico, o cuando menos comprensible para el usuario, todos los detalles del servicio brindado. b) El horario en que se proveerá el servicio. c) Los costos asociados o valor del servicio. d) El dueño y el usuario del servicio.
Acuerdos de Niveles Operativos **OLA**	Documentos de carácter interno de la propia dependencia o entidad que determinen los procesos y procedimiento necesarios para ofrecer los niveles de servicio acordados con los usuarios. Por su naturaleza, involucra detalles sobre la prestación del servicio que deben ser “cajas negras” para el usuario, pero que resultan imprescindibles a la dependencia o entidad para el cumplimiento de los SLA. Algunos puntos que deben ser considerados en este documento son: a) Las responsabilidades y compromisos de los diferentes departamentos de la

Producto	Descripción
	dependencia o entidad en la prestación del servicio brindado. b) Proceso y procedimientos internos para la entrega del servicio.
Contratos de soporte **UC**	Determinan las responsabilidades de los proveedores externos en el proceso de prestación de servicios, en los que se deben representar compromisos claros y perfectamente delimitados. Pueden considerarse como una extensión "externa" de los OLA en el sentido de que persiguen el mismo fin como lo es organizar los procesos y procedimientos necesarios para la correcta provisión del servicio. Algunos puntos que deben de ser considerados en este documento son: a) Los objetivos que se requiere satisfacer para el cumplimiento de los SLA b) Condiciones y penalizaciones asociadas a la entrega del servicio.
Plan de mejora del servicio **SIP**	Plan formal de implementación de mejora de servicios y procesos de las TIC. que es utilizado para gestionar y dar seguimiento a las iniciativas que son consecuencia de la mejora continua del servicio. Las mejoras se derivan de iniciativas internas identificadas por el proveedor de servicio, por ejemplo mejora de procesos o mejor utilización de recursos, iniciativas que requieren cooperación del usuario del servicio, o que algún SLA ya no sea adecuado a las necesidades iniciales del usuario. Es el documento base para negociar la renovación del SLA con el usuario y debe constituir un documento de referencia para la gestión de otros procesos de las TIC como la administración de cambios. Algunos puntos que deben de ser considerados en este documento son: a) Las medidas correctivas a fallas detectadas en los niveles de servicio. b) Las propuestas de mejora basadas en el avance de la tecnología. c) Los responsables y tiempos comprometidos de implementación de las acciones.
Requerimientos de medición y análisis de los servicios de TIC	Necesidades de información para la evaluación del desempeño de los servicios de TIC. Incluye la documentación de las métricas y análisis que se requieren para evaluar el logro a las metas de servicio establecidas en los SLA
Reporte de niveles de servicio alcanzado	Informe acerca del desempeño actual y grado de cumplimiento a las metas y niveles de servicio acordados
Reporte de revisión de servicios	Reporte resultado de la revisión a los niveles de servicio, incluyendo las oportunidades de mejora detectadas y las no conformidades

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.9.3.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Niveles de servicio	Disminuir las desviaciones en el nivel de servicio	Medir los niveles de servicio recibidos contra los acordados	Eficacia	Eficiencia operativa	Nivel de servicio recibido / Nivel de servicio acordado	El Titular de la UTIC	Mensual

7.9.3.4	Reglas del proceso
1.1	La UTIC a través del proceso de administración de niveles de servicio deberá establecer niveles de servicio que correspondan al portafolio de servicios que provee por medio de las soluciones tecnológicas que libera a producción.
1.2	El titular de la UTIC deberá designar un responsable del proceso de Administración de niveles de servicio.
1.3	El responsable del proceso de administración de niveles de servicio deberá asegurar que los niveles de servicio se encuentran alineados a los objetivos de servicio de TIC de la dependencia o entidad.
1.4	El responsable del proceso de administración de niveles de servicio deberá definir procedimientos para medir y reportar el desempeño de los niveles de servicio.
1.5	El responsable del proceso de administración de niveles de servicio deberá definir un programa de mejora continua de los servicios internos y externos.
1.6	El responsable del proceso de administración de niveles de servicio deberá asegurar que en la definición de los niveles de servicio se incluyan niveles de servicio soportados en situaciones de contingencia.
1.7	Para comprometer niveles de servicio con los usuarios de red, colaboración y de las soluciones tecnológicas que proporcionan a los usuarios internos y finales, el responsable del proceso de Administración de niveles de servicio deberá instrumentar los mecanismos para establecer los niveles operacionales de servicio entre los diversos servicios técnicos asociados a infraestructura de TIC, de tal manera que cuente con los indicadores necesarios.
1.8	El responsable del proceso de administración de niveles de servicio deberá instrumentar metodologías y herramientas que aseguren la mejora en la administración de los servicios proporcionados.

7.9.3.5	Documentación soporte del proceso
	No aplica

7.9.4 Administración de la seguridad de la información

7.9.4.1 Objetivos del proceso

General.-

Garantizar la confidencialidad, integridad y disponibilidad de la información mediante el establecimiento de un sistema de gestión de seguridad de la información “SGSI” de acuerdo a las mejores prácticas internacionales

Específicos.-

1. Asegurar que se establezca un sistema de gestión de seguridad de la información en la dependencia o entidades.
2. Asegurar que la información sea accesible o revelada solo para quienes estén facultados.
3. Asegurar que la información sea exacta y esté completa y protegida.

7.9.4.2 Descripción del proceso

7.9.4.2.1 Mapa general del proceso

Diagrama de flujo de información

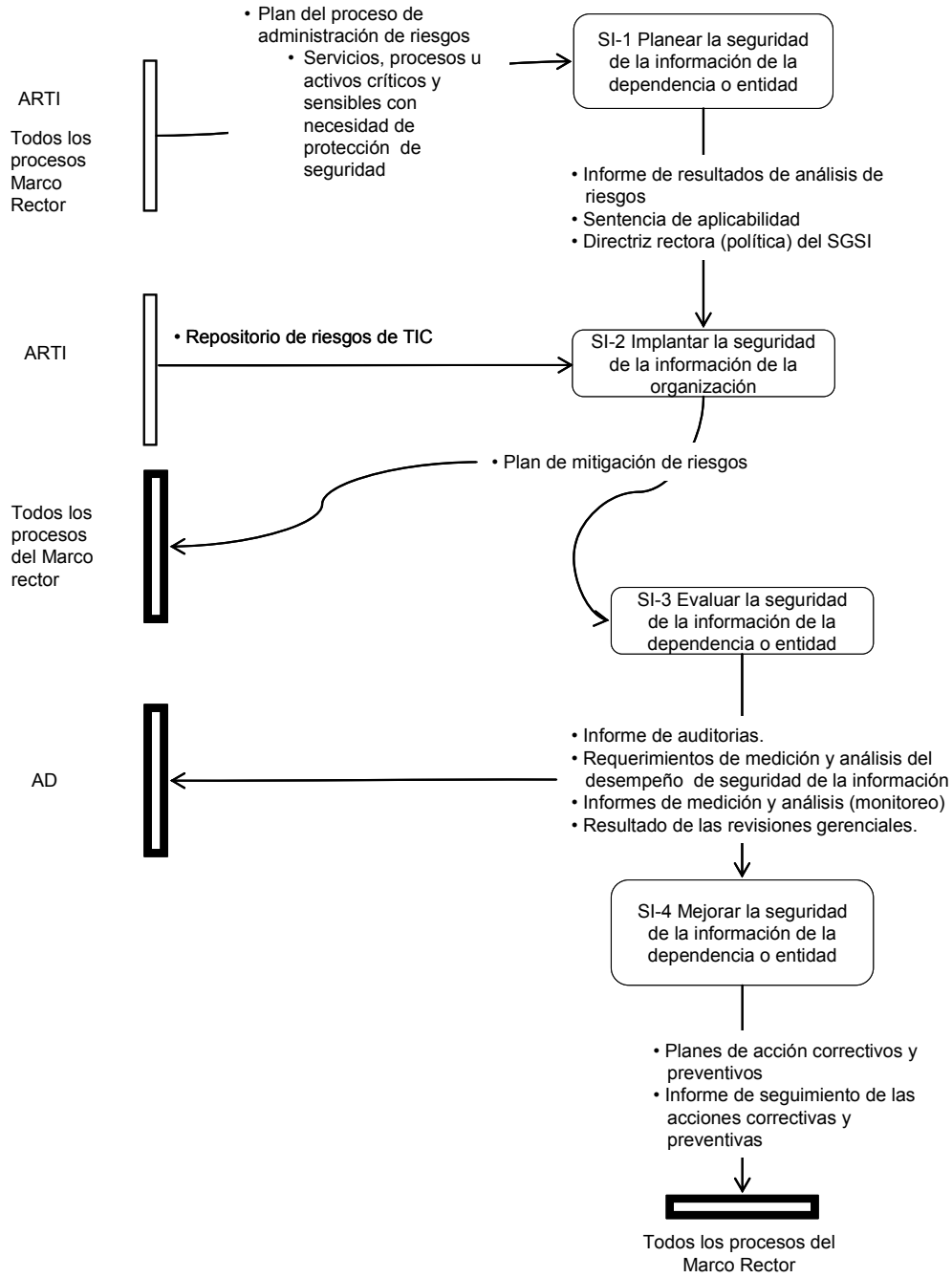
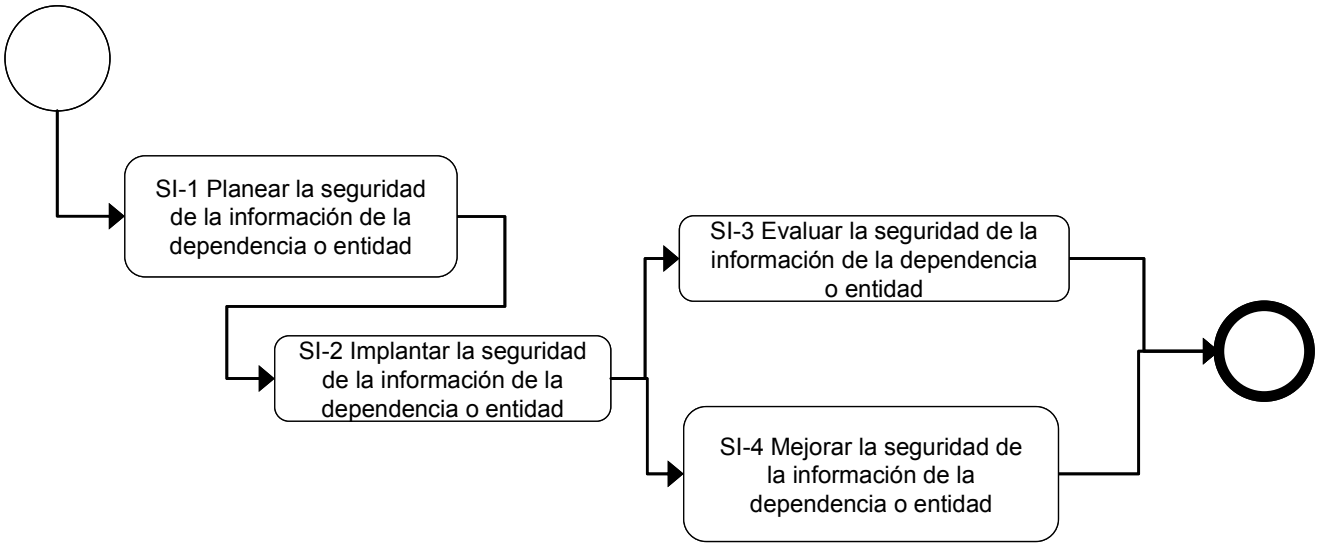


Diagrama de flujo de actividades



7.9.4.2.2 Descripción de las prácticas clave del proceso

ASI-1 Planear la seguridad de la información de la dependencia o entidad

Descripción	Definir los objetivos y directrices de seguridad de la información basadas en un entendimiento de los riesgos y requerimientos de seguridad de la dependencia o entidad
Factores Críticos	1. Declarar el alcance del SGSI el cual aclare los límites de protección desde la perspectiva de áreas, procesos o activos de la dependencia o entidad incluyendo la justificación de lo excluido en el alcance. 2. Realizar un diagnóstico de los requerimientos de la seguridad de la información de la dependencia o entidad a través de la realización de un análisis de riesgos de seguridad de la información. 3. Documentar una SoA donde se listen los controles de seguridad necesarios para mitigar los riesgos identificados. 4. Documentar una directriz rectora del SGSI que refleje las necesidades de seguridad percibidas por los mandos medios y superiores.
Relación de Productos	• Informe de resultados del análisis de riesgos • Enunciados de aplicabilidad • Directriz rectora del SGSI

ASI-2 Implantar la seguridad de la información de la dependencia o entidad

Descripción	Asegurar que los controles, procesos y procedimientos del SGSI sean implementados de manera que se cumpla con los requerimientos de seguridad regulatorios, contractuales y para mitigar los riesgos identificados.
Factores Críticos	1. Documentar un plan de mitigación de riegos que contenga las estrategias de corto, mediano y largo plazo para tratar y mitigar los riesgos de seguridad de la información identificados. 2. Implementar los controles de seguridad identificados y documentados en la SoA.
Relación de Productos	• Plan de mitigación de riesgos

ASI-3 Evaluar la seguridad de la información de la dependencia o entidad

Descripción	Evaluar y medir el desempeño de los procesos en cumplimiento con la política, y objetivos definidos en el SGSI.
Factores Críticos	1. Realizar auditorías internas/externas de seguridad para verificar la eficiencia y eficacia de los controles implementados y validar el cumplimiento de la Directriz rectora de seguridad. 2. Revisar si las métricas establecidas para evaluar los controles utilizados y determinar si fueron eficaz y eficientemente implementados, son las adecuadas y están proporcionando la información requerida. 3. Efectuar monitoreo de la seguridad de la información para validar intentos exitosos y no exitosos de violaciones e incidentes de seguridad. 4. Llevar a cabo revisiones gerenciales.

Relación de Productos	• Informe de auditorías • Requerimientos de medición y análisis del desempeño de seguridad de la información • Informes de medición y análisis (monitoreo) • Resultado de las revisiones gerenciales

ASI-4 Mejorar la seguridad de la información de la dependencia o entidad

Descripción	Mejorar la seguridad de la información a través de la aplicación de las acciones preventivas y correctivas basadas en los resultados de auditorías realizadas por los servidores públicos designados o por terceros contratados para tal fin con el propósito de lograr la mejora continua del SGSI.
Factores Críticos	1. Documentar los planes de acción correctiva y preventiva con la finalidad de minimizar las brechas de seguridad identificadas. 2. Implantar los planes de acción correctiva y preventiva.
Relación de Productos	• Planes de acción correctivos y preventivos • Informe de seguimiento de las acciones correctivas y preventivas

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.9.4.2.3 Descripción de roles

Rol	Descripción
Grupo de trabajo de seguridad de la información y continuidad de servicios de TIC	Responsable de llevar a cabo las revisiones gerenciales con el fin de aprobar las iniciativas que promuevan la mejora continúa de la seguridad de la información.
Oficial de seguridad de la información	Responsable de implementar controles de seguridad en su ámbito de competencia y orientar a otras áreas de la dependencia o entidad en la adecuada implementación de los controles de seguridad.
Auditores de seguridad	Responsables de llevar a cabo las auditorias (internas o externas) de seguridad de la información para garantizar el cumplimiento de la Directriz rectora de seguridad.
Dueños o propietarios de la información	Responsables de asegurar que la información que esté bajo su área o ámbito de control esté adecuadamente protegida.

7.9.4.2.4 Descripción de productos

Producto	Descripción
Informe de resultados de análisis de riesgos	Documenta las necesidades y requerimientos de seguridad estratégicos de la dependencia o entidad, los requerimientos de seguridad de las entidades regulatorias y los riesgos de seguridad a los que se encuentra expuesta la información sensible de la dependencia o entidad, describe al menos los siguientes aspectos:

	a) Activo b) Controles actualmente implementados c) Vulnerabilidades d) Amenazas e) Riesgos f) Impactos g) Controles a implementar
Enunciado de Aplicabilidad (SoA)	Documenta los objetivos de control y controles que son relevantes y aplicables al SGSI de la dependencia o entidad, describe al menos los siguientes aspectos: a) Objetivos de control y controles seleccionados b) Razones para la selección c) Objetivos de control y controles actualmente implementados d) Exclusión de cualquier objetivo de control o control que este en ISO 27002 y la justificación de la exclusión
Directriz rectora del Sistema de Gestión de Seguridad de la Información (SGSI)	Denominada también Política del SGSI, documenta los valores y las necesidades de seguridad percibidas por los mandos medios y superiores de la dependencia o entidad sobre la seguridad de la información, para que la información como un activo valioso de la dependencia o entidad, tenga el nivel de seguridad requerido por la dependencia o entidad, describe al menos los siguientes aspectos: a) Las justificaciones de la dependencia o entidad para proteger la información b) Propósito de la Directriz rectora c) Alcance de aplicabilidad d) Alineación a los objetivos estratégicos de negocio e) Toma en cuenta requerimientos de negocio, legales y contractuales f) Asegurará que existan los roles y responsabilidades para asegurar la aplicación y cumplimiento de la Directriz rectora g) Las consecuencias en caso de incumplimiento de la Directriz rectora h) Exige que exista un marco metodológico para la gestión de riesgos i) Un apartado donde asegure que la Directriz rectora sea dada a conocer a todo el personal de la dependencia o entidad j) Un apartado donde asegure su revisión periódica k) Un apartado donde asegure que se realicen revisiones del cumplimiento de la Directriz rectora l) Define acciones y consecuencias aplicables por su no cumplimiento
Plan de mitigación de riesgos	Documenta la información relativa a la planeación estratégica de seguridad de la información de una dependencia o entidad, describe al menos los siguientes aspectos: i) Descripción de la dependencia o entidad, marco regulatorio y funciones

	sustantivas j) Análisis del ambiente externo e interno con relación a la seguridad de la información k) Misión y visión de la dependencia o entidad l) Inventario de iniciativas de seguridad m) Portafolio de proyectos de seguridad n) Presupuesto de seguridad o) Priorización de iniciativas y proyectos p) Mecanismos de comunicación q) Mecanismos de seguimiento y control
Resultado de las revisiones gerenciales	Documenta diversos aspectos relacionados con la mejora de la seguridad en la dependencia o entidad, describe al menos pero no limitado a los siguientes aspectos: e) Mejora de la efectividad de la administración de la seguridad de la información en la dependencia o entidad f) Actualización de la evaluación de riesgos y plan de administración de riesgos g) Requerimientos de recursos h) Revisión del desempeño de las métricas de seguridad i) Modificación de procedimientos y controles, conforme se requiera para responder a eventos externos o internos que puedan impactar la seguridad de la información, incluyendo cambios en: • Requerimientos de negocio • Requerimientos de seguridad de la información • Requerimientos de los procesos sustantivos de la dependencia o entidad con un efecto en los requerimientos de la dependencia o entidad existentes • Ambiente regulatorio y legal • Obligaciones contractuales • Niveles de riesgo de seguridad y/o criterios de aceptación de acuerdo a los niveles y umbrales de riesgo de la dependencia o entidad
Requerimientos de medición y análisis del desempeño de seguridad de la información	Describe de manera cuantitativa cómo una dependencia o entidad a través del uso de métricas de seguridad de la información, identifica la idoneidad de la eficiencia y eficacia de los controles de seguridad implementados, describe al menos pero no limitado a los siguientes aspectos: a) Objetivo de la medición b) Métricas obtenidas por los mandos medios y superiores involucrados c) Entidad a ser medida

	d) Responsable de obtención de la métrica e) Frecuencia f) Objetivo de control y control asociado
Informes de medición y análisis (monitoreo)	Documenta información relativa a los accesos a las soluciones tecnológicas y aplicaciones críticas de la dependencia o entidad. Algunos de los reportes que pueden ser generados se enuncian a continuación: a) Intentos de acceso exitosos y fallidos a las soluciones tecnológicas y aplicaciones críticos de la dependencia o entidad b) Eventos e incidentes de seguridad asociados a los accesos exitosos y fallidos c) Actividad de los administradores de sistemas y aplicaciones d) Resumen de revisión de bitácoras de eventos
Planes de acción correctivas y preventivas	Documenta soluciones de causa raíz a implantar con el fin de mitigar brechas de seguridad identificadas en la etapa de revisión, a continuación se enuncian algunos aspectos: h) Descripción del incumplimiento i) Riesgo que genera j) Impacto a la dependencia o entidad k) Planteamiento de la solución de raíz l) Fecha de implantación de la solución (acción correctiva o preventiva) m) Responsable de la implantación n) Responsable de verificar su cumplimiento
Informe de seguimiento de las acciones correctivas y preventivas	Documenta la confirmación de la implementación de las acciones correctivas y preventivas, a continuación se enuncian algunos aspectos: a) Hallazgo asociado b) Plan de acción correctiva o preventiva c) Se cumplió o no d) Nueva fecha compromiso (solo si no se cumplió) e) Comentarios
Informe de auditorías	Documenta las inconformidades mayores y menores con relación al cumplimiento de la política de seguridad, describe al menos pero no limitado a los siguientes aspectos: a) Objetivo b) Alcance c) Exclusiones d) Hallazgos e) No conformidades (mayores y menores) f) Oportunidades de mejora

	g) Oportunidades de mejora (recomendaciones) h) Equipo auditor y auditado i) Localización de los sitios auditados j) Conclusiones

7.9.4.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Incidentes de seguridad	Reducir la vulnerabilidad	Medir la cantidad de incidentes de seguridad	Eficacia	De gestión	Número de incidentes de seguridad	A ser definido por el titular de la UTIC	Trimestral
Vulnerabilidad	Reducir la vulnerabilidad	Medir la proporción de intentos exitosos y no exitosos	Eficacia	De gestión	(Intentos exitosos/ Total de intentos)*100	A ser definido por el titular de la UTIC	Trimestral
Observaciones en auditorias de la seguridad	Reducir las observaciones en auditorias de seguridad	Identificar las observaciones realizadas en auditorias	Eficacia	De gestión	Número de observaciones en auditorias a la seguridad	A ser definido por el titular de la UTIC	Trimestral

7.9.4.4 Reglas del proceso

1.1	La UTIC deberá promover y asegurar que los mandos superiores de la dependencia o entidad apoyen las iniciativas y estrategias de seguridad a través de: • Proveer de los recursos suficientes para administrar la seguridad de la información • La definición y autorización de una Directriz rectora de seguridad • Establecer roles, funciones y responsabilidades de seguridad • Asegurar que se establezcan objetivos y planes de seguridad de la información • Comunicar a la dependencia o entidad la importancia del cumplimiento de la política • Asegurar que se realizan auditorias de seguridad para el mejoramiento de la protección de la información • Realizar revisiones de mandos medios de la seguridad llevada a cabo por grupos directivos conformados por personal responsable de diferentes áreas de la dependencia o entidad
1.2	La UTIC deberá iniciar y controlar la implementación de la seguridad de la información dentro de la dependencia o entidad a través de la implantación de un SGSI.
1.3	El personal de la UTIC designado como responsable de la seguridad de los recursos de TIC deberá certificar que el personal externo que utilice, administre o desarrolle sobre infraestructura y servicios informáticos al prestar sus servicios de manera permanente o temporal cumplan las disposiciones de este manual.

1.4	La UTIC deberá seguir las mejores prácticas para establecer el SGSI de manera que se generen o adecuen los procedimientos en estricto apego a las mejores prácticas y factores críticos descritos en este proceso, para la administración de éste y del SGSI.

Reglas aplicables a procedimientos que rige el proceso.
Ordenadas por objetivo de control según ISO 27001

A.5 Política de Seguridad

1. Todo el personal de la dependencia o entidad está obligado a operar en un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información, de acuerdo a las disposiciones de la presente norma.

2. Las reglas de operación de los procedimientos de seguridad de la información, deberán revisarse y actualizarse cuando cambien las condiciones de las soluciones tecnológicas o cuando cambie la legislación aplicable.

A.6 Organización de la Seguridad de la Información

1. El personal de la UTIC designado como responsable de la seguridad de los recursos de TIC deberá certificar que el personal externo que tenga cualquier tipo de contacto con recursos de TIC institucionales cumplan las disposiciones de este manual.

2. Las dependencias o entidades no otorgarán el derecho de intercambio de información con entidades externas en caso de que los controles identificados en éstas últimas por la UTIC no cumplan satisfactoriamente con la prevención de los riesgos de integridad y confidencialidad de la información de la dependencia o entidad.

3. Se permitirá al personal de los proveedores de servicios el acceso a los puntos de red únicamente con la autorización del responsable asignado al proyecto o proceso al que pertenezca el personal de que se trate. El personal de los proveedores de servicios deberá portar en todo momento una identificación oficial y de la empresa que representa al momento de acceder a las áreas físicas de TIC, independientemente de la razón de su acceso.

4. El personal de la UTIC con la atribución será el responsable de autorizar los accesos del personal de los proveedores de servicios y del registro correspondiente.

A.7 Administración de activos

1. Los propietarios de la información designados son los responsables de la custodia y buen uso de la información que se almacena, procesa y transmite dentro de las dependencias o entidades.

2. Los usuarios de TIC y en particular los propietarios de la información almacenada en medios electrónicos definirán los requerimientos de seguridad de su información y de sus sistemas de información así como cuando se requiera compartir información con entidades externas.

3. La UTIC en conjunto con los usuarios responsables de la información clasificada como confidencial o reservada determinarán los esquemas de seguridad que se aplicarán para mantener la confidencialidad, disponibilidad e integridad de la misma.

4. La información clasificada según la LFTAIPG como confidencial o reservada deberá residir en territorio nacional. Los servicios de almacenamiento y administración de la misma deberán realizarse de igual manera dentro del territorio nacional.

5. Las UTIC y sus usuarios deberán apegarse al esquema de la APF para la clasificación de la información a fin de definir los niveles de protección de la misma.

6. La información que se genera, almacena, procesa y transmite por medios electrónicos será almacenada, resguardada y administrada por la UTIC en función de la clasificación otorgada por la los usuarios propietarios o responsables de la misma.

7. Las UTIC y los usuarios que apliquen deberán observar que cada medio de almacenamiento desmontable o removible, que contenga información clasificada como confidencial, reservada o pública, sea etiquetado por el responsable del mismo de acuerdo a la normatividad vigente aplicable.

8. La UTIC en conjunto con los usuarios de la información en medios electrónicos clasificada como confidencial o reservada determinarán los esquemas de seguridad que se aplicarán para mantener la confidencialidad, disponibilidad e integridad de la misma.

A.8 Seguridad de los recursos humanos

1. El usuario debe dar cumplimiento a todas las disposiciones que le sean comunicadas por la UTIC tanto relacionadas con el uso de las soluciones tecnológicas, los servicios de tecnologías de la información así como de equipos PC, cuáles son sus responsabilidades por lo que deben firmar, bajo protesta de decir verdad, que conoce las disposiciones, el inventario de software y hardware instalado en su equipo así como el conocimiento de la Ley Federal de derechos de autor.

2. Las UTIC deberán fijar los mecanismos de seguridad de la información para el personal en aquellos cargos en dónde se maneje información de tipo confidencial para la dependencia o entidad, debiendo considerar en ellas la protección de la información y el uso correcto de los recursos que se asignen al personal para el desempeño de sus funciones.

A.9 Seguridad física y ambiental

1. La UTIC deberá implementar mecanismos de control de acceso a las instalaciones del centro de datos, centro de telecomunicaciones y todas aquellas instalaciones en las que se encuentre equipo de almacenamiento, procesamiento y/o transmisión de información la UTIC debe contar con los mecanismos de control que permitan asegurar que el personal que ingrese a sus instalaciones cuente con la autorización correspondiente.

2. El personal de la UTIC que administre la infraestructura de TIC debe llevar un registro del personal que accede a las áreas en las que se encuentran elementos de la infraestructura de TIC incluyendo. En el registro de acceso deberá incluir los datos relevantes del personal que accede de manera que sea posible su fácil localización asimismo deberá incluirse el motivo por el cual accedió al área correspondiente.

3. El personal de la UTIC que administre la infraestructura de TIC debe mantener actualizadas las listas de autorización de acceso a personal contratado de proveedores de servicios de terceros y llevar el control de accesos presenciales y remotos indicados en el punto anterior.

4. Se permitirá al personal de los proveedores de servicios el acceso a los puntos de red siempre bajo la supervisión del responsable de las instalaciones físicas de TIC incluyendo el acceso a los nodos de la red de la dependencia o entidad. El personal de los proveedores de servicios deberá presentar una identificación oficial y de la empresa que representa al momento de acceder a las áreas físicas de infraestructura de TIC independientemente de la razón de su acceso.

5. El personal de la UTIC debe instalar la infraestructura de TIC en ambientes físicos adecuados para su operación, administración, monitoreo y control de acceso, para minimizar las riesgos, amenazas y condiciones de operación fuera de las especificaciones indicadas por los proveedores correspondientes.

6. Los usuarios de equipos de computo deben asegurase de utilizar y mantener cerradas las chapas de seguridad de éstos equipos. Para el caso de equipos portátiles deberán asegurarse de colocar el cable y candado de seguridad correspondiente.

7. Vía la mesa de servicios, el personal responsable de la seguridad de los recursos de TIC se asegurará de que el equipo que utilizará la conexión a la red institucional se encuentre libre de virus informático así como necesario para mantener la seguridad de éste y de la propia red institucional.

8. El personal de la UTIC que administre la infraestructura de TIC debe evaluar y certificar la seguridad de las instalaciones eléctricas, comunicaciones, sistemas contra incendios, de aire acondicionado y demás recursos, que garanticen las condiciones adecuadas de seguridad para la operación de la infraestructura de TIC de la dependencia o entidad.

9. Las UTIC deberán asegurar que los nodos de comunicaciones WAN deberán estar ubicados en lugares cerrados y resguardados dentro de los edificios institucionales.

A.10 Gestión de las comunicaciones y operaciones

1. Vía la mesa de servicios, el personal responsable de la seguridad de los recursos de TIC se asegurará de que el equipo que utilizará la conexión a la red institucional se encuentre libre de virus informático así como necesario para mantener la seguridad de éste y de la propia red institucional.

2. Los usuarios y el área de soporte técnico de la UTIC de forma periódica (semestral, mensual, quincenal) deben realizar copias de seguridad de la información crítica que almacenen en su equipo.

1.37 El área de la UTIC designada como responsable de la ejecución de los respaldos deben ser efectuados en estricto apego al plan de respaldo de información, definido por las UR’s y aprobado por la UTIC.

3. La UTIC deberá solicitar por escrito a los usuarios responsables de los servicios las necesidades de respaldo tomando en cuenta, el tipo de información y las necesidades de operación, de los propios servicios.

4. El área de la UTIC designada como responsable deberá elaborar e informar a la UTIC el calendario de respaldos que será ejecutado, en base a las necesidades de los usuarios responsables de los servicios así como a las necesidades de las soluciones tecnológicas y del propio centro de datos de la UTIC.

5. El área de la UTIC designada como responsable del calendario de respaldos deberá conservar la evidencia del respaldo efectuado asimismo deberá garantizar la integridad de de la información.

6. El área de la UTIC designada como responsable deberá mantener los controles necesarios para conocer el estado de cada copia de respaldo y su ubicación.

7. El área de la UTIC designada como responsable deberá implantar procedimientos para preparar, almacenar y probar periódicamente la integridad de los respaldos y de toda la información necesaria para restaurar el respaldo a una operación normal.

8. El área de la UTIC designada como responsable deberá mantener una copia del software, soluciones tecnológicas, aplicativos, parámetros de configuración de ambientes, estructuras de datos y datos; anterior a la versión en operación.

10. El área de la UTIC designada como responsable deberá generar las copias de los respaldos necesarios y almacenarlos en inmuebles diferentes a fin de garantizar la recuperación de la operación en caso de ejecutase algún plan de contingencia.

11. El área de la UTIC designada como responsable deberá registrar en una bitácora de evidencia las recuperaciones realizadas, indicando al menos, número de solicitud de la restauración, dueño de la información, nombre del sistema, sección solicitada, número de serie del respaldo utilizado.

12. El área de la UTIC designada como responsable deberá atender solamente las solicitudes de restauración que se hayan efectuado por escrito, la solicitud deberá contener al menos: nombre y firma del propietario de la información, nombre del sistema del cual se desea recuperar la información, especificaciones de la información que se desea recuperar (periodo, clasificación, entre otros).

13. El área de la UTIC designada como responsable en conjunto con las UR propietarias de la información y/o las soluciones tecnológicas determinará la permanencia y la vigencia de la información respaldada.

14. El área de la UTIC designada como responsable deberá en conjunto con las UR propietaria de la información definir el mecanismo de eliminación de respaldos, específico por sistema o por tipo de información.

15. Los usuarios que requieran conectarse a la red Institucional utilizando equipo de cómputo de escritorio o portátil propio o Institucional, deberán obtener autorización de la UTIC vía la mesa de servicios, la cual será responsable de habilitar su conexión.

16. Los medios de almacenamiento que hayan contenido información con clasificación confidencial o reservada que vayan a salir de uso, deberán ser borrados mediante un medio que garantice la eliminación física de la información, si van a ser reutilizados o entregados a un tercero (reparación, préstamo) deberán ser borrados con anterioridad.

17. El personal de la UTIC que administre la infraestructura de TIC debe proteger los respaldos en los medios físicos de información del acceso a éstos de personal no autorizado.

18. Las UTIC deben asegurarse de implementar bitácoras de seguridad en las que queden

registrados todos los eventos realizados por cuentas con permisos especiales al menos: administrator, guest, root y system.

19. La UTIC deberá implementar un mecanismo de seguridad para que la bitácora electrónica de auditoria sólo pueda ser accedida por la cuenta de administración del responsable de seguridad del elemento de TIC que se trate, facultado por la UTIC.

20. La UTIC se debe definir e instrumentar un mecanismo de seguridad ante intentos de intrusión a la infraestructura de TIC incluyendo ataques externos vía Internet, extranet e inclusive intranet.

21. La UTIC debe implementar un mecanismo para mantenerse informado día a día de la existencia de actualizaciones de seguridad del software utilizado por la dependencia o entidad, de la aparición de nuevos virus informáticos que puedan atacar las soluciones tecnológicas y los equipos de los usuarios de la dependencia o entidad, con la finalidad de disminuir los riesgos o huecos de seguridad.

22 La UTIC debe implementar un mecanismo de difusión a nivel al institucional, para que, al encontrar una actualización de prevención de virus notifique de manera inmediata a las áreas responsables de la administración del software afectado, para que evalúe y en su caso aplique dicha actualización.

22 La UTIC al identificar la existencia de un virus informático no cubierto por los antivirus institucionales en operación en servidores y en equipos de los usuarios, notificará a la mesa de servicios de manera que a través de ésta se difundan las medidas necesarias a los usuarios y éstos se encuentren en posibilidad de protegerse hasta que la UTIC corrija la intrusión del virus y lo elimine.

23. La UTIC deberá instrumentar mecanismos de administración de los equipos de proceso y de comunicaciones que incluyan revisiones periódicas de las bitácoras de los elementos de la infraestructura de TIC para identificar si se han presentado intentos de ataques o de explotación de vulnerabilidades.

24. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas deberá habilitar el registro de los eventos de seguridad, relacionado con los accesos a las soluciones tecnológicas y las actividades realizadas por los usuarios.

A.11 Control de acceso

25. El personal de la UTIC que administre la infraestructura de TIC debe controlar el acceso presencial y remoto a los componentes de cada uno de los elementos de la infraestructura de TIC de la de la dependencia o entidad.

26. Las UTIC deberán implantar los mecanismos de seguridad para el acceso a los datos almacenados, que permitan contar con los principios de identidad, responsabilidad y rastreabilidad de los usuarios que los acceden en función del nivel de exposición y revelación de los mismos, de acuerdo al grado de criticidad.

27. Las UTIC deberán asegurar que las capacidades de los usuarios para acceder a datos están limitadas de acuerdo al perfil que corresponda a sus funciones, previa definición de las UR propietarias de los datos y de las soluciones tecnológicas que hacen uso de ellos

28. Las UTIC son las encargadas de implementar los mecanismos de seguridad necesarios para la asignación de los permisos de acceso a los usuarios, determinados por las UR responsables de la información.

29. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe instrumentar el registro de usuarios y la administración de la seguridad de las soluciones tecnológicas de información que son accedidos en forma local y/o remota a través de la red de comunicaciones.

30. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe instrumentar mecanismos para que se efectúe la personalización de las cuentas para las actividades de administración de servidores, bases de datos, servicios o sistemas Institucionales, así como para el monitoreo de las actividades realizadas por los usuarios.

31. La UTIC deberá instrumentar un mecanismo de seguridad para que, desde su creación, todo usuario tenga definido el ambiente de trabajo acorde a sus funciones y éste no deberá poder ser modificado por el usuario mismo, sino a través de una solicitud a la mesa de servicios.

32. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas deberá asegurar que la asignación de cuentas de usuario para cualquiera de los servicios y/o sistemas que operan dentro de la dependencia o entidad deberá identificar a un solo responsable de ésta.

33. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas indicará a los usuarios las características para la selección de una contraseña.

34. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas deberá identificar y autenticar claramente al usuario antes de asignarle una cuenta.

35. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas deberá eliminar cualquier cuenta de usuario del cual le sea notificado el cambio de situación laboral o baja definitiva de la Dependencia.

El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas o en su defecto las soluciones tecnológicas y aplicaciones designadas como sensibles o criticas deberán forzar el cambio de la contraseña de la cuenta de usuario en un periodo máximo de 60 días, la cual debe ser distinta, por lo menos, a las últimas 10 usadas por la misma cuenta de usuario.

36. Las contraseñas no deben ser mostradas en pantalla mientras son tecleadas, ni deben viajar por la red sin ser cifradas.

37. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas deberá facilitar a los usuarios del correo electrónico el cambio de contraseña cuando éstos lo estimen conveniente o de acuerdo en lo establecido en el lineamiento de cambio de contraseña por caducidad

38. Los usuarios deben verificar que su equipo de cómputo tenga configurado el protector de pantalla con contraseña, con la finalidad de evitar el acceso no autorizado a su información en caso

de retiro temporal.

39. Los usuarios están obligados a considerar que las cuentas y contraseñas asignadas son personales e intransferibles, las consecuencias jurídicas y/o administrativas de los actos ejecutados con las mismas son responsabilidad exclusiva del usuario dueño de la cuenta.

