

SECRETARIA DE LA FUNCION PUBLICA

ACUERDO que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Secretaría de Gobernación.- Secretaría de la Función Pública.

MIGUEL ÁNGEL OSORIO CHONG, Secretario de Gobernación y JULIÁN ALFONSO OLIVAS UGALDE, Subsecretario de Responsabilidades Administrativas y Contrataciones Públicas en ausencia del Secretario de la Función Pública, con fundamento en los artículos 10, 27, fracciones X, XXVI, XXVIII, XXIX y XLIII, y 37, fracciones VI y XXVI, de la Ley Orgánica de la Administración Pública Federal, este último en relación con el Segundo Transitorio del Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 2 de enero de 2013; 12, fracciones II y VII, 18 y 55 de la Ley de Seguridad Nacional; 10, 11 y 24, fracción VII, del Reglamento para la Coordinación de Acciones Ejecutivas en materia de Seguridad Nacional; 1, 5, fracciones II, XXV y XXVIII, y 71 del Reglamento Interior de la Secretaría de Gobernación; así como 1, 6, fracciones I y XXIV, 7, fracción XII, y 86 del Reglamento Interior de la Secretaría de la Función Pública, y

CONSIDERANDO

Que el Plan Nacional de Desarrollo 2013-2018, aprobado por Decreto publicado en el Diario Oficial de la Federación el 20 de mayo de 2013, propone dentro de la Estrategia transversal "Un Gobierno Cercano y Moderno", el establecer una Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las tecnologías de la información y comunicaciones (TIC), e impulsar un gobierno eficaz que inserte a México en la Sociedad del Conocimiento.

Que el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado por Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013, indica que para alcanzar la Estrategia transversal "Un Gobierno Cercano y Moderno", es fundamental reconocer que las nuevas TIC son una herramienta básica que brinda amplias oportunidades para mejorar la eficiencia del gobierno, por lo que en este sentido, en su Objetivo 5 "Establecer una Estrategia Digital Nacional que acelere la inserción de México en la Sociedad de la Información y del Conocimiento", indica que este impulso se efectuará mediante el uso de las TIC, lo cual permitirá el desarrollo de la modernización del gobierno y la mejora de los servicios y bienes públicos, lo que supone contar con habilitadores digitales como la conectividad, asequibilidad, inclusión y alfabetización digital, la interoperabilidad y el uso de datos abiertos, así como el marco jurídico adecuado para tales efectos.

Que el Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicado el 10 de diciembre de 2012 en el Diario Oficial de la Federación, prevé en materia de TIC, que se deberán establecer programas de optimización, sistematización y digitalización de procesos administrativos; que los nuevos sistemas consolidarán la operación e integración de diferentes sistemas y bases de datos; que se deberán adoptar las políticas de la Estrategia Digital Nacional, la cual fomentará dentro de sus objetivos un cambio de cultura para que el gobierno utilice las TIC y con ello ofrezca servicios gubernamentales transparentes y de mayor calidad con posibilidad de interoperabilidad a través de conexiones rápidas y seguras, y que se deberán implementar las recomendaciones que se emitan en materia de política de Estrategia Digital Nacional, respecto a las contrataciones de bienes o servicios en materia de TIC, así como las mejores prácticas susceptibles de desarrollarse e instrumentarse a través de proyectos estratégicos.

Que los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, difundidos en el Diario Oficial de la Federación el 30 de enero de 2013, disponen la necesidad de privilegiar la unificación e integración de aplicaciones para su optimización, homologación y estandarización, a fin de consolidar los sistemas y servicios de TIC y disminuir los costos de mantenimiento de los portafolios de aplicaciones.

Que en ese contexto, y como resultado de la revisión de las disposiciones administrativas en materia de TIC y de seguridad de la información, así como del Manual Administrativo de Aplicación General en esas materias, establecidos por Acuerdo publicado en el Diario Oficial de la Federación el 13 de julio de 2010 y sus reformas publicadas el 6 de septiembre y 29 de noviembre de 2011, así como el 22 de agosto de 2012; se observó la necesidad de homologar los procesos contenidos en dicho manual a la Estrategia Digital Nacional, para agilizar y optimizar su gestión al interior de las dependencias y entidades de la Administración Pública Federal y en la Procuraduría General de la República, por lo que hemos tenido a bien expedir el siguiente:

ACUERDO QUE TIENE POR OBJETO EMITIR LAS POLÍTICAS Y DISPOSICIONES PARA LA ESTRATEGIA DIGITAL NACIONAL, EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, Y EN LA DE SEGURIDAD DE LA INFORMACIÓN, ASÍ COMO ESTABLECER EL MANUAL ADMINISTRATIVO DE APLICACIÓN GENERAL EN DICHAS MATERIAS

Capítulo I

Objeto, Ámbito de Aplicación y Definiciones

Artículo 1.- El presente Acuerdo tiene por objeto emitir políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias, contenido en su Anexo Único, que serán de observancia obligatoria en la Administración Pública Federal y en la Procuraduría General de la República.

Las Secretarías de la Defensa Nacional y de Marina, así como el Comisionado Nacional de Seguridad, las unidades administrativas y órganos administrativos desconcentrados adscritos a éste, y el Centro, en atención a las atribuciones a su cargo, estarán exceptuadas de la aplicación de lo dispuesto en el presente Acuerdo y su Anexo Único cuando ello pueda vulnerar su operación.

Artículo 2.- Para los efectos del presente Acuerdo, se entiende por:

- I. **Activos de TIC:** los aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos;
- II. **Aplicativo de Cómputo:** el software y/o los sistemas informáticos, que se conforman por un conjunto de componentes o programas contruidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos;
- III. **Arquitectura Empresarial:** la información del estado actual y futuro de una Institución, a partir del análisis con perspectiva estratégica; considerando modelos de negocio, procesos, aplicativos y tecnología de la información y comunicaciones;
- IV. **Arquitectura Orientada a Servicios:** la metodología y marco de trabajo, para construir componentes de software reutilizables para la interoperabilidad de aplicativos de cómputo;
- V. **Bases de Colaboración:** los instrumentos consensuales celebrados por las Instituciones para establecer acciones que modernicen y mejoren la prestación de los servicios públicos, promuevan la productividad en el desempeño de sus funciones y reduzcan gastos de operación, a fin de incrementar la eficiencia y eficacia y cumplir con los objetivos previstos en el Programa y formalizar los compromisos, así como sus respectivos indicadores de desempeño;
- VI. **Borrado Seguro:** el proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital;
- VII. **Centro:** el Centro de Investigación y Seguridad Nacional, órgano desconcentrado de la Secretaría de Gobernación;
- VIII. **Centro de Datos:** el lugar físico en los que se ubiquen los activos de TIC y desde el que se provén servicios de TIC;
- IX. **CNTSE:** el Catálogo Nacional de Trámites y Servicios del Estado, al que se alude en el Programa;
- X. **Cómputo en la Nube:** al modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios;
- XI. **Decreto:** el Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 10 de diciembre de 2012;
- XII. **Dependencias:** las Secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como a la Oficina de la Presidencia de la República y la Procuraduría General de la República;
- XIII. **Diseminación:** la transmisión o entrega de información considerada de seguridad nacional, a quienes cumplan con los requisitos para conocer esa información, de acuerdo con el nivel de acceso autorizado;
- XIV. **Dominio Tecnológico:** las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo;

- XV. **EDN:** la Estrategia Digital Nacional contenida en el Objetivo número 5 del Programa;
- XVI. **EIDA:** el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, establecido mediante Acuerdo publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011;
- XVII. **Entidades:** los organismos descentralizados, empresas de participación estatal mayoritaria, instituciones nacionales de crédito, organizaciones auxiliares nacionales de crédito e instituciones nacionales de seguros y de fianzas, y fideicomisos públicos que en términos de la Ley Orgánica de la Administración Pública Federal y de la Ley Federal de las Entidades Paraestatales, sean considerados entidades de la Administración Pública Federal Paraestatal;
- XVIII. **ERISC:** equipo de respuesta a incidentes de seguridad en TIC en la Institución;
- XIX. **Esquema de Tiempo y Materiales:** los servicios en que el proveedor asigna, durante un periodo, un determinado número de recursos humanos, que cumplirán actividades definidas mediante un contrato;
- XX. **Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;
- XXI. **Iniciativas de TIC:** la conceptualización o visualización temprana de una oportunidad para ofrecer un aplicativo de cómputo, solución tecnológica o servicio de TIC o una solución tecnológica en beneficio de la Institución, las cuales podrán o no concretarse en uno o más proyectos de TIC;
- XXII. **Instancias de Seguridad Nacional:** las Instituciones o autoridades que en función de sus atribuciones participen directa o indirectamente en la seguridad nacional, conforme a lo dispuesto en la fracción II del artículo 6 de la Ley de Seguridad Nacional, incluidas aquellas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;
- XXIII. **Institución:** las dependencias y entidades de la Administración Pública Federal, tal y como se definen en este Acuerdo;
- XXIV. **Lineamientos:** los Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, publicados en el Diario Oficial de la Federación el 30 de enero de 2013;
- XXV. **MAAGMAASSP:** el Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público;
- XXVI. **MAAGTICSI:** el Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información, Anexo Único del presente Acuerdo;
- XXVII. **PETIC:** el Plan Estratégico de Tecnologías de la Información y Comunicaciones que elaboran las Instituciones en los términos señalados en el MAAGTICSI;
- XXVIII. **Programa:** el Programa para un Gobierno Cercano y Moderno 2013-2018, aprobado mediante Decreto publicado en el Diario Oficial de la Federación el 30 de agosto de 2013;
- XXIX. **Proyectos de TIC:** el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado de TIC;
- XXX. **Seguridad de la información:** la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma;
- XXXI. **Seguridad Nacional:** las acciones a las que se refiere el artículo 3 de la Ley de Seguridad Nacional;
- XXXII. **SEGOB:** la Secretaría de Gobernación;
- XXXIII. **SFP:** la Secretaría de la Función Pública;
- XXXIV. **Tecnologías Verdes:** el conjunto de mecanismos y acciones sobre el uso y aprovechamiento de las tecnologías de la información y comunicaciones, que reducen el impacto de éstas sobre el medio ambiente, contribuyendo a la sustentabilidad ambiental; considerando inclusive el reciclaje de componentes utilizados en el uso de estas tecnologías;
- XXXV. **TIC:** las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video, y
- XXXVI. **Unidad:** la Unidad de Gobierno Digital de la SFP.

Capítulo II

Responsables de la Aplicación

Artículo 3.- La aplicación de las políticas y disposiciones contenidas en el presente Acuerdo y su Anexo Único, corresponde a los Titulares de las unidades administrativas o áreas responsables de las TIC en las Instituciones, así como a los servidores públicos cuyas atribuciones o funciones estén relacionadas con la planeación, contratación y administración de bienes y servicios de TIC y con la seguridad de la información.

Capítulo III

Políticas para la Estrategia Digital Nacional

Artículo 4.- La planeación estratégica de TIC que elaboren las Instituciones, deberá atender las metas nacionales, estrategias, objetivos y líneas de acción e indicadores, establecidos en el Plan Nacional de Desarrollo 2013-2018, la EDN, así como las disposiciones establecidas en el Decreto y en las Bases de Colaboración que haya suscrito cada Institución.

Artículo 5.- El PETIC se integrará con las Iniciativas y Proyectos de TIC que determinen las Instituciones, sujetándose al artículo anterior, para lo cual atenderán lo siguiente:

- I. Favorecer el uso del cómputo en la nube para el aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental y estandarización de las TIC, teniendo en consideración la seguridad de la información;
- II. Privilegiar la aplicación de Tecnologías Verdes;
- III. Establecer una ficha técnica base para cada una de las Iniciativas y Proyectos de TIC, en la cual se registre el presupuesto estimado y, de ser el caso, el presupuesto autorizado para el ejercicio fiscal, así como necesidades adicionales en este rubro;
- IV. Identificar Iniciativas y Proyectos de TIC que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, de la EDN y del Decreto, en el ámbito de sus atribuciones, identificándolos como estratégicos;
- V. Identificar las estrategias, líneas de acción y habilitadores de la EDN contenidas en el Programa, a las cuales contribuirán para su cumplimiento;
- VI. Relacionar las características, especificaciones y estándares generales de los principales componentes por cada dominio tecnológico;
- VII. Determinar Iniciativas y Proyectos de TIC para la digitalización de los trámites y servicios registrados en el CNTSE, considerando estrategias de interoperabilidad con aplicativos de cómputo de otras Instituciones que resulten necesarios para la prestación de esos trámites y servicios;
- VIII. Establecer estrategias de interoperabilidad al interior de la propia Institución y con otras Instituciones que requieran compartir datos que obren en su posesión, puedan o no formar parte de un mismo proceso, y
- IX. Someter a la aprobación de la Unidad las aplicaciones de cómputo para dispositivos móviles que planeen desarrollar.

Artículo 6.- Una vez elaborado el PETIC, conforme al proceso de Planeación Estratégica que se establece en el MAAGTICSI, se estará a lo siguiente:

- I. Las Instituciones presentarán a la Unidad, en el mes de octubre de cada año, el PETIC del año siguiente, identificando un máximo de 7 Iniciativas y/o Proyectos de TIC, como estratégicos, y considerando como criterio preferentemente para su identificación, que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, de la EDN y del Decreto. Dichas Iniciativas y/o Proyectos de TIC se propondrán a la Unidad para su seguimiento.

Una vez presentado el PETIC, la Unidad remitirá a las Instituciones, en su caso, la autorización correspondiente, a más tardar el 31 de diciembre del año anterior al que corresponda el PETIC.

En el supuesto de que la Unidad formule observaciones, las Instituciones contarán con diez días hábiles a partir de que se les notifiquen, para solventarlas y presentar nuevamente su PETIC para autorización;

- II. La Unidad seleccionará de entre las Iniciativas y Proyectos de TIC propuestos por las Instituciones como estratégicos, aquéllos a los que dará seguimiento, tomando como base los que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, de la EDN y del Decreto, y
- III. La Unidad verificará, para su aprobación, que las aplicaciones de cómputo para dispositivos móviles que las Instituciones planeen desarrollar, sean concordantes con estas políticas y demás disposiciones aplicables.

Artículo 7.- Las Instituciones deberán tomar en cuenta para la optimización interna de los trámites y servicios, el modelado de la Arquitectura Empresarial, debiendo utilizar las guías, lineamientos, manuales y documentos técnicos de interoperabilidad que para este efecto ponga a disposición la Unidad, a través de su portal.

Artículo 8.- Las Instituciones deberán compartir recursos de infraestructura, bienes y servicios en todos los dominios tecnológicos utilizando soluciones tecnológicas comunes a nivel institucional, sectorial y de la Administración Pública Federal, conforme a las directrices que emita la Unidad, teniendo en consideración la seguridad de la información.

Artículo 9.- Las Instituciones para la contratación de adquisiciones y arrendamientos de bienes muebles y de prestación de servicios, en materia de TIC, además de sujetarse a las disposiciones que se establecen en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento, el MAAGMASSP y demás disposiciones aplicables en la materia, deberán observar lo siguiente:

- I. En la planeación de las contrataciones, se sujetarán a las estrategias y líneas de acción de la EDN contenidas en el Programa;
- II. En la investigación de mercado que deban realizar para seleccionar el procedimiento de contratación, verificarán si existe algún ente público que, conforme a su objeto, esté en posibilidad de suministrar los bienes o prestar los servicios que se requieran, a efecto de considerarlo en dicha investigación, tomando en cuenta la información del catálogo de entes públicos que la Unidad publique en su portal;
- III. En la contratación para la prestación de servicios, se establecerá en la convocatoria a la licitación pública, en la invitación a cuando menos tres personas o en las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, la obligación de presentar, además de los precios unitarios del servicio, un desglose de los componentes que integren el servicio a prestar, y
- IV. Prever, en su caso, acciones por parte del proveedor para el adiestramiento formal especializado, para quienes resulte pertinente, de acuerdo al dominio tecnológico objeto de la contratación.

Para la contratación de adquisiciones, arrendamientos y servicios en materia de TIC, las Instituciones deberán obtener el dictamen favorable de la Unidad, para lo cual presentarán solicitud acompañada del formato que se establece en el MAAGTICSI, con al menos 20 días hábiles previos al inicio del procedimiento de contratación respectivo, o bien, al de la celebración de los contratos con otros entes públicos, según corresponda.

La Unidad podrá dar trámite a solicitudes que de manera excepcional se presenten fuera del plazo anterior, cuando a su juicio, la Institución de que se trate, justifique que se encontró impedida para realizar la solicitud de manera oportuna.

La Unidad emitirá, en su caso, el dictamen favorable, por vía electrónica, a más tardar a los quince días hábiles posteriores a la recepción de la solicitud correspondiente; de requerir mayor información, la Unidad la solicitará a la Institución, caso en el cual reiniciará el cómputo del plazo señalado a partir de la presentación de la información requerida. La contratación se tendrá por dictaminada favorablemente, si transcurrido el plazo anterior la Unidad no emite pronunciamiento alguno.