40. Los usuarios deben evitar la repetición de contraseñas al efectuar los cambios periódicos de las mismas.

41. Los usuarios deben cambiar su contraseña en caso de sospechar que alguien más la conoce.

42. Los usuarios deben evitar exponer o difundir su contraseña independientemente del medio en el cual sea almacenada.

43. En caso de utilizar hardware de seguridad, tales como generadores de contraseñas o tarjeta inteligente, los usuarios deben traerlos siempre consigo.

44. La UTIC facultará personal técnico para asegurar que todos los equipos de cómputo de escritorio y portátiles que se puedan conectar a la red Institucional de la dependencia o entidad cumplan con los siguientes controles de acceso: nombre de equipo que identifique al responsable del equipo y su ubicación; integración a un dominio; tener instalado el software de antivirus y el respectivo agente de actualización automática; estar actualizado a la ultima versión y parche del sistema operativo liberado por el proveedor; la usuario asignada no es la del administrador local del equipo.

45. La UTIC deberá implementar un mecanismo de seguridad en todos los elementos de comunicaciones para que todos los intentos de conexión hacia la infraestructura de TIC que soporta las aplicaciones o servicios institucionales pasen a través de un firewall.

46. La UTIC deberá implementar los mecanismos necesarios para el área de producción in sitio, y para el caso de accesos de manera remota deberá instrumentar el uso de software de cifrado de canal.

47. La UTIC deberá implementar un mecanismo de control para proveer del servicio de acceso remoto a la red Institucional, las soluciones tecnológicas , los servicios de red y colaboración así como la propia información sea otorgado únicamente a los funcionarios y a los proveedores que lo requieran derivado de sus funciones, atribuciones y/o los proyectos Institucionales en que se encuentren involucrados.

48. La UTIC deberá definir e implementar las herramientas de detección de intrusos y protección a vulnerabilidad alineadas a la infraestructura de TIC, sistemas de información y necesidades de servicios de red y colaboración de la dependencia o entidad.

49. El personal de la UTIC que administre la seguridad de la infraestructura de TIC debe limitar el acceso a los servidores; los sistemas operativos de éstos; las soluciones tecnológicas institucionales y las bases de datos, mediante la identificación del usuario, a través de su cuenta única y contraseña; la UTIC deberá llevar el control de perfil y privilegios de acceso por usuario.

50. Las UTIC deberán implementar en las soluciones tecnológicas y servicios que provee a los usuarios mensajes de ingreso a los usuarios en los cuales se le advierta que: el sistema y/o servicio

sólo podrá ser utilizado por personal autorizado, que las actividades realizadas son monitoreadas y rastreables así como también que cualquier intento de ingreso no autorizado será sancionado.

51. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas o en su defecto las soluciones tecnológicas y aplicaciones deberán bloquear el acceso a toda cuenta de usuario después de 3 intentos consecutivos fallidos de acceso en las soluciones tecnológicas o red.

52. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas o en su defecto las soluciones tecnológicas y aplicaciones designadas como sensibles o críticas deberán restringir el número de sesiones por usuario.

53. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas o en su defecto las soluciones tecnológicas y aplicaciones designadas como sensibles o criticas deberán bloquear cualquier cuenta de usuario la cual no se haya firmado en el sistema o la red después de 30 días.

54. El área de la UTIC designada como responsable de la asignación de cuentas de usuario y contraseñas o en su defecto las soluciones tecnológicas y aplicaciones designadas como sensibles o criticas deberá bloquear cualquier cuenta de usuario que no se utilice por un período de 15 días, si no hay causa justificada o previo aviso por el usuario vía la mesa de Ayuda.

55. La UTIC deberá implementar los mecanismos necesarios para identificar todos aquellos reportes de información que contengan datos Confidenciales o Reservados y limitar el acceso a éstos de acuerdo a las leyes y normatividad vigentes.

A.12 Adquisición, desarrollo y mantenimiento de información

1. Para la información que se almacene o viaje a través de las redes internas o externas correspondiente al nivel de clasificación confidencial o reservada la UTIC deberá asegurarse de que la información se encuentre cifrada: archivos de contraseñas y bases de datos.

2. La UTIC deberá implementar un mecanismo de control para que todo el personal responsable o poseedor de manuales, procedimientos, guías e instructivos de operación (en cualquier tipo de medio bien sea electrónico o papel) de los equipos de cómputo, telecomunicaciones y sistemas, controle y reporte el acceso y uso de los mismos, bajo su estricta responsabilidad.

A.13 Gestión de incidentes en la seguridad de la información.

1. Los usuarios que presencien o sospechen actos citados en la disposición anterior deberán notificarlo por escrito a su inmediato superior y el responsable del área de seguridad de la información.

2. El siniestro, extravío o robo de equipo de cómputo y/o periféricos deben ser reportados de forma inmediata por el usuario afectado (aquel que tiene bajo su resguardo el equipo siniestrado) al área administrativa correspondiente, para que se realicen las gestiones pertinentes

A.15 Cumplimiento

1. Los datos clasificados como Confidenciales o Reservados deberán tener fechas programadas de

eliminación y deberá destruirse la identificación del medio y cualquier marca de uso, esto en estricto apego a la normatividad vigente aplicable y con la evidencia correspondiente.

2. La información confidencial o reservada no necesaria deberá ser destruida, los listados deberán ser triturados y los desechos empacados antes de deshacerse de ellos, esto en estricto apego a la normatividad vigente aplicable y con la evidencia correspondiente.

3. En caso de inobservancia, y a fin de garantizar la integridad, confiabilidad y disponibilidad de la información de las dependencias o entidades, el personal responsable de la seguridad de los recursos de TIC tendrá la obligación de suspender de manera inmediata los servicios de TIC a él o los usuarios que hubieren infringido alguna de las disposiciones del presente manual.

4. Los intentos (exitosos o fallidos) para obtener acceso no autorizado a las soluciones tecnológicas e infraestructura, servicios o datos, revelación no autorizada de su información, interrupción o denegación no autorizada de sus servicios, el uso no autorizado de las soluciones tecnológicas e infraestructura para procesar, almacenar o transmitir datos, cambios a las características de sus sistemas de hardware, firmware o software sin conocimiento y la autorización correspondiente de los administradores del mismo o cualquier otra actividad que afecte a los intereses de la dependencia o entidad, serán sancionados con la aplicación de la reglamentación vigente y la legislación vigente aplicable, como lo es la Ley Federal de Responsabilidades de los Servidores Públicos y en su caso, la Ley Federal de Responsabilidad Patrimonial del Estado; sin que ello implique limitación alguna de la aplicación de cualquier ordenamiento que sancione tales conductas y conllevará a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal aplicables.

7.9.4.5	Documentación soporte del proceso

	No aplica

7.10. ADMINISTRACIÓN DE ACTIVOS

7.10.1. Administración de dominios tecnológicos

7.10.1.1. Objetivos del proceso

General.-

Planear e implementar arquitecturas tecnológicas robustas y efectivas para cada una de las agrupaciones lógicas denominadas dominios tecnológicos.

Específicos.-

1. Definir e instrumentar arquitecturas tecnológicas para cada dominio tecnológico.
2. Asegurar la existencia de un repositorio de conocimiento de los dominios tecnológicos, de acuerdo a los lineamientos del proceso de administración de conocimientos.
3. Proveer directrices para la administración de la operación y el mantenimiento de infraestructura.

7.10.1.2 Descripción del proceso

7.10.1.2.1 Mapa general del proceso

Diagrama de flujo de información

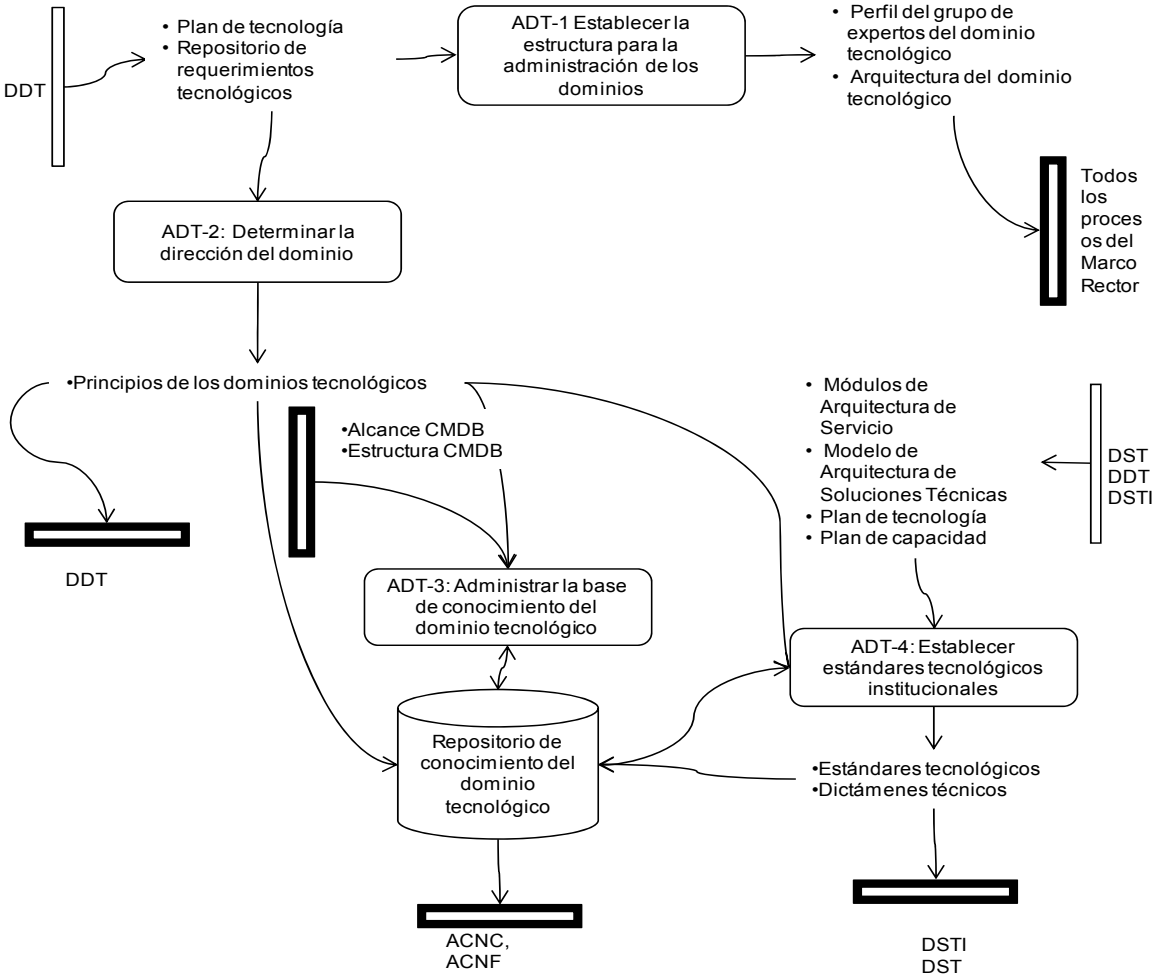
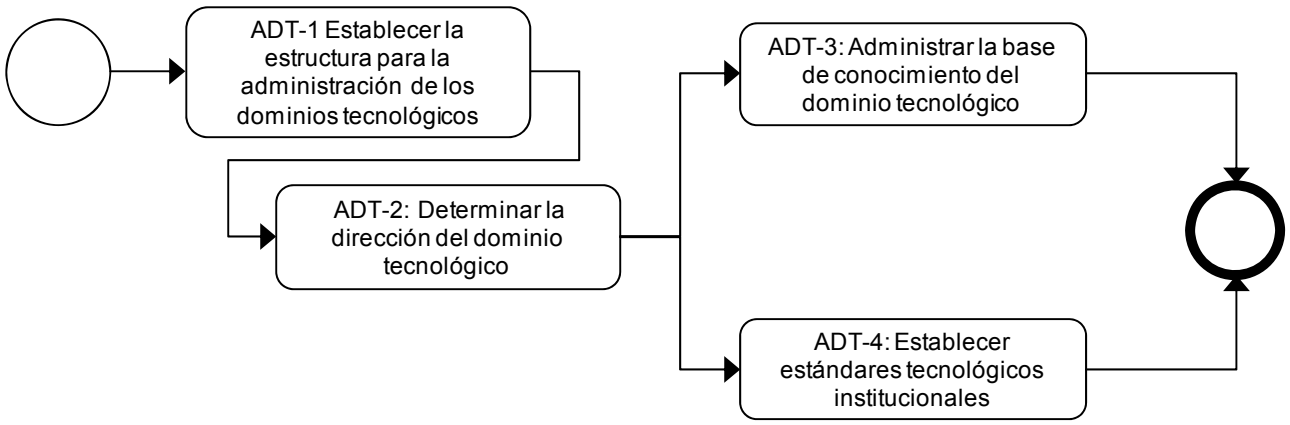


Diagrama de flujo de actividades.-



7.10.1.2.2 Descripción de las actividades del proceso

ADT-1: Establecer la estructura para la administración de los dominios tecnológicos

Descripción	Determinar las agrupaciones lógicas de tecnologías denominadas dominios con el propósito de facilitar su estudio, aplicación, la especificación de los servicios que aporta y la definición de los componentes de arquitectura.
Factores Críticos	1. Determinar los dominios tecnológicos que conformarán la arquitectura tecnológica. 2. Determinar las tecnologías que formarán parte del dominio tecnológico. 3. Determinar al grupo de expertos del dominio tecnológico. Definir y comunicar el alcance, objetivos, participantes, roles y responsabilidades del grupo de expertos. 4. Seleccionar al responsable del dominio tecnológico y comunicar a los involucrados la asignación. • El responsable del dominio tecnológico deberá participar en el grupo de trabajo de arquitectura tecnológica
Relación de Productos	• Perfil del grupo de expertos del dominio tecnológico • Arquitectura del dominio tecnológico

ADT-2: Determinar la dirección del dominio tecnológico

Descripción	Llevar los requerimientos tecnológicos y las directrices de la dependencia o entidad a la arquitectura tecnológica especificada en el Plan de Tecnología de manera que se obtenga un conjunto de principios rectores para el dominio tecnológico.
Factores Críticos	1. Traducir, en un conjunto de principios rectores para el dominio tecnológico, los requerimientos tecnológicos y las directrices de la dependencia o entidad para la arquitectura tecnológica especificada en el plan de tecnología. 2. Realizar regularmente un análisis de las fortalezas, oportunidades, debilidades y amenazas (FODA), de todos los activos críticos del dominio tecnológico. 3. Dar seguimiento a la evolución del mercado y a las tecnologías emergentes asociadas al dominio. 4. Identificar las tecnologías del dominio que puedan tener un impacto en el éxito de la dependencia o entidad. 5. Determinar la arquitectura para cada dominio consistente en un conjunto de principios, modelos, normas y estándares. 6. Participar en la actualización del plan de tecnología de la dependencia o entidad. 7. Participar en los consejos y grupos colegiados que se establezcan en la Administración Pública Federal para el dominio tecnológico, con el propósito de compartir experiencias y participar en la determinación de los estándares que se requieran a nivel de una arquitectura y que minimicen la incompatibilidad entre los recursos de infraestructura procurando la interoperabilidad de tecnologías a nivel de gobierno federal.

Relación de Productos	• Principios de los dominios tecnológicos

ADT-3: Administrar la base de conocimiento del dominio tecnológico

Descripción	Contar con la información que se necesita para dirigir, controlar y administrar un dominio tecnológico.
Factores Críticos	1. Definir y mantener actualizados los repositorios de conocimiento del dominio tecnológico. 2. Los repositorios de conocimiento de los dominios tecnológicos deberán ser administrados de acuerdo a lo establecido en el proceso de administración del conocimiento. 3. Se debe considerar en el diseño de estos repositorios los datos e información acerca de la infraestructura que se esté administrando en el sistema de administración de la configuración del proceso de administración de las configuraciones. 4. Para soportar los servicios de TIC y darle mantenimiento y operar la infraestructura tecnológica, se debe considerar en el diseño de estos repositorios los datos e información que identifican las habilidades y conocimiento requeridos asociados, al dominio tecnológico en cuestión inclusive, la información sobre cuáles recursos humanos cuentan con esas habilidades y conocimiento.
Relación de Productos	• Repositorio de conocimiento del dominio tecnológico

ADT-4: Establecer estándares tecnológicos Institucionales

Descripción	Elaborar, instrumentar y vigilar el cumplimento a políticas, lineamientos y estándares en materia de las tecnologías del dominio tecnológico. Brindar asesoría y proporcionar lineamientos sobre la selección de la tecnología. Impulsar mediante foros el uso de los estándares y las mejores prácticas en cuestión tecnológica con base a su importancia y riesgo, para la dependencia o entidad y en el cumplimiento a requerimientos externos.
Factores Críticos	1. Asegurar que los estándares tecnológicos institucionales son aprobados por el consejo de arquitectura de TIC y se comunican a lo largo de la dependencia o entidad mediante foros tecnológicos. 2. Asegurar que se establezca y mantenga una lista actualizada de proveedores y componentes tecnológicos conforme al plan de tecnología y los estándares tecnológicos. 3. Establecer un proceso para prevenir la adquisición de soluciones tecnológicas no conformes. 4. Dirigir la emisión de dictámenes técnicos asociados a los proyectos de TIC y el desarrollo de soluciones tecnológicas. 5. Revisar y actualizar periódicamente los estándares tecnológicos institucionales del dominio en conjunto con el plan de infraestructura tecnológica. 6. Alinear el plan de entrenamiento y capacitación, así como los requerimientos de

	contratación con los estándares tecnológicos. 7. Establecer como parte del proceso la estructura del plan de capacidad de conformidad con lo establecido en el proceso de determinación de la dirección tecnológica.
Relación de Productos	• Estándares tecnológicos • Dictámenes técnicos

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.10.1.2.3 Descripción de roles

Rol	Descripción
Grupo de expertos técnicos	Especialistas que cuentan con el conocimiento y experiencia en las tecnologías del dominio, quienes interactúan y comparten sus conocimientos y experiencias, y que participan en la definición y administración de la arquitectura del dominio tecnológico.
Responsable de dominio tecnológico	El responsable de establecer los principios tecnológicos de su dominio y elaborar en conjunto con los expertos, los modelos, normas y estándares necesarios para administrar los recursos de la UTIC pertenecientes a su dominio.

7.10.1.2.4 Descripción de productos

Producto	Descripción
Perfil del grupo de expertos del dominio tecnológico	Documento que contiene la estructura de los expertos que cuentan con el conocimiento y experiencia en las tecnologías que deberán integrarse.
Arquitectura de dominio tecnológico	Descripción lógica de los componentes del dominio. La siguiente es una lista inicial de dominios, misma que puede ser complementada dependiendo del tamaño de la operación de la dependencia o entidad. Por cada dominio tecnológico se sugiere determinar los servicios tecnológicos que sustenta: • **Comunicaciones.** Incluye la infraestructura de comunicación para el ambiente de cómputo distribuido y consiste en los elementos lógicos como estructura, topología, ancho de banda, administración, entre otros; los elementos de hardware como routers, cableado, LAN, entre otros; los servicios de transporte y los protocolos. • **Seguridad.** Define la infraestructura requerida para proteger la transmisión de información en la red y en los servidores centrales, así como los estándares institucionales de acceso a la información. • **Colaboración y Correo Electrónico.** Describe las reglas y comportamientos de las herramientas que soportan la interacción entre usuarios, así como las reglas de comportamientos de las actividades propias de la institución. • **Internet / intranet.** Explota la tecnología web para crear mecanismos de acceso a

Producto	Descripción
	aplicaciones universales e independientes de la plataforma. La arquitectura abarca seguridad, herramientas de desarrollo, máquinas de búsqueda y lógica de negocio. • **Cómputo Central.** Define los componentes de la infraestructura de procesamiento para aplicaciones de negocio centralizadas y ubicadas en bases de datos institucionales. Incluye la plataforma de hardware en servidores, los sistemas operativos que se ejecutan en esas plataformas, el ambiente de base de datos y las interfaces soportadas. • **Cómputo distribuido.** Define la infraestructura de ambientes de cómputo distribuido como UNIX y NT, incluye elementos de hardware y software. • **Cómputo de usuario final**. Está conformado por los elementos de hardware y software que integran y dan funcionalidad al usuario final. • **Aplicativo**. La arquitectura de aplicaciones establece cómo deben ser diseñadas y estructuradas, cómo deben cooperar y comunicarse, así como dónde deben residir. • **Datos y Data Warehouse.** Determina las estructuras lógicas, bases de datos y estándares para la explotación de la información estratégica.
Principios de los dominios tecnológicos	Directrices que conducen el uso y evolución del dominio tecnológico y que asociadas a un principio, se podría documentar como el nombre, la definición, el motivo de la elección, así como lo que implica para la dependencia o entidad el uso y la aplicación de este principio.
Repositorio de conocimiento del dominio	Repositorio con los datos e información que sustenta al conocimiento de un dominio, y que incluye el conjunto de principios, modelos, normas y estándares del dominio.
Estándares tecnológicos	Lineamientos que establecen disposiciones acerca del tipo y propiedades que deberán cumplir los componentes de un dominio tecnológico.
Dictámenes técnicos	Documento del resultado del análisis conforme a los estándares tecnológicos Institucionales de la arquitectura involucrada en un proyecto de tecnologías de la información y/o desarrollo o compra de una solución tecnológica.

7.10.1.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de Integridad de la Estructura del dominio	Incrementar el Grado de cumplimiento de la estructura (roles) del grupo de expertos de dominio	Indicador que sirve para identificar la suficiencia e Integridad de la estructura (roles) del grupo de expertos de dominio	Eficiencia	De gestión	(Número de responsables de dominio / Número de dominios tecnológicos determinados) x 100	Dirección de la dependencia o entidad	Anual

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de Actualización de los dominios tecnológicos	Establecer las vigencias de los principios de dominios tecnológicos mediante la actualización o ratificación de los mismos	Revisión de la actualización del plan de tecnología que incluya el grado de evolución de la Arquitectura tecnológica, los insumos requeridos para la actualización anual del FODA, y la evolución del mercado de tecnología	Eficiencia	De gestión	(Principios de dominio actualizados/número de dominios tecnológicos determinados) x 100	Dirección de TIC	Anual
Índice de actualización de los repositorios de conocimiento	Mantener el repositorio de conocimiento del dominio actualizado	Revisión de la administración y actualización de los repositorios de conocimiento de dominios tecnológicos	Eficiencia	De gestión	(Número de actualizaciones de(los) repositorio(s) de conocimiento / Número de demandas de actualización “aplicables”) x 100	Dirección de TIC	Anual
Índice de actualización de estándares tecnológicos	Establecer, someter a autorización y publicar los estándares de los dominios tecnológicos que soporten lo estipulado en el plan estratégico institucional y a los lineamientos establecidos en el proceso de dirección	Desarrollo o actualización de los estándares tecnológicos Institucionales	Eficiencia	De gestión	(Estándares tecnológicos Institucionales actualizados, autorizados y publicados / número de dominios tecnológicos determinados) x 100	Dirección de TIC	Anual

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
	tecnológica						
Porcentaje de aprobación de estándares tecnológicos	Determinar la alineación de proyectos de TIC en la emisión de dictámenes técnicos de proyectos	Medición del cumplimiento de los proyectos emitidos por el área usuaria vs. Los estándares de dominio tecnológico establecidos	Calidad	De gestión	(Dictámenes técnicos de cumplimiento de estándares de dominios tecnológicos emitidos / Dictámenes técnicos de cumplimiento de estándares de dominios tecnológicos solicitados) x 100	Dirección de TIC	Anual

7.10.1.4	Reglas del proceso
1.1	La administración de la Arquitectura tecnológica deberá estar sustentada en dominios tecnológicos.
1.2	Los responsables de los dominios tecnológicos deberán asegurar que la arquitectura de cada uno de los dominios tecnológicos sea diseñada en sustento y acorde al plan de tecnología elaborado en el proceso determinación de la dirección tecnológica.
1.3	El responsable de cada uno de los dominios tecnológicos deberá asegurarse que el dominio bajo su responsabilidad esté considerado en los planes de capacidad.
1.4.	El responsable de cada uno de los dominios tecnológicos deberá asegurarse que exista y se mantenga actualizado un inventario de los bienes (hardware y software) pertenecientes al dominio del cual es responsable.
1.5	Los responsables de los dominios tecnológicos deberán aprobar cualquier modificación que se solicite en la operación o uso de los bienes bajo su responsabilidad (hardware y software) con la finalidad de garantizar su correcto desempeño.
1.6	El responsable de cada uno de los dominios tecnológicos deberá aprobar la instalación y puesta en operación de las soluciones tecnológicas que entrarán a servicio y/o que tuvieron adecuaciones.
1.7	Los responsables de los dominios tecnológicos deberán asegurar que la operación y la infraestructura del dominio del cual son responsables se reflejen en los planes de contingencia.

	Reglas de aplicables a procedimientos regidos por el proceso
	El responsable del dominio tecnológico en el que se ubiquen los componentes de comunicaciones deberá establecer e implementar el sistema operativo a utilizar en los servidores de red así como mantenerlos con las últimas actualizaciones de seguridad y herramientas de administración y monitoreo incluyendo aquellas para evitar los accesos no autorizados.
	El responsable del dominio tecnológico en el que se ubiquen los componentes de comunicaciones deberá asegurar que todos los servidores de producción pertenezcan a los segmentos de red definidos de acuerdo a la arquitectura tecnológica establecida y seguridad establecidas.
	El responsable del dominio tecnológico en el que se ubiquen los componentes de comunicaciones deberá asegurar que las actividades relacionadas con la operación de la red interna en donde se

	encuentren ubicadas las estaciones de administración y monitoreo, deben ser independientes de la red de datos de las áreas usuarias.
	El responsable del dominio tecnológico en el que se ubiquen los componentes de comunicaciones deberá elaborar la planeación de la capacidad de la red WAN, de respaldo, LAN´s y sus componentes para asegurarse de contar con la disponibilidad y desempeño adecuados para satisfacer la demanda de los servicios en operación y planeados.
	Todos los equipos de comunicaciones alojados en el centro de cómputo, deberán contar con equipos de respaldo de energía eléctrica, a fin de proteger su integridad y evitar daños por variaciones de corriente eléctrica o interrupciones de energía eléctrica.
	En el caso de equipamiento nuevo se deberán seguir las indicaciones de utilización y mantenimiento del fabricante para no afectar las condiciones de garantía durante el tiempo de vigencia de la misma.
	El responsable del dominio tecnológico de Internet/Intranet deberá asegurar la instrumentación, operación y administración de los elementos de éste para la habilitación de los servicios de Internet, intranet así como los servicios asociados de los sitios Internet institucionales, sitios intranet, servicios de colaboración y acceso a sistemas de la dependencia o entidad incluyendo todos aquellos que servicios que se publiquen por estas vías.
	El responsable del dominio tecnológico de Internet/Intranet deberá definir, establecer y administrar la plataforma de operación de éstos servicios con el soporte y ayuda de las demás áreas involucradas de la UTIC.
	El responsable del dominio tecnológico de Internet/Intranet deberá asegurar la disponibilidad, adecuada operación y funcionalidad de los servicios descritos en el punto anterior.
	El responsable del dominio tecnológico de Internet/Intranet deberá establecer los mecanismos de vigilancia de las bitácoras de los servicios que operan en el dominio.
	El responsable del dominio tecnológico de Internet/Intranet deberá establecer conjuntamente con el responsable del dominio tecnológico de seguridad, todos aquellos mecanismos necesarios para mantener la integridad de la información.
	El responsable del dominio tecnológico de Internet/Intranet deberá determinar el estado de contingencia de los servicios, en caso de ser necesario, y será el único facultado para dirigir las acciones que se requieran previa aprobación de responsable del proceso de Administración de Riesgos de TIC.
	El responsable del dominio tecnológico de Internet/Intranet será el responsable de evaluar la contratación del servicio de Internet.
	El responsable del dominio tecnológico de seguridad deberá asegurar que todos los equipos de cómputo de usuario que se conecten a la red de datos tengan instalada una herramienta de antivirus, antispyware y las últimas actualizaciones del sistema operativo.
	El responsable del dominio tecnológico de cómputo central deberá asegurar que se instrumente un plan de contingencia en materia de TIC.
	El responsable del dominio tecnológico de cómputo central deberá asegurar que el plan de contingencia sea revisado y actualizado cada 6 meses como periodo mínimo.
	El responsable del dominio tecnológico de cómputo central deberá asegurar que los cambios en la operación y en la infraestructura del dominio se reflejen de inmediato en el plan de contingencia.

7.10.1.5	Documentación soporte del proceso

No aplica

7.10.2. Administración del conocimiento

7.10.2.1. Objetivos del proceso

General.-

Asegurar que los el personal de la UTIC pueda difundir y compartir información que genere conocimiento.

Específicos.-

1. Establecer y mantener actualizado un repositorio central de información que permita compartir información teórica de TIC, histórica de eventos, proyectos y lecciones aprendidas de la UTIC.
2. Asegurar la calidad de la información contenida en el repositorio central de información para que sea fuente de conocimiento.

7.10.2.2 Descripción del proceso

7.10.2.2.1 Mapa general del proceso

Diagrama de flujo de información

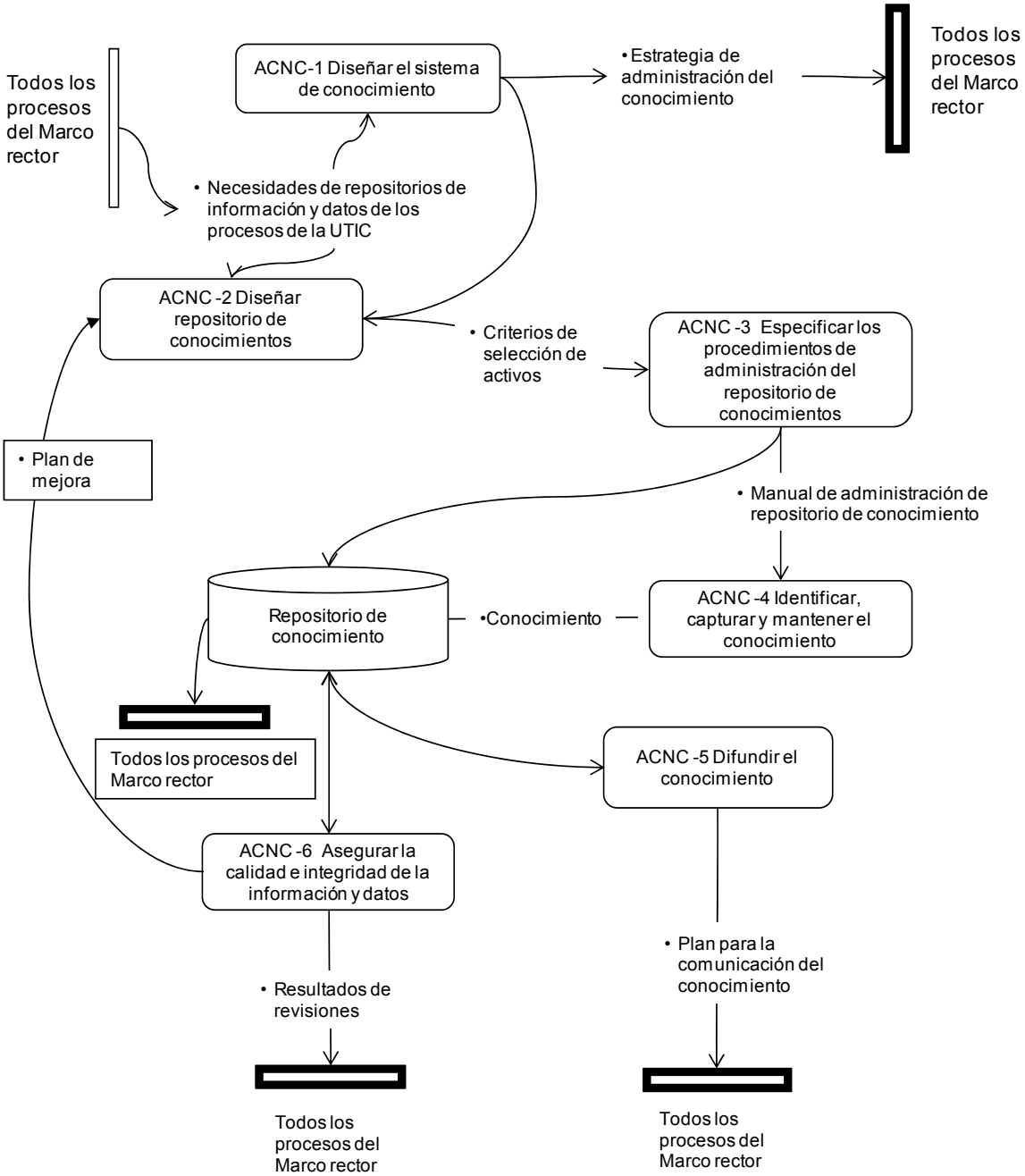
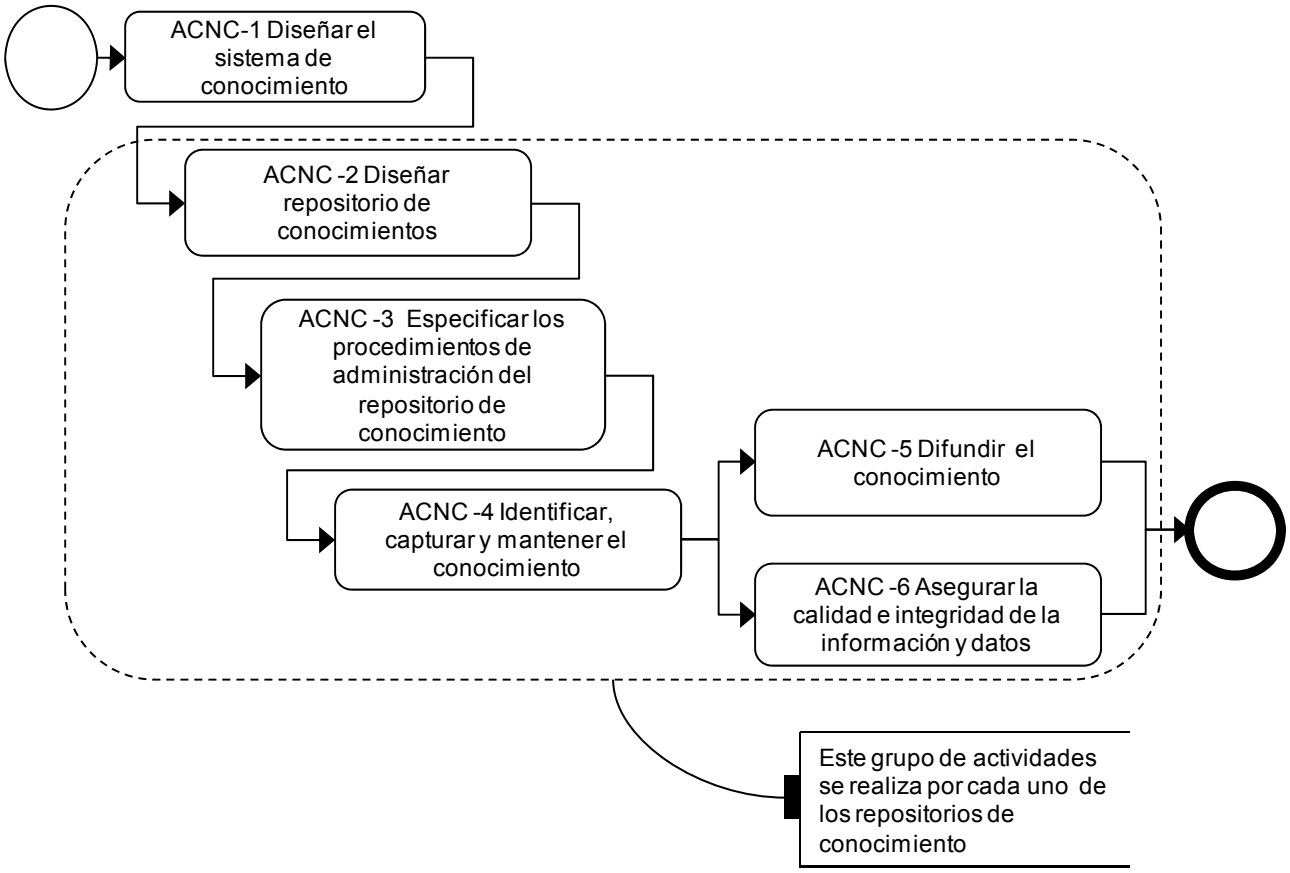


Diagrama de flujo de actividades.-



7.10.2.2.2. Descripción de actividades del proceso

ACNC-1 Diseñar el sistema de conocimiento

Descripción	Determinar una estrategia para la administración del conocimiento de la UTIC que dé respuesta a las necesidades de información de todos los involucrados en los procesos de la UTIC.
Factores Críticos	1. Determinar las directrices para la administración del conocimiento de la UTIC acorde con la estrategia de administración del conocimiento de la dependencia o entidad. 2. Comunicar las directrices para la administración del conocimiento de la UTIC en correspondencia con la estrategia de administración del conocimiento de la dependencia o entidad. 3. Diseñar la estrategia de administración del conocimiento de la UTIC con base a la identificación de las necesidades de información de todos los involucrados, incluyendo las perspectivas de procesos, proyectos, servicios y arquitectura tecnológica. 4. Diseñar la arquitectura lógica del sistema de conocimiento, incluyendo los subsistemas de conocimiento y la estructura de los repositorios de activos de conocimiento (datos e información). 5. Establecer los roles y responsabilidades sobre la administración de los repositorios de activos de conocimiento.
Relación de Productos	• Estrategia de administración del conocimiento

ACNC-2 Diseñar repositorio de conocimiento

Descripción	Definir cómo se identificarán los datos e información para el conocimiento de acuerdo a su tipo y configuración, para ser agrupados, clasificados y documentados de acuerdo a sus características propias, con el objetivo de asegurar que son administrables.
Factores Críticos	1. Definir y documentar criterios para seleccionar datos e información de acuerdo a su tipo. En el diseño de los repositorios de conocimientos se debe considerar entre otros: • Qué conocimiento es necesario basado en las decisiones que va a sustentar. • Cuáles condiciones requieren ser monitoreadas. • Que datos/información se encuentran disponibles (que pueden ser almacenados). Este análisis puede originar requerimientos para ajustar prácticas de trabajo, con el propósito de facilitar la captura de datos que de otra manera no están disponibles. • El costo de captura y mantenimiento de los datos y el valor potencial de los datos para la dependencia o entidad, considerando el impacto negativo de una sobrecarga de datos en la transferencia del conocimiento. Estándares, normatividad y otras políticas aplicables. Asuntos relacionados con la propiedad y los derechos sobre la información.

	2. Documentar las características que deben contener los datos e información para almacenarlos en el repositorio de conocimiento. 3. Seleccionar la configuración por tipo de datos e información que compone cada uno de los repositorios de conocimiento. 4. Clasificar los datos e información de conocimiento por tipo de dato e información como ayuda para identificar el uso, estado y localización. 5. Especificar los atributos de mayor importancia por cada tipo de activo. 6. Identificar aquellos datos e información de conocimiento que deben alojarse en los repositorios de conocimiento.
Relación de Productos	• Criterios de selección de datos e información

ACNC-3 Especificar los procedimientos de administración del repositorio de conocimientos

Descripción	Determinar las políticas y procedimientos para administrar el contenido de cada uno de los repositorios de conocimiento. Incluye la determinación de los medios de almacenamiento, procedimientos, y herramientas para registrar y acceder a los elementos del repositorio.
Factores Críticos	1. Especificar los procedimientos para almacenar y recuperar elementos del repositorio. 2. Definir los mecanismos de operación y control: alimentación, consulta, mantenimiento y respaldo. • Identificar el momento en el ciclo de vida de los procesos, servicios y/o proyectos en los que se deberá coleccionar los datos. • Establecer la autoridad y la responsabilidad sobre todos los elementos del repositorio. 3. Documentar los mecanismos de operación y control: alimentación, consulta, mantenimiento y respaldo. • Identificar el momento en el ciclo de vida de los procesos, servicios y/o proyectos en los que se deberá coleccionar los datos. • Establecer la autoridad y la responsabilidad sobre todos los elementos del repositorio. 4. Determinar las vistas y perspectivas de elementos disponibles para los usuarios del repositorio. 5. Definir los procedimientos requeridos para mantener disponible los datos y la información a sus usuarios. 6. Para asegurar su confidencialidad, integridad y disponibilidad, establecer niveles de clasificación y acceso a los elementos del repositorio de acuerdo a las políticas de seguridad.
Relación de Productos	• Manual de administración de repositorio de conocimiento • Repositorio de conocimiento

ACNC-4 Identificar, capturar y mantener el conocimiento

Descripción	Identificar, capturar y mantener el conocimiento mediante la incorporación de los datos e información de conocimiento en los repositorios del sistema de conocimiento de acuerdo a lo establecido en el manual de administración del repositorio.
Factores Críticos	1. Incorporar los datos e información de conocimiento de acuerdo a las políticas y mecanismos acordados en los manuales de administración de repositorios durante la ejecución de los procesos, proyectos y servicios. 2. Generar nuevo conocimiento. Acceder a fuentes de conocimiento externas y adaptarlas para extender el conocimiento de la UTIC datos e información y conocimiento de fuentes diversas tales como bases de datos, sitios web, empleados, proveedores y socios.
Relación de Productos	• Conocimiento

ACNC-5 Difundir el conocimiento

Descripción	La dependencia o entidad deberá tener énfasis en la obtención, compartimiento y uso del conocimiento mediante la solución de problemas, aprendizaje dinámico, planeación y toma de decisiones. Para lograr lo anterior se requiere difundir el conocimiento a ciertos puntos de la dependencia o entidad, de acuerdo a un plan para la comunicación de conocimiento que considere sus necesidades de información.
Factores Críticos	1. Determinar las necesidades de conocimiento a ser difundido en la dependencia o entidad. 2. Desarrollar un plan para la comunicación del conocimiento. 3. Difundir el conocimiento de acuerdo al plan para la comunicación del conocimiento.
Relación de Productos	• Plan para la comunicación del conocimiento • Repositorio de conocimiento

ACNC-6 Asegurar la calidad e integridad de la información y datos

Descripción	Ejecutar revisiones para mantener la integridad de la configuración de los datos e información de conocimiento (repositorio).
Factores Críticos	1. Revisar los repositorios de conocimiento de la dependencia o entidad periódicamente, incluyendo la revisión cuando nuevos elementos son agregados, eliminados o actualizados. 2. Realizar revisiones independientes al repositorio de conocimiento, para asegurar la calidad de los datos e información y garantizar el apego a las directrices establecidas y a la estrategia de administración del conocimiento. 3. Determinar las acciones correctivas y de mejora derivadas de los hallazgos. 4. Asegurar que las acciones correctivas y de mejora efectuadas hayan sido efectivas.
Relación de Productos	• Resultado de revisiones

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.10.2.2.3 Descripción de roles

Rol	Descripción
Responsable de la administración del conocimiento	Persona responsable de la efectividad y eficiencia del proceso de administración del conocimiento y del sistema de conocimiento en su totalidad.
Responsable del repositorio de conocimiento	Persona o personas responsables de administrar el contenido de un repositorio de conocimiento.

7.10.2.2.4 Descripción de productos

Producto	Descripción
Estrategia de administración del conocimiento	Documento que contiene las directrices para la administración integral del conocimiento de la UTIC. La estrategia de administración del conocimiento típicamente contiene: • Modelo de gobierno • Diseño lógico de la estructura del sistema de conocimiento • Establecimiento de roles y responsabilidades • Políticas, procesos y procedimientos para la administración del conocimiento • Requerimientos tecnológicos y de otro tipo de recursos • Mediciones de desempeño
Criterios de selección de activos	Documento que contiene las políticas, procesos y procedimientos para la clasificación de datos e información.
Manual de administración de repositorios de conocimiento	Documento que contiene las políticas, procesos y procedimientos para la administración de un repositorio de conocimiento. El manual de administración típicamente incluye: • Esquema de gobierno del repositorio de conocimiento • Activos de conocimiento seleccionados a ser incluidos en el repositorio • Catálogo de elementos del repositorio de conocimientos • Mecanismos para la identificación, captura y mantenimiento de los elementos del repositorio

Producto	Descripción
	• Políticas de seguridad
Repositorios de Conocimiento	Repositorios de conocimiento (información y datos en sus distintas manifestaciones incluyendo: modelos, patrones, estándares, plantillas y otros artefactos).
Conocimiento integrado a los repositorios de conocimiento	Denominación conjunta de todos los datos, información y el conocimiento que se deriva de éstos, integrado en los repositorios de conocimiento en sustento de la toma de decisiones de la dependencia o entidad, asegurando que datos e información confiable se encuentren disponibles. El sistema de conocimiento deberá considerar en su diseño lógico a todos los repositorios de datos, información y conocimiento requeridos por la UTIC para cumplir con sus objetivos y funciones, incluyendo entre otros: • El sistema de conocimiento de los procesos • El sistema de conocimiento de los servicios • El sistema de conocimiento de los proyectos • El sistema de conocimiento de la arquitectura tecnológica • El repositorio de configuración (CMDB)
Plan para la comunicación del conocimiento	Documento que contiene cronológicamente las actividades que se deberán desarrollar para la difusión de los repositorios de conocimiento.
Resultado de revisiones	Documento que contiene el resultado de las diversas evaluaciones realizadas a los repositorios de conocimiento.
Plan de acciones correctivas y de mejora	Contiene las acciones correctivas y de mejora derivadas del análisis causa raíz de los hallazgos resultantes de las revisiones efectuadas a repositorios de conocimiento.

7.10.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de Incorporación de activos de conocimiento	Integración de activos	Integración de activos de conocimiento conforme al manual de administración de repositorios de conocimientos	Eficacia	De gestión	% eficiencia=(Número de activos de conocimiento integrados / Número de requerimientos de integración de activos “aplicables“) x 100	Áreas de tecnologías de la UTIC	Trimestral
Tasa de comunicación del Plan de	Difusión alcanzada	Elaboración de un plan de comunicación	Eficacia	De gestión	% eficiencia= (Número de personas	Áreas de tecnologías de la UTIC	Trimestral

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
activos de conocimiento		de activos de conocimiento			comunicadas/ Numero de Personas Programadas)		
Índice de revisión de repositorios de conocimiento	Revisiones de calidad de los activos	Ejecutar revisión de calidad a los repositorios de conocimiento existentes	Eficacia	De gestión	% eficiencia= (Número revisiones realizadas / Número de revisiones programadas) x 100	Dirección TIC	Trimestral
Porcentaje de atención en la creación de repositorios	Crear repositorios de conocimiento con base en los criterios, la demanda y el análisis de la selección de activos	Repositorios de conocimiento creados	Eficacia	De gestión	% de eficiencia = (Número de repositorios de conocimiento creados/ Número de requerimientos de creación de repositorios) x 100	Dirección TIC	Trimestral
Porcentaje de incorporación de activos de conocimiento	Integración de activos	Integración de activos de conocimiento conforme al manual de administración de repositorios de conocimiento	Eficacia	De gestión	% eficiencia=(Número de activos de conocimiento integrados / Número de requerimientos de integración de activos “aplicables“) x 100	Áreas de tecnologías de la UTIC	Trimestral
Tasa de comunicación del plan de activos de conocimiento	Difusión alcanzada	Elaboración de un plan de comunicación de activos de conocimiento	Eficacia	De gestión	% eficiencia= (Número de personas comunicadas/ Numero de Personas Programadas)	Áreas de tecnologías de la UTIC	Trimestral
Índice de Revisión de repositorios de conocimiento	Revisiones de calidad de los activos	Ejecutar revisión de calidad a los repositorios de conocimiento existentes	Eficacia	De gestión	% eficiencia= (Número revisiones realizadas / Número de revisiones programadas) x 100	Dirección TIC	Trimestral

7.10.2.4	Reglas del proceso
1.1	La UTIC deberá establecer un sistema de datos e información para el conocimiento que contemple repositorios de todos los datos e información, relacionados con TIC.
1.2	La UTIC deberá asignar a un responsable del sistema de datos e información para el conocimiento.
1.3	La UTIC deberá asignar a un responsable del proceso de Administración del conocimiento.

7.10.2.5	Documentación soporte del proceso
	No aplica

7.10.3 Desarrollo del personal

7.10.3.1 Objetivo general del proceso

General.-
Desarrollar las habilidades y el conocimiento del personal de TIC para que puedan realizar sus funciones con eficacia y eficiencia.

Específicos.-

1. Identificar las necesidades estratégicas de desarrollo y capacitación del personal de la UTIC.
2. Definir e implementar un programa de desarrollo del personal para la UTIC.
3. Proveer la formación y entrenamiento de acuerdo al programa de desarrollo del personal de la UTIC.
4. Evaluar la efectividad de las actividades de desarrollo y capacitación del personal de la UTIC.
5. Establecer un sistema de actualización y seguimiento de los programas de desarrollo y capacitación del personal en la UTIC.

7.10.3.2 Descripción del proceso

7.10.3.2.1 Mapa general del proceso

Diagrama de flujo de información

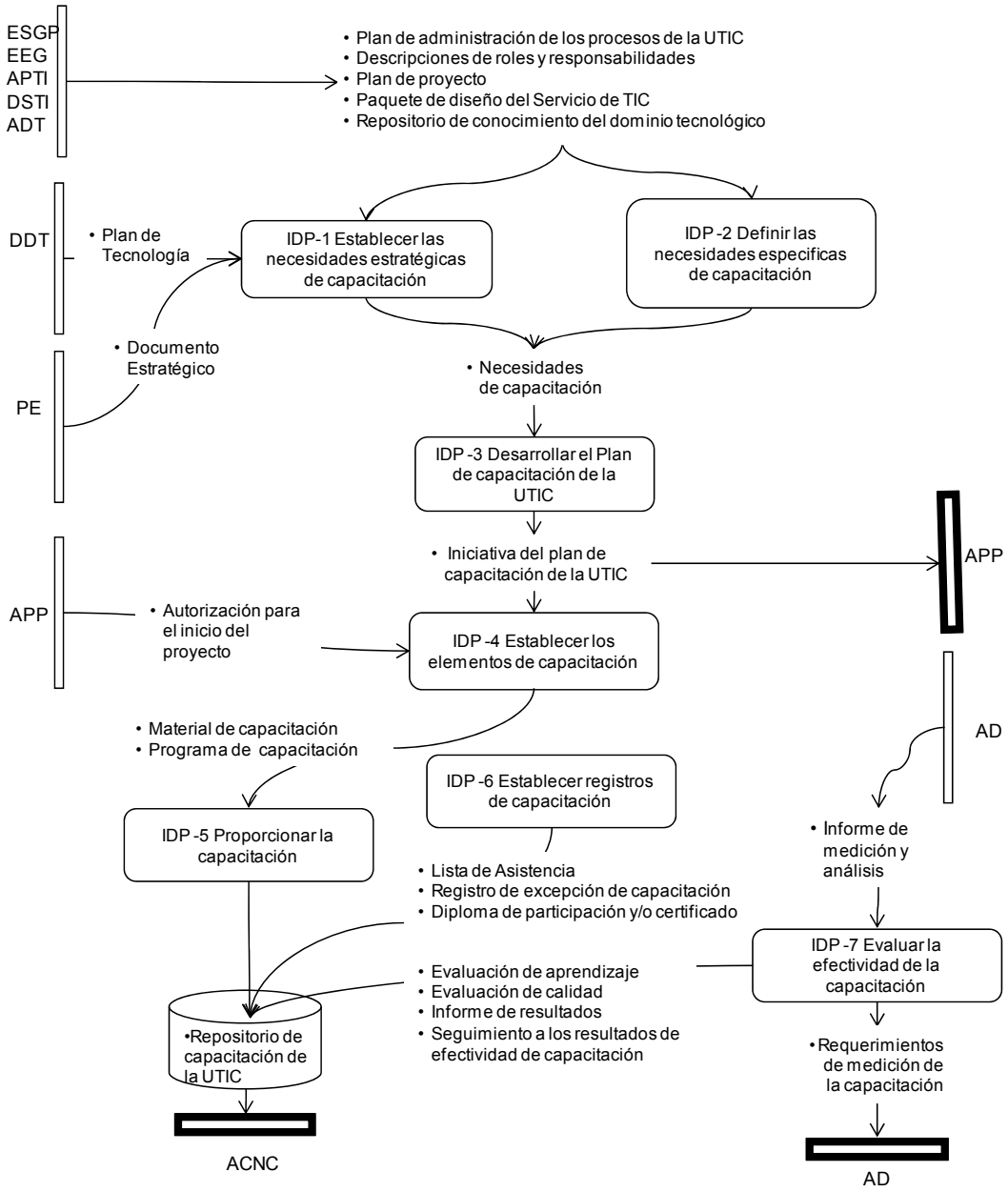
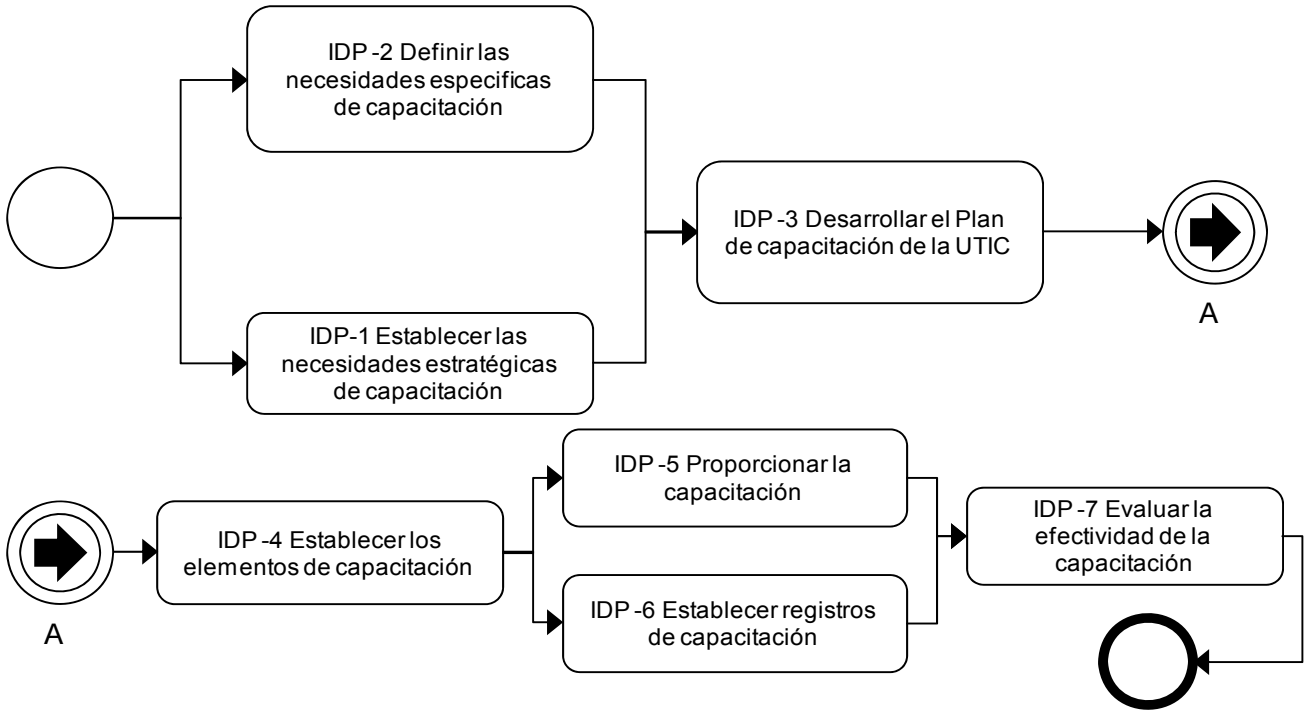


Diagrama de flujo de actividades



7.10.3.2.2 Descripción de las actividades del proceso

IDP-1 Establecer las necesidades estratégicas de capacitación

Descripción	Establecer las necesidades estratégicas de capacitación para la UTIC. Actualizar las necesidades estratégicas de capacitación para la UTIC. Las necesidades estratégicas de capacitación están orientadas hacia objetivos a corto, mediano y largo plazo para crear las capacidades que eliminen las brechas de conocimiento con la introducción de nueva tecnología y facilitando cambios en el comportamiento del personal.
Factores Críticos	1. Analizar los objetivos estratégicos de negocio de la dependencia o entidad, las capacidades y habilidades necesarias para la ejecución de los procesos de la UTIC y los planes de proyectos, servicios y procesos, para identificar necesidades potenciales de capacitación. 2. Documentar las necesidades estratégicas de capacitación de la UTIC. 3. Determinar los roles y habilidades necesarias para ejecutar el sistema de procesos de la UTIC. 4. Documentar las necesidades de capacitación para desempeñar las funciones específicas de los procesos de la UTIC. 5. Documentar las necesidades de capacitación para mantener sin riesgo, segura y continua la operación de la dependencia o entidad. 6. Revisión, actualización y seguimiento sistemático de las necesidades estratégicas de la dependencia o entidad, en materia de capacitación, requerida por la UTIC determinando claramente su periodo de reciclaje, acorde con el dinamismo de las TIC.
Relación de Productos	• Necesidades de capacitación

IDP-2 Definir las necesidades específicas de capacitación que son responsabilidad de la UTIC

Descripción	Determinar las necesidades de capacitación específicas para los proyectos, servicios y procesos.
Factores Críticos	1. Determinar específicamente las competencias necesarias para el personal que realiza trabajos que afectan a la calidad y continuidad del producto/servicio. (Como grupo de soporte) 2. Analizar las necesidades de capacitación identificadas por los proyectos y grupos de expertos técnicos. 3. Negociar y documentar con los diversos proyectos y grupos de expertos sobre cómo serán satisfechas sus necesidades específicas de capacitación.
Relación de Productos	• Necesidades de capacitación

IDP-3 Desarrollar el Plan de capacitación de la UTIC

Descripción	El Plan de capacitación de la UTIC es un plan para desplegar la capacitación responsabilidad de la UTIC y es necesario para que las personas desempeñen sus funciones con eficacia y eficiencia. Este plan se refiere a la ejecución a corto, mediano y largo plazo de la capacitación y se ajusta periódicamente en respuesta a los cambios y evaluaciones de efectividad, para proporcionar a los servidores públicos de TIC la orientación necesaria al momento de la contratación y durante el entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, y conciencia sobre la seguridad y controles internos, al nivel requerido para alcanzar las metas de la dependencia o entidad.
Factores Críticos	1. Documentar el Plan de capacitación de la UTIC. El Plan de capacitación de la UTIC deberá contemplar al menos los siguientes conceptos: • Necesidades estratégicas de capacitación. • Necesidades de capacitación específicas. • Tópicos de capacitación. • Compromisos de capacitación. • Métodos a ser usados para la capacitación. • Requerimientos y estándares para materiales de capacitación. • Tareas de capacitación, roles y responsabilidades. • Recursos requeridos incluyendo herramientas, instalaciones, ambiente, personal, así como sus habilidades y conocimientos. • Cronograma. 2. Establecer compromisos con el plan. (Documentar los compromisos con los principales responsables de implementar y soportarlo). 3. Revisar y aprobar el plan de capacitación.
Relación de Productos	• Iniciativa del plan de capacitación de la UTIC

IDP-4 Establecer los mecanismos de capacitación

Descripción	Establecer y mantener los elementos de entrenamiento orientados a satisfacer las necesidades de capacitación. Identificar la forma como se generará la capacitación, los instructores requeridos, definir el contenido de la capacitación y materiales de apoyo.
Factores Críticos	1. Seleccionar los enfoques apropiados para satisfacer las necesidades de capacitación específicas de la dependencia o entidad. (Existen factores que pueden afectar la selección de los enfoques de capacitación, incluyendo conocimientos específicos de la audiencia, costos y horarios, ambiente de trabajo, y otros. La selección de un enfoque requiere la consideración de los medios para proporcionar las habilidades y conocimientos de la manera más efectiva, tomando en cuenta las restricciones existentes.) 2. Determinar si se desarrolla el material de capacitación internamente o se adquiere

	externamente. (Hacer un análisis costo-beneficios de desarrollar la capactiación interna o de obtener capacitación externa). 3. Determinar si se proporciona la capacitación a través de capacitadores internos o externos. (La capacitación puede ser proporcionada por el proyecto, por grupos de soporte, por la dependencia o entidad o por un proveedor externo. El personal de capacitación de la dependencia o entidad debe coordinar la adquisición y despliegue de la capacitación independientemente de su origen.) 4. Desarrollar u obtener instructores calificados. (Para asegurar que los instructores que proporcionan la capacitación interna tienen el conocimiento y habilidades necesarias, se pueden definir criterios para identificar, desarrollar y calificarlos. En el caso de ser capacitación proporcionada por externos el personal responsable puede investigar cómo el proveedor determina qué instructores pueden proporcionar la capacitación. Esto puede ser también un factor para la selección o continuidad de un proveedor de capacitación.) 5. Describir e integrar la capacitación en el programa de capacitación global de la dependencia o entidad. 6. Revisar y actualizar el material de capacitación y sus elementos de soporte tanto como sea necesario.
Relación de Productos	• Material de capacitación • Programa de capacitación

IDP-5 Proporcionar la capacitación

Descripción	Desarrollar la capacitación siguiendo el plan de capacitación de la UTIC.
Factores Críticos	1. Identificar por parte de los responsables de las UTIC los requerimientos específicos de capacitación para el trabajo en cada uno de los cargos de su área. Estos requerimientos deben documentarse en el plan de capacitación de la UTIC. 2. Asegurar que todos los servidores públicos de nuevo ingreso cuenten con una inducción a su cargo que incluya capacitación sobre: a. Las políticas y procesos. b. La importancia de satisfacer los requerimientos del usuario, los estatutarios y los legales y, la necesidad de garantizar la satisfacción del usuario. c. La importancia y la trascendencia de sus actividades y la manera en que contribuyen al logro de los objetivos de la dependencia o entidad. 3. Seleccionar a las personas que recibirán la capacitación necesaria para desarrollar sus funciones efectivamente. La capacitación es destinada a impartir conocimiento y habilidades a las personas que realizan diversas funciones dentro de la dependencia o entidad. Algunas personas ya cuentan con conocimientos y habilidades necesarias para desempeñarse bien en sus funciones. La capacitación puede no ser obligatoria para estas personas, pero se debe tener cuidado de que las dispensas de capacitación no sean objeto de abusos.

	4. Establecer los programas de capacitación, incluyendo los recursos que sean necesarios. La capacitación debe ser planeada y programada. La capacitación es proporcionada para que tenga un impacto directo sobre las expectativas de desempeño en el trabajo. Por lo tanto, la capacitación óptima ocurre en una manera oportuna con respecto a las expectativas que se tienen del trabajo a ejecutar. 5. Conducir la capacitación. Instructores experimentados deben ejecutar la capacitación. La capacitación debe proporcionarse de forma cercana a las condiciones de trabajo actuales e incluir actividades para simular situaciones de trabajo reales. Éste enfoque incluye integración de herramientas, métodos y procedimientos para el desarrollo de competencias. La capacitación está vinculada a las responsabilidades de trabajo, así que una vez terminada, las actividades en el trabajo u otras experiencias deberán reforzar la capacitación dentro de un periodo de tiempo razonable. 6. Seguimiento del desarrollo de la capacitación contra el plan de capacitación de la UTIC.
Relación de Productos	• Repositorio de capacitación de la UTIC

IDP-6 Establecer registros de capacitación

Descripción	Establecer y mantener los registros de capacitación de la UTIC en su conjunto. Se deben mantener los registros apropiados de la educación, formación, habilidades y experiencia del personal. Los registros deben permanecer legibles, fácilmente identificables y recuperables. Debe establecerse un procedimiento documentado para definir los controles necesarios para la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición de los registros.
Factores Críticos	1. Guardar los registros de todos los participantes que completaron exitosamente cada curso de capacitación u otras actividades de capacitación aprobadas, así como aquellos que no tuvieron éxito. 2. Guardar registros de todo el personal que no recibió la capacitación. La justificación para la concesión de una exención debe estar documentada, y tanto el administrador responsable como los participantes deben autorizar la exención. 3. Generar registros de capacitación apropiados para las personas que están relacionadas con las asignaciones. Los registros de capacitación pueden ser parte de una matriz de habilidades desarrolladas por el área de capacitación de la dependencia o entidad, para proporcionar un resumen de las experiencias y educación de las personas, así como de la capacitación propia. Todos estos registros deberán estar debidamente capturados, procesados y consolidados en el repositorio de capacitación de la UTIC o, en su defecto, en el sistema institucional de capacitación dependencia o entidad.
Relación de Productos	• Lista de asistencia • Registro de excepción de capacitación

	• Diploma de participación y/o certificado

IDP-7 Evaluar la efectividad de la capacitación

Descripción	Evaluar la efectividad del plan de capacitación de la UTIC estableciendo un proceso para determinar su eficacia. Es posible obtener métricas para evaluar los beneficios de la capacitación contra los proyectos y objetivos de la dependencia.
Factores Críticos	1. Evaluar proyectos en progreso o completados para determinar si el conocimiento del personal es adecuado para desarrollar tareas en el proyecto. 2. Proporcionar un mecanismo para evaluar la efectividad de cada curso de capacitación con respecto a los objetivos de la dependencia o entidad, proyecto u objetivos individuales aprendidos (o desarrollados). 3. Obtener evaluaciones de participantes de cómo las actividades de capacitación cumplen con sus necesidades.
Relación de Productos	• Requerimientos de medición de la capacitación

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.10.3.2.3 Descripción de roles

Rol	Descripción
Administrativo de capacitación	Área encargada de administrar y supervisar las actividades para realizar la capacitación de la UTIC de acuerdo al presupuesto autorizado.
Responsable de capacitación de la UTIC	Responsable de definir el contenido del plan de capacitación de la UTIC, coordina las actividades de planeación para la capacitación y actualiza los datos generados de las capacitaciones para evaluar la efectividad de las mismas.
Unidad de coordinaciones	Es responsable de aprobar el plan de capacitación de la UTIC y establecer el presupuesto que será asignado a las actividades de capacitación.
Participantes	Persona o grupo de personas a las que se les imparte la capacitación.
Grupo de soporte	Especialistas técnicos que cuentan con el conocimiento y experiencia en las tecnologías del dominio. Estos especialistas interactúan y comparten sus conocimientos y experiencias, y participan en la definición y administración de la arquitectura del proceso de administración de dominios tecnológicos.

7.10.3.2.4 Descripción de productos

Producto	Descripción
Plan de capacitación de la UTIC	Plan que describe las necesidades de capacitación, alcance de la misma y resultados esperados. Características • Resultados de la evaluación de necesidades de la dependencia o entidad. • Necesidades de capacitación (comunes para proyectos y grupos de soporte). • Tópicos de capacitación. • Compromisos de capacitación. • Programa basado en actividades de capacitación y sus dependencias. • Métodos usados para capacitación. • Requerimientos y estándares de calidad para materiales de capacitación. • Tareas de capacitación, roles y responsabilidades. • Recursos requeridos incluyendo herramientas, facilidades, ambiente, personal, habilidades y conocimientos
Necesidades de Capacitación	Documento base para realizar el plan de capacitación que contiene el análisis del plan de proyecto, servicio y procesos de la UTIC.
Material de capacitación	Son los materiales que se generan para llevar a cabo la capacitación (guías, manuales, libros, CD).
Repositorio de capacitación de la UTIC	Sitio centralizado donde se mantienen almacenados los datos e información que se han generado a lo largo de las capacitaciones realizadas en la dependencia o entidad. Contiene entre otros: el catálogo de instructores habilitados y el programa de capacitación, registros de la capacitación, cursos a ser impartidos, programa de capacitación correspondiente y su registro en el repositorio de capacitación de la UTIC.
Lista de asistencia	Registro de los participantes en las capacitaciones que están incluidas en el plan de capacitación de la UTIC.
Registro de excepción de capacitación	Registros para las personas que omitieron una capacitación específica, este documento es aprobado y comunicado.
Diploma de participación y/o certificado	Documento que avala la participación en una capacitación. Debe proporcionarse una vez culminada la capacitación.
Evaluación de aprendizaje	Evaluación para medir el aprendizaje. Ésta se realiza en tres momentos diferentes: Antes de la capacitación (evaluación inicial), intermedia y final.
Evaluación de calidad	Evaluación que mide la calidad de la capacitación considerando diferentes aspectos de la misma. La evaluación es personal y tiene por objetivo medir el nivel de actuación tanto del

Producto	Descripción
	instructor como del ambiente, participantes y materiales, y contenido del curso; los comentarios deben de ser constructivos con el propósito de mejorar los cursos por impartir.
Informe de resultados	Síntesis de los resultados por la capacitación impartida. Características • Comparación de resultados esperados y resultados alcanzados. • Tiempo de ejecución. • Indicadores. • Beneficiarios. • Información de cursos impartidos y no impartidos
Seguimiento a los resultados de efectividad de capacitación	Se da seguimiento a la capacitación registrando los cursos que se han impartido, los pendientes y las acciones a tomar. Características • Información de cursos impartidos y No impartidos. • Plan de acción. • Matriz de responsabilidades.
Requerimientos de medición de la capacitación	Necesidades de datos e información asociados a indicadores y métricas acerca del desempeño de la capacitación realizada.
Programa de capacitación	Planes detallados de la capacitación autorizada integrados en un cronograma que define entre otros: • Fechas estimadas • Asistentes • Temas y cursos • Proveedor • Medio

7.10.3.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de programación de los programas de capacitación	Establecer el conjunto de elementos de capacitación que satisfagan las necesidades determinadas	Índice de la medición de los elementos de capacitación cubiertos establecidos en el plan de capacitación	Eficiencia	De gestión	(Número de elementos de capacitación proporcionados /número de elementos de capacitación programados) x 100	Área de capacitación	Anual

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
	en el plan de capacitación de la dependencia o entidad	de la dependencia o entidad					
Índice de asistencia a programas de capacitación	Medir el porcentaje de participación en los programas de capacitación definidos	Índice de asistencia a programas de capacitación	Eficiencia	De gestión	(Número de asistentes / Número de participantes programados) x100	Área de capacitación	Trimestral
Índice de actualización del Repositorio de capacitación	Actualizar el repositorio de registros de capacitación de la dependencia o entidad	Índice de actualización de registros del repositorio de capacitación de la dependencia o entidad	Eficiencia	De gestión	(Número de registros actualizados / Número de registros programados) x 100	Área de capacitación	Trimestral
Índice de acreditación de programas de capacitación	Medir el porcentaje de acreditación en los programas de capacitación definidos	Índice de acreditación de programas de capacitación	Eficiencia	De gestión	(Número de participantes acreditados / Número de participantes programados) x100	Área de capacitación	Trimestral

7.10.3.4 Reglas del proceso

1.1	La UTIC deberá desarrollar y presentar para su autorización anualmente un Plan de capacitación de personal de la UTIC al grupo de trabajo para la dirección de TIC.
1.2	El Plan de capacitación de la UTIC se deberá elaborar de acuerdo a los roles y responsabilidades del personal.
1.3	El Plan de capacitación debe incluir el análisis de las necesidades estratégicas de capacitación así como los mecanismos de capacitación y formación.
1.4	Se deberán establecer y mantener los registros y controles de las actividades de capacitación y formación realizadas en la dependencia o entidad.

7.10.3.5 Documentación soporte del proceso

No aplica

7.11 OPERACIONES

7.11.1 Administración de la operación

7.11.1.1 Objetivos del proceso

General.-

Administrar y operar la infraestructura para entregar los servicios de TIC conforme a los niveles acordados.

Específicos.-

1. Asegurar la ejecución segura y oportuna de las tareas y procesos programados.
2. Monitorear y registrar los resultados de las tareas y procesos.
3. Asegurar que los servicios y la infraestructura de las TIC puedan resistir a fallas ocasionadas por errores, ataques deliberados o desastres y recuperarse.
4. Asegurar la estabilidad y continuidad de la operación de la infraestructura de manera que los servicios de las TIC estén disponibles.