Se exceptúa de la obtención del dictamen de la Unidad a que se refiere el párrafo anterior en los casos de adquisición de dispositivos móviles de almacenamiento, discos compactos (CD y DVD), memorias RAM para equipos de escritorio o portátiles, unidades reproductoras de CD-R o RW, DVD-R o RW, teclados, apuntadores, bocinas, diademas, micrófonos, cámaras digitales o cámaras web para equipos de escritorio o portátiles y lectores de tarjetas de memoria.

Artículo 10.- En las contrataciones relacionadas con los servicios de desarrollo, implementación, soporte a la operación y mantenimiento de aplicativos de cómputo, las Instituciones deberán prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que se celebren con otros entes públicos, según corresponda, lo siguiente:

- I. Requerir a los participantes en el procedimiento de contratación o al ente público con el que se pretenda contratar, cuando se considere aplicable, la presentación de certificaciones o acreditaciones de Normas Oficiales Mexicanas, Normas Mexicanas, o ambas en términos de la Ley Federal sobre Metrología y Normalización, así como de Normas Internacionales.
Previo a establecer el requerimiento de certificaciones o acreditaciones a que se refiere el párrafo anterior, las Instituciones deberán obtener la dictaminación favorable de la Unidad, para lo cual presentarán la justificación correspondiente en el formato establecido en el MAAGTICSI, sujetándose a los plazos establecidos en el artículo 9 de este Acuerdo;
- II. Incluir el diseño detallado del aplicativo que se vaya a desarrollar, considerando por lo menos, requerimientos del negocio, de seguridad de la información, técnicos, casos de uso, módulos, matriz de trazabilidad y protocolos de pruebas y, en su caso, lo dispuesto en la fracción IV del artículo 19 del presente Acuerdo;
- III. Especificar el conjunto de aplicativos de cómputo, en caso de que se prevea utilizar un esquema de tiempo y materiales, debiendo incluir como entregables las bitácoras de actividades del personal que se asigne a tales aplicativos, ya sea desarrollos, implementaciones, soportes a la operación o mantenimientos;
- IV. Requerir, en las contrataciones entre entes públicos, que el ente público proveedor, de ser el caso, detalle los terceros con quienes contratará para suministrar los bienes o prestar los servicios de que se trate, acreditando la solvencia técnica de dichos terceros;
- V. Señalar, en el desarrollo y en su caso, mantenimiento de aplicativos de cómputo, que se constituirán a favor de la Institución contratante los derechos patrimoniales inherentes a la propiedad intelectual, derivados de las contrataciones a que se refiere el presente artículo, a través del registro correspondiente, en el que se incluirán la totalidad de los componentes del aplicativo de cómputo de que se trate, como son, el código fuente, el diseño físico y lógico, los manuales técnicos y de usuario;
- VI. Establecer que los aplicativos de cómputo deben ser contruidos de forma modular, basados en una Arquitectura Orientada a Servicios, con el objeto de generar aplicaciones reutilizables e interoperables entre diversas áreas de la Institución o entre Instituciones;
- VII. Prever que la transferencia de datos se realice sobre canales seguros en donde se favorezca el cifrado y la integridad de los datos críticos, confidenciales sensibles, en concordancia con el MAAGTICSI, en lo referente a Seguridad de la Información, y
- VIII. Requerir, para el caso del desarrollo de aplicativos de cómputo, por lo menos un modelo de tres capas: de datos, del negocio y de presentación.

Artículo 11.- Con respecto a las redes de telecomunicaciones, las Instituciones deberán observar lo siguiente:

- I. Establecer un dominio o segmento virtual en el uso compartido de redes de telecomunicaciones, lo cual se podrá realizar de manera individual o conjunta;
- II. Contar con mecanismos estándares de cifrado de datos, de acuerdo a lo que se establece en las reglas del proceso de administración de servicios del MAAGTICSI, considerando la criticidad de los datos en sus etapas de tratamiento, especialmente en su transmisión a través de redes de telecomunicaciones, y
- III. Incluir mecanismos que soporten y habiliten servicios de multidifusión en redes privadas o locales, así como en redes de área amplia, para soportar el envío de información y datos en video, así como los beneficios en reducción de costos operativos, capacitación, agilidad gubernamental y experiencia al ciudadano.

Artículo 12.- En las contrataciones relacionadas con los servicios de Internet, las Instituciones deberán prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, que los servicios cuenten con lo siguiente:

- I. Mecanismos de protección a ataques de denegación de servicios, desde la propia red del proveedor e independientemente de los controles de seguridad de la información que implemente la Institución, debiendo atenderse mediante las actividades que se señalan en el MAAGTICSI para el establecimiento de controles de seguridad de la información, y
- II. En caso de ser necesario, la distribución y balanceo del tráfico para más de un enlace de Internet, considerando disponibilidad, confidencialidad, criticidad y redundancia.

Artículo 13.- En el caso de servicios de Centros de Datos, las Instituciones, deberán observar lo siguiente:

- I. Identificar la infraestructura de Centro de Datos con la que cuentan y la utilización de ésta, así como espacio físico, energía eléctrica, capacidad de procesamiento y almacenamiento.
En caso de haber identificado que tienen capacidad no utilizada deberán comunicarlo a la Unidad para su aprovechamiento;
- II. Evaluar la conveniencia de contratar servicios de Centro de Datos, tomando en cuenta el beneficio económico, eficiencia, privacidad, seguridad de los datos y de la información, en comparación con la de utilizar un Centro de Datos propio o compartido con otra Institución;
- III. Establecer en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que se celebren con otros entes públicos con los que se pretenda contratar, que el proveedor cuente por lo menos con dos certificaciones vigentes que acrediten sus niveles de servicio, en el caso de que se opte por la contratación del servicio de Centro de Datos. Se establecerá como valor mínimo aquel que se cumpla en ambas certificaciones;
- IV. Analizar el alojamiento de su infraestructura de operación crítica en un Centro de Datos de una Institución agrupada en su mismo sector, o en su defecto, en un Centro de Datos de otra Institución, bajo un modelo de cómputo en la nube, cuando no cuenten con un Centro de Datos propio y no tengan contratados servicios de Centro de Datos;
- V. Almacenar y administrar en los Centros de Datos que se encuentren en las instalaciones de las Instituciones, los datos considerados de seguridad nacional, seguridad pública e información reservada y confidencial, conforme a la normatividad aplicable;
- VI. Mantener en la infraestructura de los Centros de Datos una arquitectura que permita la portabilidad, de forma tal que las aplicaciones de cómputo puedan migrar entre distintos Centros de Datos y sean interoperables, dicha infraestructura deberá ser compatible con el uso de máquinas virtuales.
En caso de contrataciones de servicios de Centro de Datos, se incluirá en la convocatoria a la licitación pública, en la invitación a cuando menos tres personas o en las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, la opción de efectuar la migración de los aplicativos de cómputo de las plataformas con las que cuenta la Institución, a una versión virtualizada de las mismas, así como el acompañamiento para dicho proceso, y
- VII. Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios, incluyendo en éstas las necesarias para el personal involucrado, conforme a los controles de seguridad de la información que se definan atendiendo a lo previsto en el MAAGTICSI.

Artículo 14.- En las contrataciones relacionadas con los servicios de correo electrónico, las Instituciones deberán prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, lo siguiente:

- I. El servicio deberá comprender soluciones de filtrado para correo no deseado o no solicitado, antivirus y de suplantación de identidad que protejan el envío y recepción de correos;
- II. La obligación del proveedor de entregar a la Institución la evidencia digital necesaria en caso de incidentes de seguridad o aquella que le sea requerida, y
- III. La obligación del proveedor de entregar a la Institución la totalidad de los correos electrónicos y bitácoras, así como de no conservar información alguna mediante borrado seguro, al término del contrato.

Artículo 15.- En las contrataciones relacionadas con servicios de plataformas de procesamiento de datos, las Instituciones deberán prever en la convocatoria a la licitación pública, en la invitación a cuando menos tres personas o en las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, que en la prestación de los servicios:

- I. Se separe en capas el acceso a dichas plataformas, y
- II. La administración e infraestructura esté clasificada en zonas de seguridad basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento.

Artículo 16.- Las Instituciones, respecto de componentes de bases de datos, deberán observar lo siguiente:

- I. Contar con el inventario institucional de bases de datos en las que se identifique cuáles tienen interacción con otras bases de datos;

- II. Impulsar su integración en instancias o esquemas para los diversos aplicativos de cómputo, de manera que se eficienten los recursos con que cuentan sus servidores, y
- III. Salvaguardar los derechos de la propiedad intelectual, portabilidad y recuperación de los datos generados y procesados de acuerdo al ciclo de vida de la información, incluyendo el borrado seguro.

Artículo 17.- Con respecto a sistemas de comunicaciones unificadas de telefonía y video, las Instituciones deberán observar lo siguiente:

- I. Utilizar tecnología basada en protocolo de internet y mecanismos de cifrado estándar en las comunicaciones de voz y video, tanto en la media como en la señalización;
- II. Utilizar marcación unificada, considerando en el diseño un máximo de ocho dígitos y la integración de las Instituciones que se encuentren agrupadas a un mismo sector;
- III. Establecer interconexión de sistemas de telefonía entre Instituciones, que disminuya costos e incremente la seguridad de las conversaciones, mediante la implementación de sistemas de seguridad de frontera específicos para comunicaciones de voz y video, y se asegure el soporte de trans-codificación de señalización entre diferentes formatos de comunicación;
- IV. Prever la infraestructura que quedará a favor de la Institución al término del contrato, en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, en el caso de contrataciones de servicios que requieran algún tipo de infraestructura de soporte para su prestación;
- V. Utilizar tecnologías de mensajería instantánea, presencia y movilidad, a fin de incrementar la productividad de los usuarios y un mayor uso de éstas, teniendo en consideración la seguridad de la información;
- VI. Utilizar esquemas de consulta y acceso a directorio u otra base de datos normalizada para control de accesos y usuarios en caso de unificaciones con Instituciones del sector;
- VII. Privilegiar el uso de teléfonos de bajo consumo de energía;
- VIII. Utilizar tecnologías de gestión y monitoreo a fin de facilitar la implementación, operación y planeación de la capacidad instalada de telefonía y video, y
- IX. Prever en las convocatorias a la licitación pública, en las invitaciones a cuando menos tres personas o las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, como parte del servicio la elaboración y ejecución conjunta de un plan de adopción tecnológica para maximizar el uso de los sistemas de voz, de video o de ambos.

Artículo 18.- Las Instituciones, en lo referente al software de capa intermedia, deberán observar lo siguiente:

- I. Estandarizar, al interior, el software de capa intermedia a utilizar;
- II. Establecer servidores de presentación para los diversos aplicativos de cómputo existentes, y
- III. Ejecutar rutinas de análisis de vulnerabilidades acordes con el software de capa intermedia que se establezca, a fin de disminuir el riesgo por falta de disponibilidad.

Artículo 19.- Las Instituciones, por lo que respecta a las plataformas digitales de páginas web, deberán observar lo siguiente:

- I. Estandarizar su presencia en páginas web, de acuerdo a las guías, lineamientos, manuales y documentos técnicos de interoperabilidad que emita la Unidad, a través de su portal;
- II. Verificar en la investigación de mercado la existencia de posibles proveedores a nivel nacional e internacional para la contratación de servicios de hospedaje de páginas web y de cualquier otro tipo de presencia digital;
- III. Prever en la convocatoria a la licitación pública, en la invitación a cuando menos tres personas o en las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, que en la contratación de servicios de hospedaje de páginas web y, de ser el caso, de cualquier otro tipo de presencia digital, el hospedaje se encuentre protegido bajo estándares nacionales, y en los casos que aplique, estándares internacionales de seguridad; asimismo, que sea provisto mediante enlaces de internet con protección ante amenazas y ataques, que permita mantener los niveles de servicio conforme a lo que se establece en el MAAGTICSI, y
- IV. Contar con una versión móvil de su portal, cuyo desarrollo corresponda al lenguaje estándar basado en marcas de hipertexto, en versión 5 o superiores. Para el desarrollo de aplicativos para dispositivos móviles nativos se privilegiará el uso de dicho estándar o versiones superiores.

Artículo 20.- Las Instituciones, por lo que respecta a los sistemas automatizados de control de gestión, deberán atender lo siguiente:

- I. Asegurar que el sistema automatizado de control de gestión opere de conformidad con el EIDA, y demás normatividad aplicable, y
- II. Efectuar las adecuaciones necesarias para que su sistema automatizado de control de gestión pueda ser utilizado en sus procesos.

Capítulo IV

Disposiciones generales para la seguridad de la información

Sección I

Seguridad de la información

Artículo 21.- Las Instituciones deberán observar, implementar y operar los criterios generales de seguridad de la información conforme a los procesos de administración de la seguridad de la información y, de operación de los controles de seguridad de la información y del ERISC, establecidos en el MAAGTICSI.

Artículo 22.- Las Instituciones establecerán un modelo de gobierno de seguridad de la información, el cual incluirá la designación del responsable de la seguridad de la información de la Institución y la constitución de un grupo estratégico de la seguridad de la información, que serán responsables de operar el sistema de gestión de seguridad de la información. Dicho modelo deberá contar con un equipo de respuesta a incidentes de seguridad en TIC, de acuerdo a lo que se señala en el MAAGTICSI.

Artículo 23.- Las Instituciones elaborarán su catálogo de infraestructuras críticas e identificarán, en su caso, las que tengan el carácter de infraestructuras críticas de seguridad nacional y activos clave. El catálogo deberá mantenerse actualizado a fin de facilitar la definición de los controles que se requieran para protegerlas, en términos de lo previsto en el MAAGTICSI.

Artículo 24.- Las Instituciones desarrollarán un análisis de riesgos, que identifique, clasifique y priorice los mismos de acuerdo a su impacto en los procesos y servicios en la Institución, conforme se dispone en el MAAGTICSI.

Artículo 25.- Las Instituciones instrumentarán un proceso de fortalecimiento de la cultura de la seguridad de la información, así como de mejora continua sobre los controles de seguridad de la información y del sistema de gestión de seguridad de la información, con base en lo señalado en el MAAGTICSI.

Artículo 26.- Las Instituciones conforme a lo indicado en el MAAGTICSI, previo al inicio de la puesta en operación de un aplicativo de cómputo, realizarán el análisis de vulnerabilidades correspondiente, el cual preferentemente será realizado por un tercero, distinto a quién desarrolló el aplicativo. El resultado del análisis deberá preservarse para efectos de auditoría.

Artículo 27.- Las Instituciones mantendrán los componentes de software y de seguridad de los dominios tecnológicos actualizados para evitar vulnerabilidades, de acuerdo a lo que se establece en el MAAGTICSI, para lo cual implementarán, entre otros, elementos de seguridad de la información, los siguientes:

- I. Establecer directrices de seguridad de la información, mismas que podrán ser complementadas con base en mejores prácticas y estándares internacionales en la materia;
- II. Establecer controles de seguridad en los Activos de TIC, priorizando aquellos de mayor nivel de riesgo, entre éstos los dispositivos móviles que acceden a la red o interactúan con los dispositivos conectados a la infraestructura, incluyendo aquellos propiedad de terceros que sean utilizados al interior de las Instituciones;
- III. Mantener, evidencia auditable del proceso de borrado seguro;
- IV. Utilizar mecanismos de autenticación y cifrado de acuerdo a estándares internacionales, con un grado no menor a 256 bits para la protección de la comunicación inalámbrica;
- V. Utilizar redes abiertas únicamente al proporcionar servicios a la población, las cuales deberán estar separadas y aisladas de su red de datos;
- VI. Implementar mecanismos de cifrado en los medios de almacenamiento en Centros de Datos centralizados, determinando que la administración de dichos mecanismos de cifrado esté a cargo de servidores públicos;
- VII. Implementar medidas y procedimientos para el respaldo de información, y
- VIII. Establecer filtros de contenido, búsquedas e imágenes en Internet, que permitan la segmentación del mismo en distintas categorías, reportes y soporte de sitios de nueva generación y/o micro-aplicaciones.

Sección II

Seguridad de la información considerada de seguridad nacional

Artículo 28.- Las Instancias de Seguridad Nacional observarán las disposiciones siguientes:

- I. La información relacionada con la seguridad nacional, generada o custodiada, que pretendan diseminar, deberá identificarse previamente, mediante la asignación de alguno de los niveles de diseminación que a continuación se indican:
 - a) "AAA": se asignará este nivel cuando se trate de información requerida para el proceso de decisiones políticas fundamentales, esto es, para la adopción de decisiones sobre riesgos y amenazas a la seguridad nacional, por parte del Presidente de la República, previa consideración del Consejo de Seguridad Nacional, cuya revelación no autorizada pueda dañar la integridad, estabilidad o permanencia del Estado mexicano;
 - b) "AA": este nivel se asignará a la información resultante del ejercicio de atribuciones sustantivas, cuya revelación no autorizada pueda actualizar o potenciar un riesgo o amenaza a la seguridad nacional en términos de la Ley de la materia, o bien, comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal, y
 - c) "A": se asignará este nivel a aquella información que derive del cumplimiento de las disposiciones jurídicas en materia de ejercicio del gasto, transparencia y rendición de cuentas, cuya revelación no autorizada pueda comprometer su operación, las condiciones de seguridad de las instalaciones estratégicas o la integridad física de su personal;
- II. Asegurarse de que el destinatario de la información que se pretende diseminar tenga la necesidad de conocer de la misma, por ser el destinatario expreso de la información con motivo de las facultades conferidas por virtud de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza legal, en términos de la normativa aplicable y de acuerdo con el nivel de diseminación que le corresponda, en razón de su jerarquía o nivel jerárquico, o bien conforme al nivel de privilegio asignado;
- III. Al diseminar la información identificada conforme a los niveles señalados en la fracción I, deberán asegurarse que aquélla que se contenga en medios magnéticos, ópticos o electrónicos, cuente al menos, con las medidas de protección siguientes:
 - a) Se incluya una carátula al inicio del documento, con la leyenda relativa al nivel de diseminación asignado, así como el nombre y cargo o código de seguridad del destinatario;
La leyenda a que se refiere el párrafo anterior se contendrá en cada una de las partes que integren el documento electrónico, en formato de fondo de agua, siempre que el documento lo permita, y en el centro del mismo;
 - b) El documento electrónico deberá diseminarse en un formato de archivo que no permita su edición o manipulación y protegido de origen contra impresión o copiado no autorizado, parcial o total, de su contenido;
 - c) Se utilizarán mecanismos de cifrado de llave pública y privada, canales cifrados de comunicación y, cuando corresponda, de firma electrónica avanzada, que permitan la diseminación de la información únicamente al destinatario autorizado al que esté dirigida;
 - d) Verificar ante el Centro el registro de los destinatarios de información de seguridad nacional;
 - e) Comunicar a los destinatarios sobre la responsabilidad que éstos adquieren al recibir la información a que se refiere este artículo, por lo que estarán obligados a:
 - i. Acusar de recibido al remitente, utilizando los mismos mecanismos de cifrado de llave pública y privada, canales cifrados de comunicación y, cuando corresponda, de firma electrónica avanzada. Cuando no sea posible acusar de recibo al remitente, los mecanismos utilizados deberán generar registros de envío-recepción de la información diseminada;
 - ii. Resguardar la información que reciban en repositorios de información cifrados y controlados con mecanismos de autenticación, para usuarios autorizados y, en los cuales, se lleve un registro sobre los accesos a la información contenida en los mismos;
 - iii. Abstenerse de efectuar reproducciones totales o parciales de los documentos electrónicos, sin la previa autorización de la Instancia de Seguridad Nacional remitente, y
 - f) Las demás medidas de protección que, de acuerdo a los riesgos y amenazas identificados, el Centro considere necesario adoptar.

- IV. Asegurarse que la información identificada conforme a los niveles señalados en la fracción I, contenida en medios impresos que provengan de Infraestructura de TIC, cuente para efectos de su diseminación, como mínimo, con las medidas de protección señaladas en los incisos a), d) y f) de la fracción anterior, y con las siguientes:
- a) Contenerse en sobre cerrado y sellado, cuyo traslado será a cargo de servidores públicos de la Instancia de Seguridad Nacional de que se trate, para su entrega de manera personal al destinatario. En la medida de lo posible, en cada traslado se remitirá solamente un documento o pieza de información, y
 - b) Comunicar a los destinatarios sobre la responsabilidad que éstos adquieren al recibir la información a que se refiere este artículo, por lo que estarán obligados a:
 - i. Firmar el acuse de recibo correspondiente, haciendo constar hora y fecha de recepción, así como la integridad del sobre recibido, registrando al efecto, que no existan indicios de violación o cualquier otra irregularidad;
 - ii. Mantener resguardada la información en área cerrada y dentro de mobiliario provisto de cerradura, caja de seguridad o estructura de seguridad equivalente, y
 - iii. Abstenerse de efectuar reproducciones totales o parciales de la información recibida, sin la previa autorización de la Instancia de Seguridad Nacional remitente, y
- V. Realizar las acciones necesarias para contener la circulación de información diseminada, que sea revelada sin autorización, con independencia de que se promuevan las responsabilidades que, en su caso, procedan.

La diseminación al interior de las Instancias de Seguridad Nacional deberá realizarse mediante controles de seguridad consistentes con los previstos en este artículo, que garanticen la seguridad de la información.

Las Instituciones que, aun sin tener el carácter de Instancia de Seguridad Nacional, generen o sean destinatarias de información considerada de seguridad nacional, deberán observar lo establecido en este artículo en los casos en que compartan o transmitan dicha información.

Lo dispuesto en este artículo se aplicará sin perjuicio de lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y demás disposiciones aplicables.

Artículo 29.- Las Instituciones deberán comunicar al Centro, los datos de los servidores públicos que designen como responsables de la seguridad de la información; así como de los enlaces responsables de mantener comunicación con los equipos de respuesta a incidentes de seguridad en TIC, para efectos de su registro.

Lo anterior será aplicable para los órganos desconcentrados, salvo para aquellos que el Centro exceptúe.

Asimismo, se deberán comunicar al Centro los nombres de las personas autorizadas para conocer información de seguridad nacional, en razón de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, así como el nivel de diseminación a que se refiere la fracción I del artículo 28 de este Acuerdo, acompañada de las promesas de confidencialidad previstas en el artículo 53 de la Ley de Seguridad Nacional, para efectos de su registro y consulta por parte de las demás Instituciones.

Cualquier modificación a la información a que se refieren los párrafos anteriores deberá comunicarse al Centro de inmediato.

Capítulo V

Interpretación, Seguimiento y Vigilancia

Artículo 30.- La interpretación del presente Acuerdo, como de su Anexo Único, para efectos administrativos, así como la resolución de los casos no previstos en el mismo, corresponderá:

- I. En las materias de TIC y de seguridad de la información, a la Secretaría de la Función Pública, por conducto de la Unidad, y
- II. En materia de seguridad de la información considerada de seguridad nacional, a la Secretaría de Gobernación, a través del Centro.

Artículo 31.- El presente Acuerdo y su Anexo Único, se revisarán por las autoridades a que se refiere el artículo anterior, cuando menos una vez al año para efectos, en su caso, de su actualización.

Artículo 32.- Los órganos internos de control en las Instituciones, vigilarán el cumplimiento de lo dispuesto por el presente Acuerdo y el MAAGTICSI.

TRANSITORIOS

Primero.- El presente Acuerdo entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Segundo.- Se abroga el Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, publicado en el Diario Oficial de la Federación el 13 de julio de 2010 y sus reformas del 6 de septiembre y 29 de noviembre de 2011, así como la del 22 de agosto de 2012.

Tercero.- Quedan sin efectos las disposiciones administrativas que se opongan a lo establecido en este Acuerdo.

Cuarto.- Las referencias que en cualquier manual o disposición administrativa se hacen del Acuerdo que se abroga o a sus reformas, se entenderán hechas al Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Quinto.- Todos aquellos procesos, proyectos, trámites, autorizaciones y demás actos iniciados con base en el Acuerdo que se abroga deberán concluirse conforme a lo previsto en el mismo y a las disposiciones que resulten aplicables.

Las Instituciones que a la entrada en vigor del presente Acuerdo, cuenten con contratos vigentes en materia de TIC, se sujetarán a lo establecido en los mismos y a las disposiciones conforme a las cuales se hayan celebrado.

Sexto.- Las Instituciones que, como parte de su patrimonio, cuenten con redes de telecomunicaciones y sistemas de comunicaciones unificadas de telefonía y video, que no se ajusten a lo previsto en los artículos 11 y 17 del presente Acuerdo, deberán establecer en su PETIC la viabilidad de efectuar las adecuaciones que permitan cumplir con las disposiciones de este Acuerdo.

Séptimo.- Las Instituciones dentro del plazo de 20 días hábiles a partir de la entrada en vigor del presente Acuerdo, comunicarán, en su caso, confirmarán al Centro, los datos de los servidores públicos designados responsables de la seguridad de la información y enlaces responsables, a los que se refiere el artículo 29 del presente ordenamiento, en los términos que señala el MAAGTICSI.

Octavo.- Las Instituciones deberán remitir a más tardar a los 15 días hábiles de la entrada en vigor de este Acuerdo, su PETIC a la Unidad, acompañando el inventario de sus aplicaciones para dispositivos móviles, indicando nombre, descripción, fecha de inicio de operación y lenguaje en el que están desarrolladas.

Noveno.- La Unidad podrá exceptuar de cumplir el plazo previsto en el segundo párrafo del artículo 9 del presente Acuerdo, a las Instituciones que tengan programado efectuar contrataciones durante los 45 días hábiles siguientes a la entrada en vigor de este instrumento.

Décimo.- Las Instituciones deberán remitir a la Unidad, en un plazo de 30 días hábiles, a partir de la entrada en vigor del presente Acuerdo, un proyecto de implementación del MAAGTICSI, el cual contendrá cuando menos, objetivo, cronograma, actividades, puntos de control, duración, responsables, consideraciones de administración de riesgos, fecha de inicio y conclusión.

Las Instituciones que habiendo realizado acciones de mejora funcional y digitalización de sus procesos en materia de TIC y de seguridad de la información, continuarán operando éstos, siempre que acrediten ante la Unidad, que los mismos son acordes y consecuentes a las reglas generales y a los procesos establecidos en el Manual, en cuyo caso, acompañarán al proyecto referido en el párrafo anterior, un anexo en el que se contengan las consideraciones técnicas correspondientes.

El inicio de la implementación del MAAGTICSI será a partir del día hábil siguiente de la entrada en vigor del presente Acuerdo, y su conclusión deberá realizarse como máximo a los 160 días hábiles siguientes. Al término de dicho plazo deberán encontrarse en operación la totalidad de los procesos establecidos en el MAAGTICSI.

Décimo Primero.- En tanto se encuentren vigentes los numerales 33 y 35 de los Lineamientos, los plazos y procedimientos para obtener el dictamen correspondiente, en tratándose de adquisiciones de bienes de TIC y de contratación de hospedaje de infraestructura y aplicaciones en un Centro de Datos, no resultará aplicable lo previsto en los párrafos segundo y tercero del artículo 9 de este Acuerdo.

Sufragio Efectivo. No Reelección.

Dado en la Ciudad de México, Distrito Federal, a los treinta días del mes de abril de dos mil catorce.- El Secretario de Gobernación, **Miguel Ángel Osorio Chong**.- Rúbrica.- En ausencia del Secretario de la Función Pública, en términos de lo dispuesto por los artículos 18 de la Ley Orgánica de la Administración Pública Federal; 7, fracción XII, y 86 del Reglamento Interior de la Secretaría de la Función Pública, el Subsecretario de Responsabilidades Administrativas y Contrataciones Públicas, **Julián Alfonso Olivas Ugalde**.- Rúbrica.

ANEXO ÚNICO

MANUAL ADMINISTRATIVO DE APLICACIÓN GENERAL EN LAS MATERIAS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES Y DE SEGURIDAD DE LA INFORMACIÓN.

CONTENIDO

OBJETIVOS.

ÁMBITO DE APLICACIÓN.

MARCO JURÍDICO.

DEFINICIONES.

REGLAS GENERALES.

PROCESOS EN LAS MATERIAS DE TIC Y DE SEGURIDAD DE LA INFORMACIÓN.

I. PROCESOS DE GOBERNANZA.

I.A Proceso de Planeación Estratégica (PE).

I.B Proceso de Administración del Presupuesto y las Contrataciones (APCT).

II. PROCESOS DE ORGANIZACIÓN.

II.A Proceso de Administración de Servicios (ADS).

II.B Proceso de Administración de la Configuración (ACNF).

II.C Proceso de Administración de la Seguridad de la Información (ASI).

III. PROCESOS DE ENTREGA.

III.A Proceso de Administración de Proyectos (ADP).

III.B Proceso de Administración de Proveedores (APRO).

III.C Proceso de Administración de la Operación (AOP).

III.D Proceso de Operación de Controles de Seguridad de la Información y del ERISC (OPEC).

IV. APÉNDICES.

IV.A Formatos para los productos de los procesos.

IV.B Matriz de metodologías, normas y mejores prácticas aplicables a la gestión de las TIC.

IV.C Diagramas de actividades de los procesos.

OBJETIVOS

Objetivo General:

Definir los procesos con los que, en las materias de TIC y de seguridad de la información, las Instituciones deberán regular su operación, independientemente de su estructura organizacional y las metodologías de operación con las que cuenten.

Objetivos Específicos:

1. Enfocar el monitoreo y control sobre las actividades vinculadas con las TIC, en un esquema de gobernanza, organización y entrega.
2. Fortalecer el control sobre los recursos de TIC y mantener alineada la planeación estratégica de las Instituciones al Programa, a la EDN, las Bases de Colaboración celebradas por la Institución y a las disposiciones que de estos instrumentos emanen.
3. Mantener indicadores orientados a resultados basados en el ejercicio del presupuesto y en la entrega de servicios de valor.

ÁMBITO DE APLICACIÓN

El presente manual es de aplicación general en la Administración Pública Federal y en la Procuraduría General de la República.

El lenguaje empleado en el manual no busca generar ninguna clase de discriminación, ni marcar diferencias entre hombres y mujeres, por lo que las referencias o alusiones hechas al género masculino representan siempre a todos o todas, hombres y mujeres, abarcando claramente ambos sexos.

MARCO JURÍDICO

Los ordenamientos jurídicos referidos en este apartado, se citan de manera enunciativa y no limitativa.

1. Constitución Política de los Estados Unidos Mexicanos.
2. Código Penal Federal.
3. Ley Orgánica de la Administración Pública Federal.
4. Ley Orgánica de la Procuraduría General de la República.
5. Ley General de Bienes Nacionales.
6. Ley Federal de las Entidades Paraestatales.
7. Ley Federal de Presupuesto y Responsabilidad Hacendaria.
8. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
9. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
10. Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
11. Ley Federal de Telecomunicaciones.
12. Ley Federal sobre Metrología y Normalización.
13. Ley Federal de Archivos.
14. Ley de Seguridad Nacional.
15. Ley de Firma Electrónica Avanzada.
16. Ley del Sistema de Horario en los Estados Unidos Mexicanos.
17. Reglamento de la Oficina de la Presidencia de la República.
18. Reglamento Interior de la Secretaría de Gobernación.
19. Reglamento Interior de la Secretaría de la Función Pública.
20. Reglamento de Ley Federal de las Entidades Paraestatales.
21. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.
22. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
23. Reglamento de la Ley de Firma Electrónica Avanzada.
24. Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional.
25. Plan Nacional de Desarrollo 2013-2018.
26. Programa para un Gobierno Cercano y Moderno 2013-2018.
27. Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.
28. Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.
29. Lineamientos de Protección de Datos Personales, expedidos por el entonces Instituto Federal de Acceso a la Información Pública.
30. Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales, emitidos por el entonces Instituto Federal de Acceso a la Información Pública.
31. Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.
32. Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.
33. Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.
34. Documento Técnico para la Interoperabilidad de los Sistemas Automatizados de Control de Gestión.

DEFINICIONES

Para efectos de este manual, además de las definiciones del artículo 2 del Acuerdo por el que se expide éste, se entenderá por:

Términos:

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Activo de información clave: El activo de información que resulta esencial o estratégico para la operación y/o el control de una infraestructura crítica, o incluso de una que no tenga este carácter, pero cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.

Activo primario: El activo de información asociado a las funciones sustantivas de una Institución.

Activos de proceso: Los elementos de información que son parte de un proceso y que reflejan características específicas del mismo.

Activo de soporte: El que apoya o complementa a un activo primario en su función.

Acuerdo: el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.

Acuerdo de nivel de servicio SLA: El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (Service Level Agreement, por sus siglas en inglés).

Acuerdo de nivel operacional OLA: El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (Operational Level Agreement por sus siglas en inglés).

Ambiente de trabajo: El conjunto de herramientas, utilerías, programas, aplicaciones, información, facilidades y organización que un usuario tiene disponible para el desempeño de sus funciones de manera controlada, de acuerdo con los accesos y privilegios que tenga asignados por medio de una identificación única y una contraseña.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Área contratante: A la facultada en la Institución para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios.

Área requirente: A la que, en la Institución, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o aquella que los utilizará.

Área solicitante o usuaria: A la que, en la Institución, efectúa originalmente la petición a la UTIC para obtener un bien o servicio de TIC y/o que hará uso del mismo.

Área técnica: A la que, en la Institución, elabora las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, evalúa la propuesta técnica de las proposiciones y es responsable de responder en la junta de aclaraciones las preguntas que sobre estos aspectos realicen los licitantes. El área técnica podrá tener también el carácter de área requirente.

Arquitectura tecnológica: A la estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Bitácora de seguridad: El registro continuo de eventos e incidentes de seguridad de la información que ocurren a los activos de información.

Cambios administrados: La integración controlada, eficiente, segura y oportuna de componentes y/o activos de TIC, aplicativos de cómputo, soluciones tecnológicas o servicio de TIC, que modifican el ambiente operativo de la UTIC; mediante criterios técnicos y mecanismos para la planeación y ejecución de dichos cambios, a fin de que éstos sean efectuados satisfactoriamente sin exponer el ambiente operativo y la operación de los servicios de TIC.

Confidencialidad: La característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.