7.11.1.2 Descripción del proceso

7.11.1.2.1 Mapa general del proceso

Diagrama de flujo de información

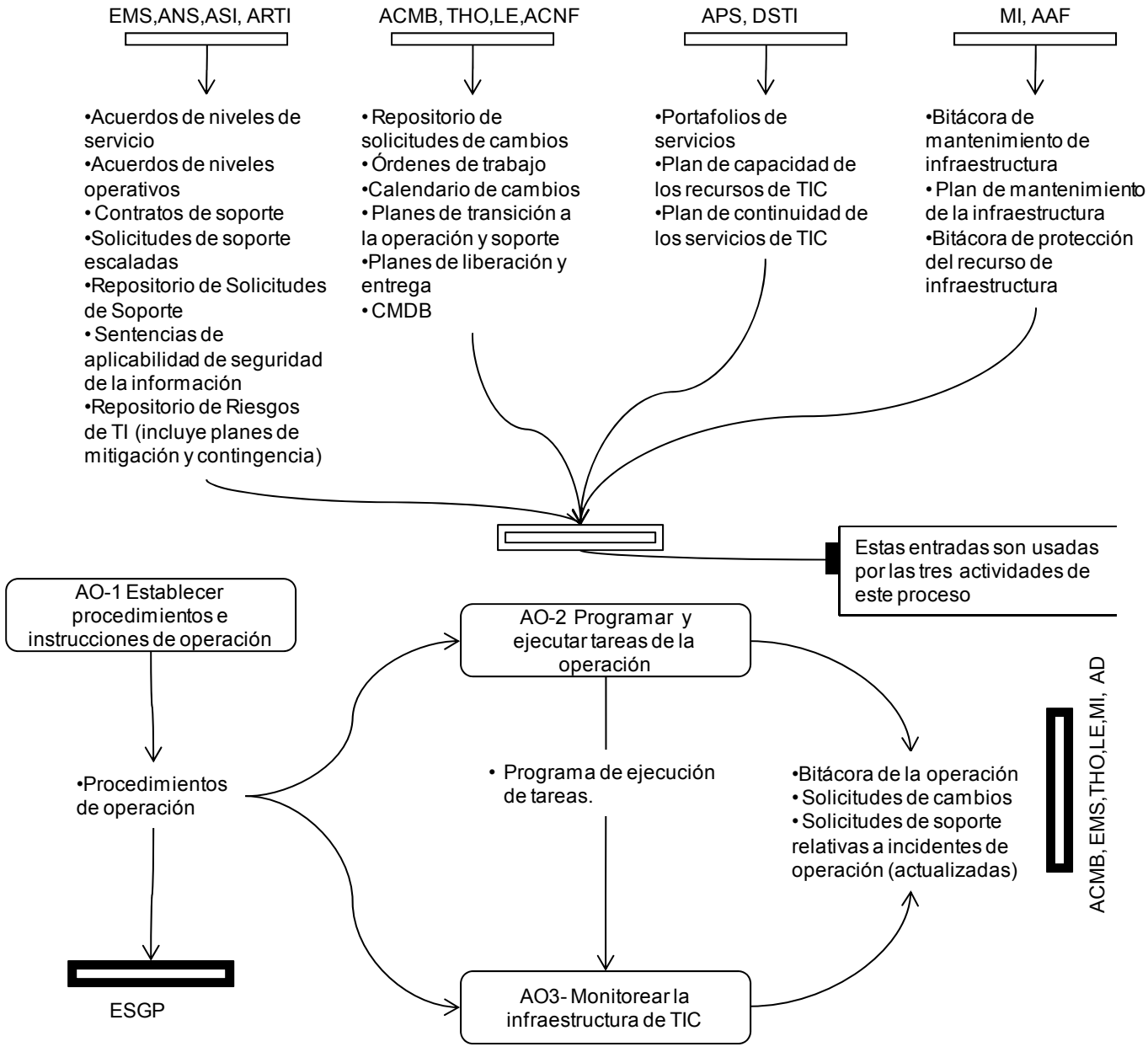
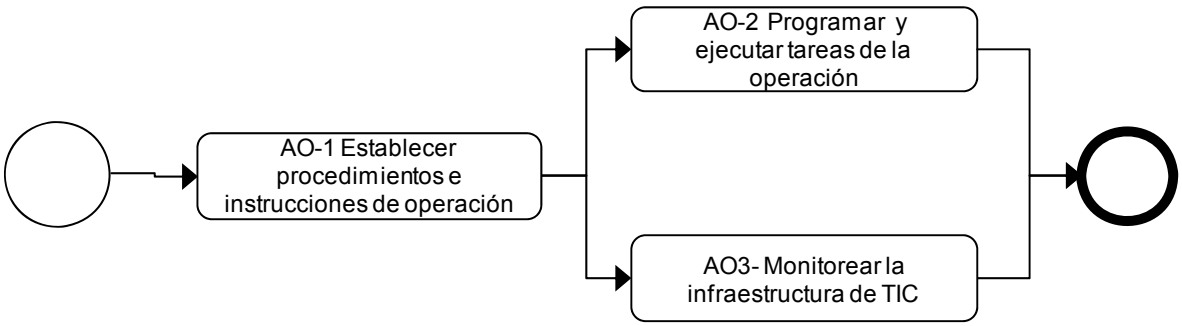


Diagrama de flujo de actividades



7.11.1.2.2 Descripción de las actividades del proceso

AO-1 Establecer procedimientos e instrucciones de operación

Descripción	Contar con procedimientos para la operación y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos.
Factores Críticos	1. Desarrollar, implementar y mantener un procedimiento estándar operacional de las TIC que comprenda la definición de roles y responsabilidades, incluyendo aquellos que son suministrados por un proveedor. • Para asegurar la continuidad de las operaciones y el seguimiento de los incidentes a través de la mesa de servicio, los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales). • Estos documentos contienen la descripción de las actividades rutinarias que se requieren ejecutar en cada dispositivo o sistema. • Contienen los procedimientos que deben de seguirse en caso de surgir una excepción o de requerir un cambio. • Debe contener la definición de los niveles estándares de rendimiento para cada uno de los dispositivos o procedimientos, así como establecer el nivel de servicio de cada proceso o tarea, y la forma en que se medirá y reportará. 2. Definir procedimientos y responsabilidades para transferir funciones, por cambios y ausencias planeadas o no planeadas. 3. Definir procedimientos para el manejo de excepciones conforme a la administración de incidentes y cambios y para tratar aspectos de seguridad. 4. Entrenar al personal de soporte en procedimientos operacionales y tareas relacionadas de las cuales son responsables. 5. Asegurar que la segregación de funciones está acorde a los riesgos asociados, seguridad y requerimientos de auditoría.
Relación de productos	• Procedimientos de operación

AO-2 Programar y ejecutar tareas de la operación

Descripción	Organizar la programación de tareas y procesos automatizados, en orden de eficiencia, maximizando el desempeño y la utilización, para cumplir con los requerimientos de la dependencia o entidad.
Factores Críticos	1. Usar el proceso de administración de cambios para la planificación de las actividades en ejecución que podrían tener un impacto en los servicios proporcionados. • Se deberá obtener autorización de la planificación inicial y a sus cambios. • Deberán de autorizarse todos los procesos y tareas que se incluyan al calendario de ejecución, así como cualquier cambio que se les aplique ya sea a los componentes o a

	su programación. 2. Establecer procedimientos e implementarlos para identificar, investigar, supervisar y aprobar las salidas de los procesos, tareas y programas calendarizados. 3. Establecer y coordinar el calendario de ejecución diaria, y asegurar que la planificación de las tareas y procesos programados considera los requerimientos de la dependencia o entidad, sus prioridades, conflictos entre los procesos y tareas así como el balanceo de cargas. 4. Definir e implementar un procedimiento para resolver las fallas que resulten en la ejecución de las tareas y procesos programados de la operación. 5. Implementar herramientas automatizadas y procesos para notificar y rectificar inmediatamente fallas críticas del proceso.
Relación de productos	• Bitácora de la operación • Solicitudes de cambios • Solicitudes de soporte relativas a incidentes de operación (actualizadas) • Programa de ejecución de tareas

AO-3 Monitorear la infraestructura de TIC

Descripción	Asegurar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que rodean las operaciones.
Factores Críticos	1. Definir y establecer herramientas que permitan validar el estado de los dispositivos para asegurar que operan dentro de los límites aceptables. 2. Definir e implementar reglas para la administración de eventos. Un evento es una ocurrencia que es significativa para la administración de la infraestructura o la entrega de un servicio. Los eventos se crean típicamente por un servicio de TIC, un elemento de configuración o una herramienta de monitoreo. • Los eventos pueden ser programados para comunicar información de la operación así como alertas y excepciones y pueden ser la base para automatizar muchas de las tareas rutinarias de operación. • Definir los distintos tipos de eventos para establecer reglas de administración para cada tipo. Un ejemplo de tipos de eventos puede ser: o Eventos que denotan operaciones normales. Por ejemplo, la notificación de que una carga de información programada fue efectuada. o Eventos que denotan excepciones. Por ejemplo, un usuario intenta acceder a una aplicación a la que no tiene acceso. o Eventos que denotan operación inusual pero que no son excepciones. Por ejemplo, el nivel de utilización de la memoria de un servidor alcanza un 5% de su nivel más alto aceptable. 3. Asegurar que cualquier tarea o proceso que se ejecute como parte de la operación sea registrada. • Los datos registrados se usan para detectar la causa raíz de los incidentes detectados, así como confirmar la ejecución satisfactoria de las tareas y procesos.

	4. Identificar y mantener una lista de datos e información de infraestructura que necesitan ser monitoreados y/o supervisados, basados en servicios críticos y la relación entre los datos e informacion de configuración y servicios que dependen de ellos. 5. Definir e implementar reglas para la detección de incidentes relacionados con la administración de eventos. 6. Se deberán de catalogar en incidentes menores y mayores para no generar un registro de información innecesaria. 7. Resguardar la información de los incidentes para poder realizar un análisis en la solución de problemas, prevención o mejora. 8. Establecer procedimientos para monitorear los registros de incidentes y conducir revisiones periódicas. 9. Asegurar que los registros de incidentes son creados a tiempo cuando se identifican desviaciones durante el monitoreo.
Relación de productos	• Bitácora de la operación • Solicitudes de cambios • Solicitudes de soporte relativas a incidentes de operación (actualizadas) • Programa de ejecución de tareas

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.11.1.2.3 Descripción de roles

Rol	Descripción
Administrador de la operación	Ejecutar las actividades y procesos programados, monitorea la ejecución y da seguimiento a la resolución de los incidentes que resulten en la ejecución de los procesos y tareas día a día. Es responsable de que las actividades programadas se lleven de acuerdo al horario y forma establecida, así como comunicar los resultados de acuerdo a los procedimientos establecidos.

7.11.1.2.4 Descripción de productos

Producto	Descripción
Bitácora de la operación	Contiene el registro de las actividades realizadas en forma programada. El formato de las bitácoras de operación es muy variado dependiendo de las soluciones tecnológicas e infraestructura. Ejemplos de bitácoras de operación incluyen: • Registros de los sistemas operativos de cada dispositivo. • Registros de actividades de aplicaciones almacenadas en un servidor. • Registros de eventos almacenados en la herramienta de monitoreo.

Producto	Descripción
	• Registro de accesos físicos a instalaciones restringidas. • Registro manual de actividades realizadas.
Procedimientos de la operación	Conjunto de documentos con instrucciones detalladas y actividades calendarizadas para cada uno de los equipos, departamentos o grupos que participen en la administración de la operación.
Programa de ejecución de tareas	Documento con instrucciones detalladas y actividades calendarizadas para cada una de las tareas en que participen los equipos de operación, así como de los servicios que prestan a los usuarios.
Solicitudes de soporte relativas a incidentes de operación (actualizadas)	Actualización de la información de las solicitudes de soporte relativas a los incidentes que ocurran durante la operación, en el repositorio de información que establezca la mesa de servicio para este propósito.
Solicitud de cambio	Formato para documentar el propósito y detalles del cambio propuesto que es sometido a consideración y valoración por parte los roles con la autoridad para decidir su procedencia o rechazo. Características: Contiene los detalles de las propuesta del cambio Nombre y detalles del contacto Se le asigna un identificador único Se anexan al formato, documentos de soporte: evidencias de pruebas unitarias, de usuario, integrales, entre otros.

7.11.1.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Índice de personal familiarizado con la operación	Asegurar que el personal este actualizado con los procedimientos de operación de la UTIC	Indicador que sirve para mostrar el grado de personas que están actualizados en el uso de procedimientos de operación	Eficiencia	De gestión	Número de personas evaluadas /número de personas operativas de la UTIC	Titular de la UTIC	Anual/Semestral
Porcentaje de tareas y procesos de la operación programados	Asegurar que las tareas y procesos de la operación de la UTIC se integren a un programa de operación	Indicador que muestra el grado de integración de las tareas y procesos de la operación en un programa de operación	Eficiencia	De gestión	Número de tareas y procesos integrados al programa/número de tareas y procesos totales	Titular de la UTIC	Anual/Semestral

		de la UTIC					

7.11.1.4	Reglas del proceso

1.1	La UTIC a través del responsable del proceso de Administración de la operación deberá establecer las instructivos de operación que contengan los datos necesarios para la ejecución, monitoreo, resolución de problemas y niveles de escalamiento en caso de incidentes.
1.2	El responsable del proceso de Administración de la operación es el responsable del área de centro de datos y operación.
1.3	La UTIC a través del responsable del área de centro de datos y operación deberá asegurar el cumplimiento de lo establecido en los planes de continuidad y procedimientos de la operación.
1.4	La UTIC a través del área de centro de datos y operación es la responsable de la administración de operación de la red de área local y la red de área extendida y demás infraestructura relativa a comunicaciones.

Reglas de aplicables a procedimientos que sean regidos por el proceso
El área responsable del centro de datos y operación deberá hacerse cargo de la configuración de equipos en la red, deberá asegurar que los datos del usuario y del equipo estén actualizados y que sean los correctos.
El área responsable del centro de datos y operación deberá asegurar que los equipos de videoconferencia estén encendidos y conectados a la red con la anticipación necesaria antes del inicio de un evento que implique su uso.
El área responsable del centro de datos y operaciones deberá conservar la integridad del equipo de TIC ubicados en éste.

7.11.1.5	Documentación soporte del proceso
	No aplica

7.11.2 Administración de ambiente físico

7.11.2.1 Objetivos del proceso

General.-
Proporcionar y mantener un ambiente físico adecuado para proteger los activos de las TIC contra acceso físico no autorizado, daño, robo, o mal uso de los recursos, minimizando el riesgo de una interrupción del servicio.

Específicos.-

1. Administrar y mantener las condiciones de energía eléctrica, temperatura, seguridad, necesarias en para la operación del centro de datos.
2. Definir las mediciones para monitorear la estabilidad del ambiente físico del centro de datos, tomando las medidas preventivas y correctivas pertinentes.
3. Asegurar el mínimo impacto a la dependencia o entidad en caso de variaciones en el ambiente físico que afecten los servicios de TIC.

7.11.2.2 Descripción del proceso

7.11.2.2.1 Mapa general del proceso

Diagrama de flujo de información

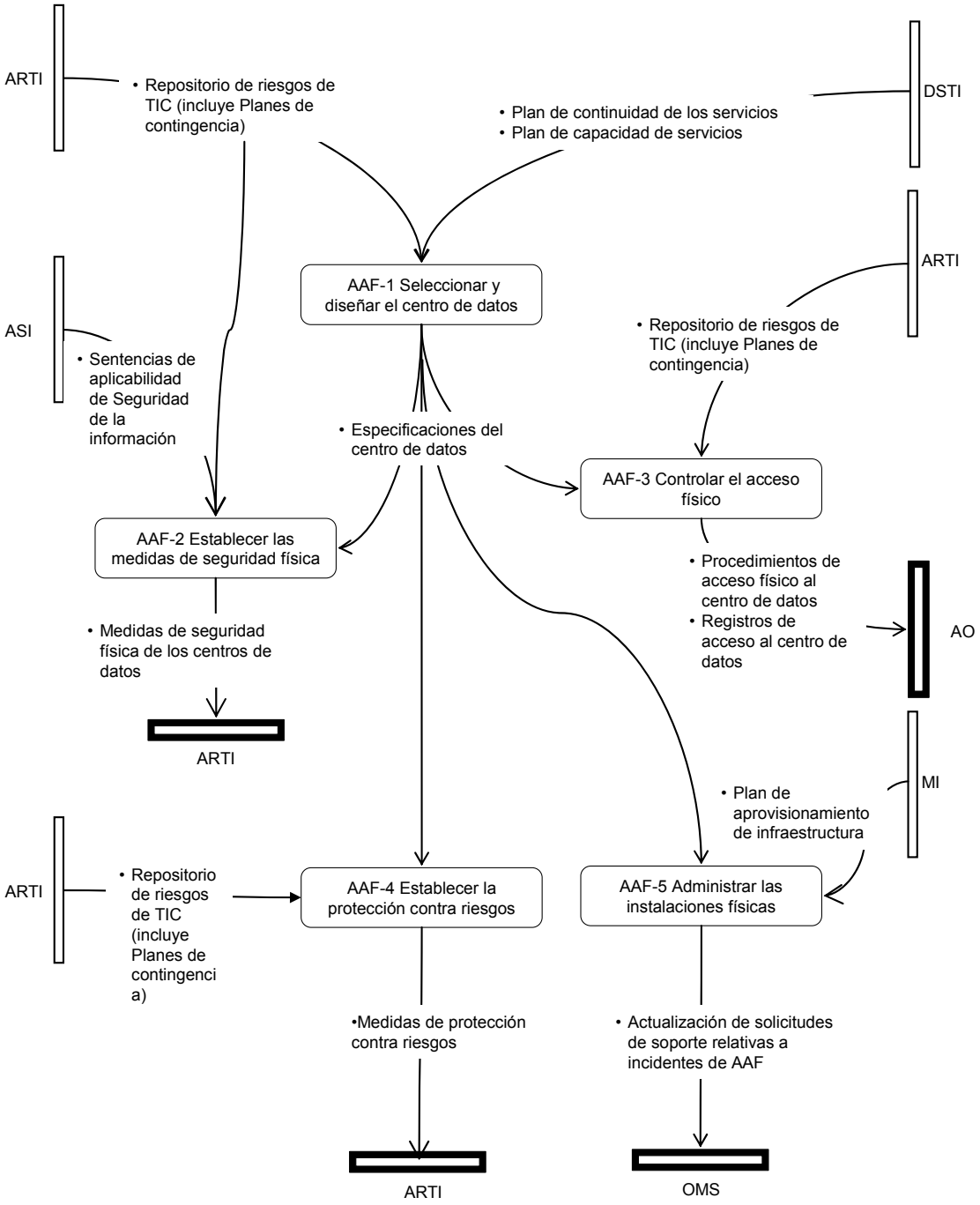
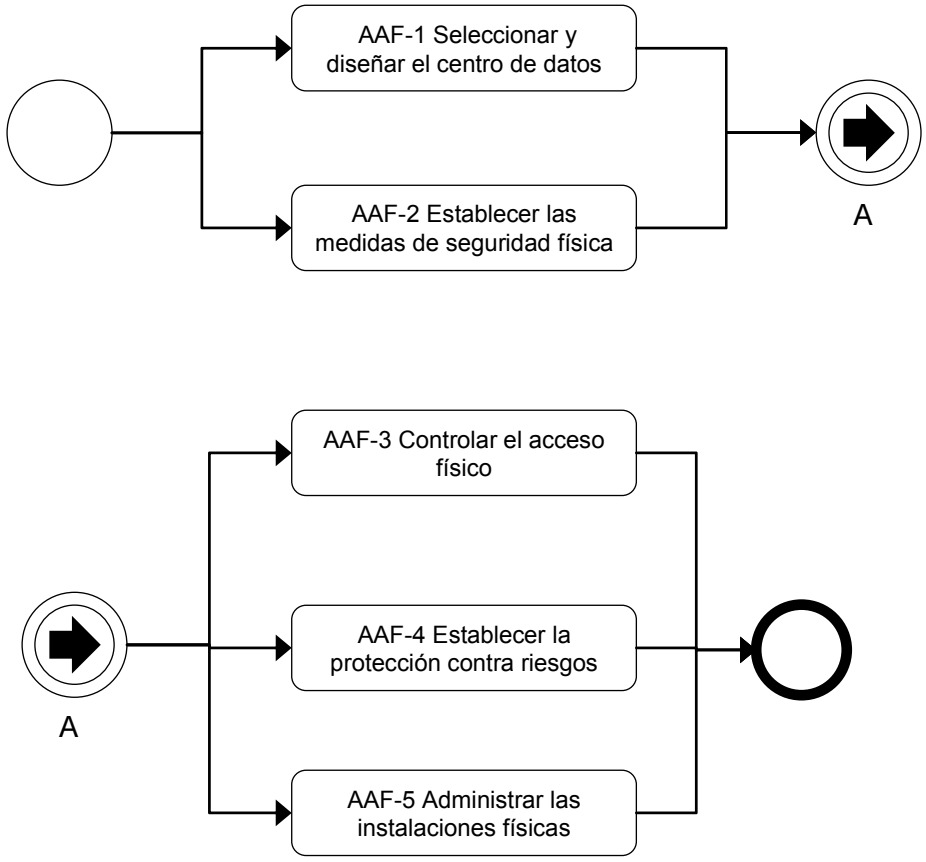


Diagrama de flujo de actividades



7.11.2.2.2 Descripción de las actividades del proceso

AAF-1: Seleccionar y diseñar el centro de datos (site)

Descripción	Definir y seleccionar los centros de datos físicos para el equipo de las TIC, para soportar la estrategia de tecnología ligada a la estrategia de la dependencia o entidad.
Factores Críticos	1. Seleccionar los equipos (infraestructura) para el centro de datos que cumpla los requerimientos, presentes y escalabilidad futura, de la dependencia o entidad y la política de seguridad. • Asegurar que la selección y/o diseño del centro de datos toma en consideración las leyes y regulaciones aplicables. 2. Identificar los riesgos potenciales y las amenazas para los centros de datos y evalúe el impacto hacia la dependencia o entidad. • Estas actividades deberán estar alineadas a los procesos de administración de la seguridad de la información y administración de riesgos de TIC.
Relación de productos	• Especificaciones del centro de datos

AAF-2: Establecer las medidas de seguridad física

Descripción	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos de la dependencia o entidad y establecer las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.
Factores Críticos	1. Definir e implementar una política de seguridad física y las medidas de control de acceso de los centros de datos. 2. Limitar el acceso a la información sensible de los centros de datos, de acuerdo a la estrategia de seguridad. Diseñar las medidas de seguridad física tomando en consideración los riesgos asociados a la naturaleza de la dependencia o entidad y su operación. 3. Probar y documentar las medidas de seguridad física, preventivas, correctivas y de detección de eventos e incidentes para verificar diseño, implementación y efectividad. 4. Retirar, transportar y almacenar el equipo de forma segura. 5. Asegurar que se elimine toda la información de los dispositivos de almacenamiento que dejarán de ser utilizados y destruidos. 6. Asegurar que todos los dispositivos de almacenamiento fijos removibles y externos se apeguen a la estrategia de seguridad. 7. Asegurar que todos los incidentes sobre la seguridad física, sean registrados, supervisados, administrados, reportados y resueltos. • Estas actividades deberán estar alineadas a lo señalado en el proceso de operación de la mesa de servicios.
Relación de productos	• Medidas de seguridad física de los centros de datos

AAF-3: Controlar el acceso físico

Descripción	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades de la dependencia o entidad, incluyendo las salidas de emergencia.
Factores Críticos	1. Definir e implementar un mecanismo para controlar y registrar el acceso físico. • Administrar las solicitudes y la concesión del acceso a las instalaciones de cómputo. • Asegurar que los perfiles de acceso estén actualizados. • Registrar y monitorear todos los puntos de acceso a los centros de datos. • Definir un método y/o sistema de monitoreo. 2. Vigilar que todo el personal propio o externo cumpla con la estrategia de seguridad. Restringir el acceso a los centros de datos sensibles, estableciendo restricciones de perímetro. 3. Asegurar que el personal cuenta con el entrenamiento necesario para asegurar la seguridad física. • Estas actividades deberán estar alineadas a lo señalado en el proceso de integración y desarrollo del personal.
Relación de productos	• Procedimientos de acceso físico al centro de datos • Registros de acceso al centro de datos

AAF-4: Establecer la protección contra riesgos

Descripción	Diseñar e implementar medidas de protección contra riesgos.
Factores Críticos	1. Identificar posibles riesgos así como aquellas amenazas causadas por desastres naturales y provocados por el hombre, que pueden ocurrir en el área en la cual están situadas las instalaciones de TIC. 2. Identificar cómo el equipo de TIC, incluyendo el equipo móvil y fuera de sitio, se protege contra riesgos y amenazas ambientales. 3. Situar y construir las instalaciones de TIC para minimizar y mitigar la vulnerabilidad a los riesgos y las amenazas ambientales • Asegurar que los centros de datos se construyan y diseñen para minimizar el impacto de los riesgos ambientales de acuerdo a su ubicación geográfica. 4. Monitorear y mantener en forma periódica los dispositivos que detectan amenazas ambientales y para responder a las alarmas ambientales y a otras notificaciones • Deben instalarse dispositivos y equipo especializado para monitorear y controlar las alertas asociadas al medio ambiente. 5. Comparar las medidas y los planes de contingencia contra los clausulados y requisitos de las pólizas de seguro, cuando aplique. 6. Mantener el centro de datos y los cuartos de servidores en condiciones aptas y seguras.
Relación de productos	• Medidas de protección contra riesgos

AAF-5: Administrar las instalaciones físicas

Descripción	Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y de la dependencia o entidad, las especificaciones del proveedor y los lineamientos de seguridad y salud.
Factores Críticos	1. Cumplir con los requerimientos para la protección contra condiciones ambientales, descargas atmosféricas, fluctuaciones de la energía y sobrecargas eléctricas de las instalaciones de TIC, en conjunto con otros requerimientos de continuidad de la dependencia o entidad. 2. Probar y mantener los mecanismos de suministro de energía ininterrumpible (UPS) y asegurar que el suministro se puede cambiar directamente a la línea comercial o generador sin ningún efecto significativo sobre operaciones de la dependencia o entidad. 3. Asegurar que las instalaciones para alojar las soluciones tecnológicas de TIC tengan más de un suministro de energía. • Verificar que los cableados horizontales y verticales así como acometidas externas de los centro de datos estén instalados de acuerdo a las normas y políticas de seguridad establecidas. 4. Proveer sistemas de cableados con esquemas de redundancia y alta disponibilidad para alojar sistemas que así lo requieran. Asegurar que los centros de datos y las instalaciones estén en conformidad con las leyes relevantes de salud y de seguridad, regulaciones, pautas, y especificaciones del vendedor. 5. Capacitar al personal en leyes de salud y de seguridad, regulaciones, y pautas relevantes. 6. Asegurar que todos los incidentes sobre la seguridad física, sean registrados, supervisados, administrados, reportados y resueltos. Estas actividades deberán estar alineadas a lo señalado en el proceso de operación de la mesa de servicios. 7. Asegurar que los centros de datos y equipo se mantienen operando conforme a los parámetros y especificaciones de servicio requeridos por el proveedor, además de verificar la vigencia de las garantías y contratos de servicios. 8. Elaborar y cumplir con un programa de mantenimiento y actualización de acuerdo a los requerimientos de los activos y las necesidades de aprovisionamiento de infraestructura. Analizar las alteraciones físicas de los centros de datos o las premisas para volver a examinar el riesgo ambiental.
Relación de productos	• Solicitudes de soporte relativas a incidentes de AAF actualizadas

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.11.2.2.3 Descripción de roles

Rol	Descripción
Administrador del proceso de Administración de ambiente físico	Es responsable de definir, establecer y aplicar las mejoras al proceso de Administración del ambiente físico.

7.11.2.2.4 Descripción de productos

Producto	Descripción
Especificaciones del centro de datos	Contiene las características físicas que debe tener el centro de datos de la dependencia o entidad.
Medidas de seguridad físicas de los centros de datos	Contiene las medidas de seguridad física y de control de acceso de los centros de datos.
Procedimientos de acceso físico al centro de datos	Contienen los elementos necesarios para controlar el acceso físico del centro de datos, y en los cuales se deben administrar las solicitudes y la concesión del acceso a las instalaciones de cómputo, los perfiles de acceso y los puntos de acceso.
Registros de acceso al centro de datos	Documento donde se lleva el registro y control de las personas que acceden al centro de datos.
Medidas de protección contra riesgos	Contiene las medidas de cómo el equipo de TIC se protege contra los riesgos identificados en el proceso de administración de riesgos de TIC incluyendo amenazas por factores ambientales.
Solicitudes de soporte relativas a incidentes de administración de ambiente físico actualizadas	Actualización de las solicitudes de soporte relativas a de los incidentes que ocurren en las instalaciones del centro de datos.

7.11.2.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de cumplimiento de las políticas de seguridad física	Asegurar que el centro de datos de la UTIC cumpla con las medidas de seguridad física establecidas	Indicador que muestra el grado en que el centro de datos de la UTIC cumple con las políticas de seguridad	Eficiencia	De gestión	Número de medidas con las que se cumple/número de medidas totales verificadas	Titular de la UTIC	Semestral

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
		física					
Índice de incidencias en seguridad física que afectan la operación	Evitar que los servicios del centro de datos se afecten por aspectos de seguridad física	Indicador que muestra el grado en que el centro de datos de la UTIC es afectado por carecer de medidas de seguridad física	Eficiencia	De gestión	Número de incidencias de seguridad física/número de incidencias totales	Titular de la UTIC	Mensual

7.11.2.4 Reglas del proceso

1.1	La UTIC es la responsable de diseñar y generar las especificaciones de un centro de datos que permita soportar la estrategia de TIC ligada a la estrategia de la dependencia o entidad.
1.2	La UTIC es la responsable de establecer y operar un centro de datos con la capacidad para soportar la infraestructura tecnológica y los servicios de TIC.
1.3	La UTIC deberá designar un Administrador del proceso de Administración de ambiente físico.
1.4	El Administrador del proceso de Administración de ambiente físico deberá asegurar que se realicen las actividades periódicas de mantenimiento al ambiente físico de TIC, a fin de mantener operando los servicios de manera adecuada.
1.5	El Administrador del proceso de Administración de ambiente físico deberá asegurar que se han establecido los mecanismos de control para garantizar la seguridad del centro de datos.
1.6	El Administrador del proceso de Administración de ambiente físico deberá asegurar que se han establecido los mecanismos que mitiguen los riesgos de falla causados por factores ambientales.
1.7	El Administrador del proceso de Administración de ambiente físico deberá asegurar que se han establecido los controles suficientes para el acceso al centro de datos y a los activos de TIC que ahí se resguarden.
1.8	Se deberán realizar de manera periódica revisiones de los mecanismos de control y de seguridad a fin de evaluar su efectividad para garantizar la seguridad y el correcto funcionamiento del centro de datos.
1.9	El Administrador del proceso de Administración de ambiente físico es responsable del cumplimiento de las sentencias de aplicabilidad de seguridad de la información de la dependencia o entidad.
1.10	La UTIC asegurará que se mantenga la temperatura óptima de operación de los equipos de comunicaciones a través de aire acondicionado y evitar fallas por altas temperaturas.

7.11.2.5 Documentación soporte del proceso

No aplica

7.11.3. Mantenimiento de infraestructura

7.11.3.1. Objetivos del proceso

General.-

Adquirir, instalar y mantener actualizada la infraestructura tecnológica para garantizar la continuidad de los servicios de TIC

Específicos.-

1. Establecer un plan de adquisición de tecnología alineado con los planes de tecnología y de capacidad de los recursos de TIC.
2. Adquirir y mantener una infraestructura de TIC integrada y estandarizada.

7.11.3.2 Descripción del proceso

7.11.3.2.1 Mapa general del proceso

Diagrama de flujo de información

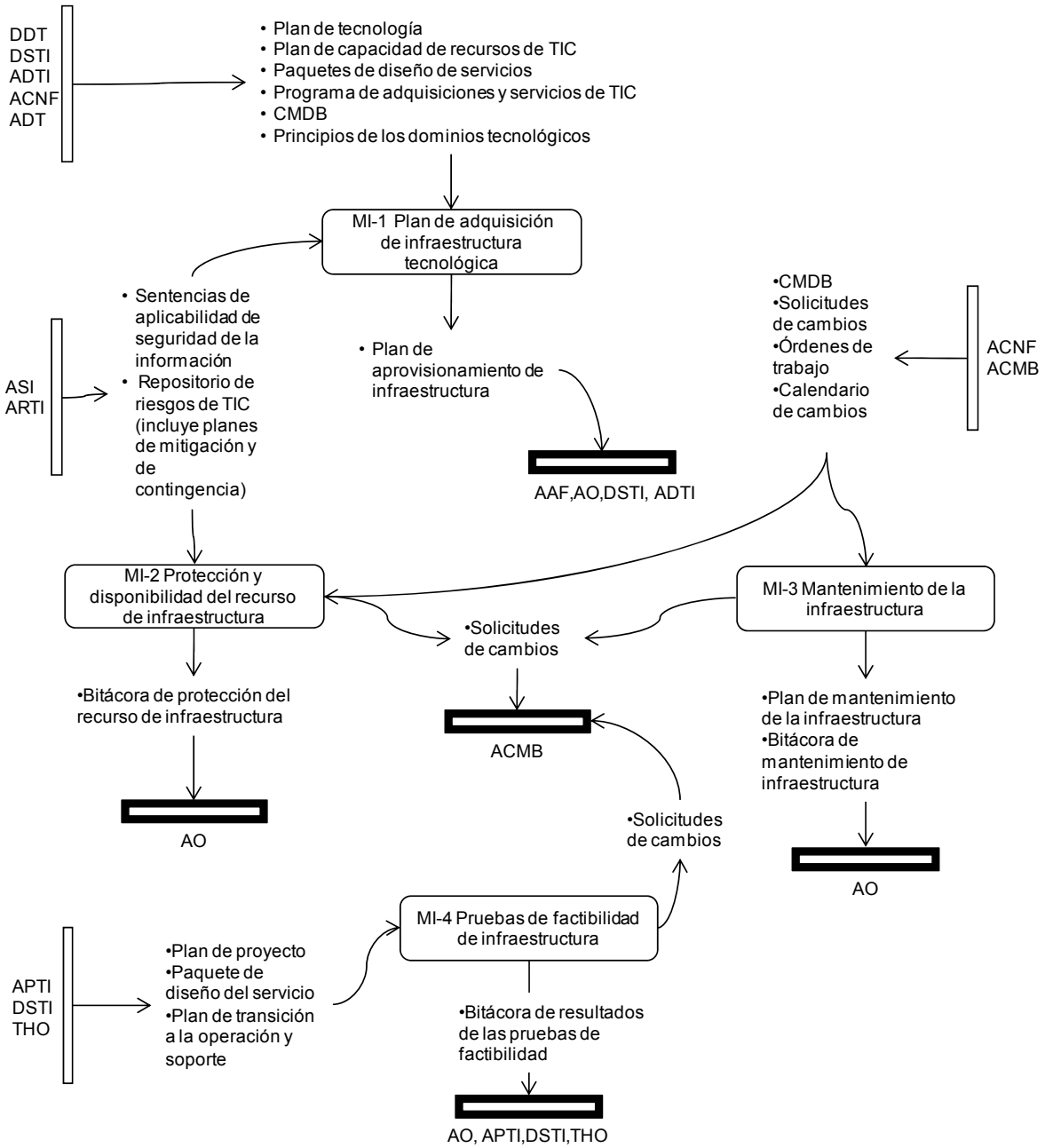
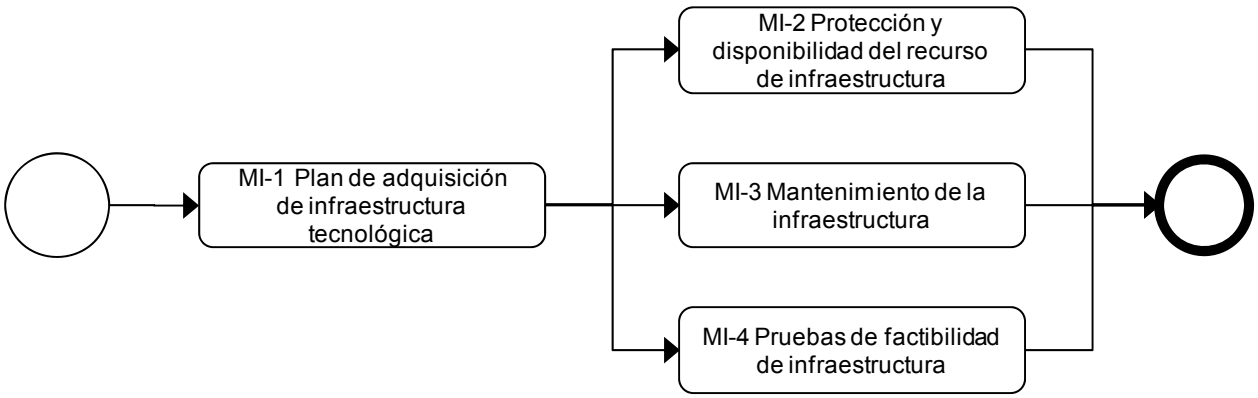


Diagrama de flujo de actividades



7.11.3.2.2 Descripción de las actividades del proceso

MI-1: Plan de adquisición de infraestructura tecnológica

Descripción	Generar un plan para adquirir e implementar la infraestructura tecnológica de acuerdo con la dirección tecnológica de la dependencia o entidad. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.
Factores Críticos	1. Contar con un plan de adquisiciones de infraestructura y darle seguimiento. Asegurar que el plan cuenta con una evaluación del estado financiero así como el ROI durante el ciclo de vida de la infraestructura. 2. Monitoreo y control de los planes para el aprovisionamiento. 3. Establecer un proceso de soporte y mejora continua de la infraestructura tecnológica. 4. Evaluar los planes de adquisición considerando los riesgos, costos, beneficios y el cumplimiento a los estándares de tecnología. Cualquier desviación deberá ser autorizada por el grupo de trabajo de arquitectura tecnológica.
Relación de productos	• Plan de aprovisionamiento de infraestructura

MI-2: Protección y disponibilidad del recurso de infraestructura

Descripción	Implementar medidas de control interno, seguridad y auditoria durante la configuración, implementación y mantenimiento de componentes de la infraestructura para proteger los recursos.
Factores Críticos	1. Asegurar que se establezcan los controles de riesgos establecidos en el sistema de gestión de la seguridad de la información (SGSI ver proceso ASI). Asegurar que los controles de riesgos consideren entre otros: • Respaldar y proteger todos los datos de infraestructura y software antes de la instalación o de las tareas de mantenimiento. • Validar ambiente de la aplicación. o Comprobar si el ambiente de desarrollo y pruebas de la aplicación está separado, pero lo suficientemente similar a la producción para comprobar la funcionalidad y establecer su seguridad, la disponibilidad o las condiciones de integridad. Esto asegura que operen adecuadamente y cumplan con los requisitos establecidos en el aprovisionamiento y el mantenimiento de la infraestructura de tecnología. • Aplicar procedimientos de aceptación usando criterios de aceptación objetivos para garantizar que el rendimiento del producto (incluida la seguridad y funcionalidad) es consistente con las especificaciones acordadas y/o requerimientos de nivel de servicio. • Evaluar todos los aspectos de seguridad asociados con la instalación del sistema y mantenimiento de procesos. o Monitorear la modificación de contraseñas originales asignadas por proveedores de servicios, acceso temporal para instalación y la configuración

	de parámetros que pueden afectar la seguridad, como establecer la configuración por defecto de los parámetros. • Controlar movimientos de programas, software y datos entre los repositorios para asegurar que son ejecutados por un grupo independiente. o Revisar el proceso para asegurar que la instalación del software se desempeña de acuerdo con las directrices del proveedor y cualquier desviación se discute con el vendedor para evaluar un impacto potencial. o Monitorear el registro de acceso y mantenimiento de componentes sensibles de la infraestructura, y asegurar que estos se revisan periódicamente, así como las licencias apropiadas de software que son probadas e instaladas. 2. Dar seguimiento a la implantación de los planes de mitigación de riesgos establecidos en el proceso de Administración de riesgos de TIC relativos a componentes de infraestructura. 3. Comunicar claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos involucrados en las actividades de configuración, implementación y mantenimiento. 4. Registrar las actividades de protección y de mitigación de riesgos ejecutadas.
Relación de productos	• Bitácora de protección del recurso de infraestructura • Solicitudes de cambio

MI-3: Mantenimiento de la infraestructura

Descripción	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el proceso de administración de cambios de la dependencia o entidad. Establecer un mecanismo para efectuar la revisión de la infraestructura contra las necesidades de los servicios de TIC, administración de actualización de versiones o corrección de defectos y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
Factores Críticos	1. Establecer una estrategia y un plan de mantenimiento de la infraestructura para proporcionar orientación general en correspondencia con los procedimientos de administración de cambios de la dependencia o entidad. 2. Asegurar que se ejecute el mantenimiento de infraestructura. 3. Asegurar que el mantenimiento del software del sistema instalado (actualización de versiones o corrección de defectos, y otras actualizaciones) se gestiona mediante el establecimiento de procesos de administración del cambio y se realiza en conformidad con los procedimientos y directrices correspondientes. 4. Establecer la gestión de la documentación que sirve como referencia del mantenimiento realizado, con el objetivo de analizar la existencia de vulnerabilidades dentro de la infraestructura. 5. Revisar sobre una base regular la cantidad de mantenimiento que se realiza y la vulnerabilidad de la infraestructura no compatible; considerar los riesgos futuros, incluyendo vulnerabilidades de seguridad. Informar de cualquier problema identificado para su consideración en el proceso de planificación de la gestión de incidencias.

Relación de productos	• Plan de mantenimiento de la infraestructura • Bitácora de mantenimiento de infraestructura • Solicitudes de soporte relativas a incidentes de mantenimiento

MI-4: Pruebas de factibilidad de infraestructura

Descripción	Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Esto incluye la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de las versiones, datos y herramientas de prueba y seguridad.
Factores Críticos	1. Diseñar un enfoque acorde con la tecnología de los planes estratégicos que permitan la creación y simulación de ambientes adecuados para verificar la viabilidad de las adquisiciones previstas o desarrollos. Considere la posibilidad de que sea en sitio y también opciones externas, incluidas las visitas de referencia, laboratorios de pruebas de proveedores, creación de prototipos, los pilotos de modelos, y prueba de concepto de la evolución, en función de la complejidad, los aspectos prácticos y los costos. 2. Crear un entorno de prueba que considere la funcionalidad, configuración de hardware y de software, integración y pruebas de rendimiento, la migración entre los entornos, control de versión, datos de prueba, herramientas, y seguridad.
Relación de productos	• Bitácora de resultados de las pruebas de factibilidad • Solicitudes de cambios

TIEMPO TOTAL DEL PROCESO: VARIABLE

7.11.3.2.3 Descripción de roles

Rol	Descripción
Administrador del mantenimiento a infraestructura	Responsable de administrar las actividades de mantenimiento de la infraestructura de la dependencia o entidad.