Declaraciones de aplicabilidad: El documento que contiene los controles aplicados mediante el SGSI de la Institución como resultado del análisis de riesgos.

Directriz rectora: El documento estratégico en el que se establecen principios tecnológicos de alto nivel.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Documento de planeación del proyecto: El documento que contiene la definición de un proyecto, el control de su avance, así como sus documentos de planeación subsidiarios y documentación complementaria.

Documentos de planeación subsidiarios: Los documentos de planeación del proyecto que se deben instrumentar cuando un proyecto es autorizado, entre otros: plan de administración de riesgos, plan de recursos, plan de presupuestos y plan de comunicación, los cuales se incorporan al documento de planeación del proyecto.

Entregable: El producto adquirido, desarrollado o personalizado, con características cuantificables y medibles en términos de su valor, integralidad, funcionalidad y capacidades.

Evento: El suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes.

Funcionalidad: Las características de los aplicativos de cómputo, soluciones tecnológicas o de un servicio de TIC, que permiten cubrir las necesidades o requerimientos de un usuario.

Gestión de riesgos: La identificación, valoración y ejecución de acciones, para el control y minimización de los riesgos que afecten a los activos de TIC, a la infraestructura crítica o a los activos de información de la Institución.

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

Infraestructuras críticas: Las instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso.

Interdependencia: La interconexión estrecha que existe entre las infraestructuras críticas, y que conlleva a que la falla o falta de una de ellas impacte negativamente en otras infraestructuras críticas, presentándose como consecuencia un efecto cascada de fallas en la prestación de servicios.

Interoperabilidad: La capacidad de organizaciones y sistemas, dispares y diversos, para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las Instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnologías de la información y comunicaciones.

Mesa de servicios: El punto de contacto único, en el cual se reciben las solicitudes de servicio de los usuarios de equipos y servicios de TIC en la Institución.

Objetivos estratégicos de TIC: El conjunto de resultados que se prevé alcanzar y que se integran en el PETIC, los cuales describen el alcance de las acciones que serán llevadas a cabo por la UTIC.

Problema: La causa de uno o más incidentes, del cual se plantea una solución alterna en espera de una solución definitiva.

Programa de capacidad: El documento de planeación que contiene la información sobre la capacidad de la infraestructura de TIC considerando los escenarios de necesidades futuras y los acuerdos de niveles de servicio establecidos.

Programa de contingencia: El documento de planeación en el que se plantea la estrategia, el recurso humano en la UTIC, los activos y las actividades requeridas, para recuperar por completo o parcialmente un servicio o proceso crítico, en caso de presentarse un desastre o la materialización de un riesgo.

Programa de continuidad: El documento de planeación que contiene los elementos y las acciones necesarios para asegurar que la operación de los servicios y procesos críticos de TIC de la Institución no se interrumpa.

Programa de disponibilidad: El documento de planeación que contiene los elementos y acciones necesarios para que los componentes de la infraestructura de TIC estén operando y sean accesibles.

Programa de proyectos: La integración de uno o más proyectos de TIC que pueden ser administrados en su conjunto para la obtención de beneficios adicionales a los que se lograrían de ser administrados individualmente durante su ejecución.

Programa de tecnología: El documento de planeación en el que se establecen las acciones estratégicas para la conformación de las arquitecturas de cada dominio tecnológico y de todos ellos en su conjunto, considerando los servicios de TIC existentes y proyectados.

Recursos de TIC: La infraestructura, los activos, el recurso humano en la UTIC y el presupuesto de TIC.

Recursos humanos en la UTIC: Los servidores públicos adscritos a la UTIC, o inclusive los servidores públicos de otras áreas de la Institución o personal de terceros cuando participen en alguno de los procesos previstos en el manual y que hayan sido acreditados por algún servidor público facultado para llevar a cabo actividades específicas en dichos procesos.

Repositorio: El espacio en medio magnético u óptico en el que se almacena y mantiene la información digital.

Requerimientos funcionales: La característica que requiere cumplir un producto o entregable asociado a una función en un proceso o servicio automatizado, o por automatizar.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.

Sistema informático: El conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos.

Software de código abierto: El software cuya licencia asegura que el código pueda ser modificado y mejorado por cualquier persona o grupo de personas con las habilidades correctas, debido a que el conocimiento es de dominio público.

Unidad administrativa solicitante: La unidad administrativa de la Institución que solicita un aplicativo de cómputo o servicio de TIC y que es responsable de definir sus requerimientos, funcionalidades y niveles de servicio.

Usuarios: Los servidores públicos o aquéllos terceros que han sido acreditados o cuentan con permisos para hacer uso de los servicios de TIC.

Validación: La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

Acrónimos:

CIDGE: La Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.

DTISACG: El Documento Técnico de Interoperabilidad de los Sistemas Automatizados de Control de Gestión emitido por la Secretaría de la Función Pública.

ERISC: El equipo de respuesta a incidentes de seguridad en TIC en la Institución.

MAAG: Los manuales administrativos de aplicación general de la Administración Pública Federal.

SFP: La Secretaría de la Función Pública.

SGSI: El sistema de gestión de seguridad de la información que, por medio del análisis de riesgos y de la definición de controles, define las guías para la implementación, operación, monitoreo, revisión y mejora de la seguridad de la información.

UTIC: La unidad administrativa en la Institución responsable de proveer de infraestructura y servicios de TIC a las demás áreas y unidades administrativas.

REGLAS GENERALES

Las reglas generales aplicables a los nueve procesos de este manual son las siguientes:

1. El titular de la UTIC es el responsable de asegurar que se cumplan las presentes reglas generales.
2. El responsable de cada proceso de este manual, debe asegurar que se cumplan las actividades, factores críticos y reglas que lo constituyan.
3. El titular de la UTIC es responsable de asegurar que la totalidad del personal adscrito a esa unidad administrativa conozca la EDN y el Programa, y que oriente a estos ordenamientos, sus actividades, y el ejercicio de sus atribuciones y facultades, de acuerdo a su competencia y la normatividad aplicable.

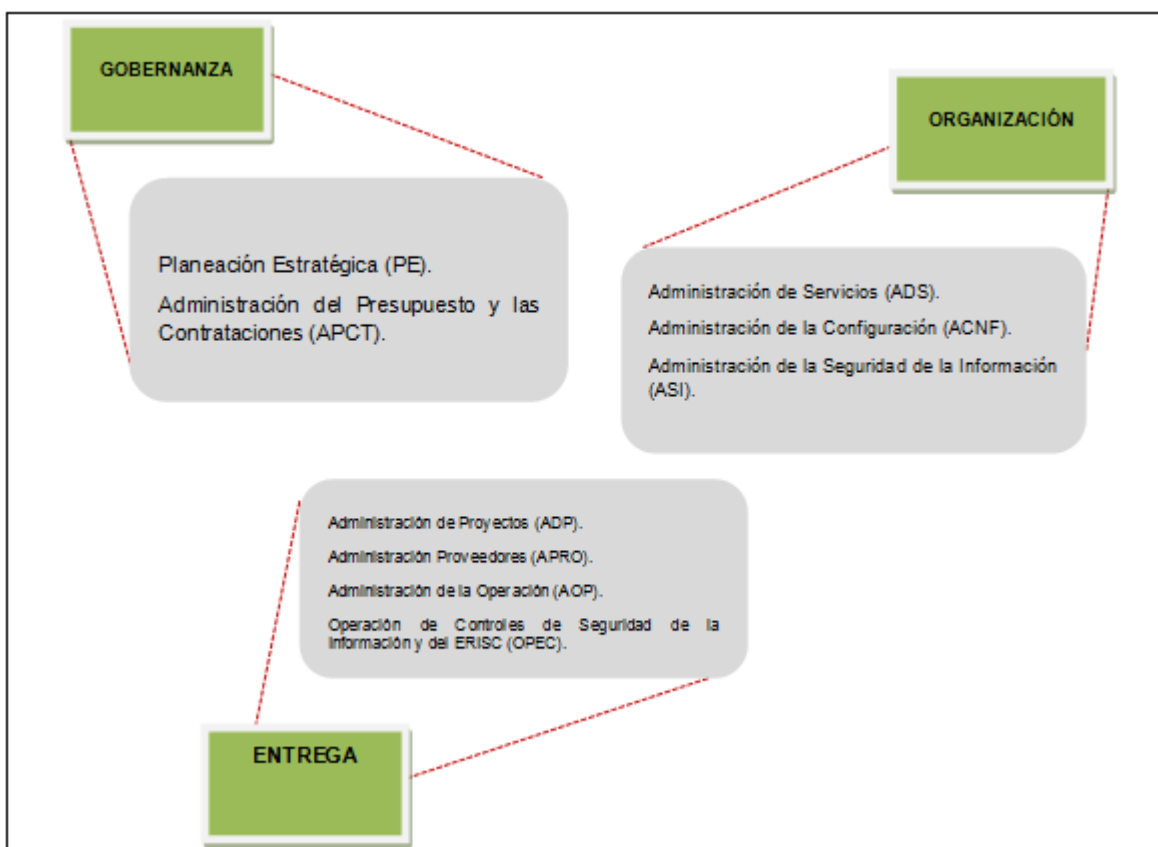
4. Los servidores públicos de la UTIC y los usuarios involucrados, al operar los procesos de este manual, deberán apegarse estrictamente a las políticas, líneas de acción, criterios y estándares que se establecen en la EDN, o que de ella emanen, al Programa y a las Bases de Colaboración que la Institución haya celebrado.
 5. Los servidores públicos de la UTIC, así como de las otras unidades administrativas de la Institución, serán responsables de las actividades que en los diversos procesos de la UTIC, les sean asignadas.
 6. Los responsables de los procesos de este manual, deberán apegarse a lo que establece la Ley Federal sobre Metrología y Normalización, y hacer uso de las metodologías, mejores prácticas nacionales e internacionales listadas en la matriz de metodologías, normas y mejores prácticas aplicables a la gestión de las TIC, que se integran en el Apéndice IV.B de este manual.
 7. Para determinar las erogaciones que como área requirente se pretendan realizar en cada ejercicio fiscal en materia de contratación de TIC, la UTIC deberá atender lo dispuesto en los numerales 4.1.1.1 a 4.1.1.6 del MAAGMAASSP, incluyendo la verificación de la existencia de contratos marco en materia de TIC.
 8. Cuando se requiera llevar a cabo una contratación en materia de TIC, la UTIC, como área requirente, deberá llevar a cabo las actividades previstas en los numerales 4.2.1.1.1 a 4.2.1.1.9, 4.2.1.1.11 y 4.2.1.1.12, así como en su caso, el 4.2.1.1.10 del MAAGMAASSP. Asimismo, en caso de identificar la existencia de un contrato marco cuyo objeto sea los bienes o servicios que se pretendan contratar, la UTIC lo indicará al área contratante de la Institución, para los efectos procedentes.
 9. El titular de la UTIC deberá asegurar que se integre y mantenga actualizado el registro de los activos de información y recursos de TIC en la Herramienta Diagnóstico Inventario que para tal efecto ponga a disposición la Unidad, a través de su portal.
10. La Institución deberá, con apego a los procesos del presente manual, a las líneas de acción de la EDN y a las definiciones técnicas que de éstas emanen, instrumentar los servicios de TIC comunes en la Administración Pública Federal, relativos a: monitoreo de activos de información y restauración de fallas; operación de la red de datos; telefonía; correo electrónico; autenticación de certificados digitales y de mensajes y validación de documentos con firma electrónica avanzada; procesamiento de la información; operación de aplicativos y mesa de servicios. Estos servicios deberán ser integrados al catálogo de servicios, de acuerdo a lo que establece el Proceso de Administración de Servicios (ADS).
 11. La Institución, a través de la UTIC, con apego a las líneas de acción de la EDN, deberá instrumentar, entre otros, los componentes y servicios transversales de acceso e interoperabilidad para habilitar los trámites y servicios digitalizados en www.gob.mx, así como aplicaciones únicas para la sustitución del uso de papel, y aquéllas para la administración de recursos institucionales en oficinas mayores o áreas homólogas.
 12. La UTIC como área requirente deberá, previo a la solicitud que formule al área contratante de la Institución para llevar a cabo un procedimiento de contratación, cumplir las disposiciones relacionadas con la modernización de la Administración Pública Federal mediante el uso de TIC, que se establecen en los Lineamientos, atendiendo a las guías, criterios, procedimientos o instructivos que deriven de éste.
 13. Los responsables del Proceso de Planeación Estratégica (PE) y del catálogo de servicios de TIC de la Institución, deberán mantener actualizados el inventario de aplicaciones de la Administración Pública Federal y su catálogo de servicios de TIC, poniendo este último a disposición de la Unidad.
 14. Las Instituciones deberán integrar y mantener actualizado su catálogo de servicios de TIC, considerando al menos la información que se menciona en el Proceso Administración de Servicios (ADS) de este manual.
 15. Los roles que se señalan en cada uno de los procesos de este manual, con excepción de los mencionados en el Proceso de Administración de la Seguridad de la Información (ASI) y el Proceso de Operación de los Controles de Seguridad de la Información y del ERISC (OPEC), deberán ser asignados por el titular de la UTIC de acuerdo a sus facultades y a la normatividad aplicable. En el caso de los procesos ASI y OPEC, los servidores públicos que tomarán cada rol serán designados por el responsable de la seguridad de la información institucional (RSII).
 16. Los servidores públicos de la UTIC, así como los de otras unidades administrativas de la Institución, serán responsables, de acuerdo a los roles que les sean asignados, de las actividades que en los diversos procesos de este manual se señalen para dichos roles.
 17. El titular de la UTIC deberá asegurarse de difundir las disposiciones de las Políticas para la EDN que se establecen en el Acuerdo por el que se expide este manual, y de que los responsables de cada proceso, así como la totalidad del personal de la UTIC, se apeguen a dichas disposiciones, dejando

en todo momento evidencia de ello.

18. Los responsables de cada proceso se asegurarán, cuando utilicen formatos propios, que los productos de los procesos a su cargo, se elaboren, describan y documenten considerando al menos la información que se indica en los formatos del Apéndice IV.A de este manual, o utilizar éstos.
19. La evidencia derivada de la operación de los procesos de este manual, podrá ser presentada impresa o a través de sistemas o medios informáticos, siempre y cuando el responsable de los mismos documente el tipo de entrega de las evidencias.
20. El titular de la UTIC deberá asegurarse, conjuntamente con las áreas solicitantes de los aplicativos de cómputo o servicios de TIC, que se incluyan en éstos, cuando así resulte necesario, como campos llave en los esquemas de datos, la Clave Única de Registro de Población (CURP) o la clave del Registro Federal de Contribuyentes (RFC), según corresponda.

PROCESOS EN LAS MATERIAS DE TIC Y DE SEGURIDAD DE LA INFORMACIÓN

El manual contiene, en tres grupos, los procesos necesarios para propiciar la operación ágil y oportuna de las actividades de TIC de las Instituciones, conforme a lo siguiente:



I. PROCESOS DE GOBERNANZA

I.A. PROCESO DE PLANEACIÓN ESTRATÉGICA (PE)

Objetivo General:

Establecer un modelo de gobierno de TIC en la Institución, para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC, la planeación estratégica de TIC y asegurar la adecuada organización al interior de la UTIC para la gestión de sus procesos y vinculación ordenada con sus usuarios.

Objetivos Específicos:

1. Promover que los mandos medios y los titulares de las unidades administrativas de la Institución, coadyuven con la UTIC en la toma de decisiones para la dirección y control de las TIC, así como para la entrega efectiva y eficiente de los sistemas y servicios de TIC.
2. Constatar que la asignación de roles en la UTIC, permita la operación eficiente de los procesos que en ésta se llevan a efecto.
3. Prever que la Institución cuente con un PETIC, con el objeto de establecer líneas de acción en materia de TIC y su seguimiento, alineadas a los objetivos institucionales, al Plan Nacional de Desarrollo 2013-2018, a los programas sectoriales y especiales que resulten aplicables, así como al Decreto, el Programa, las Bases de colaboración que haya celebrado la Institución y las líneas de acción de la EDN.

Reglas del proceso:

1. El Titular de la UTIC es el responsable de este proceso y de la Planeación estratégica de TIC de la Institución. El titular de la UTIC podrá designar como corresponsable del proceso y de la Planeación estratégica de TIC en la Institución a un colaborador de un nivel inmediato inferior que le reporte directamente.
2. El Titular de la UTIC deberá asegurarse de que el PETIC de la Institución cumpla con las disposiciones del Acuerdo.
3. El Grupo de trabajo para la dirección de TIC deberá apoyar la implementación, operación y mejora del SGSI, así como las acciones que realice el Grupo estratégico de seguridad de la información.
4. El Responsable de este proceso deberá asegurarse que la aplicación de los recursos de TIC de la Institución se encuentren alineados al Decreto, al Programa, así como a la EDN, en lo que a la materia de TIC se refiere.
5. El Responsable de este proceso deberá constatar que para cada iniciativa y proyecto de TIC que se conceptualice, se identifiquen los Objetivos y Habilitadores de la EDN a los cuales dará cumplimiento como resultado de su ejecución. Para lo anterior, tomará como base la Relación de Líneas de Acción, que contiene el Programa relacionadas con TIC.
6. El Responsable de este proceso deberá asegurarse que el PETIC se integre en el sistema que para tales efectos informe la Unidad, habiendo cubierto previamente las autorizaciones correspondientes al interior de la Institución, tal y como lo establece el presente proceso.
7. El Responsable de este proceso deberá atender las disposiciones de las Políticas para la Estrategia Digital Nacional, en lo que se refiere a la entrega del PETIC de la institución a la Unidad, para su revisión y autorización. Tal entrega deberá efectuarse por medio del sistema informático que determine la Unidad.

Roles del proceso:

1. Titular de la UTIC.
2. Responsable del Proceso de Planeación Estratégica (PE).
3. Responsable de la Planeación estratégica de la UTIC.
4. Grupo de trabajo para la dirección de TIC.

Actividades del Proceso.

PE 1 Establecer la gobernabilidad de las operaciones de la UTIC.

Descripción: Establecer el grupo de trabajo para la dirección de TIC, que lleve el gobierno de TIC, tanto en la operación de los procesos de la UTIC y áreas vinculadas, como en la entrega de los servicios de TIC.

Factores Críticos:

El responsable de este proceso deberá:

1. Solicitar la intervención del titular de la Institución para establecer el grupo de trabajo para la dirección de TIC, el cual deberá integrarse por mandos superiores con capacidad de toma de decisiones sobre los objetivos, metas y proyectos institucionales de TIC, y formalizarse mediante una

acta la integración y forma de operación del grupo de trabajo para la dirección de TIC.
2. Definir, implementar y mantener una adecuada organización al interior de la UTIC, mediante la asignación de roles y responsabilidades para la gestión de los procesos de ésta, atendiendo a las necesidades de los procesos y proyectos de la UTIC.
3. Informar al titular de la Institución acerca de los resultados, recomendaciones y acuerdos del grupo de trabajo para la dirección de TIC.
El grupo de trabajo para la dirección de TIC deberá efectuar, entre otras, las siguientes actividades:
4. Determinar oportunidades en el uso de las TIC.
5. Determinar las prioridades de las iniciativas de TIC alineadas con las prioridades institucionales, así como de los programas sectoriales y especiales que le competan.
6. Verificar que las principales inversiones en materia de TIC se encuentren alineadas a los objetivos estratégicos de la Institución.
7. Evaluar el cumplimiento de los niveles de servicio establecidos para los servicios de TIC e identificar los riesgos de las iniciativas de TIC.
8. Autorizar los proyectos estratégicos de la Institución a integrarse en el PETIC.
9. Mantenerse informado del seguimiento del PETIC, conforme a lo señalado en este proceso.
10. Establecer la coordinación necesaria con el responsable de seguridad de la información en la Institución para armonizar el gobierno de TIC, la administración de riesgos y el SGSI.
11. Conocer los criterios técnicos que proponga el responsable de la seguridad de la información en la Institución para gestionar los riesgos.

PE 2 Integrar la información estratégica del PETIC, así como el conjunto total de iniciativas y proyectos de TIC, sus métricas e indicadores.

Descripción: Integrar la información estratégica del PETIC, así como el conjunto total de iniciativas y proyectos de TIC, sus métricas e indicadores.

Factores críticos:

El responsable de la planeación estratégica de la UTIC, para integrar el PETIC, deberá:

1. Integrar los elementos regulatorios y tecnológicos que influyan o puedan influir en la ejecución de las actividades y servicios que provee la UTIC, conforme a:
 - a) Disposiciones en las materias de TIC y seguridad de la información.
 - b) Disposiciones vinculadas, nacionales y/o internacionales, que resulten aplicables.
 - c) Estándares de observancia obligatoria como son los de integración y publicación de información geoespacial, domicilios geográficos y articulación de padrones, entre otros.
 - d) Tendencias tecnológicas emergentes.
2. Integrar en el PETIC los objetivos estratégicos, las metas y acciones que permitan cumplir los objetivos estratégicos de TIC, considerando elementos de arquitectura empresarial.
3. Establecer en el PETIC, la relación existente entre indicadores, metas y acciones. Considerar la evaluación resultante de los indicadores de los procesos de este manual.
4. Determinar el conjunto total de iniciativas y proyectos de TIC, identificando aquellos que se consideren estratégicos, e integrar cada iniciativa y proyecto de TIC, incluyendo su descripción, alcance, línea base y programa de trabajo.
5. Priorizar las iniciativas y proyectos de TIC, considerando su relevancia para cumplir con los objetivos institucionales y los estratégicos de TIC.
6. Estimar la inversión requerida para las iniciativas y proyectos de TIC, desagregando de ésta al menos los rubros de recursos financieros, materiales y humanos.
7. Identificar en el PETIC un máximo de 7 iniciativas y/o proyectos de TIC que se consideren estratégicos, aplicando como criterio preferente para su identificación que aporten mayores beneficios a la población o cuenten con alto impacto en el cumplimiento de los objetivos institucionales, del Decreto y la EDN; debiendo asegurar que éstos se integren al portafolio de proyectos de TIC que se establece en el Proceso Administración de Proyectos (ADP).
8. Las iniciativas y proyectos de TIC que se integren en esta actividad deberán categorizarse, de acuerdo a la siguiente lista:
 - a) Optimización. En donde por medio de la aplicación de TIC se logra una mejor manera de llevar a cabo actividades.
 - b) Digitalización. Aplicación de TIC para la conversión de contenidos a medios digitales en la generación de trámites y servicios por este medio, así como el acceso a información en este formato.

- c) Simplificación. Aplicación de TIC para la reducción de tiempos, costos y requisitos en los trámites y servicios, así como en la eliminación o automatización de actividades en los procesos.
- d) Racionalización. Reducción en el costo de los recursos e insumos obtenidos de mejores prácticas y estrategias en la contratación.

PE 3 Validar, aprobar, comunicar y adecuar, de ser necesario, el PETIC.

Descripción: Validar, aprobar, comunicar y adecuar, de ser necesario, el PETIC.

Factores críticos:**El titular de la UTIC, en la fecha que se determina en el Acuerdo, deberá:**

1. Revisar y validar el PETIC.
2. Presentar el PETIC para la autorización del grupo de trabajo para la dirección de TIC, así como gestionar la aprobación de la Institución coordinadora de sector que le corresponda.
3. Registrar el PETIC, una vez cumplido el factor crítico anterior, en el sistema informático al que se alude en la regla 7 del presente proceso.

El responsable de este proceso deberá:

4. Verificar que se obtenga la autorización del PETIC por parte de la Unidad, utilizando para ello el sistema informático al que se alude en la regla 7 del presente proceso.
5. Difundir el PETIC a todos los involucrados en la UTIC y en la Institución.

PE 4 Dar seguimiento a la planeación estratégica de TIC.

Descripción: Dar seguimiento a los avances en el cumplimiento de la planeación estratégica de TIC.

Factores críticos:**El responsable de la planeación estratégica de la UTIC deberá:**

1. Dar seguimiento al avance del PETIC y reportarlo trimestralmente a la Unidad, previa aprobación del titular de la UTIC por medio del sistema informático aludido en la regla 7 del presente proceso.
2. Informar trimestralmente al grupo de trabajo para la dirección de TIC, así como a las instancias que se determinan en el Acuerdo, sobre el cumplimiento del PETIC, así como de la situación de los indicadores en el tablero de seguimiento de la planeación estratégica de TIC y de sus indicadores.
3. Identificar, registrar y administrar las acciones correctivas en caso de desviación en el avance real del PETIC, verificando el cumplimiento de sus indicadores.
4. Verificar que los indicadores de los procesos de este manual se encuentren actualizados de acuerdo a la periodicidad del indicador, efectuar su evaluación y difundir los resultados.

Relación de Productos del proceso:

1. "Acta de integración y forma de operación del grupo de trabajo para la dirección de TIC". Formato PE F1.
2. Plan estratégico de tecnologías de la información y comunicaciones (PETIC), en el sistema informático señalado en la regla 7 del presente proceso.
3. Tablero de seguimiento de la planeación estratégica de TIC y de sus indicadores (formato de acuerdo a las necesidades y recursos de la Institución).

Indicador del proceso:

Nombre: Eficiencia del PETIC.

Objetivo: Medir la eficiencia en la elaboración del PETIC.

Descripción: Obtener la eficiencia en la elaboración del PETIC, con base en el número de ajustes técnicos que se hayan efectuado como una adecuación al PETIC.

Fórmula: % de eficiencia = la desviación estándar de las variables que intervienen en la ejecución de las iniciativas y proyectos de TIC estratégicos, respecto de la línea base autorizada en el PETIC.

Responsable: El responsable del Proceso de Planeación Estratégica de TIC (PE).

Frecuencia de cálculo: Trimestral.

I.B. Proceso de Administración del Presupuesto y las Contrataciones (APCT)

Objetivo General:

Coordinar las acciones para el ejercicio del presupuesto destinado a las TIC, a fin de maximizar su aplicación en las contrataciones de TIC requeridas por la Institución, así como las acciones para efectuar el acompañamiento necesario a las unidades facultadas para realizar los procedimientos de contrataciones en la Institución, de manera que se asegure su ejecución en tiempo y forma, alineado al presupuesto autorizado; así como el seguimiento a los contratos que se celebren.

Objetivos Específicos:

1. Identificar y consolidar los requerimientos de recursos financieros de los proyectos y servicios de TIC existentes en los portafolios correspondientes.
2. Elaborar el listado de bienes y servicios de TIC que la UTIC requiera contratar en cada ejercicio fiscal, considerando las directrices de la Institución, así como las disposiciones que en materia presupuestaria, de adquisiciones, arrendamientos y servicios resulten aplicables.
3. Proporcionar al área contratante, el apoyo y los elementos técnicos necesarios para llevar a cabo los procedimientos de contratación de TIC y participar en los mismos de acuerdo a su ámbito de atribuciones.

Reglas del proceso:

1. El responsable del seguimiento del presupuesto autorizado, de los procedimientos de contratación de TIC y de los contratos celebrados en materia de TIC, deberá ser designado por el titular de la UTIC, y tener un nivel jerárquico inmediato inferior al de éste.
2. El responsable del proceso deberá asegurarse que éste se ejecute con apego a las disposiciones que en materia presupuestaria resulten aplicables, así como a los procesos de las unidades administrativas facultadas para administrar los recursos financieros y elaborar el anteproyecto anual de presupuesto de la Institución.
3. El responsable de este proceso deberá asegurarse que éste se efectúe con apego a las disposiciones en materia de adquisiciones y arrendamiento de bienes muebles y servicios, al Acuerdo por el que se expide el MAAGMAASSP, al Acuerdo y aquellas en materia presupuestaria, que resulten aplicables.
4. El titular de la UTIC, deberá designar a un representante con los conocimientos técnicos suficientes que permitan dar respuesta clara y precisa a las solicitudes de aclaración de los licitantes en las juntas de aclaraciones de los procedimientos de contratación a los que fuere convocada la UTIC como área técnica.
5. Cuando otras áreas o unidades administrativas de la Institución diversas a la UTIC, tengan asignados recursos financieros para la contratación de bienes o servicios de TIC necesarios para el cumplimiento de sus funciones, deberán contar previo al inicio del procedimiento de contratación de que se trate, con la aprobación por escrito de la UTIC, por medio de un dictamen técnico.
6. En el supuesto a que se refiere la regla anterior, corresponderá al área o unidad administrativa de que se trate, fungir como área técnica, por lo que la UTIC deberá proporcionar el apoyo técnico que le sea requerido por ésta.
7. En aquellos casos en que se integren o adicionen componentes de software a un aplicativo de cómputo o a un servicio de TIC ya existente, el responsable del proceso se deberá asegurar de que se consideren las siguientes pruebas: integrales, de funcionalidad, estrés, volumen, aceptación del usuario y de seguridad, con el propósito de comprobar que la funcionalidad del aplicativo de cómputo o servicio de TIC existente se mantiene inalterada y que la relativa al componente integrado o adicionado es consistente.
8. El responsable de este proceso deberá verificar que cada vez que se suscriba un contrato para la adquisición, arrendamiento o servicios de TIC, éste sea registrado en el sistema electrónico de compras gubernamentales denominado CompraNet, con apego a la normatividad aplicable.
9. El titular de la UTIC será el responsable de la firma de aprobación del formato F2 APCT, así como de su trámite ante la Unidad.

Roles del proceso:

1. Responsable del Proceso de Administración del Presupuesto y las Contrataciones (APCT).
2. Responsable del seguimiento del presupuesto autorizado de TIC.
3. Responsable del listado de bienes y servicios de TIC que la UTIC requiere se contraten.

Actividades del Proceso.

APCT 1 Establecer el seguimiento del presupuesto de TIC.

Descripción: Definir las acciones necesarias para dar seguimiento al presupuesto autorizado de TIC por las instancias competentes, utilizando la información de los portafolios de proyectos y de servicios de TIC, así como la de los programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica.

Factores Críticos:

El responsable del seguimiento del presupuesto deberá:

1. Mantener comunicación efectiva con las unidades administrativas responsables de administrar los recursos financieros y materiales de la Institución.
2. Gestionar ante las unidades administrativas facultadas, de acuerdo con sus procesos y las disposiciones presupuestarias aplicables, la asignación de recursos para la ejecución de los proyectos de TIC autorizados, contenidos en los portafolios de proyectos y de servicios de TIC, así como para mantener la operación de los sistemas y servicios de TIC mediante los programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica.
3. Coordinar, en el ámbito de competencia de la UTIC, el seguimiento del ejercicio de los recursos presupuestarios de TIC.
4. Proponer escenarios para organizar los portafolios de proyectos y servicios de TIC y participar en el control de los gastos efectuados con cargo al presupuesto asignado a la UTIC, para la ejecución de los proyectos y servicios de TIC, así como para el aprovisionamiento de la infraestructura tecnológica,

- que aseguren la operación de los sistemas y servicios de TIC.
5. Mantener actualizados los portafolios de proyectos y de servicios de TIC, en lo que respecta a verificar que el costo de operación y mantenimiento de los activos de TIC esté adecuadamente reflejado en el programa de mantenimiento de la infraestructura tecnológica y en el presupuesto asignado a la UTIC.
 6. Verificar con la unidad administrativa competente de la Institución, que los elementos que conforman las iniciativas de los portafolios de proyectos y de servicios de TIC, así como los relativos a los programas aprovisionamiento y de mantenimiento de la infraestructura tecnológica, estén identificados de acuerdo con la partida de gasto correspondiente.
 7. Mantener actualizados y disponibles los registros sobre el ejercicio del presupuesto de TIC, incluida la programación de gasto comprometido, montos y fechas de pago para la operación y mantenimiento de los activos de TIC.
 8. Proveer de la información sobre el presupuesto de TIC a los responsables de la elaboración de los documentos para la dictaminación de contrataciones de TIC, para documentar las iniciativas y proyectos de TIC.
 9. Comunicar al grupo de trabajo para la dirección de TIC y a los responsables de los procesos de la UTIC, la información sobre el presupuesto de TIC, para apoyar la toma de decisiones en la priorización de su asignación y la coordinación de su aplicación a la ejecución de iniciativas y proyectos de TIC.
 10. El titular de la UTIC deberá constatar que se revise el inventario de aplicaciones de la APF para determinar si existe, con el propósito de su reutilización, un aplicativo de cómputo de características similares a los requerimientos que la UTIC reciba o que se generen dentro de la misma. En el caso de que en la revisión se haya determinado la existencia de algún aplicativo de cómputo susceptible de ser reutilizado, deberá dar aviso a la Unidad y gestionar dicha reutilización ante la UTIC de la Institución responsable del aplicativo de cómputo de que se trate.

APCT 2 Participar en el establecimiento de prioridades del presupuesto de TIC.

Descripción: Participar en la definición de los proyectos, servicios e iniciativas de TIC, a los que se dará prioridad al asignar los recursos financieros destinados a las TIC.

Factores Críticos:

El responsable del seguimiento del presupuesto, con apoyo de los responsables de los procesos de la UTIC, deberá:

1. Identificar los proyectos, servicios e iniciativas de TIC incluidos en los portafolios de proyectos y de servicios de TIC, de acuerdo con el PETIC, para los que sea necesaria una asignación presupuestaria.
2. Establecer escenarios para el adecuado ejercicio del presupuesto destinado a las TIC, indicando los gastos indispensables para garantizar la continuidad de la operación, los riesgos operativos y los correspondientes a las iniciativas de TIC comprometidas, acordes con el PETIC.
3. Presentar al titular de la UTIC los escenarios a que se refiere el factor crítico anterior, para la toma de decisiones sobre el ejercicio del presupuesto destinado a las TIC.
4. Documentar las reducciones presupuestarias y presiones de gasto que sean informadas a la UTIC por las unidades administrativas facultadas, y realizar el análisis que permita identificar los riesgos o contingencias que deriven de tales reducciones y presiones de gasto.
5. Gestionar ante la unidad administrativa facultada para administrar los recursos financieros de la Institución, las constancias de suficiencia presupuestaria para sustentar la contratación de bienes y servicios de TIC que sean requeridos por la UTIC.