7.11.3.2.4 Descripción de productos

Producto	Descripción
Plan de mantenimiento de infraestructura	Este plan contiene todas las tareas necesarias para prevenir los principales fallos que puede tener la instalación de algún elemento de la infraestructura. El plan de mantenimiento es un conjunto de tareas de mantenimiento agrupadas, y el objetivo de este plan es evitar la presencia de determinadas fallas.

Bitácora de mantenimiento de infraestructura	Registros de soporte y documentación de las actividades del mantenimiento efectuado a la infraestructura.
Bitácora de protección del recurso de infraestructura	Registros de las actividades de protección del recurso de infraestructura efectuadas.
Bitácora de resultados de las pruebas de factibilidad	Registros de los resultados del plan de pruebas para soportar las acciones a desarrollar con los elementos probados.
Solicitud de cambio	Formato para documentar el propósito y detalles de un cambio propuesto (ver proceso ACMB).
Solicitud de soportes relativas a incidentes de mantenimiento	Actualización de la información de las solicitudes de soporte relativas a incidentes que ocurran en el mantenimiento de infraestructura.
Plan de aprovisionamiento de infraestructura	Documento donde se establece la estrategia a seguir para adquirir e instalar infraestructura tecnológica de acuerdo a las necesidades de la dependencia o entidad, contiene: especificaciones funcionales, especificaciones técnicas, extensiones futuras de la infraestructura, costos, riesgos, vida útil, retorno de inversión y la fecha probable en que será requerida.

7.11.3.3 Indicadores:

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
Porcentaje de cumplimiento del Plan de mantenimiento de la infraestructura	Mantener una infraestructura operativa y actualizada	Indicador que muestra el porcentaje de cumplimiento del plan de mantenimiento, establecido para la infraestructura	Eficiencia	De gestión	Actividades realizadas/numero total de actividades	Responsable de mantenimiento de la UTIC	Mensual
Índice de actividades de mantenimiento con registro en el repositorio	Contar con información que permita identificar vulnerabilidades o riesgos	Indicador que muestra la cantidad de actividades del plan	Eficiencia	De gestión	Actividades con registro/numero total de actividades	Responsable de mantenimiento de la UTIC	Mensual

Nombre	Objetivo	Descripción	Dimensión	Tipo	Fórmula	Responsable	Frecuencia de cálculo
		de mantenimiento que cuentan con registros en el repositorio					

7.11.3.4 Reglas del proceso

1.1	Deberá generarse un plan de adquisición de infraestructura y un plan de mantenimiento por cada dependencia o entidad con el objetivo de promover el desarrollo tecnológico.
1.2	La dependencia o entidad, deberá establecer e implementar el proceso de Mantenimiento de la infraestructura con el objetivo de prevenir fallas y/o errores tecnológicos
1.3	Las dependencias o entidades deberán definir los indicadores pertinentes para este proceso. Una vez definido el catálogo de servicios.
1.4	La UTIC y las UR son las áreas facultadas para establecer las especificaciones técnicas de las bases de licitación para contratar los servicios de mantenimiento preventivo y correctivo que se aplicarán a la infraestructura de tecnología de información.
1.5	Las UTICS deberán elaborar un calendario de mantenimiento preventivo para proporcionar mantenimiento a los equipos de cómputo o comunicaciones, y evitar la ocurrencia de una falla parcial o total de cualquier equipo instalado en el centro de datos.
1.6	El mantenimiento correctivo requerido para solucionar fallas en los equipos de cómputo o de comunicaciones, ya sea que se trate de equipos en periodo de garantía o equipos bajo contrato administrado por la UTIC, invariablemente deberá reportarse al área resolutoria a través de mesa de servicios de la UTIC
1.7	La UTIC es responsable de proporcionar el soporte técnico a todos los usuarios y equipos de la dependencia o entidad, teniendo como respaldo el reporte de mesa de ayuda o su equivalente.
1.8	La UTIC es responsable de contar con la infraestructura y herramientas necesarias para proporcionar soporte técnico a los usuarios y equipos de cómputo.
1.9	La UTIC instalará los equipos multifuncionales, o impresoras, copiadoras y escáneres dentro de la red institucional, de manera que puedan ser compartidas por múltiples usuarios. Configurará el acceso al servicio de los equipos multifuncionales de acuerdo a un perfil de usuario y grupo de trabajo de manera que lleve la contabilización de la utilización de los 3 servicios: impresión, fotocopiado y escaneo.
1.10	El personal facultado por la UTIC revisará que la sala dónde se instalará el equipo de videoconferencia cumple con las características necesarias.
1.11	El personal facultado por la UTIC instalará y configurará los equipos de videoconferencia de acuerdo a los parámetros indicados por la UTIC.

7.11.3.5 Documentación soporte del proceso

No aplica

8 ÓRGANOS COLEGIADOS

No aplica

9 ANEXOS/FORMATOS

ANEXO I

SOLICITUD DE CERTIFICADO DIGITAL DE FIRMA ELECTRONICA AVANZADA
ANVERSO DE LA SOLICITUD DE CERTIFICADO DIGITAL DE FIRMA ELECTRONICA AVANZADA
1. CLAVE UNICA DE REGISTRO DE POBLACION DEL SOLICITANTE:

_____
2. REGISTRO FEDERAL DE CONTRIBUYENTES DEL SOLICITANTE:

_____
3. NOMBRE DEL SOLICITANTE:

_____
Primer apellido Segundo apellido Nombre(s)
4. DOMICILIO DEL SOLICITANTE:
CALLE _____
NUMERO INTERIOR _____
NUMERO EXTERIOR _____
COLONIA _____
CODIGO POSTAL _____
ENTIDAD FEDERATIVA _____
5. DOCUMENTO DE IDENTIDAD QUE PRESENTA:
_____ CARTILLA DEL SERVICIO MILITAR NACIONAL
_____ PASAPORTE EXPEDIDO POR LA SECRETARIA DE RELACIONES EXTERIORES
_____ CEDULA PROFESIONAL
_____ CREDENCIAL DE ELECTOR
_____ IDENTIFICACION EXPEDIDA POR EL GOBIERNO FEDERAL, ESTATAL O MUNICIPAL, INCLUYENDO EL GOBIERNO DEL DISTRITO FEDERAL, QUE CUENTE CON FOTOGRAFIA, FIRMA Y CURP DEL TITULAR.
6. DOCUMENTO PROBATORIO DE IDENTIDAD QUE PRESENTA:
_____ COPIA CERTIFICADA DEL ACTA DE NACIMIENTO
_____ DOCUMENTO MIGRATORIO
_____ CARTA DE NATURALIZACION
_____ CERTIFICADO DE NACIONALIDAD MEXICANA
FIRMA DEL SOLICITANTE.

_____
REVERSO DE LA SOLICITUD DE CERTIFICADO DIGITAL DE FIRMA ELECTRONICA AVANZADA
TERMINOS:
El suscrito, cuyos datos generales aparecen al anverso de la presente solicitud de Certificado Digital de Firma Electrónica Avanzada, y a quien en lo sucesivo se le denominará como “El Solicitante” para todos los efectos legales que deriven del presente documento a que haya lugar, manifiesta ante ***<poner aquí el nombre de la dependencia>*,** a quien en lo sucesivo se le denominará como “La Agencia o Autoridad Certificadora” (AC), que es su libre voluntad contar con un Certificado Digital de Firma Electrónica Avanzada en el que conste la clave pública que se encuentra asociada a la clave privada y frase de seguridad que manifiesta haber generado previamente y en absoluto secreto, sin que persona alguna lo haya asistido durante dicho proceso.
• Asimismo manifiesta su conformidad en que “La AC” utilice el procedimiento de certificación de identidad que estime conveniente.

• “La AC” manifiesta que los datos personales recabados de “El Solicitante” durante su comparecencia serán protegidos, incorporados y tratados en el sistema ***<poner aquí el nombre del sistema de enrolamiento>*****,** con fundamento en ***<poner aquí fundamento legal>*****,** y cuya finalidad es garantizar el vínculo que existe entre un Certificado Digital de Firma Electrónica Avanzada y su titular, el cual fue registrado en el “Listado de Sistemas de Datos Personales” ante el Instituto Federal de Acceso a la Información Pública (www.ifai.gob.mx), y serán transmitidos al Registro Nacional de Población, para la conformación del “Sistema Integral del Registro Nacional de Población”.
• La Unidad Administrativa responsable de este sistema es ***<poner nombre aquí>***. “El Solicitante” podrá ejercer los derechos de acceso y corrección de datos a través de ***<poner aquí el mecanismo o ubicación del inmueble en donde se pueden ejercer estos derechos>*****.** Lo anterior se informa en cumplimiento del DECIMO SEPTIMO de los “Lineamientos de Protección de Datos Personales”, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.
• “El Solicitante” reconoce que para la emisión del referido Certificado Digital de Firma Electrónica Avanzada, “La AC” revisó la documentación que se indica en el anverso de este documento, con la cual el propio usuario se identificó, constatando a simple vista que los documentos corresponden a los rasgos fisonómicos y caligráficos de “El Solicitante”, por lo que este último asume la responsabilidad exclusiva respecto de la autenticidad de los datos y documentación por él proporcionada a “La AC”. De la misma forma “El Solicitante” asume la responsabilidad exclusiva del debido uso del Certificado Digital de Firma Electrónica Avanzada.
• “El Solicitante” en este acto acepta el certificado digital mencionado, sirviendo este documento como el acuse de recibo más amplio que en derecho proceda.
• Adicionalmente, “El Solicitante”, acepta que el uso de la clave privada y frase de seguridad con base en las cuales dicho certificado fue elaborado, quedarán bajo su estricta y absoluta responsabilidad, la cual incluye en forma enunciativa, los daños y perjuicios, incluso aquéllos de carácter financiero, que pudieran causarse por su uso indebido, no pudiendo alegar que tal uso se realizó por persona no autorizada.
• “El Solicitante” conoce y acepta que la clave pública proporcionada por él y contenida en el Certificado Digital de Firma Electrónica Avanzada, así como en cualquier otro certificado digital que con posterioridad se obtenga, será de carácter público y podrá ser consultada libremente por cualquier interesado a través de los medios y formas que disponga “La AC”.
• Por lo anterior, “El Solicitante” se obliga a mantener absoluta confidencialidad respecto de las aludidas clave privada y frase de seguridad, así como a realizar los trámites necesarios para la revocación de dicho certificado ante “La AC”, mediante los mecanismos y procedimientos que el mismo establezca, en el evento de que por cualquier causa dicha información sea divulgada o se realice cualquier supuesto por el que “El Solicitante” deba solicitar su revocación en los términos de las disposiciones legales vigentes.
• Por otra parte “El Solicitante” manifiesta conocer el contenido y alcance de las disposiciones legales y reglamentarias relativas a la celebración de actos jurídicos mediante el uso de medios electrónicos, digitales o de cualquier otra tecnología, por lo que asume plena responsabilidad respecto de la información y contenido de todo documento electrónico o digital elaborado y enviado en el que se haga uso de la citada clave privada, toda vez que por ese solo hecho se considerara que el documento electrónico o digital le es atribuible.
• “El Solicitante” reconoce y acepta que “La AC” únicamente es responsable de los errores que, en su caso, llegaren a cometer con motivo de culpa grave en el proceso de generación, registro, entrega y revocación del certificado digital, según corresponda, así como que no será responsable por los daños y perjuicios que se pudieran causar a “El Solicitante” o a terceros, cuando por caso fortuito o fuerza mayor no puedan realizarse registros, verificaciones, revocaciones o tramitar documentos electrónicos cifrados con las claves públicas y privadas relacionadas con dicho certificado. Por caso fortuito o fuerza mayor se entenderá todo acontecimiento o circunstancia inevitable, más allá del control razonable de “La AC”, que le impida el cumplimiento de sus funciones con el carácter que le corresponde y reconoce a través de su firma autógrafa asentada en el espacio designado para ello en el anverso y reverso de este formato, al presente como prueba fehaciente de la aceptación de todo lo especificado en el mismo.

CONDICIONES:

• El Certificado Digital que se genere derivado de la realización de este trámite, estará disponible en ***<poner aquí dirección electrónica>*;** para que "El Solicitante" realice la descarga del mismo.
• La Firma Electrónica Avanzada asignada es personal e intransferible y el uso de la misma es responsabilidad de la persona que la solicite.
• La Firma Electrónica Avanzada tendrá los mismos alcances y efectos que la firma autógrafa.
• Con esta firma podrá hacer uso de servicios y trámites electrónicos disponibles en las Dependencias, Entidades, Organizaciones e Instituciones.
• "El Solicitante" será responsable de las obligaciones derivadas del uso no autorizado de su firma.
• "El Solicitante" acepta que deberá notificar oportunamente a "La AC", la invalidación, pérdida o cualquier otra situación que pudiera implicar la reproducción o uso indebido de su clave privada.
• "El Solicitante" acepta las condiciones de operación y límites de responsabilidad de ***<poner aquí el nombre de la dependencia>*** en su calidad de "La AC" que se encuentran disponibles en la dirección electrónica ***<poner aquí la dirección electrónica>*** para su consulta.

INSTRUCCIONES DE LLENADO:

1. Clave Única de Registro de Población (CURP):
Se deberá anotar la clave única de registro de población.

2. Registro Federal de Contribuyentes (RFC):
Se deberá anotar la clave del RFC a trece posiciones.

3. Nombre del Solicitante:
Deberá anotar su nombre empezando por el primer apellido, segundo apellido y nombre[s].

4. Domicilio del Solicitante:
Indicará en este rubro el domicilio en el que actualmente reside el solicitante.

5. Documento de Identidad.
Indicar el Documento de Identidad que se presenta.

6. Documento Probatorio de Identidad
Indicar el Documento Probatorio de Identidad que se presenta.

FIRMA DEL SOLICITANTE

_____

A N E X O II

COMPROBANTE DE EMISION DE CERTIFICADO DIGITAL DE FIRMA ELECTRONICA AVANZADA

<Imprimir aquí el nombre de la Agencia o Autoridad Certificadora (AC) aquí> certifica que el Solicitante: ***<<Imprimir aquí nombre del Solicitante>*,** entregó un requerimiento de certificación que contiene la solicitud para la generación de su Certificado Digital de Firma Electrónica Avanzada.
Estando presente el Solicitante se llevó a cabo el procedimiento de emisión y registro de certificados digitales de conformidad con lo establecido en las disposiciones de firma electrónica avanzada de este manual, al respecto de la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal publicado en el Diario Oficial de la Federación el ***<Imprimir fecha aquí>***.

Asimismo, que como resultado del proceso se generó su Certificado Digital con número de serie: ***<Imprimir aquí número de serie>*** y clave pública: ***<Imprimir clave pública en cadena de caracteres>****.*

Previo a la emisión del presente certificado, el titular reconoce haber leído y aceptado los Términos y Condiciones de uso establecidos en el anverso del formato "Solicitud de Certificado Digital de Firma Electrónica Avanzada".

El resguardo de la clave privada relacionada con el certificado amparado por el presente Acuse, así como su medio de almacenamiento, es responsabilidad del titular del Certificado Digital.

_____

Firma de conformidad
Nombre: *<Imprimir nombre del Solicitante aquí>*
CURP: *<Imprimir CURP> aquí*
RFC: *<Imprimir RFC aquí>*
<Imprimir aquí el nombre de la AC que emite el certificado> a ***<Imprimier fecha aquí>***

NOTA: Para descargar posteriormente su certificado digital, deberá acceder a la dirección electrónica:
<Imprimir dirección aquí>

A N E X O III

COMPROBANTE DE REVOCACION DE CERTIFICADO DIGITAL DE FIRMA ELECTRONICA AVANZADA

<Imprimir el nombre de la Agencia o Autoridad Certificadora (AC) aquí> certifica que el Titular: ***<<Imprimir aquí nombre del Titular>***, solicitó la revocación de su Certificado Digital con número de serie: ***<<Imprimir aquí número de serie>*** y clave pública: ***<<Imprimir clave pública en cadena de caracteres>*** de conformidad de conformidad con lo establecido en las disposiciones de firma electrónica avanzada del presente manual, al respecto de la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal publicado en el Diario Oficial de la Federación el ***<Imprimir fecha aquí>****.*
Por consiguiente, ***<Imprimir el nombre de la Agencia o Autoridad Certificadora (AC) aquí>*** llevó a cabo la revocación del referido Certificado Digital, siendo las <***Imprimir hora aquí>*** del ***Imprimir fecha aquí****>.*

_____

Firma de conformidad
Nombre: *<Imprimir nombre del Titular aquí>*
CURP: *<Imprimir CURP aquí>*
RFC: *<Imprimir RFC aquí*>

8.1. Relativos al marco rector de procesos del presente manual.

Materiales de referencia de las mejores prácticas de TIC empleadas:

- COBIT ®, marca registrada del IT Governance Institute (www.itgi.org)
- ITIL ®, marca registrada ante el Office of Government Commerce. (UK) (www.itil.co.uk)
- CMMI ®, marca registrada ante el U.S. Patent and Trademark Office por Carnegie Mellon University. (www.sei.cmu.edu/cmmi/)
- TOGAF©, The Open Group Architecture Framework /TOGAF, copyright del The Open Group (www.opengrouop.org)
- RISK-IT ®, marca registrada del IT Governance Institute (www.itgi.org)
- VAL-IT ®, marca registrada del IT Governance Institute (www.itgi.org)
- ISO/IEC 27001©, estándar de la International Organization for Standardization (www.iso.org
- ISO 9001:2000©, estándar de la International Organization for Standardization (www.iso.org), norma internacional de calidad
- The Standard for Portafolio Management ©, Copyright del Project Management Institute (PMI)

- Project Management Body of Knowledge (PMBoK®) Guide, marca registrada del Project Management Institute
- BSC, Cuadro de mando integral, (Balanced Scorecard)
- ISO/IEC 20000:2005, norma internacional para gestión de servicio de TIC
- MOPROSOFT, modelo de procesos para la industria mexicana de desarrollo y mantenimiento de Software

Descripción general breve de las mejores prácticas:

En el diseño de las actividades de los procesos del marco rector de procesos de este manual se tomaron como base un conjunto de mejores prácticas y modelos de referencia que fueron unificados y adecuados a las circunstancias de la APF.

A continuación se describen brevemente mas mejores prácticas y se enuncian los procesos del marco rector de procesos que se encuentran dentro del ámbito de influencia de la mejor práctica.

Modelo Rector	Descripción general
CMMI ® **marca registrada ante el U.S. Patent and Trademark Office por Carnegie Mellon University. (www.sei.cmu.edu/cmmi/)**	El modelo CMMI (Capability Maturity Model Integration) es una guía para la mejora de procesos que provee a la organización una descripción de los elementos esenciales para el desarrollo de procesos efectivos; es una recolección de las mejores prácticas para el desarrollo, y mantenimiento de servicios y productos de software. El objetivo de CMMI es establecer una guía que permita a las organizaciones mejorar sus procesos y su habilidad para organizar, desarrollar, adquirir y mantener productos y servicios del área de TI. El CMMI tiene una suite de productos complementarios que cubre las necesidades del área de TI como los son el desarrollo de aplicaciones (CMMI-DEV) y los procesos de adquisición (CMMI-ACQ) de servicios de TI. En el núcleo común a todos estos modelos se encuentran las áreas de procesos que contiene las mejores prácticas para la gestión de proyectos, la gestión de los procesos organizacionales, y las relacionadas con las actividades de soporte; las cuales tienen como objetivo asegurarse de salvaguardar los productos/servicios desarrollados por la organización en sus diferentes proyectos, el aseguramiento de la calidad de los productos y procesos y el establecimiento y recolección de las métricas que permitan conocer el nivel de cumplimiento de los objetivos. El CMMI-DEV es el modelo de procesos para la mejora y evaluación de de la capacidad de los procesos de una organización que desarrolla y da mantenimiento a software. Especifica los procesos de desarrollo de soluciones tecnológicas desde la perspectiva de la organización que desarrolla. El CMMI-ACQ es el modelo de procesos que guía a las organizaciones en la gestión de la adquisición de productos y servicios, el modelo se centra en desarrollar las capacidades de los procesos de una organización que adquiere servicios de desarrollo de software. El modelo se centra en el proceso de compra e integra los cuerpos de conocimiento que son esenciales para que las adquisiciones resulten exitosas, utilizando las mejores prácticas desde la concepción de la compra, establecimiento de los requisitos necesarios, los acuerdos requeridos con el proveedor, conducir la adquisición, evaluar el progreso y los productos/servicios resultantes, los proceso para ejecutarlo así como su aceptación, transición y liberación. Este modelo complementa al CMMI-DEV al especificar los procesos desde la perspectiva del comprador.

	Ámbito de Influencia en el marco rector • En el contexto del marco rector de Procesos de TIC, El **CMMI-DEV** fue usado como referencia primaria para la selección de las prácticas clave y factores críticos de los procesos de desarrollo de soluciones tecnológicas **y calidad de soluciones tecnológicas.** • **CMMI-ACQ** fue usado como referencia primaria para la selección de las prácticas clave y factores críticos de los procesos de **administración de proveedores, administración de adquisiciones y administración técnica de adquisiciones.**
COBIT® **RISK-IT®** **VAL-IT®** **marcas registradas del IT Governance Institute (www.itgi.org)**	**Descripción** **COBIT (Control Objectives for Information and related Technology).** Es el marco aceptado internacionalmente para el control de la información, la función de TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de TI y mejorar los controles de TI. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez. COBIT está conformado por cuatro dominios, cada uno de los cuales están organizados en procesos (34 en total) que su vez se sub-dividen en actividades y objetivos de control. Por cada proceso COBIT detalla objetivos, indicadores de desempeño, mediciones de resultado, roles y responsabilidades. COBIT asegura que la función de TI sustenta y extiende los objetivos estratégicos de la organización. El ITGI reconoce que para implementar COBIT es necesario complementarlo con mejores prácticas que prescriben cómo manejar áreas específicas de la función de TI. Consciente de esta necesidad los objetivos y prácticas de control de COBIT fueron diseñados para armonizar con los estándares y mejores prácticas de referencia para la gestión de TI. Todos los estándares seleccionados como Modelos Rectores, enunciados en esta tabla, se encuentran dentro de la selección de estándares de COBIT una descripción detallada de cómo se relacionan con COBIT se puede consultar en el documento *COBIT Mapping Overview of International IT Guidance, 2nd Edition* disponible en la página Internet del ITGI. El ITGI ha publicado una serie de documentos que complementan COBIT, en particular para el diseño del marco rector fueron considerados: • VAL-IT: Documento que detalla las mejores prácticas para la gestión de las inversiones en TI. • RISK-IT: Documento que detalla las mejores prácticas para la gestión de riesgos de TI. **Ámbito de Influencia en el marco rector** • **COBIT** fue usado como referencia primaria para la selección de las prácticas clave y los factores críticos de los procesos de, **los grupos de procesos de dirección y control.** De forma más general, COBIT fue usado como referencia secundaria en

	el diseño de las prácticas clave del resto de los procesos del marco rector. • **VAL-IT** fue usado como referencia secundaria para la selección de las prácticas clave y los factores críticos del proceso de **administración del portafolio de proyectos de TIC.** • **RISK-IT** fue usado como referencia secundaria para la selección de las prácticas clave y los factores críticos del proceso de **administración riesgos de TIC.**
ISO 9001© **Estándar de la International Organization for Standardization. (www.iso.org)**	**Descripción** El término ISO 9000 se refiere a una serie de normas internacionales referentes a Sistemas de Gestión de la Calidad desarrolladas por la Organización Internacional de Normalización (ISO) y adoptado por 90 países en todo el mundo. En particular la ISO 9001 es la norma que establece los requisitos para la certificación de Sistemas de Gestión de la Calidad. La ISO 9001 es el estándar de referencia mejor establecido para la gestión de procesos con foco en la efectividad y mejora continua basada en un modelo de mejora continua (Plan- Do – Check – Act). La versión que fue usada como referencia del marco rector de procesos de TIC es la versión 2008. **Ámbito de Influencia en el marco rector** • La norma **ISO 9001** fue usado como referencia secundaria para la selección de las prácticas clave y el diseño de los factores críticos de los grupos de procesos de **administración de procesos, administración de recursos y de control**.
ISO 27001© **Estándar de la International Organization for Standardization. (www.iso.org)**	**Descripción** La serie de normas ISO/IEC 27000 documentan las mejores prácticas para la gestión de la seguridad de la información. La norma ISO 27001 establece los requisitos para certificar al Sistema de Gestión de la Seguridad de la Información de una organización. Este marco de referencia establece las mejores prácticas para determinar los estándares de seguridad de aplicaciones. Establece los controles de seguridad que garantizan los niveles apropiados de confidencialidad, disponibilidad e integridad de la información. **Ámbito de Influencia en el marco rector** • La norma **ISO 27001** fue usada como referencia primaria para la selección de las prácticas clave y factores críticos de **procesos de administración de riesgos de TI y administración de la seguridad.**
ITIL® **marca registrada ante el Office of Government Commerce. (UK) (www.itil.co.uk)**	**Descripción** ITIL (Information Technology and Infraestructure Library) es el estándar más ampliamente conocido para la gestión de los servicios TI. Una correcta gestión de servicios permite un alto nivel de disponibilidad de dichos servicios y un alto nivel de satisfacción de clientes y empleados de una organización. ITIL se centra en brindar servicios de alta calidad para lograr la máxima satisfacción del cliente a un costo manejable. En otras palabras: determina la forma de ejecutar procesos estándar ayudados de la tecnología para lograr la satisfacción de las personas, usuarios de los servicios de TI. Ahora, con la versión 3 del modelo, se incorpora la gestión de servicios, desde una perspectiva de Ciclo de Vida, tomando como premisa los requerimientos y líneas

	estratégicas, para diseñar, transitar y operar los servicios conforme a lo necesita y plantea la organización. ITIL ha probado consistentemente su utilidad a escala mundial, iniciando por resolver temas de administración de infraestructura y operación, asegurando los procesos de cambios y configuraciones y realizando los mejores modelos para la administración de acuerdos de nivel de servicio **Ámbito de Influencia en el marco rector** • **ITIL** fue usado como referencia primaria para la selección de las prácticas clave y factores críticos de **los grupos de procesos de administración de servicios,** en **transición y entrega y operación de servicios.** En forma secundaria ITIL influyó en el diseño de los procesos de los grupos de **administración de activos y operaciones.**
Project Management Body of Knowledge (PMBoK®) Guide **marca registrada del *Project Management Institute*** **The Standard for Portafolio Management ©** **Copyright del *Project Management Institute***	**Descripción** El PMBOK es el modelo más difundido y aceptado para la administración de proyectos en general (no solo proyectos de TI). El Project *Management Institute* (PMI) es una organización sin fines de lucro dedicada a desarrollar la Disciplina de Administración de Proyectos en todo el mundo, tiene más de 112.000 miembros en 125 países. El PMBOK se basa en un conjunto de buenas prácticas divididas en 9 áreas de conocimiento, cada una de las cuales se sub-divide en procesos (siendo 42 en total). En su conjunto las prácticas de administración de proyectos permiten incrementar la probabilidad de que los proyectos terminen dentro de las restricciones de costo, tiempo y con la calidad especificada. **Ámbito de Influencia en el marco rector** • El **PMBoK** fue usado como referencia primaria para la selección de las prácticas clave y factores críticos del proceso de **administración de proyectos de TIC.** **Descripción** *The Standard for Portafolio Management* es emitido por el PMI. Contiene las mejores prácticas de administración de portafolios de inversiones asociadas a la inversión de programas/proyectos. Estas prácticas se refieren a la administración centralizada de programas y/o proyectos con el propósito de cumplir con los objetivos de una organización y maximizar el valor de la inversión. Las prácticas contenidas en este estándar le permiten a una organización identificar, priorizar, seleccionar, gobernar, monitorear y reportar el desempeño de los proyectos/programas que componen un portafolio y su alineación a los objetivos de la organización. **Ámbito de Influencia en el marco rector** • El ***Standard for Portafolio Management*** fue usado como referencia primaria para la selección de las prácticas clave y factores críticos del proceso de

	administración del portafolio de proyectos de TIC.
TOGAF© **The Open Group Architecture Framework /TOGAF) es copyright del The Open Group (www.opengrouop.org)**	**Descripción** TOGAF es un marco metodológico que refleja el consenso de la industria en las mejores prácticas para el desarrollo de una arquitectura empresarial. TOGAF fue desarrollada por miembros del *Open Group*. TOGAF provee las mejores prácticas para la creación y actualización de una arquitectura que proporciona a una organización el contexto tecnológico y de negocio que requiere para establecer y evolucionar su estrategia tecnológica que permite a su vez evolucionar sobre bases sólidas las soluciones tecnológicas y los servicios de TI en respuesta a las necesidades cambiantes y crecientes de la organización. **Ámbito de Influencia en el marco rector** • **TOGAF** fue usado como referencia primaria para la selección de las prácticas clave y factores críticos de los **procesos de determinar la dirección tecnológica y administración de dominios tecnológicos.**

10. VIGENCIA

El presente Manual tendrá vigencia a partir del día siguiente a su publicación en el DOF.

11. EMISOR, FECHA Y FIRMA

Dado en la Residencia Oficial de Los Pinos, el día ___ de _____ del año 2010.

FELIPE DE JESÚS CALDERÓN HINOJOSA, Presidente de los Estados Unidos Mexicanos, en ejercicio de la facultad que me confiere el artículo de la Constitución Política de los Estados Unidos Mexicanos, con fundamento en los artículos 11, 13, 17, 26 a 43, 48, 49 y 50 de la Ley Orgánica de la Administración Pública Federal, y

CONSIDERANDO

Que el Ejecutivo Federal a mi cargo ha emprendido un importante ejercicio para abatir el exceso de regulación que impera en la Administración Pública Federal, y está resuelto en avanzar consistentemente en la actualización del marco jurídico y con ello consolidar un régimen de certidumbre jurídica, en donde la plena eficacia de las normas aplicables a particulares y a gobernantes les garantice el ejercicio pleno de sus derechos y libertades;

Que en consecuencia la Administración Pública Federal Centralizada y Paraestatal, ha emprendido y deberá revisar a fondo el marco jurídico administrativo que rige tanto en su interior, como en sus relaciones con los particulares, con el propósito de identificar, analizar y determinar aquellas disposiciones cuya necesidad hoy día no es clara y en su caso, no se encuentra plenamente justificada, ni garantiza procesos, trámites y servicios eficaces;

Que la revisión emprendida ha propiciado una eminente desregulación y orientado a la sistematización y codificación de las disposiciones administrativas y de sus principales procesos en materia de tecnologías de información y comunicaciones, de modo que se homologuen trámites, servicios y procesos administrativos, asegurando mayor consistencia en el actuar de los servidores públicos de las dependencias y entidades de la Administración Pública Federal; ajustándoles a las expectativas y condiciones de nuestro tiempo y evitando considerablemente las diferencias entre norma y realidad, asegurando además una mayor certidumbre jurídica a todos los usuarios de los servicios proporcionados por el Estado Mexicano, lo que sin duda alguna hará al servicio público más transparente y menos proclive a la corrupción.

Que la revisión de disposiciones normativas y de los procesos de trabajo, han permitido identificar un gran número de disposiciones que ya cumplieron con su cometido y otras tantas que pese a su denominación no revisten el carácter de disposiciones propiamente dichas, asimismo otro importante número de disposiciones se encuentran derogadas tácitamente o que con el transcurso del tiempo y el cambio de condiciones que llevaron a su expedición se han vuelto innecesarias, en tanto que regulan situaciones jurídicas rebasadas por la realidad, y que por lo tanto todas deben ser abrogadas expresamente, para garantizar seguridad jurídica a los particulares, a la sociedad en general y a las propias autoridades;

Que el Estado de Derecho impone el deber de actuar acorde con sus principios y normas, y por ende resulta imperativo, el que a fin de propiciar su debida observancia, se establezcan condiciones que inhiban por una parte a la autoridad administrativa a establecer normas que si bien, pueden encontrarse ajustadas a la ley, generalmente imponen a la Administración Pública Federal excesivos controles y altos costos administrativos, que se traducen en procedimientos ineficaces, y su curva de

aprendizaje y dominio es alcanzado en el momento en que se emiten nuevas normas que incluso no abrogan expresamente las anteriores ; y por otra parte, determinar un esquema de revisión y mejora de las normas, que además de lograr mayor eficiencia, propicie cambios estructurales y de organización en la medida en que se incrementa el uso de tecnologías de la información, se acorten plazos y simplifiquen procedimientos, contribuyen incluso a generar ahorros y distribuir éstos a las altas prioridades de la Nación;

Que es precisamente con estas acciones que se logrará una Mejora de la Gestión Pública, impulsando su modernidad en forma ordenada y dinámica para cumplir nuestros más caros anhelos de justicia, transparencia y legalidad, principios de observancia general en el servicio público, y así proveer de una regulación al interior de las dependencias y entidades de la Administración Pública Federal, como en sus relaciones con los particulares, por lo que en ejercicio de las facultades que me confieren los artículos 89, 90 y 92 de la Constitución Política de los Estados Unidos Mexicanos en relación con las disposiciones de la Ley Orgánica de la Administración Pública Federal, es que en materia de tecnologías de la información y comunicaciones en el Gobierno Federal, es necesario establecer condiciones de mejores prácticas en el uso y aprovechamiento de los recursos, así como estandarizar y optimizar sus procesos rectores.

Que en base a las consideraciones anteriores se estima una transformación de fondo y con una clara orientación a la atención y solución de las demandas de la sociedad, así como propiciar la solución eficaz de los diversos problemas que aquejan a nuestro País, erradicar la opacidad y la corrupción, resulta necesario contar con un marco normativo claro, preciso y congruente a las necesidades actuales, dotado de mecanismos de revisión y adecuación del mismo, he tenido a bien emitir las siguientes:

REGLAS GENERALES PARA LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Del Objeto

Artículo 1.- Las presentes Reglas Generales para las tecnologías de información y comunicaciones, regularán en la Administración Pública Federal Centralizada y Paraestatal la planeación, operación, supervisión, seguimiento, transparencia, control y vigilancia en la materia.

Del Ámbito de Aplicación

Artículo 2.- Las presentes Reglas Generales son de observancia general y obligatoria en la Administración Pública Federal, regirán al interior de las dependencias y entidades, y serán aplicables en su ámbito interno y en sus relaciones con la ciudadanía sin demérito de lo previsto en la legislación federal.

Cuando las leyes refieran la emisión de disposiciones administrativas, lineamientos, normas, procesos generales o específicos en las materias a que se circunscribe este ordenamiento a cargo de

alguna o en lo general de las dependencias y entidades, se entenderá por aquéllas las presentes Reglas Generales.

De los Responsables de su Aplicación, Seguimiento y Vigilancia

Artículo 3.- Corresponde en razón de la materia que se regula a la Secretaría de de la Función Pública, interpretar para efectos administrativos las presentes Reglas Generales y su Manual, así como resolver sobre los casos no previstos en los mismos relativos a su aplicación, seguimiento y vigilancia.

Para el caso de las disposiciones relativas a la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión para efectos administrativos, la interpretación corresponde a la Subcomisión de los Sistemas Automatizados de Control de Gestión de la CIDGE.

Toda solicitud de aclaración sobre la aplicación o interpretación relacionada con las presentes Reglas Generales y su Manual, deberán resolverse dentro del plazo de veinte días hábiles contados a partir de la recepción de la solicitud respectiva por la instancia competente.

Cuando los particulares formulen solicitudes de aclaración o interpretación a las presentes disposiciones, el plazo para otorgar respuesta considerará adicionalmente quince días hábiles, siempre que se requiera a una dependencia o entidad información que permita complementar la atención de la misma.

Las solicitudes de información que se formulen en términos de lo dispuesto por la normatividad en materia de transparencia y acceso a la información, se atenderán en los plazos y términos precisamente aplicables por las regulaciones específicas de dichas materias.

Artículo 4.- La interpretación sobre la aplicación de las Reglas Generales o de su Manual, se ajustará a los principios de austeridad, objetividad, eficiencia, oportunidad, legalidad, transparencia y rendición de cuentas que rigen al servicio público.

Las dependencias y entidades de la Administración Pública Federal al aplicar las Reglas Generales o su Manual deberán igualmente observar dichos principios, privilegiando la literalidad de sus disposiciones.

Artículo 5.- Los Titulares de las dependencias y entidades de la Administración Pública Federal en el ámbito de sus respectivas atribuciones, y cuando corresponda, los órganos de gobierno de las entidades paraestatales, supervisarán que las presentes Reglas Generales se observen adecuadamente.

Asimismo dichas autoridades deberán evitar al interior de las dependencias o entidades a su cargo, regular las materias a que se circunscriben las presentes Reglas Generales, sin que exista una justificación para ello y que ésta cuente con el dictamen favorable del Comité de Regulación Interna de la Administración Pública Federal.

Artículo 6.- Son responsables de su aplicación en las dependencias y entidades, los servidores públicos de las mismas, en el grado y medida que establezcan las Leyes, Reglamentos, las presentes Reglas Generales y su Manual y que señalen las demás disposiciones jurídicas que resulten aplicables.

Artículo 7.- Las dependencias y entidades en el marco de sus atribuciones proveerán lo necesario a efecto de que sus procedimientos se sujeten a las presentes Reglas Generales y su Manual.

Artículo 8.- Son responsables de vigilar o fiscalizar la aplicación adecuada de las presentes Reglas Generales, los órganos colegiados que en cada dependencia o entidad se integren para el control interno, cuando corresponda los Comisarios Públicos, la Secretaría de la Función Pública por si misma o a través de los órganos internos de control.

Del Comité de Regulación Interna de la Administración Pública Federal

Artículo 9.- Las presentes Reglas Generales serán adicionadas o reformadas, una vez que se cumpla con el procedimiento señalado en el artículo 12. Dicho procedimiento no podrá regularse específicamente.

Artículo 10.- El Comité de Regulación Interna de la Administración Pública Federal será el responsable de dictaminar la procedencia de adicionar o reformar las presentes Reglas Generales, y en su caso, de otorgar su visto bueno, para regular aspectos específicos al interior de las dependencias y entidades.

Artículo 11.- El Comité de Regulación Interna de la Administración Pública Federal se integra con un representante de cada dependencia de la Administración Pública Federal, un representante de la Comisión Federal de Mejora Regulatoria y un representante de la Presidencia de la República quien lo presidirá.

Los representantes deberán ocupar un puesto de la estructura orgánica básica cuando menos del rango de Titular de Unidad, los que se podrán hacer representar hasta en dos ocasiones, en los términos establecidos en el Reglamento Interior de la dependencia a que pertenezcan, para integrar el Comité de Regulación Interna de la Administración Pública Federal.

El Presidente de Comité de Regulación Interna de la Administración Pública Federal solicitará a los Titulares de las dependencias y de la Comisión Federal de Mejora Regulatoria la designación de sus representantes.

Artículo 12.- Durante la primera semana de [mes], se reunirá el Comité de Regulación Interna de la Administración Pública Federal para conocer e integrar el proyecto de disposiciones que en su caso habrían de adicionarse, en su caso, los apartados que deberán reformarse, y excepcionalmente cuando corresponda la emisión de nuevas Reglas Generales.

Las dependencias y entidades formularán propuestas y se presentarán a través del sistema electrónico que determine la Presidencia de la República, ésta señalará la dependencia que por

conducto de su Representante le apoyará como Secretario Técnico. Asimismo, definirá el programa de trabajo y el periodo en que se realizará la consulta pública del proyecto de disposiciones, ésta será al menos de 10 días naturales.

La integración del proyecto de disposiciones y su dictamen no será mayor a dos meses a partir de la constitución del Comité de Regulación Interna de la Administración Pública Federal, si en ese plazo no se ha sujetado a consulta pública, su revisión deberá esperar al siguiente ejercicio.

Artículo 13.- El Consejero Jurídico del Ejecutivo Federal someterá al Ejecutivo Federal el respectivo proyecto, para en su caso aprobación y emisión, dentro de los 10 días hábiles siguientes a que haya vencido el plazo de dos meses señalado en el artículo anterior.

Artículo 14.- Cuando las dependencias y entidades excepcionalmente requieran emitir disposiciones específicas en materia de tecnologías de la información y comunicaciones, que regirán al interior de las mismas, someterán a la consideración de la Presidencia de la República, su proyecto de disposiciones y la justificación de su necesidad, ésta incluirá la manifestación de no implicar presiones de gasto de ninguna índole ni la creación de estructuras a través de movimientos compensados ni la transferencia de recursos federales para su aplicación; asimismo, comprenderá la motivación suficiente para establecer las disposiciones, señalando la problemática que tendría por objeto resolver y las posibles consecuencias directas e inmediatas de no contar con esa regulación.

La Presidencia de la República, dentro del plazo de quince días naturales, realizará el proyecto de dictamen de la propuesta y convocará al Comité de Regulación Interna de la Administración Pública Federal. Dicho Comité contará con diez días naturales para resolver otorgar o no su dictamen favorable a la propuesta.

La dependencia o entidad de que se trate, al recibir un dictamen no favorable, sólo podrá presentar nuevamente su propuesta de regulación interna en el mismo sentido, cuando haya transcurrido un año desde la notificación de ese dictamen.

Artículo 15.- Las dependencias y entidades de la Administración Pública Federal cuyas propuestas de disposiciones de regulación interna sean dictaminadas favorablemente por el Comité de Regulación Interna de la Administración Pública Federal, una vez que se formalice su establecimiento o emisión deberán publicarlas en el Diario Oficial de la Federación para su debida obligatoriedad.

Artículo 16.- La elaboración de proyectos de adiciones o de reformas, en su caso, de regulación interna, deberán observar asimismo las demás disposiciones legales que resulten aplicables.

Uso de Tecnologías de la Información y Comunicaciones

Artículo 17.- Las aplicaciones y soluciones tecnológicas existentes y aquellas que se desarrollen para sistematizar los procesos de trabajo a que se refiere las Reglas Generales y su Manual, deberán tener interoperabilidad con aquellas aplicaciones de tecnologías de información y comunicaciones que generen o reciban datos relacionados con la materia de estas reglas Generales y su Manual.

Artículo 18.- Las dependencias y entidades de la Administración Pública Federal deberán propiciar la sistematización, ejecución, control y supervisión de los procesos que establecen las presentes Reglas Generales y su Manual, mediante la adopción de soluciones de tecnologías de la información y comunicaciones.

Artículo 19.- Las dependencias y entidades de la Administración Pública Federal, en la adopción de tecnologías de la información y comunicaciones deberán observar lo previsto en las Reglas Generales respectivas, y propiciar un mejor aprovechamiento de los recursos públicos, adecuada administración de la información, propiciar una apertura de la información pública y garantizar la rendición de cuentas.

De la Transparencia y Acceso a la Información

Artículo 20.- Toda información que se genere como resultado de la aplicación de las presentes Reglas Generales, se presumirá pública y por ende susceptible de ponerse a disposición de cualquier solicitante salvo que se encuentre clasificada como reservada o contenga datos personales tal y como lo dispone la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Artículo 21.- Toda información que se genere como resultado de la aplicación de las presentes Reglas Generales y su Manual sin menoscabo de lo previsto en las disposiciones legales, podrá trasmitirse entre las dependencias, entre éstas y las entidades, así como entre las entidades, para el ejercicio de sus atribuciones.

En todos los casos, invariablemente deberán observarse las disposiciones en materia de protección, tratamiento, difusión, transmisión y distribución de datos personales que resulten aplicables.

Artículo 22.- Las dependencias y entidades, difundirán en sus respectivos portales de Internet, los resultados de su gestión en tecnologías de la información y comunicaciones en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y su reglamento, siguientes:

I. Servicios Digitalizados (en operación);

II. Software de Sistemas (soluciones en operación), y

III. Indicadores de desempeño de los procesos del Manual.

De las definiciones de uso general

Artículo 23.- Para efectos de las Reglas Generales y su Manual de procesos, sin demerito de las definiciones, acrónimos, anglicismos y siglas previstas en otros ordenamientos jurídicos, se entenderá por:

AC: Las Dependencias, Entidades, Organizaciones, Instituciones y Proveedores de Servicios de

Certificación que cuentan con la infraestructura tecnológica para la emisión y registro de Certificados Digitales de Firma Electrónica Avanzada. Estas Dependencias, Entidades, Organizaciones, Instituciones y Proveedores de Servicios de Certificación también serán entendida como Agencia o Autoridad Certificadora;

Activo: Cualquier elemento que tenga valor tangible o intangible para la organización, entre los cuales se encuentran, en forma no limitativa: información en cualquier tipo de soporte, bases de datos, programas de cómputo, bienes informáticos físicos y sistemas de información;

Activos Críticos: Los recursos que podrían degradar la habilidad de la dependencia o entidad para el desempeño de sus funciones cuando se encuentre comprometida su seguridad -integridad, confidencialidad y disponibilidad;

Administrador: son todas aquellas personas responsables de mantener la disponibilidad y la funcionalidad de la infraestructura y servicios Institucionales de acuerdo a las necesidades de operación de la Entidad o Dependencia;

Administración de ambientes: (que abarque desarrollo, pruebas, preproducción y producción/operación)

Adquisición: Es la obtención de las soluciones tecnológicas que cubran la totalidad de los requerimientos, cabe mencionar que puede ser por compra directa, tercerización, o cualquier otra práctica;

AGD: Agenda de Gobierno Digital, establece las estrategias de desarrollo que deberá seguir el gobierno federal mediante el uso de las TIC, así como fomentar la participación ciudadana, a través de las dependencias y entidades de la Administración Pública Federal, en colaboración con los poderes Legislativo y Judicial, los gobiernos estatales y municipales, la industria, la academia y la sociedad en general;

Alineación: Enfocar las acciones comunes ligadas efectiva y eficientemente, hacia la obtención de las metas institucionales, estrategias, objetivos y prioridades;

Ambiente de trabajo: se refiere al conjunto de herramientas, utilerías, programas, aplicaciones e información que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, en relación con los privilegios de su cuenta;

Amenaza (s): Causa potencial de un incidente no deseado que puede provocar daños a uno o más activos o a la propia dependencia o entidad; es una condición causada por una mala configuración o instalaciones realizadas con opciones por omisión, que permite explotar vulnerabilidades de una entidad atentando contra las propiedades de confidencialidad, disponibilidad e integridad de la información. Causa potencial de un incidente no deseado que puede provocar daños a uno o más activos o a la propia dependencia o entidad;

Análisis de protocolos: software que permite conocer los paquetes que conforman la información durante los procesos de comunicación, procesamiento o manipulación de datos, mediante la

separación de estas partes;

Análisis de riesgos: Método analítico de la gestión de riesgos que permite la identificación de vulnerabilidades y amenazas de seguridad, así como la evaluación de la magnitud o impacto de los daños a efecto de determinar dónde sería necesaria la implementación de controles o salvaguardas y la cantidad máxima razonable de recursos que sería necesario invertir. Este análisis es indispensable ya que permite tomar decisiones para determinar cuáles riesgos serán asumidos, cuáles serán mitigados, cuáles transferidos y cuáles evitados;

Antivirus: software especializado diseñado para detectar, eliminar y prevenir virus informáticos en los dispositivos de la red Institucional;

Arquitectura Empresarial: Modelo que ayuda a la dirección de TIC a razonar sobre su organización de manera global. La arquitectura captura una amplia variedad de información y la relaciona de manera que los responsables de la organización puedan consultarla para identificar problemas o tomar decisiones sobre posibles cambios.

Auditoría de Seguridad de la Información: Comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores. Los resultados reportan a los responsables, quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas. Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad;

Autenticación: al proceso en virtud del cual se constata que un servidor público de una dependencia o entidad de la Administración Pública Federal es el que dice ser y que tal situación es demostrable ante terceros;

Autenticidad: al proceso mediante el cual se puede constatar si la clave pública de un mensaje de datos corresponde a la clave privada con la cual se firmó, permitiendo que el mensaje pueda ser interpretado, validando que fue realmente creado por el titular de un certificado digital o que está reconociendo como propio su contenido;

Bases de datos: es un conjunto estructurado de datos, gestionado bajo el control de un Manejador de Bases de Datos, el cual se encarga de controlar el acceso concurrente, evitar redundancia, cumplimiento de las restricciones y reglas de integridad, usar elementos que aceleren el acceso físico a los datos (índices, agrupamientos, funciones de dispersión, ...), distribuir los bloques del disco del modo más adecuado para el crecimiento y uso de los datos, controlar el acceso y los privilegios de los usuarios, recuperar ante fallas, entre otros;

Biblioteca de programas: es una colección o conjunto de archivos que contienen código, desarrollados por un mismo fabricante bajo ciertos criterios, mismos que suelen ser compatibles y tener interoperabilidad entre ellos;

Cadenas: son mensajes enviados a través del servicio de correo electrónico que se caracterizan por solicitar dentro del cuerpo del mismo ser enviados a cierta cantidad de personas, con el fin de obtener algo a cambio;

Carta de aceptación de un producto: Es aquella en donde se confirma que se ha aceptado un producto, después de haber cumplido o sobrepasado con los requerimientos que el usuario;

Cartucho: sistema de almacenamiento que incluye una cinta magnética sin fin, lo que le permite mayor velocidad que las cintas magnéticas tradicionales y la posibilidad de ser manejado por un sistema automatizado que no requiera la intervención de un operador;

Catálogo de proveedores de la dependencia o entidad: Listado que proporciona información de los proveedores registrado en la propia dependencia o entidad;

CD: es un dispositivo de almacenamiento óptico que requiere de un dispositivo de grabado, el cual utiliza un láser para imprimir puntos sobre la superficie brillante, mismas que al ser leídas con un láser de menor intensidad, son transformadas en cadenas de bits;

Certificado Digital: El mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada; al conjunto de datos firmados electrónicamente que vincula a un servidor público con una clave pública;

Ciclo de vida del Proyecto: Conjunto de fases administrativas por las que pasa un proyecto desde su inicio hasta su finalización;

CIDGE: Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, que fue creada con el objetivo de promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones en la Administración Pública Federal;

Cifrar o Cifrado: es el proceso de transformar un mensaje para ocultar su contenido, de tal manera que el receptor sea la única persona que pueda recuperar el mensaje original, permite proteger su confidencialidad y garantizar la integridad del mensaje;

Cintas: es un dispositivo de almacenamiento basado en una bobina magnética que requiere de un lector/reproductor especial;

Clave Privada: Los datos que el firmante genera de manera secreta y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha Firma Electrónica Avanzada y el firmante; documento electrónico que genera el uso del algoritmo asimétrico, con esta llave privada se realiza el firmado digital, mismo que codifica el contenido de un mensaje y que sólo debe ser conocido y resguardado por el propietario del par de llaves (pública/privada);

Clave Pública: Los datos contenidos en un Certificado Digital que permiten la verificación de la autenticidad de la Firma Electrónica Avanzada del firmante; documento electrónico que genera el uso de algoritmo asimétrico y que se publica junto con el certificado digital para cifrar la información que se desea enviar al propietario de la llave privada;

CMM: El Modelo de Capacidad y Madurez o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute);

Comité de Seguridad: Es un grupo de trabajo de participación, creado para entender y ser consultado sobre la actuación de la Dependencia y Entidad, que se encarga de establecer las políticas e iniciativas de seguridad de la información. El Comité estará formado por servidores públicos de diversas áreas. El número de miembros que integran el Comité de Seguridad, será definido por la Dependencia o Entidad;

Compilador: Un programa que genera lenguaje máquina a partir de un lenguaje de programación;

Confidencialidad: Principio de seguridad de la información que consiste en asegurar que el acceso al activo únicamente se realiza por los autorizados y a través de los procedimientos establecidos para ello; es uno de los servicios de seguridad en la información, el cual está encaminado a revelar el nivel y el tipo de información únicamente a las entidades autorizadas para acceder a la misma; aseguramiento de que la información es accesible sólo a aquellos servidores públicos autorizados para tener acceso a la misma;

Configuración de red: son los valores asignados y las opciones habilitadas para la operación de la tarjeta de red de un equipo de cómputo dentro de la red de la Dependencia o Entidad;

Contraseña: son una serie de caracteres que en conjunto con una cuenta (nombre de usuario) permiten el acceso a los recursos o servicios institucionales, misma que debe ser difícil de generar por todas las personas a excepción del dueño de la cuenta; a la serie de caracteres generada por el usuario que lo identifican y que junto con la clave de acceso, sirve para acceder a los sistemas electrónicos;

Contrato o Pedido: Documento jurídico a través del cual se formalizan las adquisiciones, arrendamientos o servicios según corresponda;

Control de cambios: Identificar, documentar, aprobar o rechazar y controlar cambios en las líneas base del proyecto;

Control de seguridad (o Control): Recurso aplicado para mitigar el riesgo. Es posible utilizar este concepto como sinónimo de contramedida, salvaguarda, mecanismo o medida de seguridad. Los controles se pueden organizar en función de la naturaleza de su implementación -administrativos, físicos y técnicos/lógicos- o en función de su naturaleza operativa -preventivos, de detección y correctivos-;

Convenio modificatorio: Documento por el cual se formaliza cualquier modificación a un contrato o pedido celebrado con anterioridad, el cuál debe suscribirse por las mismas personas que intervinieron en él o por las que los hayan sustituido;

Correo electrónico: son el grupo de tecnologías encaminadas a dar un servicio que agiliza y facilita el intercambio de mensajes, documentos e información;

Cronograma: Representación gráfica de las fechas planificadas para realizar las actividades de un proyecto, incluye las fechas planificadas para cumplir los hitos, compromisos de entrega o puntos de control del proyecto. El cronograma incluye también el seguimiento de la ejecución del proyecto (fechas reales o de avance);

Cuenta: es el identificador único y personal que está asociado a un usuario, mismo que en conjunto con una contraseña permite el acceso a recursos o servicios institucionales;

Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;

Dependencias: Las que integran la Administración Pública Federal centralizada en términos de los artículos 1o. y 2o. de la Ley Orgánica de la Administración Pública Federal incluyendo en su caso a sus órganos administrativos desconcentrados;

Desarrollador: es aquella persona que tiene acceso a la infraestructura o servicios informáticos institucionales de manera autorizada, misma que cuenta con los conocimientos necesarios para diseñar, construir y probar aplicaciones para automatizar la operación Institucional;

Dial-up: acceso remoto comúnmente usado para Internet utilizando un MODEM y una línea telefónica;

Dictamen Técnico: Documento que suscribe el titular del área usuaria o solicitante de un bien o servicio, que forma parte del Dictamen de Adquisición en el que se detalla el cumplimiento o incumplimiento de cada uno de los requisitos técnicos establecidos en las bases de licitación o invitación;

Diskette: dispositivo de almacenamiento basado en un disco magnético de pequeñas dimensiones y baja capacidad. Los disquetes se introducen en un drive para su lectura y grabación mediante el uso de una o varias cabezas lectoras-grabadoras magnéticas;

Disponibilidad: Principio de seguridad de la información que estipula que el activo puede ser utilizado por los autorizados cuando éstos lo requieran; es uno de los servicios de seguridad en la información, encaminado a mantener los servicios habilitados y listos para su uso en el momento en que sean requeridos por los usuarios;

Documento electrónico gubernamental: al instrumento que contiene datos y/o información, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, el cual debe hacer uso de la firma electrónica avanzada, lo cual permite autenticar la información que se intercambia entre los servidores públicos de las Dependencias y Entidades paraestatales; consistentes en acuerdo, acta, atenta nota, carta, circular, dictamen, informe, invitación, memorando, minuta, nota

informativa, oficio, solicitud, volante y otros que se definan en la subcomisión de Sistemas Automatizados de Control de Gestión, así como los archivos que en su caso se adjunten a éstos;

e-Gobierno: Es el uso de las tecnologías de la información y comunicaciones, particularmente el Internet, como una herramienta para mejorar el funcionamiento del gobierno y su relación con el ciudadano, al desarrollar y ofrecer información y servicios públicos digitales para satisfacer sus necesidades. Ahora también es conocido como Gobierno Digital;

Entidades: Los organismos descentralizados, las empresas de participación estatal mayoritaria y los fideicomisos públicos que tengan el carácter de Entidad paraestatal, a que se refieren los artículos 1o., 3o., 45, 46 y 47 de la Ley Orgánica de la Administración Pública Federal;

Entregable: Cualquier producto, resultado o capacidad de prestar un servicio único y verificable que debe producirse para terminar un proceso, una fase o un proyecto;

Equipo de trabajo: Conjunto de personas que trabajan directamente en la realización de un proyecto, pudiendo o no de diferentes áreas dentro de la institución;

Escenario de prueba: Es hacer una simulación del ambiente real de trabajo, en donde aplicará el desarrollo, para determinar el comportamiento de un producto o servicio;

Especificación de Requerimientos de Soluciones Tecnológicas (ERST): Documento en donde se estipulan las necesidades, se incluyen especificaciones y descripciones de las necesidades a detalle, las cuales serán mitigadas con las respectivas soluciones tecnológicas disponibles en el mercado y/o a desarrollar por el área correspondiente;

Especificaciones: Conjunto de características cuantitativas y cualitativas que debe cumplir un proyecto en su producto final, ya sea un producto o servicio;

Estándar CMM: Modelo de Capacidad y Madurez o CMM (Capability Maturity Model, por sus siglas en inglés): Es un modelo de evaluación de los procesos de una organización;

Estándar ITIL: Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library, por sus siglas en inglés). Es un marco de trabajo de buenas prácticas destinadas a facilitar la entrega de servicios de Tecnología de Información y Comunicaciones que ayuda a las organizaciones a lograr calidad y eficiencia en las operaciones de las unidades de Tecnología de Información y Comunicaciones;

Estructura: Define como se dividen, agrupan y coordinan formalmente las tareas de trabajo. El diseño de la estructura enfoca elementos clave como: especialización del trabajo, desagregación por departamentos, cadena de mando, tramo de control, centralización y descentralización y formalización;

Extensión: es el sufijo, o nombre adicional que se le da a un archivo tal como “.XXX”, el cual caracteriza el formato por el que se genera, donde “.XXX” representa un numero limitado de caracteres alfanuméricos dependiendo del sistema operativo, normalmente tiene tres caracteres pero esto es susceptible de variación;

FEA: La Firma Electrónica Avanzada que permite la identificación del Firmante y ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos;

Fideicomisos Públicos No Paraestatales: Son los fideicomisos públicos constituidos por la Secretaría de Hacienda y Crédito Público, en su calidad de fideicomitente única de la Administración Pública Federal Centralizada o alguna entidad de la Administración Pública Paraestatal en términos de las disposiciones legales y administrativas aplicables, y que no son considerados entidades paraestatales;

Firewall: es el dispositivo físico que permite crear una barrera entre la red interna y red externa, permitiendo el acceso entre las redes de acuerdo a las políticas de seguridad definidas en su configuración;

Firma electrónica avanzada: al medio de identificación electrónica que se defina en los lineamientos que emita la Subcomisión de Firma Electrónica Avanzada con base en el Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, publicado en Diario Oficial de la Federación del 9 de diciembre de 2005;

Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en éste;

Firmware: parte del software de una computadora que no puede modificarse por encontrarse en la ROM o memoria de sólo lectura, «Read Only Memory», es una mezcla o híbrido entre el hardware y el software, es decir tiene parte física y una parte de programación consistente en programas internos implementados en memorias no volátiles;

Funcionalidad: Características de un producto o servicio que hacen que sea funcional y cubra las necesidades o requerimientos de un área o un usuario;

Funciones: Hace referencia a una actividad o al conjunto de actividades genéricas, que desempeña uno o varios elementos, de forma complementaria para conseguir un objetivo concreto y definido;

Garantías: Documento por medio del cual los proveedores, arrendadores y prestadores de servicios de las dependencias o entidades de la Administración Pública Federal establece a favor de éstos un derecho económico exigible, si no se realiza el cumplimiento de sus obligaciones contraídas en los contratos o pedidos;

Generador de contraseñas: es un dispositivo físico que permite fabricar códigos (contraseñas) de referencia secretos en función de parámetros o características deseables en periodos de tiempo definidos;

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización respecto de los riesgos que afronta. La gestión de riesgos incluye la evaluación de riesgos, su tratamiento, aceptación y comunicación;

Gobernabilidad de TIC: Es la relación que existe entre la estrategia y la gestión de Tecnología de Información y Comunicaciones de la dependencia o entidad de la APF. En un modelo de Gobernabilidad los funcionarios de alto mando deben tomar las decisiones estratégicas de Tecnología de Información y Comunicaciones para asegurar la aplicación de las mejores prácticas, la eficiencia en el aprovechamiento de los recursos de Tecnología de Información y Comunicaciones y la satisfacción de los usuarios, entre otras;

Gobierno Digital: Es el uso de las tecnologías de la información y comunicaciones. El Internet por ejemplo, es una herramienta que al desarrollar y ofrecer información y servicios públicos digitales mejora el funcionamiento del gobierno y la relación que existe con el ciudadano para satisfacer sus necesidades;

Hardware: son los componentes físicos que conforman un equipo de cómputo;

HTTPS (Secure HyperText Transfer Protocol) (Protocolo Seguro de Transferencia de Hipertexto): garantizar la seguridad de las comunicaciones entre el usuario y el servidor web al que dicho usuario se conecta;

Incidente: Uno a más eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información; cualquier situación que ocurre durante un proceso y sucede en repetidas ocasiones;

Infraestructura: son todos los componentes que soportan los servicios informáticos institucionales;

Insumo: Son los bienes o servicios que se incorporan a un proceso, y que con el esfuerzo de un equipo de trabajo se transforman en otro bien o servicio con un valor agregado mayor;

Integridad: Principio de seguridad de la información que consiste en que el activo sólo puede ser modificado por los autorizados. Es una protección contra la modificación de los datos en forma intencional o accidental. Los datos deben ser mantenidos tal y como fueron proporcionados originalmente, sin sufrir ninguna modificación o eliminación;

Interfaces: Se denominan a las zonas de contacto o conexión entre dos elementos de Hardware, o entre procesos;

Internet: Conjunto de redes de computadoras y equipos físicamente unidos a través de medios alámbricos o inalámbricos que unen redes o equipos en todo el mundo;

Interoperabilidad: Capacidad de los equipos, sistemas y/o arquitecturas tecnológicas de interactuar y/o intercambiar datos y servicios de una manera ágil y segura, a través de redes en las que se asegura la confidencialidad y no exposición de los datos. Usualmente se convienen estándares para lograr la interoperabilidad.

Intrusión: Acción que una o más personas realizan para introducirse, sin derecho, en uno o más sistemas de información a fin de alterar, copiar o sustraer información que forma parte de esos sistemas, también puede ser en datos, información, bases de datos, etc.;

ISO/IEC27000: Conjunto de estándares desarrollados o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electro technical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, ya sea pública o privada, independientemente de su tamaño;

ITFEA: La Infraestructura Tecnológica que permite la interoperabilidad y el reconocimiento de Certificados Digitales de Firma Electrónica Avanzada entre las Autoridades o Agencias Certificadoras que la integran;

ITIL (Information Technology Infrastructure Library, ITIL por sus siglas en ingles): Biblioteca de Infraestructura de Tecnologías de Información, es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). Que ayuda a las organizaciones a lograr calidad y eficiencia en las operaciones de TI; (Ver Estándar ITIL)

LDAP (Lightweight Directory Access Protocol, LDAP por sus siglas en ingles): Directorio de usuarios que se utiliza principalmente para asociar nombres a números de teléfono y a direcciones e-mail, es un estándar abierto para los servicios globales o locales en una red y/o en Internet.;

Lista de control de acceso: es una lista donde se asignan permisos de acceso a los archivos y directorios por usuario;

Macros: son todos aquellos programas que se ejecutan dentro de otros programas como Word o Excel para automatizar tareas, su uso elimina la realización de tareas repetitivas, automatizándolas, básicamente, se trata de un grupo de comandos de una aplicación, organizados según un determinado juego de instrucciones y cuya ejecución puede ser solicitada y autorizada para realizar la función que se desea;

Matriz de Riesgo: Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos;

Memoria USB: dispositivo de almacenamiento que utiliza memoria flash para guardar la información;

Mensaje de datos: La información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos; al intercambio de datos o información entre un emisor y un receptor a través de medios de comunicación electrónica;

Mensajería instantánea: son aplicaciones o software que permite comunicarse, o enviar mensajes al instante, así como, intercambio de archivos;

Mesa de servicios: es el único punto de contacto encargado de recibir todas aquellas incidencias de usuarios relacionados con problemas recurrentes, el objetivo de ésta es darle lo más pronto posible solución a los usuarios, mediante el escalamiento del problema al área correspondiente; o para el otorgamiento de los servicios que le soliciten a la UTIC a través de esta función;

Metodología: Sistema de Prácticas, técnicas, procedimientos y normas utilizado por quienes trabajan en una disciplina;

Modelo de Estructuras y Funciones: Implementación de una estructura organizacional en las áreas de TIC, enfocadas a participar activamente en la planeación estratégica institucional con un enfoque al ciudadano;

Modelo de Funcionalidad: Implementación de una estructura organizacional en las unidades de Tecnología de Información y Comunicaciones, con enfoque a operar de manera eficiente sobre los procesos que, por las responsabilidades y atribuciones que se confieran a cada área de la Unidad de Tecnología de Información y Comunicaciones, deba gestionar;

Modelo de Gobernabilidad de TIC: Es parte integral del gobierno de la dependencia o entidad y está constituido por las estructuras de liderazgo y los procesos que aseguran que la Tecnología de Información y Comunicaciones de la dependencia o entidad, sostienen y extienden la estrategia y los objetivos institucionales;

Modelo de Gobierno Digital: Representa la interacción y flujo de los elementos que intervienen en el desarrollo del Gobierno Digital. Ubica al ciudadano como el centro de su estrategia y a partir de esta premisa, los elementos que intervienen se agrupan en seis niveles fundamentales (ver AGD, capítulo VI, Pág. 15);

Modelo de Procesos: Conjunto estructurado de elementos que describen las características de procesos efectivos y de calidad, que indican “qué hacer”, pero no indican “cómo hacer” ni “quién lo debe hacer”;

Modelo de Zachman: Es uno de los modelos más utilizados para la arquitectura empresarial para alinear los procesos y estructura organizacional de TI. La arquitectura basada en el modelo de Zachman proporciona una taxonomía para relacionar los conceptos que describen una organización y sus tecnologías de información a través de varias perspectivas y abstracciones.

Nivel OLA. (Operating Level Agreement, por sus siglas en inglés): Es un contrato escrito que define las relaciones técnicas internas que son necesarias en una organización proveedora de un servicio de Tecnología de Información y Comunicaciones, éste se suscribe para consistencia y objetividad a los contratos escritos de niveles de servicio hacia usuarios de la propia dependencia o entidad y/o de otra dependencia o entidad; para dar soporte a los SLA pactados entre esta y la empresa que recibe el servicio. Los OLA especifican procesos técnicos en términos entendibles por el proveedor y pueden dar soporte a uno o más SLA;

Nivel SLA: (Service Level Agreement, por sus siglas en ingles) es un contrato escrito entre un proveedor de un servicio de tecnología de la información y comunicaciones, que puede ser la Unidad

de Tecnologías de Información y Comunicaciones de la dependencia o entidad, con el propósito de fijar el nivel acordado para la calidad con que entregará el servicio;

OLA: Acuerdo o acuerdos de Nivel Operativo;

Organizaciones e Instituciones: Los gobiernos de entidades federativas y municipios; los integrantes del Poder Judicial de la Federación y de las Comisiones Legislativas del H. Congreso de la Unión; los organismos constitucionales autónomos;

PEPSU: Esquema metodológico que permite conocer, para un proceso, el proveedor, la entrada, el proceso que los consume, la salida y el cliente o usuario de la salida.

Periféricos: son todos los dispositivos que están conectados físicamente a una computadora;

PETIC: Plan Estratégico de TIC de las dependencias y entidades de la APF;

Plan de contingencia: se trata del documento en el que se plantea la estrategia, el personal y el conjunto de actividades que se requieren para recuperar por completo o parcialmente un servicio, localidad o proceso crítico, en caso de que se presente un desastre. Dentro de este documento se establecen de igual manera las actividades, roles y responsabilidades para regresar a la normalidad una vez resuelto el incidente;

PMG: Programa de Mejora de la Gestión, El instrumento del Ejecutivo Federal de carácter obligatorio que se enfoca a realizar mejoras que orienten sistemáticamente la gestión de las instituciones públicas y del Gobierno Federal al logro de mejores resultados;

Priorización: Establecer criterios para contar con un esquema para jerarquizar los proyectos de TIC y facilitar la determinación del portafolio final de proyectos;

Problema: Un asunto cuestionado o respecto del cual existe una controversia, o que no ha sido resuelto y se está analizando.

Procedimiento: Una serie de pasos que se siguen en un orden regular definitivo con un propósito;

Proceso: Conjunto de medidas y actividades interrelacionadas realizadas para obtener un conjunto específico de productos, resultados o servicios;

Protector de pantalla: se trata de un programa que se ejecuta automáticamente después de que el ratón y el teclado han estado inactivos por un periodo de tiempo determinado. Permiten: evitar que el recubrimiento fosforescente del monitor se marque como consecuencia de dejar una imagen estática por un tiempo prolongado, y proteger el acceso al equipo y/o a la información desplegada en la pantalla del monitor en ausencia del operador de la computadora;

Proveedores: Personas físicas o morales que celebren contratos de adquisiciones, arrendamientos y servicios con dependencias o entidades de la Administración Pública;

Proyecto Estratégico: Conjunto de actividades que tiene como propósito fundamental, ampliar la capacidad productiva de un sector económico y social determinado, y que en el contexto de las prioridades definidas en el plan nacional de desarrollo, contribuye de una manera particularmente significativa, para el logro de los objetivos y metas institucionales;

PSC: Prestador de Servicios de Certificación que cuenta con los elementos humanos, materiales, económicos y tecnológicos para la emisión, registro y administración de Certificados Digitales de Firma Electrónica Avanzada y que se encuentra acreditado por la Secretaría de Economía;

RCD: Registro de Certificados Digitales, el cual contiene los Certificados Digitales de Firma Electrónica Avanzada emitidos por una Autoridad o Agencia Certificadora, indicando su estado;

Recibo digital: al sello de recepción o acuse que generan los sistemas automatizados de control de gestión para el proceso de recepción del documento electrónico gubernamental. Este sello garantiza la integridad de la transacción;

Recurso: Recurso humano especializado, equipo, servicios, suministros, materias primas, materiales, presupuestos o fondos;

Red de telecomunicaciones: Sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión., así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario;

Red privada de telecomunicaciones: La red de telecomunicaciones destinada a satisfacer necesidades específicas de servicios de telecomunicaciones de determinadas personas que no impliquen explotación comercial de servicios o capacidad de dicha red;

Red pública de telecomunicaciones: La red de telecomunicaciones a través de la cual se explotan comercialmente servicios de telecomunicaciones. La red no comprende los equipos terminales de telecomunicaciones de los usuarios ni las redes de telecomunicaciones que se encuentren más allá del punto de conexión terminal;

Repositorio: Es una base de datos en la cual se colectan datos de configuración, de sistemas o de propósito general;

Requerimiento de Certificación: La solicitud electrónica de un Certificado Digital que contiene la clave pública y los datos de identificación del solicitante;

Requerimiento: Necesidad de un usuario final del producto o servicio generado por el proyecto, debiendo ser cubierta por dicho proyecto;

Riesgo: La probabilidad de que una amenaza aproveche la o las vulnerabilidades de un activo, así como las consecuencias de su impacto en una dependencia o entidad. Corresponde al Grupo de Trabajo del Comité de Seguridad determinar los niveles de riesgo máximos aceptables para la dependencia o entidad;

Rol: Una función definida que debe realizar un miembro del equipo del proyecto, como evaluar, archivar, inspeccionar o codificar;

RUP (Rational Unified Process, por sus siglas en inglés): Es un proceso internacionalmente adoptado para el desarrollo de sistemas o aplicativos;

Ruta crítica: Es el subconjunto de tareas de un proyecto, que al variar su duración impacta la fecha de finalización;

SAT: El Servicio de Administración Tributaria;

SE: La Secretaría de Economía;

Secretaría: Secretaría de la Función Pública;

Seguridad de la Información: Tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, modificación, divulgación, interrupción o destrucción no autorizada. Se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma, los datos pueden ser: electrónicos, impresos, audio u otros formatos;

Seguridad: Acciones tendentes a garantizar la confidencialidad, integridad y disponibilidad de los activos;

Servicio Electrónico: También denominado Servicio Digitalizado. Es un producto de la actividad de desarrollo de sistemas o aplicativos de una Unidad de Tecnología de Información y Comunicaciones en una dependencia o entidad que a través de la misma se ofrece a la ciudadanía;

Servicios: son todas las aplicaciones que están soportadas en la infraestructura institucional y que agilizan y automatizan las actividades diarias de los usuarios;

SFP: La Secretaría de la Función Pública;

Sistema Automatizado de Control de Gestión: el conjunto de elementos, procesos, procedimientos, herramientas e instrumentos informáticos o electrónicos, entre otros, que permiten realizar, identificar, proteger y controlar las comunicaciones, gestiones y trámites del documento electrónico gubernamental, entre los servidores públicos de las Dependencias y Entidades;

Sistema de datos personales: Conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización;

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos de administración de seguridad de la información. El término es utilizado principalmente por la ISO/IEC 27001, el término se denomina en Inglés "Information Security Management System" (ISMS) y el concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos

para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno;

Sistema o Aplicativo: Es el conjunto de componentes ó programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso de acuerdo a los requerimientos;

Sistema operativo: Es el software encargado de ejercer el control y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de hardware del sistema;

SLA: Acuerdo o acuerdos de Nivel de Servicio;

Software Comercial: Es el software o software libre comercializado, con el propósito de que las compañías que lo producen fijen un costo por el uso, distribución y mantenimiento del producto para la obtención de nuevas versiones, así como para el soporte técnico en el uso, configuración, implementación y otros servicios;

Software de Código Abierto: Es el software que puede ser distribuido y desarrollado libremente. Se puede basar en software libre y hacer uso de una mezcla de software comercial o propietario, o estar completamente basado en software comercial o propietario;

Software de escaneo: Es la aplicación que permite conocer los puertos o servicios disponibles en los dispositivos de la red;

Software libre: Es el software mediante el cual el usuario tiene la libertad de ejecutarlo, copiarlo, distribuirlo, estudiarlo, modificarlo y mejorarlo. Suele estar disponible gratuitamente, o bien a un determinado precio para hacer uso de él;

Software propietario: Es el software en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo (con o sin modificaciones), o cuyo código fuente no está disponible, o el acceso se encuentra restringido;

Software: Es el código, programa de código, conjunto de programas de código, procedimientos automatizados y rutinas de código que se asocian con la operación de equipo de cómputo y que tiene el propósito de ejecutar una función o proveer de un servicio. Generalmente son sistemas operativos, paquetería para automatización de oficinas, paquetes antivirus, paquetes para desarrollo de sistemas o aplicaciones, paquetes para operación, monitoreo y/o control redes de comunicaciones, paquetes de monitoreo de equipos de hardware y del propio código en operación, paquetes manejadores de bases de datos, navegadores para Internet, paquetes para monitoreo y seguridad de TIC, entre otros; son todas aquellas aplicaciones o programas instalados en una PC;

Solicitud de cambio: Solicitudes para ampliar o reducir el alcance de un proyecto, modificar políticas, procesos, planes o procedimientos, modificar costes o presupuestos, o revisar cronogramas. Las

solicitudes de cambio pueden hacerse directa o indirectamente, pueden iniciarse en forma externa o interna y pueden tener carácter obligatorio u opcional, ya sea desde el punto de vista legal o contractual. Únicamente se procesan las solicitudes de cambio formalmente documentadas, y solo se implementan las solicitudes aprobadas;

Soporte técnico local: Se refiere a la ayuda técnica que pueden tener los usuarios dentro de su área de trabajo en relación con la distribución geográfica;

Subcomisión: La Subcomisión de Firma Electrónica Avanzada, integrada por la Secretaría de la Función Pública, la Secretaría de Economía y el Servicio de Administración Tributaria, en términos del artículo vigésimo del Acuerdo por el cual se crea la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, a que se refiere el considerando tercero de este instrumento, y

Tarjeta inteligente: módulo de memoria del tamaño de una tarjeta de crédito en el cual es posible almacenar información para autenticación de usuarios;

TCP/IP (Transfer Control Protocol/Internet Protocol): al protocolo estándar de comunicaciones en red utilizado para conectar sistemas informáticos a través de Internet;

TIC: Tecnologías de la Información y Comunicaciones, son un conjunto de técnicas, desarrollos y dispositivos avanzados que integran funcionalidades de almacenamiento, procesamiento y transmisión de datos. Entendemos por TIC al conjunto de productos derivados de las nuevas herramientas (software y hardware), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de la información;

Titular de un Certificado Digital: La persona que crea sus claves privada y pública, genera su Requerimiento de Certificación y obtiene un certificado digital de Firma Electrónica Avanzada ante una Autoridad o Agencia Certificadora;

Trámite electrónico: Cualquier solicitud o entrega de información que las personas físicas o morales realicen por medios electrónicos ante una dependencia o entidad, ya sea para cumplir una obligación, obtener un beneficio o servicio, a fin de que se emita una resolución, así como cualquier documento que dichas personas estén obligadas a conservar, no comprendiéndose aquella documentación o información que sólo tenga que presentarse en caso de un requerimiento de una dependencia o entidad;

Trazabilidad: Se entiende como trazabilidad aquellos procedimientos preestablecidos y autosuficientes que permiten conocer el histórico, trayectoria de un producto o proceso a lo largo de la cadena de suministros en un momento dado, a través de una herramienta determinada;

UTIC: La unidad administrativa responsable de los servicios de tecnologías de la información y comunicaciones;

UC: Contratos de Servicios;

UGD: Unidad de Gobierno Digital;

Unidad administrativa: Unidad mínima a la que se le confieren atribuciones en el ordenamiento jurídico de organización de cada dependencia o entidad.