APCT 3 Estimar los recursos presupuestarios en materia de TIC para la elaboración del anteproyecto anual de presupuesto de la Institución.

Descripción: Coordinar, de acuerdo a las indicaciones de la unidad administrativa competente de la Institución, la estimación de los recursos presupuestarios en lo relativo a TIC para la elaboración del anteproyecto anual de presupuesto de la Institución.

Factores Críticos:**El responsable del seguimiento del presupuesto, con apoyo de los responsables de los procesos de la UTIC, deberá:**

1. Estimar los recursos presupuestarios de TIC, de acuerdo con los requerimientos previstos en los programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica de la UTIC.
2. Estimar los recursos presupuestarios necesarios para el desarrollo de los proyectos e iniciativas de TIC contemplados en los portafolios de proyectos y de servicios de TIC.
3. Atender lo señalado en la Regla General 7 de este manual, al integrar la estimación del presupuesto de TIC del año siguiente.
4. Elaborar, con base en la información que le provean los responsables de los procesos de la UTIC, la estimación del presupuesto de TIC del siguiente ejercicio fiscal, proporcionando la información relativa a contrataciones plurianuales.
5. Presentar la estimación del presupuesto de TIC al titular de la UTIC y por su conducto, al grupo de trabajo para la dirección de TIC para su revisión y aprobación.
6. Entregar el presupuesto estimado de TIC del ejercicio siguiente, a la unidad administrativa facultada y responsable de la integración del anteproyecto anual de presupuesto de la Institución.

APCT 4 Establecer el listado de bienes y servicios de TIC a contratar por la UTIC en cada ejercicio fiscal y ejecutar las acciones necesarias para apoyar los procedimientos de contratación correspondientes, en el ámbito de sus atribuciones.

Descripción: Elaborar el listado de bienes y servicios de TIC a contratar por la UTIC en cada ejercicio fiscal con base en su presupuesto autorizado y realizar las acciones de apoyo para las contrataciones de TIC.

Factores Críticos:**El responsable de este proceso deberá:**

1. Elaborar, de acuerdo a los procedimientos de la Institución, un listado de bienes y servicios de TIC a contratar por la UTIC en el ejercicio fiscal en curso, que incluya el cronograma de las contrataciones de TIC previstas, respecto de las iniciativas de TIC contenidas en los portafolios de servicios y proyectos de TIC que hayan sido autorizadas en términos de este manual, así como de los programas de aprovisionamiento y de mantenimiento de la infraestructura tecnológica, considerando para ello los recursos financieros con los que se cuenten en el ejercicio fiscal correspondiente destinados a TIC.
2. Verificar la posibilidad de llevar a cabo contrataciones consolidadas y de utilizar contratos marco u otras estrategias de contratación, a fin de proponerlas al área de la Institución encargada de integrar el programa anual de adquisiciones, arrendamientos y servicios.

El responsable de este proceso, con apoyo del área que solicite los bienes o servicios de TIC, deberá:

3. Asegurar que, para cada contratación que se prevea, se elabore el documento para la dictaminación de contrataciones de TIC, y remitirlo a la Unidad según se establece en el Acuerdo, a fin de obtener el dictamen correspondiente.
4. En concordancia con el factor crítico anterior, proponer la estrategia de contratación para las iniciativas o proyectos de TIC autorizados por el grupo de trabajo para la dirección de TIC, al área contratante de la Institución.
5. Definir acciones a fin de proveer al área contratante de la Institución con los elementos técnicos necesarios para llevar a cabo los procedimientos de contratación que correspondan.
6. Verificar que la documentación soporte que deba entregarse al área contratante de la Institución se encuentre debidamente integrada, en términos de lo señalado en el numeral 4.2.1.1.8 del MAAGMAASSP, y particularmente que el anexo técnico que elabore la UTIC contenga las especificaciones y requerimientos técnicos del bien o servicio de TIC que se pretenda contratar, entre otros:
 - a) Requerimientos funcionales.
 - b) Requerimientos no funcionales, tales como: la disponibilidad del bien o servicio de TIC en función de las necesidades de la unidad administrativa solicitante, así como los controles de seguridad que deberán garantizarse respecto del bien o para la prestación del servicio de TIC de que se trate.
 - c) Cuando corresponda, los casos de uso, módulos, matriz de trazabilidad y protocolos de pruebas.
 - d) Niveles de servicio.

e) Términos y condiciones de entrega y de aceptación. f) Tiempos de respuesta de soporte y de servicio. g) La previsión para que, en su oportunidad, se incluya una cláusula al contrato que se celebre que asegure a la Institución que el proveedor y su personal no harán uso indebido de la documentación, información ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio. h) La forma en que se llevará a cabo la supervisión del servicio contratado.
7. Integrar los requerimientos técnicos en materia de TIC para que se lleve a cabo la investigación de mercado correspondiente, para lo cual analizará la información enviada por la unidad administrativa solicitante y verificará que ésta contenga los criterios de calidad, de aceptación y los niveles de servicio esperados respecto de los bienes y servicios de TIC que se pretenden contratar.
8. Participar con el área contratante de la Institución, en caso de que no exista un área especializada, en la elaboración de la investigación de mercado, para lo cual podrá realizar entre otras actividades, las siguientes: a) Requerir, en su caso, a posibles proveedores, la información sobre los bienes y servicios de TIC que se pretenden contratar. b) Analizar las cotizaciones de los proveedores en cuanto a las características técnicas de los bienes o servicios que ofrecen y el monto en relación con el presupuesto autorizado para la contratación.
9. Apoyar al área contratante en la elaboración e integración del proyecto de convocatoria a la licitación pública o del proyecto de invitación a cuando menos tres personas.
10. Asistir a las sesiones del comité de adquisiciones, arrendamientos y servicios de la Institución, a las que sea convocado como invitado para apoyar al área contratante en la atención de las dudas que presenten los miembros del comité.
11. Realizar las demás actividades que las disposiciones jurídicas aplicables, así como el MAAGMAASSP, prevean que debe participar el área requirente para cada procedimiento de contratación de TIC.
El responsable de este proceso deberá:
12. Mantener informados a los responsables del seguimiento al ejercicio del presupuesto autorizado para las contrataciones de TIC y en su caso, a la unidad administrativa solicitante, sobre los avances y conclusión de los procedimientos de contratación que se hayan llevado a cabo.

APCT 5 Participar como área técnica, en los procedimientos de contratación de TIC.

Descripción: Dar acompañamiento técnico, en su carácter de área técnica, en los procedimientos de contratación de TIC, mediante su participación en los actos en que se prevea su intervención.

Factores Críticos:

El servidor público de la UTIC que se designe como representante para el acompañamiento técnico deberá:

1. Participar en la junta o juntas de aclaraciones que se lleven a cabo, apoyando al área contratante a agrupar por temas técnicos las solicitudes de aclaración y resolver las dudas correspondientes, conforme a lo previsto en los numerales 4.2.2.1.9 y 4.2.2.1.10 del MAAGMAASSP.
2. Analizar y evaluar la propuesta técnica de las proposiciones que presenten los licitantes con el apoyo, en su caso, del área contratante.

Relación de Productos del proceso:

1. "Listado de bienes y servicios de TIC que la UTIC requiere se contraten". Formato APCT F1.
2. "Anexo técnico" (formato de acuerdo a las necesidades del procedimiento de contratación y del bien o servicio que será objeto del procedimiento).
3. "Documento para la dictaminación de contrataciones de TIC" Formato APCT F2.

Indicador del proceso:

Nombre: Resultados del seguimiento al presupuesto de TIC.

Objetivo: Obtener un resultado de la gestión del proceso APCT por medio de la medición de su eficiencia.

Descripción: Conocer el porcentaje de presupuesto ejercido en tiempo y forma con respecto del autorizado.

Fórmula: % de eficiencia = (monto de presupuesto de TIC ejercido en tiempo y forma / monto de presupuesto autorizado para TIC) X 100.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Anual.

II. PROCESOS DE ORGANIZACIÓN

II.A. PROCESO DE ADMINISTRACIÓN DE SERVICIOS (ADS).

Objetivo General:

Definir los compromisos y costos de los servicios de TIC necesarios para mantener el adecuado funcionamiento de la Institución, así como identificar iniciativas de servicios de TIC que aporten beneficios importantes en el cumplimiento de los objetivos estratégicos de la Institución, con apego a la EDN y efectuar su instrumentación.

Objetivos Específicos:

1. Diseñar la arquitectura de los servicios de TIC y definir las especificaciones técnicas para satisfacer las necesidades actuales y proyectadas de la Institución, considerando que se deben incluir las definiciones de los niveles de seguridad, capacidad, disponibilidad y continuidad de la operación de TIC.
2. Identificar y administrar riesgos, desde el diseño de los servicios de TIC, para que puedan ser eliminados, transferidos o mitigados y de ser el caso, aceptados.
3. Mantener información clara y precisa sobre los servicios de TIC en operación y en proceso de diseño o desarrollo.
4. Contar con mecanismos para la toma de decisiones relacionadas con los servicios de TIC.

Reglas del proceso:

1. El responsable de este proceso deberá ser designado por el titular de la UTIC, y tener un nivel jerárquico inmediato inferior al de éste.
2. El responsable de este proceso deberá coordinarse con el responsable del Proceso de Administración de Proyectos (ADP), a efecto de que las modificaciones al catálogo de servicios de TIC sean consideradas en el portafolio de proyectos de TIC.
3. El responsable de este proceso deberá asegurarse que el hardware y el software de recuperación utilizado en la aplicación del programa de continuidad sea funcional, para restablecer, probar y renovar los respaldos al menos semestralmente.
4. El responsable de este proceso deberá asegurarse que los servicios de TIC y las soluciones tecnológicas que provea la UTIC para oficios electrónicos al interior de la Institución y entre instituciones, cumplan con lo que se establece tanto en los Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, así como en los Documentos Técnicos de Interoperabilidad vigentes y los aplicables que expida la Subcomisión de Interoperabilidad de la CIDGE, derivados del Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.
5. El responsable del diseño de servicios de TIC, conjuntamente con el responsable de la planeación estratégica de la UTIC, deberán asegurarse que el diseño de nuevas soluciones tecnológicas y servicios de TIC incluya, de ser el caso, aquéllos datos que permitan cumplir con la normatividad técnica de domicilios geográficos que para dicho fin emite el INEGI.
6. El responsable del diseño de servicios de TIC, conjuntamente con el responsable de la planeación estratégica de la UTIC, deberán asegurarse que se cumpla, para el Cifrado de Datos, como mínimo con estándares tales como 3DES de triple llave, AES-128, AES-192 y AES-256, así como redes con protocolos seguros para su envío.

Roles del proceso:

1. Responsable del proceso y administrador del catálogo de servicios de TIC.
2. Grupo de trabajo para la dirección de TIC.
3. Responsable del diseño de servicios de TIC.
4. El Responsable de la planeación estratégica de TIC.

Actividades del Proceso.**ADS 1 Establecer un catálogo de servicios de TIC.**

Descripción: Crear y mantener un registro detallado de los servicios de TIC existentes en la Institución, así como de las iniciativas para la creación y el registro del desarrollo de nuevos servicios de TIC.

Factores Críticos:

El administrador del catálogo de servicios de TIC, con apoyo del responsable de la planeación estratégica de TIC y de los responsables de los servicios de TIC en operación, deberá:

1. Recabar información de las unidades administrativas solicitantes y usuarios relacionada con:
 - a) Requerir, en su caso, a posibles proveedores, la información sobre los bienes y servicios de TIC que se pretenden contratar.
 - b) Las capacidades y recursos estimados para implementar los servicios de TIC que se identifiquen para cumplir con los objetivos referidos.
 - c) La ruta crítica para la entrega de los servicios de TIC.
2. Recabar la información técnica de los servicios de TIC existentes y los propuestos, debiendo considerar también los que son provistos por terceros.
3. Integrar los datos de los servicios de TIC durante su ciclo de vida, desde su diseño, transición, operación hasta su retiro de la operación e integrar el catálogo de servicios de TIC con esta información.

ADS 2 Mantener actualizado el catálogo de servicios de TIC.

Descripción: Mantener actualizado el catálogo de servicios de TIC, debiendo contener los datos del desarrollo de las iniciativas y de los servicios de TIC.

Factores Críticos:

El administrador del catálogo de servicios de TIC deberá:

1. Coordinar la integración del catálogo de servicios de TIC, a efecto de que contenga para cada servicio, cuando menos, la información siguiente:
 - a) Descripción del servicio, resumida y detallada.
 - b) Responsable técnico y en su caso, usuario del servicio (unidad administrativa).
 - c) Arquitectura empresarial detallando sus componentes.
 - d) Disponibilidad del servicio (comprometida y real).
 - e) Métricas e indicadores.
 - f) Costo de operar el servicio.
 - g) Estado del servicio (conservación, reemplazo, racionalización, renovación, retiro).
 - h) Garantía de cuando menos los siguientes servicios comunes (en desarrollo y existentes):
 - i. Monitoreo de activos de información y restauración de fallas;
 - ii. Operación de red de datos;
 - iii. Telefonía;
 - iv. Correo electrónico;
 - v. Procesamiento de la información;
 - vi. Operación de aplicativos;
 - vii. Operación de trámites y servicios a través de la Ventanilla Única Nacional;
 - viii. Mesa de servicios;
 - ix. Reportes estadísticos de la gestión de trámites y servicios;

x.	Servicios de apertura de información pública en formato abierto, de acuerdo a las directrices que en esta materia se expidan;
xi.	Servicios con estándares de observancia obligatoria como lo son aquellos para la integración y publicación de información geoespacial, domicilios geográficos y articulación de padrones, entre otros;
xii.	Autenticación de certificados digitales;
xiii.	Autenticación de mensajes y validación de documentos con firma digital;
xiv.	Módulo de firmado electrónico de documentos;
xv.	Aplicaciones únicas de sustitución de uso de papel y generación de oficios electrónicos, de acuerdo con los Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión, y el DTISACG;
xvi.	Aplicaciones de administración de recursos institucionales en oficialías mayores o áreas homólogas, denominadas con el acrónimo GRP, y
xvii.	Aplicaciones para la gestión sin papel y la automatización de los procesos que se establecen en los MAAG.
i)	Coordinar la actualización constante del catálogo de servicios de TIC, a cuyo efecto deberá utilizarse la información contenida en el repositorio de configuraciones del Proceso de Administración de la Configuración (ACNF).
j)	Asegurar que los datos que se mantengan en el repositorio de configuraciones del Proceso de Administración de la Configuración (ACNF), sean consistentes con los datos que registre la UTIC en la Herramienta Diagnóstico Inventario que para tales efectos ponga a disposición la Unidad, a través de su portal.
k)	Mantener informados a los responsables del diseño de los servicios de TIC, y a los responsables de los servicios de TIC en operación, sobre los cambios al catálogo de servicios de TIC.
l)	Mantener disponible el catálogo de servicios de TIC, tanto al grupo de trabajo para la dirección de TIC, como a los responsables en las unidades administrativas solicitantes.

ADS 3 Diseñar los servicios de TIC.

Descripción: Definir las especificaciones para el diseño de cada servicio de TIC, nuevo o adecuaciones a servicios existentes.

Factores Críticos:

El responsable del proceso, deberá:

1. Asignar un responsable del diseño de servicio de TIC, para cada servicio a desarrollar.

El responsable del diseño de servicios de TIC deberá:

2. Definir, en coordinación con los involucrados, los requerimientos del servicio de TIC.
3. Realizar un análisis de los requerimientos asociados al servicio de TIC, y verificar que se documenten y aprueben por los diversos involucrados. Estos requerimientos serán la base para las actividades de diseño posteriores, por lo que cualquier modificación deberá efectuarse mediante un control de cambios.

El análisis de requerimientos deberá considerar al menos lo siguiente:

a) Para servicios ya existentes:

- i) Funcionalidad e infraestructura en términos de arquitectura empresarial.
- ii) Cambios en los procesos de la Institución, prioridades, importancia e impacto.
- iii) Cambios en los volúmenes de transacciones del servicio de TIC.
- iv) Cambios en los niveles de servicio y sus metas.

b) Para servicios nuevos:

- i) Funcionalidad e infraestructura en términos de arquitectura empresarial.
- ii) Administración del servicio.
- iii) Procesos de la Institución involucrados, prioridades, importancia e impacto y beneficios.
- iv) Niveles de servicio y sus metas.
- v) Niveles de transacciones, número y tipo de usuarios y crecimiento proyectado.
- vi) Estimación sobre cambios que eventualmente pudieran presentarse en el servicio.
- vii) Niveles de capacidad y de soporte que se prevé cumplir.