Universal Serial Bus - USB: Puerto que sirve para conectar periféricos con conexión serial a una computadora;

Usuarios: Son todas aquellas personas que tienen acceso a la infraestructura o servicios Institucionales de manera autorizada;

Validación: Es la acción de comprobar que los requerimientos de el área usuaria fueron cubiertos satisfactoriamente por la solución tecnológica adoptada;

Valor público: Se refiere al valor creado por el Estado a través de servicios, leyes, regulaciones y otras acciones que benefician a la ciudadanía;

Verificación: Es comprobar o examinar la certeza de la información de los requerimientos entregados por el usuario;

Virus informático: Es un programa informático que se ejecuta en la computadora sin previo aviso y que puede corromper el resto de los programas, directorios de datos e, incluso el mismo sistema operativo;

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas comprometiendo en consecuencia la confiabilidad, disponibilidad y/o integridad de la información;

WAN: red de cómputo que se encuentra distribuida en un área geográfica determinada como una ciudad o un estado, su finalidad está encaminada a enlazar los diferentes edificios de una organización;

Webservices: a la aplicación informática accesible mediante http, https y mensajes XML; y

WWW: World Wide Web es el sistema de documentos interconectados por enlaces de hipertexto, que se ejecutan en Internet, y

XML (eXtensible Markup Language): es el metalenguaje destinado a la creación de lenguaje de definición de datos, que permiten la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre redes.

De la regulación de tecnologías de la información y comunicaciones

Artículo 24.- Las dependencias y entidades deberán sujetarse en materia de tecnologías de la información y comunicaciones a las disposiciones generales siguientes y observarán los procesos señalados en su Manual:

Proceso de Establecimiento de estructura de gobierno de TIC

I. Establecer la estructura de gobierno de Tecnologías de la información y comunicaciones con el propósito de determinar las prioridades de inversión.
II. Mantener alineado el ejercicio del gasto en materia de tecnologías de la información y comunicaciones con los objetivos de la dependencia o entidad.

Proceso de Planeación estratégica de tecnologías de la información y comunicaciones

III. Elaborar anualmente un Plan estratégico con el objeto de establecer líneas de acción en materia de tecnologías de la información y comunicaciones, tomando en cuenta las disposiciones del Plan Nacional de Desarrollo, los programas sectoriales y especiales que apliquen, la Agenda de Gobierno Digital, así como los programas que de manera general emita la Secretaría de la Función Pública.

IV. El plan estratégico en materia de tecnologías de información y comunicaciones debe impulsar el cumplimiento de los objetivos y proyectos institucionales y contar con indicadores que permitan dar seguimiento al mismo, a fin de evaluar su efectividad.

Proceso de Determinación de la dirección tecnológica

V. Definir y establecer una arquitectura tecnológica para facilitar la selección, el desarrollo, aplicación y uso de las tecnologías de información y comunicaciones, que responda a los cambios de las necesidades de la organización.

Proceso de Administración del desempeño

VI. Establecer un sistema para el seguimiento y evaluación del desempeño en la implementación de la planeación estratégica, el desempeño de los procesos, de los proyectos, así como del uso y aprovechamiento de los activos, los recursos y la entrega de los servicios de tecnologías de la información y comunicaciones

Proceso de Cumplimiento regulatorio

VII. Sujetarse a través de las UTIC al marco regulatorio establecido en materia de tecnologías de información y comunicaciones.

VIII. Realizar evaluaciones a fin de vigilar el cumplimiento de los procesos, los procedimientos, metodologías y estándares para dar cumplimiento a los requerimientos legales y regulatorios en materia de tecnologías de información y comunicaciones.

Proceso de Administración de riesgos

IX. Administrar a través de las UTIC un inventario de riesgos en materia de tecnologías de información y comunicaciones, que les permita identificar, analizar, controlar y mitigar los mismos.

Proceso de Administración del portafolio de proyectos

X. Establecer a través de las UTIC un Grupo de Trabajo Estratégico de tecnologías de información y comunicaciones responsable de la administración del portafolio de proyectos en la materia, con funciones y atribuciones para su cumplimiento.

Proceso de Administración de proyectos.

XI. Sujetarse al proceso de administración de proyectos del Marco Rector de tecnologías de información y comunicaciones, considerando como mínimo lo siguiente:

a) Designar un responsable de la administración para cada proyecto de tecnologías de información y comunicaciones, y

b) Cumplir en tiempo, costo y forma lo establecido en los proyectos de tecnologías de información y comunicaciones.

Proceso de Sistema de gestión de procesos y calidad

XII. Garantizar que los procesos de tecnologías de información y comunicaciones:
a). se sustenten en el marco rector de procesos,

b). cuenten con indicadores establecidos para poder evaluar su desempeño, y

c). establezcan acciones de mejora de gestión de procesos y calidad.

XIII. La dependencia o entidad deberá vigilar que el personal que intervenga en la ejecución de los procesos cuente con la capacidad para desempeñar las actividades inherentes a cada proceso.

Proceso de Administración financiera

XIV. Administrar a través de las UTIC el presupuesto asignado para los servicios a las tecnologías de información y comunicaciones.

Proceso de Administración de proveedores

XV. Administrar a través de las UTIC los contratos en materia de tecnologías de información y comunicaciones.

Proceso de Adquisiciones de TIC

XVI. Elaborar y ejecutar a través de las UTIC un programa de adquisiciones de tecnologías de información y comunicaciones, sujetándose a las disposiciones aplicables.

Proceso de Administración del portafolio de servicios de TIC

XVII. Elaborar un portafolio de servicios de tecnologías de información y comunicaciones que describa los servicios prestados y permita la toma de decisiones en cuanto a su valor.

Proceso de Diseño de los servicios de TIC

XVIII. Diseñar y desarrollar a través de la UTIC los servicios que se definan en el portafolio de servicios de acuerdo a la orientación tecnológica de la dependencia o entidad.

XIX. Mantener actualizadas a través de la UTIC las necesidades de los usuarios así como los avances tecnológicos a fin aplicar mejoras continuas a los servicios ya incluidos en el portafolio de servicios o de generar nuevos servicios.

Proceso de Administración técnica de adquisiciones

XX. Observar lo dispuesto por la legislación vigente, su reglamentación, así como a las disposiciones administrativas que al respecto emitan las autoridades competentes, en la adquisición de productos o servicios relacionados con tecnologías de información y comunicaciones.

XXI. Considerar en la adquisición, desarrollo e intercambio de software, sistemas y aplicativos, por igual, soluciones comerciales, propietarias, libres o de código abierto.

XXII. Inscribir en el Instituto Nacional del Derecho de Autor, al momento de la conclusión del desarrollo de software, sistemas o aplicativos que realicen por sí o mediante la contratación de un tercero.

XXIII. Sustentar en justificaciones técnicas y económicas, la adquisición o desarrollo de soluciones tecnológicas, previo dictamen soportado documentalmente de la detección de necesidades,.

Proceso de Desarrollo de soluciones tecnológicas

XXIV. Desarrollar o contratar el desarrollo de soluciones tecnológicas únicamente cuando:

a). Posterior a la revisión de las capacidades de reutilización de código de sus sistemas, aplicativos, servicios web, componentes y demás código existente;

b). Después de validar y demostrar que no existen aplicaciones de software que puedan satisfacer las necesidades del área usuaria en el catálogo de software de sistemas de la Administración Pública Federal; y

c). Confirmar que no existen productos comerciales con una funcionalidad similar a la requerida, mediante una investigación de mercado.

XXV. Mantener actualizado su catálogo de software de sistemas en la dirección electrónica que establezca la SFP.

Proceso de Calidad de soluciones tecnológicas

XXVI. Establecer un Plan de calidad en el cual se incluyan las actividades necesarias para asegurar la verificación y validación de las soluciones tecnológicas, de acuerdo a sus ciclos de desarrollo.

Proceso de Administración de cambios

XXVII. Establecer a través de la UTIC las acciones necesarias para la administración de cambios a las soluciones de tecnologías de información y comunicaciones.

Proceso de Liberación y entrega

XXVIII. Vigilar a través de la UTIC que la solución tecnológica que se entrega a operación cumpla con los requerimientos previstos.

Proceso de Transición y habilitación de la operación

XXIX. Planear y coordinar a través de la UTIC los recursos y actividades tanto de proveedores internos como externos, para transferir un servicio o elemento nuevo o modificado al ambiente productivo.

Proceso de Administración de la configuración

XXX. Implementar a través de la UTIC un procedimiento que le permita administrar la configuración de la totalidad de las soluciones de tecnologías de información y comunicaciones, con el fin de asegurar una correcta aplicación de los planes de seguridad, de recuperación, de mitigación de riesgos.

Proceso de Mesa de servicios

XXXI. Establecer a través de la UTIC una Mesa de Servicios, con las funciones y atribuciones para atender los incidentes, requerimientos de servicios u otro tipo de solicitudes que al respecto formulen los usuarios de las tecnologías de información y comunicaciones.

XXXII. Difundir a través de la Mesa de Servicios las condiciones de uso de los recursos de tecnologías de información y comunicaciones.

XXXIII. Cumplir con las condiciones para el uso correcto, óptimo y seguro de los recursos de tecnologías de información y comunicaciones.

Proceso de Administración de servicios de terceros

XXXIV. Verificar a través de la UTIC que los servicios de tecnologías de información y comunicaciones proporcionados por un tercero, cumplan con los requerimientos técnicos y operativos del servicio contratado.

Proceso de Administración de niveles de servicio

XXXV. Establecer a través de la UTIC los niveles de servicio de acuerdo a su capacidad tecnológica instalada.

XXXVI. Asegurar a través de la UTIC que los niveles de servicio de las tecnologías de información y comunicaciones se encuentren alineados a los objetivos de servicio de la dependencia o entidad.

Proceso de Administración de la seguridad de la información

XXXVII. Administrar y verificar a través de las UTIC, el cumplimiento de las condiciones de seguridad y control de los activos y servicios de tecnologías de información y comunicaciones y adoptar las medidas necesarias en consecuencia.

XXXVIII. Definir e implementar el Sistema de Gestión de Seguridad de la Información (SGSI).

Proceso de Administración de dominios tecnológicos

XXXIX. Sustentar a través de la UTIC la administración de la arquitectura tecnológica en agrupaciones lógicas denominadas dominios tecnológicos.

XL. Establecer a través de la UTIC las condiciones para el uso adecuado y el aprovechamiento de los recursos de tecnologías de información y comunicaciones.

Proceso de Administración del conocimiento

XLI. Mantener permanentemente actualizado a través de la UTIC, un sistema de datos e información para el conocimiento de todos los activos relacionados con las tecnologías de información y comunicaciones, a fin de asegurar:

a) El cumplimiento de normatividad vigente,

b) Que los recursos puedan ser eficazmente utilizados por la dependencia o entidad de que se trate, y

c) Que se cumpla con los criterios de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, niveles de servicio y confiabilidad necesarios.

Proceso de Integración y desarrollo de personal

XLII. Desarrollar e implementar programas de desarrollo de personal idóneos para cumplir, de manera eficiente, con los objetivos de tecnologías de información y comunicaciones de la dependencia o entidad, evaluando y registrando los mismos.

Proceso de Administración de la operación

XLIII. Establecer a través de las UTIC reglas de operación y procedimientos necesarios para un eficaz procesamiento de datos, resguardo de la información y monitoreo de infraestructura, debiendo incluir eventos de errores, ataques y desastres

Proceso de Administración de ambiente físico

XLIV. Contaran con un centro de datos físico dentro de sus instalaciones o fuera de ellas, en territorio nacional para resguardo de la información descrita en el artículo anterior,

Proceso de Mantenimiento de infraestructura

XLV. Generar un plan de mantenimiento de la infraestructura de tecnologías de información y comunicaciones incluyendo las adquisiciones necesarias para asegurar el cumplimiento de los objetivos de operación, niveles de servicio y seguridad.

De la Firma electrónica avanzada

Artículo 25.- Las dependencias y entidades, con relación a la Firma electrónica avanzada, se sujetarán a las bases generales siguientes:

Base Primera: En el Manual General se establecen las políticas de homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal que al efecto deberán observar y promover las Secretarías de Economía y de la Función Pública, así como el Servicio de Administración Tributaria, para el reconocimiento de Certificados Digitales de Firma Electrónica Avanzada de personas físicas.

Base Segunda: El reconocimiento de Certificados Digitales se llevará a cabo mediante la implementación de una Infraestructura Tecnológica de Firma Electrónica Avanzada conforme a los medios y mecanismos de comunicación que la CIDGE ha definido como viables y que para su consulta se encuentran en la dirección electrónica http://www.cidge.gob.mx.

Base Tercera: De conformidad con la legislación aplicable, las Dependencias y/o Entidades de la Administración Pública Federal que requieran integrarse como AC en la ITFEA, con el fin de obtener el reconocimiento de sus Certificados Digitales, deberán ajustar sus procedimientos y formas de operación a efecto de cumplir con las presentes disposiciones relativas a la firma electrónica avanzada.

Base Cuarta: Lo establecido en las disposiciones de firma electrónica avanzada en este Manual General estará sujeto a las limitaciones previstas en las leyes vigentes, convenios y acuerdos de la materia, y en caso de existir incompatibilidades se elaborarán y promoverán las iniciativas de reformas legales y reglamentarias procedentes.

Funciones de la Subcomisión en el ámbito de la ITFEA

Base Quinta: De conformidad con el Artículo Vigésimo Cuarto, Fracción VII del Acuerdo por el cual se crea la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, la Subcomisión tendrá adicionalmente las siguientes funciones en el ámbito de operación de la ITFEA:

I. Coordinar con la Secretaría de Gobernación, por medio de la Dirección General del Registro Nacional de Población e Identificación Personal RENAPO, los mecanismos de registro e identificación de las personas, así como los procedimientos de certificación electrónica de identidad;

II. Integrar grupos de trabajo para llevar a cabo la revisión documental y de operación de la infraestructura tecnológica de las Dependencias, Entidades y, en su caso, de las Organizaciones e Instituciones que soliciten su integración como AC en la ITFEA;

III. Emitir el dictamen de acreditación para la integración de una AC a la ITFEA y en su caso, para la revocación o suspensión;

IV. Publicar la acreditación, revocación y/o suspensión de una AC en el Diario Oficial de la Federación, así como difundir y promover información de interés para los titulares de los Certificados Digitales de FEA;

V. Mantener la actualización permanente de las presentes disposiciones relativas a la firma electrónica avanzada y sus anexos. Para efectos de lo anterior, los anexos serán revisados periódicamente por la Subcomisión de firma electrónica avanzada y podrán ser modificados en cualquier momento, previa publicación en el Diario Oficial de la Federación y a través de la dirección electrónica http://www.cidge.gob.mx, según corresponda;

VI. Supervisar y revisar periódicamente la operación e infraestructura tecnológica de las AC que integran la ITFEA de acuerdo a las presentes disposiciones relativas a la firma electrónica avanzada;

VII. Emitir las recomendaciones de carácter técnico y operativo para el mejor funcionamiento de las AC;

VIII. Establecer procedimientos y mecanismos comunes dentro de la ITFEA para la conservación y sellado de tiempo de mensajes de datos que utilicen FEA;

IX. Promover la celebración de acuerdos de colaboración con otras Instituciones Públicas y/o Privadas para el desarrollo de la ITFEA, y

X. Difundir el ámbito de aplicación de los Certificados Digitales emitidos por las AC integrantes de la ITFEA.

Para efectos de las fracciones I, II, III, VI y VII de esta disposición, la SE será la encargada de realizar las actividades a que se refieren dichas fracciones con respecto de los PSC acreditados por ella.

Reconocimiento de Certificados Digitales de Firma Electrónica Avanzada de la ITFEA

Base Sexta: Los integrantes de la Subcomisión de firma electrónica avanzada de la CIDGE reconocerán mutuamente los Certificados Digitales emitidos por sus correspondientes AC, cuando dichos Certificados hayan sido expedidos conforme a lo previsto en las presentes disposiciones relativas a la firma electrónica avanzada.

Los Certificados Digitales emitidos por las AC de las Dependencias, Entidades, Organizaciones e Instituciones podrán ser reconocidos cuando éstas formen parte de la ITFEA.

Integración a la ITFEA

Base Séptima: Los integrantes de la Subcomisión de firma electrónica avanzada se asegurarán de que cualquier dependencia, entidad, organización e institución que requiera integrarse como AC en la ITFEA lleve a cabo las siguientes actividades:

I. Solicitud: Las AC elaborarán la solicitud correspondiente, de acuerdo al formato de Solicitud de Integración a la ITFEA (F2) que se encuentra en la dirección electrónica http://www.cidge.gob.mx;

La SFP coordinará las solicitudes de las Dependencias y Entidades para integrase como AC en la ITFEA, y celebrará, en su caso, los acuerdos correspondientes.

Las solicitudes por parte de las Organizaciones e Instituciones deberán dirigirse a cualquiera de los integrantes de la Subcomisión de firma electrónica avanzada de la CIDGE.

La Subcomisión de firma electrónica avanzada publicará en el Diario Oficial de la Federación y por medio de la dirección electrónica http://www.cidge.gob.mx las AC que formen parte de la ITFEA. Los interesados podrán solicitar su Certificado Digital en cualquiera de estas AC;

II. Revisión documental de la infraestructura tecnológica: La Subcomisión de firma electrónica avanzada de la CIDGE revisará la información documental de la infraestructura tecnológica de la AC solicitante, de acuerdo al formato de Revisión Documental de la Infraestructura Tecnológica (F3) que se encuentra en la dirección electrónica http://www.cidge.gob.mx;

III. Revisión de la Operación de la Infraestructura Tecnológica: La Subcomisión revisará la infraestructura tecnológica de la AC solicitante, de acuerdo al formato de Revisión de la Operación de la Infraestructura Tecnológica (F4) que se encuentra en la dirección electrónica http://www.cidge.gob.mx, y

IV. Dictamen: La Subcomisión elaborará un reporte de los resultados obtenidos en la revisión documental y de operación de la infraestructura tecnológica de la AC solicitante y emitirá dentro de un plazo de 45 días hábiles un dictamen con la resolución correspondiente. En su caso, la Subcomisión de firma electrónica avanzada de la CIDGE expedirá la acreditación con una vigencia máxima de cinco años. La acreditación implica que la AC se integre a la ITFEA y que sus certificados digitales sean reconocidos por la Administración Pública Federal y por los integrantes de la ITFEA.

Para efectos de las presentes disposiciones, la SE coordinará lo relacionado con la integración a la ITFEA de los PSC acreditados por la misma y establecerá los acuerdos o convenios de colaboración correspondientes.

Para efectos del reconocimiento mutuo de los Certificados Digitales a que se alude en la **Base Sexta** de las presentes disposiciones de firma electrónica avanzada, los integrantes de la Subcomisión, de firma electrónica avanzada que no cumplan con esa disposición, no podrán ser reconocidos sus Certificados Digitales por el resto de los integrantes de la misma.

Solicitud de un Certificado Digital de Firma Electrónica Avanzada

Base Octava: Los integrantes de la subcomisión de la firma electrónica avanzada deberán asegurarse de que para la obtención de un Certificado Digital de FEA, el solicitante y la correspondiente AC lleven a cabo las siguientes actividades:

I. Obtener la Solicitud de Certificado Digital de Firma Electrónica Avanzada (F5) que se encuentra en los anexos de relativos a las disposiciones de firma electrónica avanzada. Esta Solicitud también estará disponible en la dirección electrónica http://www.cidge.gob.mx o en la ventanilla de la Dependencia, Entidad, Organización o Institución que cuente con una AC incorporada a la ITFEA;

II. Firmar de manera autógrafa la Solicitud de Certificado Digital de Firma Electrónica Avanzada, aceptando los Términos y Condiciones establecidos en la misma, reconociendo como propia y auténtica la información proporcionada;

III. Generar su clave privada y Requerimiento de Certificación, mediante los programas de cómputo que deberá poner a su disposición la AC, o bien a través de otros que cumplan con la funcionalidad requerida;

IV. Resguardar bajo su responsabilidad la clave privada en un medio electrónico, óptico o magnético de acuerdo con las disposiciones que al efecto establezcan las AC de las Dependencias, Entidades, Organizaciones e Instituciones;

V. Presentar la Solicitud de Certificado Digital de Firma Electrónica Avanzada y el archivo que contenga el Requerimiento de Certificación en la ventanilla de la Dependencia, Entidad, Organización o Institución que cuente con una AC incorporada a la ITFEA e identificarse con cualquiera de los Documentos de Identidad y Documentos Probatorios de Identidad señalados en los anexos relativos a las presentes disposiciones relativas a la firma electrónica avanzada;

VI. Permitir que la AC realice el procedimiento de certificación electrónica de identidad mediante el registro de huellas dactilares, fotografía, firma autógrafa y digitalización de documentos, y

VII. Acusar recibo del Comprobante de Emisión del Certificado Digital de Firma Electrónica Avanzada expedido por la AC al momento de recibir dicho certificado, de acuerdo a los anexos relativos a las presentes disposiciones relativas a la firma electrónica avanzada. El solicitante recibirá su Certificado Digital en un plazo no mayor a diez días hábiles.

Revocación de un Certificado Digital de Firma Electrónica Avanzada

Base Novena: Los Certificados Digitales de Firma Electrónica Avanzada quedarán sin efectos por cualquiera de las siguientes causas:

I. Por extinción del periodo de validez del propio certificado digital de firma electrónica avanzada;

II. Al comprobar la AC que la clave privada se ha duplicado o por cualquier otra razón en la que se encuentre comprometida la integridad o confidencialidad del Titular del Certificado Digital;

III. A solicitud del Titular del Certificado Digital;

IV. Por fallecimiento del Titular del Certificado Digital;

V. Por incapacidad jurídica del mismo, declarada por una autoridad competente;

VI. Por resolución judicial;

VII. Al comprobar la AC que el Titular del Certificado Digital incumplió las obligaciones contraídas al responsabilizarse de su uso;

VIII. Al comprobar la AC la falsedad o errores en los datos aportados por el Titular del Certificado Digital;

Base Décima: Los integrantes de la subcomisión de la firma electrónica avanzada deberán asegurarse de que para la solicitud de revocación de un Certificado Digital de FEA, el titular de la firma digital y la correspondiente AC lleven a cabo las siguientes actividades:

I. El titular de la firma digital acuda a la ventanilla de la Dependencia, Entidad, Organización o Institución que le emitió el Certificado Digital;

II. El titular de la firma digital presente cualquiera de los Documentos de Identidad señalados en los anexos relativos a las presentes disposiciones relativas a la firma electrónica avanzada;

III. El solicitante presente un escrito libre con firma autógrafa del Titular del certificado digital o su representante legal, en su caso, donde se señale la causa por la cual se solicita la revocación del Certificado. Este escrito deberá contener lo siguiente:

a) Nombre del titular;

b) CURP;

c) RFC;

d) Domicilio: calle, número, colonia, código postal y entidad federativa. Para solicitudes de revocación de Certificados Digitales emitidos por el SAT, los titulares deberán manifestar su domicilio fiscal, y
e) Nombre de la AC de la Dependencia, Entidad, Organización o Institución a quien va dirigida la solicitud, y

IV. Presentar un poder especial para efectos de la solicitud de revocación del Certificado Digital de que se trate, cuando dicha solicitud se realice a través de un representante legal, y

V. Acusar recibo del Comprobante de Revocación de Certificado Digital de FEA expedido por la AC, en donde conste la fecha y hora de la revocación, de acuerdo a los anexos relativos a las presentes disposiciones relativas a la firma electrónica avanzada.

Para efectos de las presentes disposiciones relativas a la firma electrónica avanzada las AC pondrán a disposición de los titulares de firma digital la opción para revocar los Certificados Digitales en línea.

Estructura del Certificado Digital

Base Décima Primera: Los Certificados Digitales de FEA para ser reconocidos dentro de la ITFEA deberán contener al menos lo siguiente:

I. Número de Serie;

II. Emisor;

III. Algoritmo de firma;

IV. Periodo de validez;

V. Nombre del Titular del Certificado Digital;

VI. Registro Federal de Contribuyentes del Titular del Certificado Digital (RFC);

VII. Clave Única del Registro de Población del Titular del Certificado Digital (CURP), y

VIII. Clave Pública.

El formato de la estructura del Certificado Digital y la información de los campos y sus atributos está definido en el anexo Estándares y Estructura del Certificado Digital (F6) que se encuentra en la dirección electrónica http://www.cidge.gob.mx.

Obligaciones de la Subcomisión de firma electrónica avanzada con relación a las AC

Base Décima Segunda: Los integrantes de la subcomisión de firma electrónica avanzada deberán asegurarse de que las AC lleven a cabo lo siguiente:

I. Publicar en su página de Internet las disposiciones que emita la Subcomisión de FEA, así como los procedimientos y requisitos que deberán cumplir los solicitantes para la obtención de un Certificado Digital;

II. Proporcionar al solicitante de un Certificado Digital de FEA, los programas de cómputo necesarios para la generación de sus claves privada y pública, en forma secreta y bajo su total control. En caso de que el solicitante requiera utilizar un programa de cómputo distinto al proporcionado por la AC, el programa deberá cumplir con lo establecido en el anexo Estándares y Estructura del Certificado Digital;

III. Requerir para la identificación del solicitante de un Certificado Digital, su comparecencia personal y directa, así como la presentación de un Documento de Identidad y de un Documento Probatorio de Identidad de los que se señalan en el Anexo I de las presentes disposiciones relativas a la firma electrónica avanzada;

IV. Obtener la Solicitud de Certificado Digital de Firma Electrónica Avanzada con firma autógrafa del solicitante, en donde manifieste su conformidad con los Términos y Condiciones de Uso establecidos;

V. Validar que el solicitante cuente con Clave Única de Registro de Población (CURP) y Registro Federal de Contribuyentes (RFC) vigentes conforme al Procedimiento para la Validación de CURP y RFC (F7) que se encuentra en la dirección electrónica http://www.cidge.gob.mx;

VI. Validar la coincidencia entre los datos de la Solicitud de Certificado Digital de Firma Electrónica Avanzada, los datos del Documento de Identidad y del Documento Probatorio de Identidad presentados por el solicitante;

VII. Registrar los datos de identidad electrónica del solicitante conforme al Procedimiento para la Captura de Elementos Biométricos (F8), que se encuentra en la dirección electrónica http://www.cidge.gob.mx;

VIII. Enviar al Registro Nacional de Población la información correspondiente al registro electrónico de los datos de identidad conforme al Procedimiento para la Integración del Registro Nacional de Población (F9) que se encuentra en la dirección electrónica http://www.cidge.gob.mx;

IX. Llevar a cabo el Procedimiento de Verificación de la Unicidad de la Clave Pública (F10), que se encuentra en la dirección electrónica http://www.cidge.gob.mx;

X. Emitir Certificados Digitales que cumplan con las características previstas en las presentes disposiciones de firma electrónica avanzada. Los Certificados deberán tener una vigencia máxima de dos años;

XI. Informar al solicitante sus derechos y obligaciones como Titular de un Certificado Digital;

XII. Obtener del Titular el Acuse de Recibo de Certificado Digital de Firma Electrónica Avanzada, conforme a los anexos relativos a las presentes disposiciones relativas a la firma electrónica avanzada;

XIII. Resguardar los datos de identidad electrónica y documentación proporcionada por el Titular para su identificación, así como de los documentos a que se refieren los numerales IV y XII de la presente disposición, conforme a la normatividad establecida en materia de transparencia, acceso a la información pública y protección de datos;

XIV. Contar con un RCD en línea, indicando el estado de los Certificados Digitales emitidos: vigentes o revocados. El registro se mantendrá disponible y actualizado en todo momento;

XV. Recibir del Titular de un Certificado Digital la Solicitud de Revocación, así como expedir un comprobante, en el que conste la fecha y hora en que ésta se lleve a cabo;

XVI. Ofrecer el servicio de revocación de Certificados Digitales en línea;

XVII. Contar con medidas de seguridad para proteger la infraestructura tecnológica, los procesos, la información y los datos derivados de la operación como AC;

XVIII. Contar con medidas y mecanismos de respaldo de información de acuerdo a la normatividad establecida en la materia;

XIX. Contar con un plan de recuperación de desastres, de respaldo de información y contingencia por fallas en la operación;

XX. Proporcionar a la Subcomisión la información que ésta le requiera en relación con sus actividades de registro y de operación, así como permitir el acceso a sus instalaciones a personas autorizadas por la misma, a fin de que puedan verificar el cumplimiento de los requisitos previstos en presentes disposiciones relativas a la firma electrónica avanzada, incluyendo la revisión de la seguridad física y lógica de su infraestructura tecnológica, y

XXI. Solicitar a la Subcomisión de firma electrónica avanzada con una antelación no menor a 60 días naturales, la revocación de la autorización que ésta le haya otorgado, cuando pretenda dejar de prestar servicios como AC. En dicha solicitud deberá señalar el nombre de la AC a quien vaya a transferir el RCD que mantiene y administra con su respectivo respaldo, así como

la información y documentación referida en la fracción XIII de esta Base. A más tardar el tercer día hábil siguiente a la presentación de la mencionada solicitud, deberá hacer del conocimiento de los titulares cuyos Certificados Digitales haya emitido, su intención de dejar de actuar como AC y el destino que pretende dar al RCD, así como los datos y documentos de identificación que recibió de ellos.

Uso de los Certificados Digitales de FEA

Base Décima Tercera: La Subcomisión de firma electrónica avanzada verificará que las dependencias, entidades, organizaciones e instituciones utilicen los Certificados Digitales emitidos por los integrantes de la ITFEA en sus sistemas informáticos, aplicaciones, trámites y servicios electrónicos, asegurando que:

I. Garanticen la interoperabilidad entre sus sistemas informáticos y los Certificados Digitales antes mencionados;

II. Definan las atribuciones que cada Titular de un Certificado Digital tenga dentro de sus sistemas informáticos, aplicaciones, trámites y servicios electrónicos y

III. Verifiquen el estado de vigencia o revocación de los Certificados Digitales antes de aceptar el uso de los sistemas informáticos, aplicaciones, trámites y servicios electrónicos.

De los Sistemas automatizados de control de gestión

Artículo 26.- Las dependencias y entidades, en materia de operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, se sujetarán a las bases generales siguientes:

Base Primera: Las presentes disposiciones relativas a la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión tienen por objeto establecer las directrices que deberán observar las Dependencias y Entidades de la Administración Pública Federal para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, que permitan homologar, estandarizar y hacer compatible su uso entre ellas, mediante la utilización de medios y firma electrónicos en el intercambio de información, a fin de:

a). Mejorar la gestión y trámites de los asuntos administrativos mediante el uso de medios electrónicos;

b). Contar con un único sistema automatizado de control de gestión por cada dependencia o entidad;

c). Asegurar la confidencialidad, integridad y resguardo de la información acorde a los ordenamientos legales aplicables;

d). Permitir la intercomunicación entre los sistemas de control de gestión con que cuenten las Dependencias y Entidades;

e). Utilizar la firma electrónica avanzada como medio de autenticación del documento electrónico gubernamental y como método alternativo a la firma autógrafa; y

f). Disminuir sustancialmente el uso de papel y mensajería.

Base Segunda.- En la operación, adquisición o desarrollo de un Sistema Automatizado de Control de Gestión, deberán ajustarse a los requerimientos mínimos de funcionalidad, comunicación y seguridad previstos en las presentes disposiciones relativas a la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.

Base Tercera.- El uso de un Sistema Automatizado de Control de Gestión deberá permitir la generación y manejo de documentos electrónicos gubernamentales, los cuales deberán cumplir con las especificaciones de formato y seguridad previstas en los presentes Disposiciones relativas a la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.

Base Cuarta.- La estandarización de los sistemas automatizados de control de gestión y la comunicación entre las Dependencias y Entidades, a través del uso de medios y firma de identificación electrónicos, se realizará de acuerdo con la suficiencia presupuestaria que resulte con cargo a sus respectivos presupuestos autorizados.

Operación y funcionalidad

Base Quinta.- Los requisitos mínimos generales de operación y funcionalidad de los sistemas automatizados de control de gestión que deberán cumplirse son los siguientes:

I. Permitir el registro de información del asunto de que se trate, así como adjuntar, digitalizar, turnar, almacenar y visualizar documentos electrónicos gubernamentales, por lo menos con los siguientes tipos de aplicaciones: manejadores de imágenes, procesadores de texto, hojas de cálculo, graficadores y presentaciones;

II. Resguardar, almacenar y respaldar la información y documentos electrónicos gubernamentales, conforme a los ordenamientos legales aplicables, garantizando el ciclo de vida de la información;

III. Utilizar plantillas para el manejo de asuntos que deben contener por lo menos la siguiente información, sin perjuicio de que, de ser el caso, se atienda lo establecido en la Ley Federal de Procedimiento Administrativo respecto de la regulación, elementos, requisitos y emisión del acto administrativo:

   a) Folios, tanto para el remitente como para el destinatario;

   b) Fechas de elaboración, de recepción, de compromiso y de respuesta del documento electrónico gubernamental;

   c) Tema y descripción del asunto;

d) Nombre, cargo e institución del remitente;

e) Nombre, cargo e institución del destinatario;

f) El escudo nacional en aquellos que en papel deban contenerlo, conforme a los ordenamientos legales aplicables;

g) En su caso, el tipo de instrucción para la atención del asunto; y

h) El estado que guarda el asunto.

IV. Dar seguimiento a los asuntos, de tal manera que se puedan identificar al menos:

a) Las fechas, en su caso instrucciones, y datos de recepción, modificación y conclusión;

b) Los turnos generados;

c) Los documentos relacionados; y

d) Las acciones realizadas para su resolución.

V. Realizar búsquedas de asuntos o documentos electrónicos gubernamentales, de tal manera que se identifiquen a través de los campos señalados en las fracciones III y IV;

VI. Generar reportes operativos y estadísticos por lo menos de los siguientes temas: estado de los asuntos, rango de fechas, temas, remitente y destinatario;

VII. - Brindar asistencia en línea para resolver dudas o preguntas frecuentes a los usuarios;

VIII. - Administrar de manera centralizada los flujos de información; y

IX. Permitir la emisión del recibo digital de documentos electrónicos gubernamentales.

Comunicaciones e interoperabilidad

Base Sexta.- Las Dependencias y Entidades que efectúen entre sí gestiones, comunicaciones y trámites del documento electrónico gubernamental, por medio de los sistemas automatizados de control de gestión, deberán cumplir con los siguientes requisitos mínimos de comunicación e interoperabilidad:

I. Contar con una interfaz basada en WEBSERVICES que permita la interoperabilidad con los sistemas automatizados de control de gestión de las otras Dependencias y Entidades;

II. Las interfaces deberán proveer al menos los siguientes servicios:

a) Envío de documentos electrónicos gubernamentales;

b) Recepción de documentos electrónicos gubernamentales; y

c) Consulta de información sobre el intercambio del documento electrónico gubernamental;

III. Envío y recepción de asuntos entre Dependencias o Entidades con generación de sellos de recibo digitales, y;

IV. La comunicación entre sistemas automatizados de control de gestión se deberá establecer utilizando conexiones con protocolo HTTPS.

Base Séptima.- El intercambio del documento electrónico gubernamental deberá tener las siguientes características:

I. Utilizar el estándar XML;

II. Ser enviado a través de Redes basadas en el protocolo TCP/IP; y

III. Cumplir con los estándares de información para WEBSERVICES, .que se definan en términos de las presentes disposiciones relativas a la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.

Seguridad

Base Octava.- Los requerimientos mínimos generales de seguridad que deberán tener los sistemas automatizados de control de gestión son:

I. . Registrar y mantener bitácoras de las operaciones efectuadas;

II. . Definir usuarios y privilegios de manera personalizada; acceder a la aplicación por medio de clave de usuario y contraseña personalizados;

III. . Almacenar claves de usuario, perfiles y contraseñas utilizando técnicas de cifrado que cumplan los estándares nacionales o internacionales;

IV. . Permitir el manejo de la firma electrónica avanzada para la autenticación del documento electrónico gubernamental;

V. . Permitir el cifrado de documentos electrónicos gubernamentales mediante el uso del certificado digital; y

VI. . Contar con herramientas de antivirus que permitan minimizar el riesgo de que los mensajes recibidos y enviados se encuentren infectados.