4. Verificar la infraestructura, componentes y servicios de TIC existentes, debiendo especificar la reutilización de elementos que se haya identificado.
5. Elaborar las especificaciones técnicas de las posibles soluciones al servicio de TIC requerido, las cuales deberán considerar lo siguiente:
 - a) El proceso o procesos de la Institución que se atenderán con el servicio de TIC.
 - b) Las instalaciones, funcionalidad e información para monitoreo del servicio de TIC del servicio en diseño.
 - c) El ciclo de vida del servicio de TIC, incluyendo su escalabilidad en base a la demanda proyectada, a través de una hoja de ruta del servicio (roadmap).
 - d) Los requerimientos y metas de los niveles de servicio, esperadas y comprometidas.
 - e) Los requerimientos para la realización de pruebas del servicio de TIC, incluida la aceptación de la unidad administrativa solicitante para ello.
 - f) Los acuerdos de nivel operacional OLA existentes y en su caso, los que deban ser acordados en la UTIC para la operación del servicio de TIC de que se trate.
 - g) Los servicios de TIC que se tengan contratados y que se relacionen con el servicio en diseño.
6. Definir los criterios técnicos para la aceptación del servicio de TIC incluyendo niveles de servicio mínimos, para lo cual definirá las métricas que estime necesarias.
7. Evaluar las diversas alternativas de solución para el servicio de TIC, en cuanto a tiempo, costo, beneficio a la Institución y grado de cumplimiento a los requerimientos del servicio de TIC, a fin de seleccionar la alternativa más apropiada.
8. Verificar si el presupuesto estimado en este proceso, es suficiente para el servicio de TIC que se está diseñando y en su caso, comunicar al responsable del proceso la necesidad de realizar ajustes al presupuesto estimado.
9. Verificar que la solución para el servicio de TIC que se hubiere seleccionado se encuentre alineada al programa de tecnología, a los objetivos institucionales y a las líneas de acción de la EDN.
10. Verificar que la solución para el servicio de TIC seleccionada, cumpla con los controles previstos en el Proceso de Administración de la Seguridad de la Información (ASI).
11. Evaluar que la solución seleccionada pueda ser operada de manera que cumpla con las metas de los niveles de servicio.
12. Efectuar el análisis del impacto al negocio, en el que se contemplen los beneficios y contribución de valor de la solución seleccionada, en cada etapa de su ciclo de vida.
13. Identificar los riesgos asociados a la solución seleccionada, y establecer los controles para su operación, seguridad, disponibilidad y continuidad.
14. Evaluar, en coordinación con la unidad administrativa solicitante, la capacidad técnica y administrativa requerida por la Institución para la operación de la solución seleccionada.
15. Evaluar la capacidad de la infraestructura de TIC de la Institución, para lo cual se deberá considerar lo siguiente:
 - a) El impacto que tendría la solución seleccionada, respecto de la operación de otros servicios de TIC y en los procesos de la UTIC.
 - b) La arquitectura tecnológica necesaria para la operación de la solución seleccionada.
16. Integrar el expediente del diseño del servicio de TIC de que se trate, con la información obtenida en esta actividad.
17. Actualizar el portafolio de servicios de TIC, con la información del expediente del servicio de TIC diseñado.
18. Asegurar que los requerimientos tecnológicos del servicio de TIC en proceso de diseño, se incorporen al programa de tecnología y al programa de aprovisionamiento de la infraestructura tecnológica.
19. Se consideren servicios de apertura de información pública en formato abierto, de acuerdo a las directrices que en esta materia se expidan.
20. Verificar que el diseño del servicio de TIC no contravenga la normativa aplicable en materia de TIC.

ADS 4 Administrar la capacidad de la infraestructura de TIC.

Descripción: Elaborar el programa de capacidad y darle seguimiento, a fin de asegurar la operación de los servicios de TIC conforme a los compromisos y niveles de servicio acordados.

Factores Críticos:

El responsable de este proceso, con apoyo de los responsables de los dominios tecnológicos de la UTIC, deberá:

1. Elaborar el programa de capacidad que le permita a la UTIC cumplir con: los niveles de servicio acordados, el crecimiento previsto de la demanda de infraestructura, la mejora de los niveles de servicio y la incorporación de los nuevos servicios de TIC que, de acuerdo al portafolio de servicios de TIC, se tiene previsto inicien su operación.
Para la elaboración del programa de capacidad, será necesario:
 - a) Determinar el balance entre la demanda de los servicios de TIC y la capacidad de la infraestructura de TIC, para conocer la suficiencia de cada uno de sus componentes.
 - b) Establecer escenarios para las diversas proyecciones de demanda de los servicios de TIC y considerar, de ser el caso, opciones respecto de los niveles y metas de servicio acordados, señalando invariablemente los riesgos que cada escenario conlleve.
 - c) Determinar los componentes de la infraestructura de TIC que son necesarios para cumplir con los requerimientos de desempeño y disponibilidad de los servicios de TIC, tanto de los existentes como de los proyectados.
 - d) Identificar los activos de TIC que requieren actualizarse, mejorarse o inclusive, sustituirse, así como las fechas propuestas y los costos estimados en cada caso.
2. Verificar, al menos trimestralmente, la capacidad y rendimiento de la infraestructura de TIC, para determinar si es suficiente para prestar los servicios de TIC con los niveles de servicio acordados, para lo cual será necesario:
 - a) Monitorear el rendimiento actual y la capacidad utilizada.
 - b) Obtener información de los incidentes que se han presentado por falta de capacidad.
 - c) Evaluar los niveles de la capacidad y rendimiento de la infraestructura con respecto a:
 - i) los niveles de servicio originalmente acordados.
 - ii) los niveles de servicio efectivamente proporcionados.
 - iii) los niveles de servicio que, de acuerdo con el programa de capacidad, se hubieren estimado.
3. Elaborar, al menos trimestralmente, un pronóstico sobre la capacidad y rendimiento de la infraestructura de TIC, para mitigar el riesgo de interrupciones o la degradación de los niveles de servicio que podrían presentarse por la falta de capacidad suficiente de la infraestructura de TIC.
4. Identificar la disponibilidad de capacidad de los distintos componentes de la infraestructura de TIC, para su posible redistribución.
5. Identificar las tendencias de las cargas de trabajo de los componentes de la infraestructura, en condiciones normales y de contingencia, así como determinar sus proyecciones, para que sean incluidas en el programa de capacidad.
6. Definir las acciones a implementar cuando la capacidad y rendimiento de la infraestructura de TIC no estén en el nivel requerido, tales como: ajustar la prioridad de las tareas de los componentes de la infraestructura de TIC, instaurar mecanismos de recuperación en caso de fallas, entre otras.
7. Incluir, en los programas de continuidad, las características de capacidad y rendimiento de cada componente de la infraestructura de TIC, con la finalidad de que éstos se puedan utilizar, en caso necesario, de manera individual.
8. Mantener informados a los responsables de los procesos de la UTIC, así como a los responsables de los dominios tecnológicos de:
 - a) Las oportunidades identificadas para mejorar la capacidad de la arquitectura tecnológica en operación y realizar recomendaciones sobre los incidentes por falta de capacidad de la infraestructura de TIC.
 - b) Los niveles de servicio alcanzados.

ADS 5 Administrar la disponibilidad de servicios de TIC.

Descripción: Elaborar el programa de disponibilidad y darle seguimiento, a efecto de asegurar los requerimientos actuales y los previstos en la entrega de servicios de TIC.

Factores Críticos:**El responsable de este proceso deberá:**

1. Elaborar el programa de disponibilidad que permita a la UTIC cumplir con los niveles de servicio

acordados, soportado en la capacidad actual de la infraestructura de TIC en operación, y en las proyecciones para los nuevos servicios incluidos en el portafolio de servicios de TIC.

Para la elaboración del programa de disponibilidad, considerar:

- a) La información contenida en el programa de capacidad.
 - b) Los requerimientos, actuales y previstos, de disponibilidad de los servicios de TIC.
 - c) La disponibilidad de los componentes de la infraestructura de TIC que soportan los servicios de TIC, incluidos los proporcionados por terceros.
 - d) Los tiempos en que se requiere adecuar la disponibilidad de los componentes de la infraestructura de TIC.
 - e) Los riesgos que pudieran materializarse al efectuar adecuaciones a los componentes de la infraestructura de TIC.
 - f) Los costos estimados para llevar a cabo las adecuaciones que permitan obtener la disponibilidad esperada.
2. Revisar, al menos trimestralmente, la disponibilidad de los servicios de TIC para determinar el cumplimiento de los niveles de servicio acordados, en función de la disponibilidad de la infraestructura de TIC.
 3. Obtener información de los incidentes que se han presentado por falta de disponibilidad.
 4. Evaluar los niveles de disponibilidad de los servicios de TIC y de los componentes de la infraestructura de TIC con respecto a:
 - a) los niveles de servicio originalmente acordados.
 - b) los niveles de servicio efectivamente proporcionados.
 - c) los niveles de servicio que, de acuerdo con el programa de disponibilidad, se hubieren estimado.
 5. Incluir en los programas que se prevén en este proceso, las características de disponibilidad, capacidad y rendimiento de cada componente de la infraestructura de TIC, con el propósito de que éstos se fortalezcan en lo individual, en caso necesario.
 6. Mantener informados a los responsables de los dominios tecnológicos de:
 - a) Las oportunidades identificadas para mejorar la disponibilidad de la arquitectura tecnológica en operación y realizar recomendaciones sobre los incidentes por falta de disponibilidad de la infraestructura de TIC.
 - b) Los niveles de servicio alcanzados.

ADS 6 Administrar la continuidad de servicios de TIC.

Descripción: Asegurar a la Institución el mínimo impacto en caso de alguna interrupción en los servicios de TIC.

Factores Críticos:

El responsable del diseño de servicios de TIC deberá:

1. Efectuar el análisis de impacto al negocio, en el que se identifiquen las funciones, actividades, áreas o unidades administrativas, así como los servicios que proporciona la Institución que podrían resultar afectados como consecuencia de la interrupción de uno o más servicios de TIC, así como el alcance de las consecuencias que se generarían.
 2. Elaborar el programa de continuidad que articule las diferentes acciones que habrían de realizarse para la continuidad de los servicios de TIC y que permita determinar la resistencia requerida por la infraestructura de TIC.
- Para elaborar el programa, será necesario tomar en cuenta lo siguiente:
- a) Los resultados del análisis de impacto al negocio y la estrategia de recuperación determinada en el Proceso de Administración de la Seguridad de la Información (ASI).
 - b) La cobertura de los responsables de los servicios de TIC, internos y externos, así como del responsable de la administración de los usuarios.
 - c) La forma para documentar, probar y ejecutar técnicamente la recuperación de un servicio de TIC en caso de desastre, así como los programas de contingencia de TIC.
 - d) Los requerimientos de resistencia, procesamiento alternativo y capacidad de recuperación de los servicios críticos de TIC.
 - e) La identificación de activos y recursos críticos de TIC, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y las directrices de respaldo y recuperación.

3. Integrar en el programa de continuidad las siguientes definiciones:
 - a) Prioridades en situaciones de recuperación para evitar la recuperación de servicios de menor impacto y asegurarse de que la respuesta y la recuperación se encuentren alineadas con las necesidades prioritarias de la Institución.
 - b) Niveles de los costos de manera que se mantengan en un nivel aceptable y que se cumpla con la normativa aplicable, así como con los compromisos asumidos en contratos vigentes relacionados.
 - c) Definir los requerimientos de resistencia, respuesta y recuperación para cada prioridad establecida.
4. Revisar y en su caso, actualizar el programa de continuidad, mediante un mecanismo de control de cambios y versiones.
5. Efectuar pruebas de recuperación, al menos semestralmente, al programa de continuidad para confirmar que los servicios de TIC puedan ser recuperados de forma efectiva, que las deficiencias serán atendidas y comprobar su vigencia o efectuar actualización.
6. Definir el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas controlados, en pruebas de punta a punta y de ser el caso, en pruebas integrales con proveedores.
7. Actualizar el programa de continuidad, con las medidas correctivas que se definan sobre los hallazgos e incidentes que se hayan presentado en las pruebas de recuperación efectuadas, así como con las lecciones aprendidas que apliquen.
8. Difundir y mantener disponible, de manera segura, el programa de continuidad y los cambios que se realicen al mismo, a efecto de que los involucrados en dicho programa lo consulten cuando así lo requieran, inclusive bajo escenarios de desastre.
9. Llevar a cabo, conjuntamente con los involucrados en el programa de continuidad, al menos cada seis meses, una revisión del contenido del mismo para que cada uno de ellos conozca de manera indubitable cuál será su desempeño en las diversas actividades que habrán de realizarse en caso de requerirse la aplicación del programa.
10. Elaborar, en coordinación con los responsables de los procesos de la UTIC y con base a los requerimientos de los responsables de los procesos sustantivos de la Institución, la propuesta sobre el contenido de los respaldos a almacenar, y presentarla al titular de la UTIC, para que, de estimarla adecuada, solicite la aprobación del grupo de trabajo para la dirección de TIC.
11. Establecer, en la medida de lo posible, fuera de las instalaciones operativas de la Institución, el resguardo de los medios que contengan los respaldos y la documentación requerida para su restauración, así como de cualquier otro recurso de TIC considerado crítico y que es necesario para la recuperación de los servicios de TIC, de acuerdo con los programas de continuidad establecidos.
12. Verificar que la administración del sitio del resguardo a que se refiere el factor crítico anterior cumpla con los controles del SGSI de la UTIC.

Relación de Productos del proceso:

1. Catálogo de servicios de TIC (conforme al formato o herramienta que defina la Institución).
2. "Programa de capacidad". Formato ADS F1.
3. "Programa de disponibilidad". Formato ADS F2.
4. "Análisis de impacto al negocio". Formato ADS F3.
5. "Programa de continuidad". Formato ADS F4.

Indicador del proceso:

Nombre: Cumplimiento del proceso. Objetivo: Medir el grado de cumplimiento del proceso. Descripción: Medir el cumplimiento en la ejecución de las evaluaciones trimestrales sobre el portafolio de servicios de TIC. Fórmula: % de eficiencia = (número de evaluaciones efectuadas / número de evaluaciones del periodo que se reporta) X 100. Responsable: El responsable de este proceso. Frecuencia de cálculo: Trimestral.
--

II.B. PROCESO DE ADMINISTRACIÓN DE LA CONFIGURACIÓN (ACNF).

Objetivo General:

Establecer y actualizar un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, con la finalidad de facilitar su acceso a los involucrados en los procesos de la UTIC, cuando éstos así lo requieran para la operación del proceso respectivo.

Objetivos Específicos:

1. Identificar, registrar, controlar y verificar los datos de los elementos de configuración, así como la información relacionada con los mismos.
2. Mantener actualizada la información contenida en el repositorio de configuraciones y disponible para los servidores públicos de la UTIC involucrados en los diversos procesos.

Reglas del proceso:

1. El responsable de este proceso es responsable de la administración del repositorio de configuraciones.
2. El responsable de este proceso deberá mantener una verificación continua del repositorio de configuraciones a fin de constatar que éste se encuentre actualizado en todo momento.

Roles del proceso:

1. Responsable del Proceso de Administración de la Configuración (ACNF).

Actividades del Proceso.

ACNF 1 Establecer la cobertura y el alcance de la administración de la configuración.

Descripción: Identificar las soluciones tecnológicas y sus componentes, así como los diversos ambientes y arquitecturas tecnológicas de la UTIC, como elementos de configuración, para establecer la cobertura que tendrá el proceso, así como el alcance de la administración sobre los elementos de la configuración y sus componentes.

Factores Críticos:

El responsable de este proceso deberá:

1. Identificar los elementos de configuración para determinar, de acuerdo a las necesidades y recursos con los que cuenta la UTIC, los que serán administrados en este proceso.
2. Elaborar un programa para la integración de los elementos de configuración en el repositorio de configuraciones, el cual, en caso de ser gradual, considerará lo siguiente:
 - a) La criticidad e impacto en caso de falla de los elementos a administrar.
 - b) El tipo de los elementos a administrar.
 - c) Los servicios actuales y los proyectados.
 - d) Las localidades en que se ubican los elementos a administrar.
3. Seleccionar los elementos de configuración que requerirán como líneas base para su administración

- del registro en el repositorio de configuraciones.
4. Implementar acciones de control para la administración del repositorio de configuraciones, considerando al menos:
 - a) Las necesarias para la implementación y mantenimiento de herramientas tecnológicas para la administración del repositorio.
 - b) El mantenimiento al modelo de datos del repositorio de configuraciones.
 - c) La definición y aplicación de criterios técnicos para realizar modificaciones a los estados de los elementos de configuración o componentes.
 - d) Que la incorporación de elementos de configuración o componentes al repositorio de configuraciones se realice mediante cambios administrados.
 - e) Las relativas a la administración de los usuarios del repositorio de configuraciones, incluyendo perfiles y permisos.
 - f) La definición del formato que permita la identificación, en el repositorio, de los elementos físicos de la configuración, sin perjuicio de lo dispuesto en el Acuerdo por el que se establecen las disposiciones en Materia de Recursos Materiales y Servicios Generales, en lo relativo a inventarios.
 - g) El calendario de respaldos del repositorio de configuraciones.
 - h) La programación de las revisiones al repositorio de configuraciones y su calendarización.
 5. Obtener la autorización del titular de la UTIC sobre las acciones definidas.
 6. Registrar las acciones autorizadas a fin de darles seguimiento, así como en su oportunidad registrar sus resultados.

ACNF 2 Definir la estructura del repositorio de configuraciones.

Descripción: Definir la estructura del repositorio de configuraciones, con base en la identificación de las características de los elementos de configuración y componentes que serán administrados en dicho repositorio, y de la infraestructura de TIC de la Institución.