Base Novena.- La seguridad del documento electrónico gubernamental deberá:

I. Proveer mecanismos para detectar y/o evitar alteraciones sobre los documentos y mensajes contemplados;

II. Permitir el uso de la firma electrónica avanzada para garantizar el no repudio, con lo cual la parte firmante no podrá negar la autoría de un mensaje enviado; y

III. En su caso, mantener la clasificación de la información con base a la legislación aplicable.

Base Décima.- Los requerimientos mínimos generales de autenticidad que deberán tener los sistemas automatizados de control de gestión se ajustarán a lo que disponga la Subcomisión de Firma Electrónica Avanzada de la CIDGE.

Base Décima primera.- Los requerimientos mínimos generales de disponibilidad que deberán tener los sistemas automatizados de control de gestión son:

I. Contar con los mecanismos necesarios que permitan la comunicación entre ellos, para garantizar el envío y la recepción de los documentos electrónicos Gubernamentales; y

II. Contar con un mecanismo alternativo de comunicación a través de un plan de contingencia.

Base Décima segunda.- Las Dependencias y Entidades serán responsables de Elaborar, con base en el estándar LDAP, el directorio de funcionarios o servidores públicos para el uso de los sistemas automatizados de control de gestión, así como mantenerlo actualizado.

Instrumentación

Base Décima tercera.- La instrumentación del Sistema Automatizado de Control de Gestión podrá ser ejecutada en cada Dependencia y Entidad considerando dos etapas:

I. Instrumentación del Sistema dentro de la Dependencia y Entidad; e

II. Instrumentación automatizada de la interoperabilidad del Sistema con otras Dependencias y Entidades.

Base Décima cuarta.- Los detalles para la operación, funcionalidad y seguridad de los sistemas automatizados de control de gestión, se establecen en anexos técnicos a estas disposiciones relativas a la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión que emita la Subcomisión de los Sistemas Automatizados de Control de Gestión de la CIDGE.

De la Seguridad de la información

Artículo 27.- Las dependencias y entidades, en materia de seguridad de la información, se sujetarán a las bases generales siguientes:

Generales

Base Primera.- Las presentes disposiciones relativas a seguridad de la información en posesión de las dependencias y entidades de la APF tienen por objeto dar a conocer los criterios que permitan administrar la seguridad de la información en posesión de las dependencias y entidades de la APF, a través del establecimiento de las medidas esenciales de índole administrativa, física y técnica que permitan mantener la confidencialidad, integridad y disponibilidad de la misma.

Base Segunda.- Las disposiciones relativas a seguridad de la información en posesión de las dependencias y entidades de la APF, deberán ser aplicados a toda la APF, con respecto a la información que tengan en su resguardo, a los recursos y procesos, sean éstos internos o externos, vinculados a la dependencia o entidad a través de contratos o acuerdos con terceros.

Sistema de Gestión de Seguridad de la Información SGSI

Base Tercera.- Las Dependencias y Entidades deberán Establecer un sistema de gestión de seguridad de la información, debidamente documentado, el cual permitirá la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de la seguridad de la información. A efecto de lo anterior, podrán basarse en estándares, normas, marcos de referencia y mejores prácticas, tanto nacionales como internacionales, alineados a la familia de estándares ISO/IEC 27000.

Base Cuarta.- El SGSI deberá comprender las siguientes fases cíclicas:

I. **Fase 1.** La definición de objetivos, procesos y procedimientos relacionados con la seguridad de la información, la aplicación de las disposiciones del presente Manual General, la gestión de riesgos y la mejora continua de la seguridad de la información, alineados a las atribuciones de las dependencias o entidades;

II. **Fase 2.** La implementación y operación de la aplicación de las disposiciones del presente Manual General, controles, procesos y procedimientos del sistema de gestión de seguridad de la información;

III. **Fase 3.** La evaluación y la medición del desempeño de los procesos en comparación con la política, objetivos y experiencia práctica del SGSI, así como la elaboración del respectivo reporte de resultados para su revisión por parte del Grupo de Seguridad de la Información; y

IV. **Fase 4.** La ejecución de acciones correctivas y preventivas basadas en los resultados de auditorías internas (las realizadas por los servidores públicos designados o por terceros contratados para tal fin) y de auditorías externas (las realizadas por las áreas designadas por la dependencia o entidad o por terceros previamente designados y autorizados por ésta), así como en la revisión del reporte de resultados del grupo de Seguridad de la Información y otra información relevante con el propósito de lograr la mejora continua del SGSI.

De los controles del SGSI

Base Quinta.- Los controles que se deben establecer con el SGSI, son:

I. **Disposiciones de seguridad:** Comprende todas las disposiciones relativas a seguridad de la información en posesión de las entidades y dependencias de la APF. Se complementan con las que se definen en el procedimiento correspondiente del presente manual General. Pueden ser también complementadas con las específicas que se deriven de los procedimientos institucionales.

II. **Organización de la seguridad de información:** Administrar la seguridad de la información dentro de las Dependencias y entidades en un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades. Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información, así como garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de las dependencias y entidades.

III. **Clasificación y control de activos**: Garantiza que los activos de información reciban un apropiado nivel de protección, así como designa a los propietarios de la información existente en el Organismo. Clasificar la información para señalar su sensibilidad y criticidad y definir niveles de protección y medidas de tratamiento especial acordes a su clasificación, incluyendo intrusiones y vulnerabilidades.

IV. **Seguridad relacionada a los recursos humanos:** Establecer las responsabilidades de los servidores públicos en cuanto a la seguridad de la información: uso de equipos e instalaciones, uso y manejo autorizados de información. Establecer acuerdos de confidencialidad con los servidores públicos y personal externo sobre la seguridad de la información.

V. **Seguridad física:** Prevenir e impedir accesos no autorizados, daños e interferencia a las dependencias o entidades de la APF, a sus instalaciones, equipo e información en su poder. Asegurar la infraestructura, equipo e información crítica, a través de áreas protegidas y resguardadas, que tengas seguridad y controles de acceso. En su caso, considerar la protección durante algún traslado y/o permanencia fuera de la dependencia o entidad, así como tomar en cuenta factores ambientales que pudieran afectar el funcionamiento del equipo o de la información. Proteger la información que manejan los servidores públicos en las oficinas en los equipos personales dentro de sus labores.

VI. **Gestión de comunicaciones y operaciones:** Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas y procedimientos para la respuesta a incidentes y separación de funciones.

VII. **Control de accesos:** Permitir o denegar el uso o acceso de un dato o información, recurso particular a una entidad en particular. Los mecanismos para el control de acceso pueden ser usados para cuidar información.

VIII. Adquisición, desarrollo, uso y mantenimiento de los sistemas de información: Se refiere a la incorporación de medidas de seguridad, como son controles y validaciones en los sistemas de información, a partir de su adquisición, desarrollo, implementación y su mantenimiento, siguiendo una metodología de ciclo de vida de los sistemas de información.

IX. Administración de incidentes de seguridad de la información: Se refiere al manejo integral de incidentes relativos a la seguridad de la información, evaluar y vigilar los incidentes, obtener reportes para identificar aquellos que sean recurrentes o de alto impacto. Establecer la necesidad de mejorar o agregar controles para eliminar o limitar su frecuencia, daño y costo en nuevos casos o de recurrencia, así como establecer dar una respuesta rápita, eficaz y sistemática al presentarse un incidente.

X. Continuidad de las operaciones: Minimizar los efectos de las posibles interrupciones de las operaciones normales de las dependencias y entidades, (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro. Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas: Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan; Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original; Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales. Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar responsabilidades para cada actividad definida.

XI. Cumplimiento de la normatividad aplicable: Cumplir con las disposiciones legales, normativas y contractuales a fin de evitar sanciones administrativas y legales a las dependencias y entidades y/o al los servidores públicos. Garantizar que los sistemas cumplan con las Políticas y estándares de seguridad. Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de las Políticas y estándares de seguridad, sobre las plataformas tecnológicas y los sistemas de información. Optimizar la eficacia del proceso de auditoría de sistemas de la información y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo. Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías y determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

XII. Seguridad de los Sistemas de Información: Es la preparación de estrategias que permitan que la información circule libremente, garantizando al mismo tiempo la seguridad del uso de los sistemas de información en toda la Dependencia o Entidad. Se concentra en garantizar el derecho a acceder a datos, información y recursos, implementando mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Base Sexta.- La definición de las disposiciones de seguridad, la Organización de la seguridad de información y la Clasificación y control de activos del SGSI, deberán incluir sin excepción, los elementos que a continuación se describen:

a) Objetivos;

b) Ámbito de aplicación;

c) Identificación de activos sujetos de protección y los responsables de tales activos;

d) Líneas de acción respecto a la seguridad de la información;

e) Asignación de responsabilidades generales y específicas a los roles involucrados; relación con procedimientos de implementación.

De las disposiciones de seguridad en el SGSI

Base Séptima.- Las UTIC en relación a las disposiciones en seguridad de la información en posesión de las dependencias y entidades de la APF del SGSI deberán asegurar:

I. La autorización de su contenido por parte del grupo de Seguridad de la Información;

II. La publicación y difusión al interior de la dependencia o entidad, por parte del Área de Seguridad de la Información; y

III. La evaluación de su implementación al interior de la dependencia o entidad, por parte de la Unidad Administrativa de Auditoría de Seguridad de la Información.

Base Octava.- Para la mejora continua del SGSI al respecto de la aplicación de las disposiciones relativas a seguridad de la información, es requisito implementar el ciclo de desarrollo, revisión y evaluación siguiente:

I. La asignación de un responsable del desarrollo, revisión y evaluación;

II. El establecimiento de mecanismos para que la revisión del cumplimiento de las políticas se realice mediante la exhibición de evidencias de cumplimiento, que permitan una evaluación cuantitativa y cualitativa de éstas. En caso de incumplimiento, se deberán precisar las acciones correctivas que la dependencia o entidad tomará mientras no quede resuelto el problema raíz, así como el plan de trabajo correspondiente;

III. La evaluación de áreas de oportunidad para mejora de la política de seguridad, considerando para ello, la retroalimentación de las áreas usuarias, estatus de acciones preventivas y correctivas, resultados de revisiones anteriores, cumplimiento de la política, nuevas amenazas y vulnerabilidades, incidentes de seguridad así como las recomendaciones que sean realizadas por el Comité de Seguridad de la Información;

IV. La interrelación continua con el Área de Seguridad de la Información a efecto de conocer los cambios en la dependencia o entidad, con respecto a la organización, marco jurídico, condiciones tecnológicas y cualquier otro que impacte en la necesaria adecuación del contenido de la política de seguridad;

V. El reporte continuo que consistirá en conservar una bitácora histórica y actualizada de las propuestas de mejora y cambios realizados en la política de seguridad; y

VI. La aprobación del Comité de Seguridad de la Información de cada uno de los cambios y/o mejoras que se realicen en la política de seguridad.

SGSI: de la organización de la Seguridad de la Información

Base Novena.- Las dependencias y entidades, deberán clasificar y organizar la información que requiera protegerse, así como establecer controles a través de los cuales se gestione la seguridad de los activos, tanto al interior de las mismas como con terceros.

Base Décima.- Con respecto a los controles de las dependencias y entidades, se debe considerar en el establecimiento de los mismos, los siguientes requisitos:

I. El apoyo y compromiso de los funcionarios de altos mandos y medios de la dependencia o entidad, manifestado a través del impulso a iniciativas, de una adecuada toma de decisiones, asignación de recursos y designación de responsabilidades en el ámbito de la seguridad de la información;

II. La clasificación de la información en términos de lo que establece la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y su normatividad derivada;

III. El contacto previo con autoridades, proveedores de servicios y centros de respuesta ante incidentes relacionados con la seguridad de la información;

IV. La interrelación con asociaciones e instituciones relacionadas con la seguridad de la información, a efecto de permanecer actualizados en las mejores prácticas relativas con la dependencia o entidad, sobre la seguridad de la información; y

V. La revisión independiente de la seguridad de la información realizada en intervalos planeados o cuando ocurran cambios significativos en la implementación, la revisión deberá llevarse a cabo por individuos independientes al área evaluada, ya sean auditores internos o externos;

VI. La identificación de riesgos derivados del intercambio de información con terceros (control externo);

VII. La identificación de controles de seguridad orientados a mitigar los riesgos que derivan de las transmisiones de información a terceros (control externo);

Base Décima primera.- Para la formalización de los controles de la seguridad de la información, es requisito que se cumpla el siguiente ciclo de gestión:

I. El proceso de autorización de los mecanismos utilizados para el procesamiento de información deberá ser expedido por el Área de Seguridad de la Información;

II. La publicación y difusión al interior de la dependencia o entidad por parte del Área de Seguridad de la Información; y

III. La evaluación de su implementación en la dependencia o entidad por parte de los servidores públicos designados o terceros contratados para tal fin.

SGSI: de la clasificación y control de activos

Base Décima segunda.- Las dependencias y dependencias, deberán establecer y revisar controles para la identificación, inventario, clasificación y valuación de activos, de acuerdo a los procedimientos y normatividad aplicable establecida en los Manuales Generales de las materias correspondientes.

Base Décima tercera.- Los documentos o expedientes, relativos a los activos, serán clasificados tanto en materia archivística como por el contenido de su información, tomando en consideración las disposiciones que establece el manual General en la materia, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su normatividad derivada y demás leyes o reglamentos establecidas por el IFAI, el AGN y demás normatividad aplicable.

Base Décima cuarta.- Los elementos del SGSI deberán incluir en su definición lo siguiente:

I. Objetivos;

II. Ámbito de aplicación;

III. Identificación de activos sujetos de protección y los responsables de tales activos;

IV. Asignación de roles y responsabilidades generales;

V. Asignación de roles y responsabilidades específicas;

SGSI: de la seguridad relacionada a los recursos humanos

Base Décima quinta.- Las dependencias y entidades, deberán establecer controles orientados a que los servidores públicos de las unidades administrativas, o terceros contratados, conozcan el alcance de sus responsabilidades respecto de la seguridad de los activos, antes, durante y al finalizar la relación laboral o contractual, para que estén conscientes de las consecuencias de la ejecución de conductas que puedan ir en contra de la normatividad aplicable en la materia.

Base Décima sexta.- Con respecto a los controles que se deben establecer antes de dar inicio a la relación laboral o contractual, se deben considerar por lo menos los siguientes requisitos:

I. El procedimiento de evaluación del personal interno, así como del personal relacionado con terceros a los que se les dará acceso a la información;

II. La inclusión de las obligaciones de los servidores públicos en relación a la custodia de los activos a los que tiene acceso en el ejercicio de sus atribuciones; y

III. La inclusión de cláusulas de confidencialidad en la contratación de terceros.

Base Décima séptima.- Con respecto a los controles que se deben establecer durante la relación laboral o contractual, se deben considerar por lo menos los siguientes requisitos:

I. La difusión de las disposiciones establecidas en los controles de seguridad de la información;

II. El programa de capacitación continua con respecto a la implementación de controles de seguridad de la información; y

III. La inclusión de un marco de sanciones.

Base Décima octava.- Con respecto a los controles que se deben establecer al finalizar la relación laboral o contractual, considerarán por lo menos el procedimiento para la devolución de activos de información al finalizar la relación laboral con personal interno y externo, incluyendo todo tipo de datos, nombres de usuario y contraseñas.

SGSI: de la seguridad física

Base Décima novena.- Las dependencias y entidades, deberán establecer controles relacionados con los perímetros de seguridad física, con el fin de prevenir accesos no autorizados, daño, robo, entre otras acciones.

Base Vigésima.- Con respecto a los controles que se relacionan con los perímetros de seguridad física se debe considerar en el establecimiento de los mismos, por lo menos los siguientes requisitos:

I. La definición de los perímetros relacionados con la seguridad física;

II. Los controles de acceso a los perímetros relacionados con la seguridad física; el diseño de medidas de seguridad física;

III. La definición de mecanismos de protección contra amenazas físicas y ambientales;

IV. Las reglas de trabajo para la realización de actividades dentro de los perímetros seguros; y

V. La coordinación entre los controles de seguridad física y los procedimientos y planes de protección civil.

Base Vigésima primera.- Con respecto a los controles que se relacionan con la seguridad de los activos se debe considerar en el establecimiento de los mismos, por lo menos los siguientes requisitos:

I. La definición de ubicación y mecanismos de protección contra amenazas y peligros ambientales;

II. El plan de continuidad de la operación orientado a prevenir la falla de suministro de energía o cualquier tipo de interrupción provocada por fallas en los servicios públicos;

III. Las medidas de seguridad física de conformidad con las Normas Oficiales Mexicanas que disponen cableado de infraestructura en materia de telecomunicaciones y equipos eléctricos;

IV. El proceso de mantenimiento continuo de los equipos informáticos para garantizar la disponibilidad e integridad de éstos, así como de la información contenida o dependiente de ellos; y

V. El proceso de baja y reasignación de equipos de cómputo con respecto a los respaldos de información y la eliminación de la misma en ellos.

SCGI: de la continuidad de las operaciones

Base Vigésima segunda.- Las dependencias y entidades, deberán establecer controles con el fin de contrarrestar las interrupciones graves de su operación y fallas mayores en los sistemas de información que comprometan la disponibilidad de la información.

Base Vigésima tercera.- Con respecto a los controles que se relacionan con la continuidad de las operaciones, se debe considerar en el establecimiento de los mismos, por lo menos, los siguientes requisitos:

I. El procedimiento para gestionar la continuidad en las operaciones de manera segura;

II. El procedimiento para la identificación de posibles amenazas que puedan generar una interrupción en la continuidad de las operaciones y a su vez, afectar la disponibilidad de la información;

III. El procedimiento para reanudar la operación segura de los sistemas de información y aplicaciones informáticas ante una interrupción grave de los servicios; y

IV. El procedimiento continuo de prueba y evaluación de los planes de continuidad de la operación para implementar su mejora continua.

SCGI: del cumplimiento de la normatividad aplicable

Base Vigésima cuarta.- Las dependencias y entidades, deberán establecer controles orientados a evitar violaciones de la normatividad vigente, de las obligaciones contractuales o de la política de seguridad interna.

Base Vigésima quinta.- Con respecto a los controles que se relacionan con el cumplimiento de la normatividad vigente, se debe considerar en el establecimiento de los mismos, por lo menos, los siguientes requisitos:

I. La identificación y documentación de la normatividad aplicable de acuerdo a las atribuciones de la dependencia o entidad;

II. El procedimiento para el control estricto de licencias de uso de programas de cómputo comerciales y otras tecnologías, incluyendo el marco de sanciones previstas en la Ley Federal del Derecho de Autor y la Ley de Propiedad Industrial, así como la reglamentación respectiva a éstas;

III. El procedimiento para el control estricto de la autoría de obras e invenciones generadas en las dependencias y entidades, incluyendo el marco de sanciones previstas en la Ley Federal del Derecho de Autor y la Ley de Propiedad Industrial así como la reglamentación respectiva a éstas; y

IV. Los procedimientos para la debida clasificación archivística y de la información con apego a lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; los Lineamientos generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal; los Lineamientos generales para la organización y conservación de los archivos de las dependencias y entidades de la Administración Pública Federal, los Lineamientos de Protección de Datos Personales y las Recomendaciones sobre medidas de Seguridad aplicables a los Sistemas de Datos Personales emitidos por el Instituto Federal de Acceso a la Información.

Base Vigésima sexta.- Con respecto a los controles que se relacionan con el cumplimiento de políticas informáticas, se debe considerar en el establecimiento de los mismos, por lo menos, los siguientes requisitos:

I. El procedimiento para la implementación efectiva de controles y políticas de seguridad; y

II. El procedimiento para la revisión periódica de los sistemas de información, a fin de que éstos cumplan con estándares y mejores prácticas de seguridad.

Base Vigésima séptima.- Con respecto a los controles que se relacionan con los procedimientos de auditoría de los sistemas de información, se debe considerar en el establecimiento de los mismos, por lo menos, los siguientes requisitos:

I. El procedimiento para la realización de auditorías de sistemas de información; y

II. El procedimiento para la protección de las herramientas utilizadas en los procesos de auditoría.

Base Vigésima octava.- La aplicación los controles establecidos en la **Base Quinta** fracciones I a XII de las presentes disposiciones relativas a seguridad de la información en posesión de las dependencias y entidades de la APF, no limita a que las dependencias y entidades puedan establecer otros controles adicionales o sustitutos que consideren necesarios y que deberán incluir en los procedimientos que deriven de la aplicación de las presentes Reglas Generales y su Manual, observando que éstos sean congruentes con los objetivos de las presentes disposiciones relativas a seguridad de la información en posesión de las dependencias y entidades de la APF.

Base Vigésimo novena.- La documentación generada para la implementación del SGSI tendrá el carácter de información reservada y será de accesos restringido, de conformidad con el Vigésimo noveno de los Lineamientos de protección de datos personales.

Base Trigésima.- El personal que tenga acceso a dicha documentación deberá evitar que ésta sea divulgada, a efecto de no comprometer la efectividad del sistema de gestión de seguridad de la información y de los controles implementados.

Protección de datos personales

Base Trigésima primera.- La implementación de medidas de seguridad administrativa, técnica y física en materia de protección de datos personales, deberá realizarse en términos de lo que establece la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y los Lineamientos de Protección de Datos Personales.

El Documento de Seguridad tendrá el carácter de información reservada de conformidad con el Vigésimo noveno de los Lineamientos de protección de datos personales.

Base Trigésima segunda.- Las medidas de seguridad referidas en la disposición anterior deberán ser incluidas en el Documento de Seguridad que la dependencia o entidad elabore de conformidad con el Trigésimo tercero y Trigésimo cuarto de los Lineamientos de Protección de Datos Personales.

Base Trigésima tercera.- Para garantizar un adecuado tratamiento de los sistemas de datos personales, las dependencias y entidades podrán considerar las medidas de seguridad establecidas en las Recomendaciones sobre Medidas de Seguridad aplicables a los sistemas de Datos Personales emitidas por el Instituto Federal de Acceso a la Información Pública Gubernamental, así como en las Recomendaciones en materia de protección de datos que emita dicho Instituto.

Estructura organizacional para la gestión de la seguridad de la información

Base Trigésima cuarta.- Las dependencias y entidades deberán conformar, en el ámbito de su competencia, un grupo multidisciplinario que se enfocará a operar, monitorear y evaluar la seguridad de la información, sin que ello implique incremento de la estructura orgánica autorizada.

Base Trigésima quinta.- Para una correcta gestión de la seguridad de la información, el Grupo superior deberá estar conformado por los siguientes elementos:

I. El Grupo de Seguridad de la Información;

II. El Área de Seguridad de la Información de la UTIC; y

III. La Unidad Administrativa de Auditoría de Seguridad de la Información.

Grupo de seguridad de la información

Base Trigésima sexta.- Las dependencias y entidades deberán conformar en el ámbito de su competencia un Grupo de Seguridad de la Información, el cual deberá estar presidido por el Titular de la dependencia o entidad e incluir al titular de la UTIC.

Base Trigésima séptima.- El Grupo de Seguridad de la Información deberá cumplir las siguientes funciones:

I. Definir las directrices en materia de seguridad de la información;

II. Asegurar que los objetivos, procedimientos y acciones del sistema de gestión de seguridad de la información estén alineados a las atribuciones, los requerimientos de la dependencia o entidad, y que estén integrados en sus procesos relevantes;

III. Aprobar y vigilar el cumplimiento de la normatividad en materia de seguridad de la información, de conformidad con las presentes Reglas generales y su manual, los procedimientos internos de la dependencia o entidad y las disposiciones de carácter general aplicables;

IV. Aprobar las principales iniciativas propuestas por el Área de Seguridad de la Información de la UTIC, tendientes a incrementar la seguridad de la información;

V. Supervisar que las unidades administrativas cumplan de manera efectiva con sus obligaciones en materia de seguridad de la información;

VI. Autorizar el manual de operación y funcionamiento del Comité; y

VII. Las demás que sean necesarias para el cumplimiento de sus funciones o sean encomendadas por el titular de la dependencia o entidad.

Área de seguridad de la información

Base Trigésima octava.- Las dependencias y entidades deberán conformar en el ámbito de su competencia un Área de Seguridad de la Información designando a un responsable para tal efecto.

Base Trigésima novena.- El Área de Seguridad de la Información tendrá las siguientes funciones:

I. Elaborar las estrategias de seguridad de la información, tomando en consideración los requerimientos de seguridad de las unidades administrativas de la dependencia o entidad;

II. Coadyuvar con las unidades administrativas de la dependencia o entidad a garantizar la confidencialidad, integridad y disponibilidad de la información que posean en el ejercicio de sus funciones;

III. Diseñar soluciones de seguridad de la información;

IV. Coordinar las actividades de implementación de los controles de seguridad de las presentes disposiciones relativas a seguridad de la información en posesión de las dependencias y entidades de la APF;

V. Monitorear constantemente el estatus de seguridad dentro de la dependencia o entidad, para la generación continua de una base de datos de conocimientos y soluciones a los incidentes reportados;

VI. Conformar grupos de trabajo que permitan garantizar la seguridad de la información;

VII. Proponer al Comité de Seguridad de la Información de la dependencia o entidad, para su aprobación, la política de seguridad de la información y sus objetivos;

VIII. Establecer, operar, monitorear, mantener y mejorar un sistema de gestión de seguridad de la información en coordinación con las unidades administrativas;

IX. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información;

X. Establecer los procedimientos para la elaboración del análisis de riesgos necesario, previo a la implementación de controles relativos a la seguridad de la información, en coordinación con las unidades administrativas;

XI. Monitorear cambios significativos en los riesgos que afectan a los activos frente a las amenazas más importantes;

XII. Desarrollar el proceso de gestión de la continuidad de las operaciones;

XIII. Promover la difusión de la cultura de seguridad de la información dentro de la dependencia o entidad;

XIV. Ser el representante de la dependencia o entidad en los consejos técnicos y grupos de trabajo de seguridad de la información que se realicen en la Administración Pública Federal; y

XV. Las demás que sean necesarias para el cumplimiento de su objeto y las que le sean encomendadas por el titular de la dependencia o entidad.

Base Cuadragésima.- Para la ejecución de sus procesos, el Área de Seguridad de la información podrá contar con personal interno de la dependencia o entidad o bien a través de la contratación de terceros.

Auditoría de la Seguridad de la Información

Base Cuadragésima primera.- El Grupo de Seguridad de la Información será el responsable de que al interior de la dependencia o entidad de que se trate, se:

I. Supervise el cumplimiento de estas disposiciones relativas a seguridad de la información en posesión de las dependencias y entidades de la APF por parte de la dependencia y/o entidad;

II. Lleven a cabo auditorías en materia de seguridad de la información, para lo cual, podrá apoyarse del personal que estime necesario o de un tercero contratado;

III. Promueva la cultura de seguridad de la información en las dependencias o entidades; y

IV. Efectúen las recomendaciones derivadas de las acciones contenidas en las fracciones I a III de la presente Base.

Responsabilidades y sanciones

Base Cuadragésima segunda.- Las responsabilidades administrativas que se generen por el incumplimiento de las disposiciones relativas a seguridad de la información en posesión de las dependencias y entidades de la APF, serán sancionadas de conformidad con las disposiciones de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos y cualquier otra del orden civil o penal que resulte aplicable.

De la Interoperabilidad

Artículo 28.- Las dependencias y entidades, al respecto de interoperabilidad, se sujetarán a las bases generales siguientes:

Generales

Base Primera.- Los elementos de interoperabilidad de TIC que adopten las dependencias y entidades de la APF, deberán apegarse a estándares y/o especificaciones técnicas soportadas por el mercado, con objeto de reducir costos económicos y riesgos tecnológicos en la concepción y desarrollo de las funcionalidades y servicios de Interoperabilidad de TIC.

Base Segunda.- Las disposiciones relativas a la Interoperabilidad de TIC que establecen especificaciones técnicas relacionadas con estándares nacionales e internacionales tienen su base en el *Modelo de Arquitectura Gubernamental de TI* definido por el CIDGE, el cual puede consultarse en la dirección electrónica:
http://www.cidge.gob.mx/doc/M_Arq_TI_v02.pdf.

Base Tercera.- La totalidad de las interfaces entre los sistemas o aplicativos de las dependencias o entidades de la APF, intermediarios u organizaciones que proporcionen información a las dependencias o entidades de la APF o que utilicen información gubernamental que provenga de sus sistemas o aplicativos, deberán apegarse a las especificaciones de interoperabilidad de TIC descritas en el Manual General de Tecnologías de Información y Comunicaciones.

Base Cuarta.- Las disposiciones relativas a la Interoperabilidad de TIC en las dependencias y entidades de la APF, deberán ser aplicadas por las UTIC en todos los casos que éstas inicien la implantación de elementos, funcionalidades y desarrollos de Interoperabilidad.

Base Quinta.- Los grupos de desarrollo de las UTIC deberán seguir las especificaciones técnicas de interoperabilidad contenidas en estas disposiciones relativas a la Interoperabilidad de TIC en las dependencias y entidades de la APF, para asegurar su integración a plataformas estándares y la posibilidad de reutilización de código.

Base Sexta.- Los desarrollos que efectúen las dependencias y entidades para la construcción de funcionalidad de interoperabilidad de TIC, deberán seguir las disposiciones que aplican para los proyectos y ciclos de desarrollo de sistemas o aplicativos de las UTIC.

Base Séptima.- Las UTIC de las dependencias y entidades que definan la utilización de algún tipo de software libre para el desarrollo de sus funcionalidades de interoperabilidad de TIC, deberán apegarse a las especificaciones técnicas contenidas en las presentes disposiciones relativas a la Interoperabilidad de TIC en las dependencias y entidades de la APF, para asegurar su integración a plataformas estándares, con el propósito de generar economías de tiempo, esfuerzo y presupuesto, deberán considerar los desarrollos desde un enfoque de reutilización de código.

Base Octava.- Los desarrollos que se efectúen en las dependencias y entidades para la construcción de funcionalidad de Interoperabilidad de TIC, bajo las especificaciones técnicas que definen estas disposiciones deberán tener la capacidad de ser modulares para habilitar los cambios por la demanda de los servicios y/o sistemas o aplicativos, cantidad de usuarios y cantidad de transacciones, entre otros.

Estándares de interoperabilidad

Base Novena.- Las dependencias y entidades deberán buscar como primera opción la implantación de estándares abiertos para las especificaciones técnicas. Los estándares propietarios sólo se implantarán cuando sea necesario reforzar la seguridad nacional, o protección de información sensible para los ciudadanos y sus organizaciones; y se deberá buscar que las implementaciones permitan tener interoperabilidad con sistemas similares y/o diversos.

Base Décima.- Al implementar funcionalidades de interoperabilidad de TIC, incluyendo aquellos denominados Servicios web o Servicios de Interoperabilidad, las dependencias y entidades que posean información considerada privada o reservada en apego a la Ley Federal de Acceso a la Información Pública Gubernamental, deberán garantizar la seguridad y privacidad de la misma, respetando y cumpliendo las leyes que la rijan, así como las restricciones de acceso a la información vigentes.

Base Décima primera.- Al establecer interoperabilidad de TIC relacionadas con sistemas o aplicaciones que hagan uso de la Internet, las dependencias o entidades deberán asegurarse de que los sistemas o aplicativos o los denominados servicios web que implementen, cumplan con las especificaciones técnicas de Internet y del World Wide Web (www).

Base Décima segunda.- Al establecer interoperabilidad de TIC para los servicios y/o sistemas o aplicativos o los denominados servicios web que implementen las dependencias o entidades deberán cumplir al menos con el estándar primario de intercambio de datos XML (eXtensible Markup Language).

Base Décima tercera.- Al establecer interoperabilidad de TIC, las dependencias o entidades deberán adoptar como principal medio de acceso los servicios y/o sistemas de información del gobierno, preferentemente, basado en Navegadores de Internet. Se permitirán otros medios de acceso en situaciones específicas donde no se cuente con otra alternativa tecnológica, previa autorización de la Subcomisión de Interoperabilidad de la CIDGE.

Base Décima cuarta.- Las UTIC, siguiendo el *Modelo de Arquitectura Gubernamental de TI* definido por la CIDGE, el cual se puede consultar en la dirección electrónica: *http://www.cidge.gob.mx/doc/M_Arq_TI_v02.pdf,* deberán integrar elementos de seguridad que garanticen la confidencialidad de los procesos y la autenticación de los ciudadanos y sus organizaciones, servidores públicos y sistemas o aplicaciones que interoperen con otros sistemas o elementos de interoperabilidad de TIC, a través de cualquier dispositivo de acceso que se implemente según las arquitecturas tecnológicas de las dependencias o entidades.

Base Décima quinta.- Las dependencias y entidades, deberán procurar una efectiva manera de compartir sistemas o aplicaciones y transferir el código fuente de los sistemas o aplicaciones que sean desarrolladas con recursos públicos en las UTIC.

Base Décima sexta.- Las dependencias y entidades de la APF, deberán instrumentar elementos para la homologación de registros de usuarios y perfiles, con la finalidad de procurar la adecuada interoperabilidad entre los sistemas y aplicativos así como entre dependencias y entidades de la APF.

Base Décima séptima.- Las dependencias y entidades de la APF, deberán tomar en cuenta que los estándares tecnológicos, incluyendo los de interoperabilidad de TIC están sujetos al avance tecnológico y a procesos de maduración propios de cualquier tecnología, por lo que es necesario que se aseguren y mantengan evidencia del conocimiento del ciclo de vida de los estándares que integren en los desarrollos de interoperabilidad de TIC.

Base Décima octava .- Las dependencias y entidades deberán adoptar normas abiertas o especificaciones técnicas nacionales e internacionales, para cubrir las interfaces entre bloques o capas con base en el *Modelo de Arquitectura Gubernamental de TI* definido por la CIDGE, el cual puede consultarse en la dirección electrónica: *http://www.cidge.gob.mx/doc/M_Arq_TI_v02.pdf,* con la finalidad de asegurar la interoperabilidad, facilitar la reutilización y el mantenimiento a largo plazo así como reducir al mínimo las restricciones técnicas.

Base Décimo novena - Las dependencias y entidades deberán construir e implementar sistemas independientes de cualquier proveedor específico, para tener el acceso permanente y el control de sus propios datos.

Base Vigésima.- Todos los niveles de interoperabilidad de TIC, deberán ser cubiertos por especificaciones técnicas, acordes a cada nivel, con base en el *Modelo de Arquitectura Gubernamental de TI* definido por la CIDGE, el cual puede consultarse en la liga: *http://www.cidge.gob.mx/doc/M_Arq_TI_v02.pdf.*

Base Vigésima primera .- La interoperabilidad de TIC, deberá considerar: interconexión, interacción entre WAN's, Red Virtual Privada, entre otros; seguridad: cambio de autenticación y autorización, firma de recursos de web, entre otros; intercambio de datos, lenguaje de marcación, entre otros; mecanismos de descubrimiento, sistema de nombre de dominio, descripción de servicios de web, entre otros; presentación y formatos de documento, formato de distribución de documento, formato gráfico, entre otros; metadatos para proceso y descripciones de datos, especificación de procesos de negocio y protocolos de interacción de negocio, estructura de documentos, entre otros; nombramiento, la identificación de recursos de Internet, país, puntuación, representaciones, entre otros.

De los Sitios de internet

Artículo 29.- Las dependencias y entidades, al respecto de sitios de Internet de la Administración Publica Federal, se sujetarán a las bases generales siguientes:

Del desarrollo y publicación de contenidos

Base Primera.- Las dependencias y entidades deberán asegurarse de que los desarrollos, estructura y contenidos de los sitios Internet de éstas se presenten homologados promoviendo la publicación de documentos informativos y estadísticas útiles al ciudadano y sus organizaciones.

Base Segunda.- Las dependencias y entidades, para lograr la homologación prevista en la disposición anterior, deberán, a través de las UATIC sujetarse a la Guía para el Desarrollo de Sitios Web de la Administración Pública Federal, disponible en la URL: http://www.sip.gob.mx así como al Manual de Imagen para Sitios de Internet del Gobierno Federal, disponible en la dirección electrónica: http://www.sip.gob.mx.

TRANSITORIOS

Primero.- Las presentes Reglas Generales y su Manual entrarán en vigor ["al día siguiente al de su publicación en el Diario Oficial de la Federación.

Segundo.- Las dependencias y entidades de la Administración Pública Federal a más tardar el xx de mes xxxx de 2010 deberán dejar sin efectos o abrogar las disposiciones administrativas que rijan al interior de las mismas, o publicar éstas en el Diario Oficial de la Federación, cuando la regulación a

que se refieran se encuentre contenida en las presentes Reglas Generales y no se encuentren listadas en los transitorios Séptimo y Octavo.

Tercero.- Lo previsto en el artículo 7 entrará en vigor a los treinta días posteriores a la publicación de las presentes Reglas.

Cuarto.- A efectos de dar cumplimiento a lo previsto en los artículos 5 y 6 del presente ordenamiento las dependencias y entidades de la Administración Pública Federal, deberán presentar en un plazo no mayor de 30 días, un cronograma de inicio de operación de los procesos del Marco Rector del Manual, ante la Secretaría de la Función pública a través de la Unidad de Gobierno Digital, para su registro, revisión y aprobación.

Quinto.- Las disposiciones administrativas expedidas en materia de TIC por las Dependencias o Entidades, vigentes al momento de la publicación de este ordenamiento se seguirán aplicando en tanto las citadas dependencias o entidades implementen el presente Manual General de acuerdo al transitorio anterior; en caso de que alguna dependencia o entidad necesite continuar con el uso de alguna disposición particular en materia de Tecnologías de Información y Comunicaciones, deberá informar puntualmente a la Secretaría de la Función Pública, enviando la justificación correspondiente, para que esta dictamine su pertinencia.

Sexto.- La Secretaría de la Función Pública por si misma o a través de sus órganos internos de control verificará que las dependencias y entidades de la Administración Pública Federal publiquen en el Diario Oficial de la Federación las disposiciones administrativas a que se refiere el transitorio Segundo.

Séptimo.- Se abroga el Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal, publicado en el Diario Oficial de la Federación con fecha 24 de agosto de 2006.

Octavo.- Los anexos técnicos a que se refiere la **Base Décima cuarta** relacionada con los sistemas automatizados de control de gestión serán emitidos por la Subcomisión de los sistemas automatizados de control de gestión de la CIDGE en un plazo no mayor a 60 días contados a partir de la entrada en vigor de las presentes Reglas Generales.

Dado en la Residencia Oficial de los Pinos, a [con letra] de [mes con letra] de 2010.

Anexo

Manual General en Tecnologías de la Información y Comunicaciones, flujogramas, formatos e instructivos