Factores Críticos:**El responsable de este proceso deberá:**

1. Definir la estructura de datos que requerirá el repositorio de configuraciones, considerando al menos:
 - a) Los atributos de los elementos de configuración y de sus componentes, como lo son, entre otros: su identificador único, nombre, descripción, ubicación, versión, responsable, interrelación con otros elementos, clase y categoría, así como el estado en que se encuentra el elemento o componente.
 - b) Los atributos mínimos para conformar las líneas base.
 - c) La nomenclatura de los elementos de configuración y de sus componentes, integrada por caracteres que refieran al nombre, versión, clase, grupo y tipo, entre otros.
 - d) La información de los elementos de configuración y en su caso, de sus componentes, que, para su administración, no requieren contar con líneas base.
 - e) Identificar la relación funcional entre los elementos de configuración y sus componentes, así como su relación con elementos de otros procesos y sistemas, tales como: líneas base, acuerdos de niveles de servicio, roles, registros de incidentes, problemas, cambios y liberaciones, así como documentación relacionada.
 - f) Identificar las relaciones de dependencia entre los elementos de configuración y sus componentes.
 - g) Integrar un catálogo que permita identificar los diferentes estados en que pueden encontrarse los elementos de configuración o sus componentes, considerando entre otros, los siguientes:
 - i) En desarrollo. Aplica a elementos o componentes en proceso de desarrollo, instalación, configuración, personalización, entre otros.
 - ii) Borrador. Aplica a elementos o componentes en proceso de elaboración no concluidos o no aprobados.
 - iii) Aprobado. Aplica a elementos o componentes cuya elaboración o desarrollo se encuentra terminado y aceptado.
 - iv) Activo. Aplica a elementos o componentes en operación.
 - v) Suspendido. Aplica a elementos o componentes que temporalmente se encuentran inactivos,

- pero que son susceptibles de entrar nuevamente en operación.
- vi) Retirado. Aplica a elementos o componentes que quedan fuera de operación, pero que son susceptibles de reutilizarse para otros elementos o componentes de configuración.
 - vii) Fuera de uso. Aplica a elementos o componentes que quedan fuera de operación y que no son susceptibles de reutilizarse.
 - h) Los criterios técnicos para la modificación de los estados de los elementos de configuración o de alguno de sus componentes.
 - i) Incluir un módulo para la administración de usuarios del repositorio, que contemple un registro de sus accesos (pistas de auditoría).
2. Desarrollar, con la información del factor crítico anterior, el modelo de datos del repositorio de configuraciones.
 3. Obtener del titular de la UTIC su autorización al modelo de datos del repositorio de configuraciones, para la implementación del repositorio y comunicar a los responsables de los demás procesos de la UTIC, sobre su disponibilidad.

ACNF 3 Registrar los elementos de configuración en el repositorio de configuraciones

Descripción: Efectuar el registro en el repositorio de configuraciones, de los datos e información de los elementos de configuración y sus componentes.

Factores Críticos:

El responsable de este proceso deberá:

1. Realizar, de acuerdo con el programa previsto en la actividad ACNF 1, el registro en el repositorio de configuraciones de:
 - a) Las líneas base de los elementos de configuración y en su caso, de sus componentes, identificando de manera particular las líneas base de aquellos elementos que cuenten con versionamiento.
 - b) La información de los elementos de configuración y en su caso, de sus componentes que, para su administración, no requieren contar con líneas base.
 - c) La información adicional de los elementos de configuración.
2. Incorporar y/o actualizar en el repositorio de configuraciones, la información proveniente de los diversos procesos de la UTIC, a fin de integrar la totalidad de los elementos de la configuración.
3. Asegurar que los datos que se mantengan tanto en el repositorio de configuraciones como en el catálogo de servicios de TIC, y sus correspondientes interrelaciones, sean consistentes con los datos que registre la UTIC en la Herramienta Diagnóstico Inventario que para tales efectos indique la Unidad.

ACNF 4 Efectuar revisiones al repositorio de configuraciones.

Descripción: Efectuar revisiones al repositorio de configuraciones y a las actividades del propio proceso, a fin de constatar que la integración de la información se haya efectuado conforme a lo previsto en el mismo.

Factores Críticos:

El responsable de este proceso deberá:

1. Establecer y ejecutar un programa de revisiones al repositorio de configuraciones, así como a las actividades de este proceso, el cual será semestral y deberá incluir actividades de revisión a:
 - a) El contenido del repositorio de configuraciones, respecto a:
 - i) Nomenclaturas de los datos de los elementos de configuración y componentes.
 - ii) Datos de los elementos de configuración y componentes, de acuerdo a la definición del modelo de datos del repositorio de configuraciones.
 - iii) Relaciones entre elementos; entre elementos y sus componentes; entre componentes de elementos y otros elementos, así como entre componentes de diversos elementos.
 - iv) Líneas base de los elementos y componentes.
 - v) La documentación de liberaciones de soluciones tecnológicas y servicios de TIC, en lo referente a los datos de los elementos y sus configuraciones registradas en el repositorio.
 - b) El contenido del repositorio de configuraciones con respecto a los ambientes de la UTIC,

considerando:
i) Las características y parámetros de operación que tienen los elementos de la configuración y sus componentes en el ambiente operativo, en relación con los datos contenidos en el repositorio.
c) La seguridad de los datos del repositorio de configuraciones, con respecto a:
i) Los respaldos del repositorio, su capacidad de recuperación y su consistencia con el ambiente en que se encuentre el repositorio.
d) El cumplimiento a las actividades del proceso, en lo relativo a:
i) La integración o actualización de información relacionada con los elementos de configuración o de sus componentes. ii) La consistencia entre los datos de usuarios y los permisos y accesos activos en relación con los controles documentados y autorizados. iii) La consistencia entre las solicitudes de actualización recibidas con respecto a las que se encuentren registradas en el repositorio.
2. Efectuar las actividades de revisión contempladas en el factor crítico anterior, cuando con motivo de la identificación de alguna inconsistencia en los datos de los elementos de configuración o de sus componentes, así se requiera.
3. Documentar el resultado de las revisiones efectuadas; las inconsistencias y hallazgos identificados, así como las acciones preventivas y correctivas propuestas.
4. Registrar los resultados de las revisiones al repositorio de configuraciones, así como determinar las acciones de mejora a ejecutar.

ACNF 5 Desarrollar y controlar los almacenes y librerías de configuraciones.

Descripción: Implementar las librerías y almacenes de los elementos de la configuración y sus componentes.

Factores Críticos:

El responsable de este proceso deberá:

1. Implementar e integrar en el catálogo de librerías y almacenes de configuraciones, los repositorios siguientes:
 - a) Librería segura del repositorio de configuraciones.
 - b) Almacén seguro del repositorio de configuraciones.
 - c) Librería definitiva de medios del repositorio de configuraciones.
 - d) Almacén de repuestos definitivos del repositorio de configuraciones.
2. Establecer perfiles y permisos para el acceso de usuarios a los repositorios que se implementen, conforme al factor crítico anterior.
3. Definir las acciones para la actualización de los repositorios que se definan en este proceso.
4. En coordinación con el RSII, definir e implementar controles de seguridad para los repositorios señalados en el factor crítico anterior, y asegurar que se integren en el SGSI.

Relación de Productos del proceso:

1. "Catálogo de librerías y almacenes de configuraciones" (Formato de acuerdo a las necesidades de la Institución).
2. "Repositorio de configuraciones" (Modelo no sujeto a formato, de acuerdo a las necesidades de la Institución).

Indicador del proceso:

Nombre: Cumplimiento del Proceso de Administración de la Configuración (ACNF).

Objetivo: Conocer el cumplimiento del proceso.

Descripción: Medir el cumplimiento del proceso mediante la obtención de su eficiencia, con base en el número de revisiones efectuadas al repositorio de configuraciones.

Fórmula: % de eficiencia = (número de revisiones efectuadas al repositorio de configuraciones / número de revisiones programadas al repositorio de configuraciones) X 100.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Semestral.

II.C. PROCESO DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ASI).**Objetivo General:**

Establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos de la Institución o constituir una amenaza para la Seguridad Nacional.

Objetivos Específicos:

1. Establecer, operar y mantener un modelo de gobierno de seguridad de la información.
2. Efectuar la identificación de infraestructuras críticas y activos clave de la Institución y elaborar el catálogo respectivo.
3. Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos.
4. Establecer un SGSI que proteja los activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.
5. Establecer mecanismos para la respuesta inmediata a incidentes a la seguridad de la información.
6. Vigilar los mecanismos establecidos y el desempeño del SGSI, a fin de prever desviaciones y mantener una mejora continua.
7. Fomentar una cultura de seguridad de la información en la Institución.

Reglas del proceso:

1. El responsable de la seguridad de la información en la Institución está a cargo de este proceso y en su caso, podrá auxiliarse de los servidores públicos que considere necesarios, debiendo para ello notificar por escrito a cada uno para que conozcan los roles que desempeñarán, actividades y responsabilidades.
2. En el caso en que el titular de la Institución tenga un nivel jerárquico equivalente o inferior a director general, el servidor público que designe como responsable de la seguridad de la información en la Institución deberá tener un nivel inmediato inferior a éste.
3. El responsable de este proceso se deberá asegurar que las acciones y productos que sean resultado de su ejecución, sean consecuentes con lo previsto en el Acuerdo por el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno, en lo relativo a la administración de riesgos y seguridad de la información, y de que los mismos se comuniquen al coordinador de control interno de la Institución que se designe conforme a lo establecido en dicho ordenamiento.
4. En caso de que la Institución cuente con infraestructuras críticas que impacten a la Seguridad Nacional, el responsable de la seguridad de la información se asegurará de que el análisis de riesgos previsto en este proceso se enfoque a éstas; y en caso de que no se cuente con dichas infraestructuras, que el análisis se oriente a los activos de información clave de la Institución.
5. El responsable de este proceso deberá establecer el equipo de respuesta a incidentes de seguridad de TIC (ERISC) y definir los roles y responsabilidades de sus integrantes, así como asegurarse de que éstos conozcan las reglas de operación del mismo y la guía técnica de atención a incidentes.
6. El responsable de la seguridad de la información de la Institución será quien mantendrá comunicación con el Centro para la atención de cualquier incidente de seguridad de la información que implique una amenaza a la Seguridad Nacional y designará un enlace para que se coordine con los ERISC de las demás Instituciones en la atención de otros incidentes que así lo requieran.
7. El responsable de la seguridad de la información de las Instituciones que tengan el carácter de instancia de Seguridad Nacional, deberá coordinarse con las diversas instancias de Seguridad Nacional involucradas cuando se presente un incidente de seguridad que supere su capacidad de respuesta.
8. El grupo estratégico de seguridad de la información deberá asegurar que se integre al SGSI un control de seguridad para evitar intrusiones a la infraestructura de TIC, incluyendo ataques externos vía Internet, Intranet o Extranet.

9. El grupo estratégico de seguridad de la información deberá asegurarse de que se integren al SGSI, controles de seguridad en los equipos del ambiente operativo y de comunicaciones de la Institución, para efectuar la revisión a las bitácoras internas de los mismos, con la finalidad de identificar intentos de ataques o de explotación de vulnerabilidades.
10. El responsable de este proceso deberá hacer del conocimiento de las autoridades competentes, los intentos de violación a los controles de seguridad y los incidentes de seguridad, incluido el acceso no autorizado a la infraestructura y servicios de TIC y a la información contenida en éstos, para que se determinen, en su caso, las responsabilidades que correspondan conforme a las disposiciones jurídicas aplicables.
11. El grupo estratégico de seguridad de la información deberá constatar que los controles de seguridad que se hayan establecido para el repositorio de configuraciones, se implementen de igual manera, para activos y elementos de configuración de los ambientes de desarrollo, pruebas y preproducción.
12. El grupo estratégico de seguridad de la información deberá coordinarse con los responsables de los procesos de la UTIC, para que se implementen controles de seguridad que impidan que el código de las soluciones tecnológicas, sus componentes y productos, y demás elementos relacionados, se copien, envíen, transmitan o difundan por cualquier medio, con fines distintos a su desarrollo.
13. El grupo estratégico de seguridad de la información deberá coordinarse con los responsables de los procesos de la UTIC, para que se implementen controles de seguridad orientados a que las herramientas para el desarrollo de las soluciones tecnológicas, sus componentes y productos, únicamente estén disponibles para los involucrados en su desarrollo y a la conclusión de éste, tales herramientas sean borradas de modo seguro de cualquier equipo del ambiente de trabajo.
14. El grupo estratégico de seguridad de la información deberá constatar que, como parte de los mecanismos que se establezcan para el ambiente operativo, se implemente un control para la elaboración y conservación de bitácoras de seguridad para los sistemas identificados como parte de una infraestructura crítica. En estas bitácoras se registrará el usuario, nombre de equipo, dirección IP, hora de entrada y salida del sistema, así como el tipo de consulta o cambios realizados en la configuración de las aplicaciones. Estas bitácoras tendrán un tiempo mínimo de almacenamiento de un año.
15. El grupo estratégico de seguridad de la información de Instituciones que tengan el carácter de instancia de Seguridad Nacional, deberá recomendar que en los procedimientos de contratación de soluciones tecnológicas o servicios de TIC prevista, se incluyan los requerimientos de continuidad de la operación, niveles de servicio y tiempos de respuesta a interrupciones, en concordancia con la criticidad de los procesos institucionales que los bienes o servicios objeto de las contrataciones soportarán.
16. El grupo estratégico de seguridad de la información deberá implementar mecanismos para asegurar que los sistemas y aplicativos para desplegar los servicios de TIC que se desarrollen o adquieran, cumplan con los controles previstos en el Proceso de Administración de la Seguridad de la Información (ASI).
17. El responsable de este proceso deberá coordinarse con los responsables de la administración de los servicios de TIC y con aquellos responsables de la operación de los mismos, a fin de que los acuerdos de nivel de servicio SLA y los acuerdos de nivel operacional OLA sean determinados y considerados en función de los programas de continuidad y de contingencia de la UTIC y del proceso.
18. El responsable de este proceso deberá enviar a la Unidad un informe semestral, en los meses de julio del año al que corresponda y en enero del año siguiente. El informe se elaborará conjuntamente con el responsable del Proceso de Operación de los Controles de Seguridad de la Información y del ERISC (OPEC), y contendrá el estado que guarda el cumplimiento del Proceso de Administración de la Seguridad de la Información (ASI) y la información relativa a la operación de la totalidad de los controles de seguridad, distinguiendo los controles de seguridad mínimos establecidos en la actividad ASI 6, de aquellos derivados del análisis de riesgos.
19. El responsable de la seguridad de la información de la Institución, podrá considerar a los equipos y/o activos de información, de propósito específico, de control, de monitoreo o industriales, como un dominio tecnológico de TIC y de esta manera integrar sus controles de seguridad al SGSI.

Roles del proceso:

1. Responsable de la seguridad de la información en la Institución o RSII.
2. Grupo de estratégico de seguridad de la información o GESI.
3. Equipo de trabajo de infraestructuras críticas.
4. Equipo de trabajo de análisis de riesgos.
5. Equipo de respuesta a incidentes de seguridad o ERISC.

Actividades del Proceso.**ASI 1 Establecer un modelo de gobierno de seguridad de la información.**

Descripción: Designar al responsable de la seguridad de la información y establecer el grupo de trabajo encargado de la implementación y adopción del modelo de gobierno de seguridad de la información en la Institución.

Factores Críticos:**Al titular de la Institución le corresponderá:**

1. Designar al responsable de la seguridad de la información en la Institución, quien deberá tener nivel jerárquico mínimo de director general o equivalente, atendiendo las reglas de este proceso.

El responsable de la seguridad de la información en la institución (RSII), deberá:

2. Informar al Centro sobre su designación y de la del enlace responsable de mantener comunicación con los ERISC de otras Instituciones.
3. Establecer el grupo estratégico de seguridad de la información (GESI), que estará integrado por servidores públicos que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante el documento de integración y operación del grupo estratégico de seguridad de la información, y asegurarse de:
 - a) Que el documento contenga, al menos: los objetivos y responsabilidades del grupo de trabajo; miembros del grupo; roles y responsabilidades de cada miembro, así como el funcionamiento del grupo.
 - b) Que se comuniquen los roles y responsabilidades de los integrantes del grupo estratégico de seguridad de la información.
 - c) Dirigir y coordinar al grupo estratégico de seguridad de la información y dar seguimiento a las acciones establecidas por el mismo.

ASI 2 Operar y mantener el modelo de gobierno de seguridad de la información.

Descripción: Institucionalizar prácticas para asegurar la implementación, seguimiento y control de la seguridad de la información en la Institución.

Factores Críticos:**El grupo estratégico de seguridad de la información deberá:**

1. Coordinar la elaboración y actualización del catálogo de infraestructuras críticas de la Institución.
2. Establecer, conjuntamente con los responsables de los procesos de la UTIC, así como en su caso con los servidores públicos que corresponda, los mecanismos para garantizar la protección de las infraestructuras críticas que éstos tengan bajo su responsabilidad.
3. Vigilar que los controles de seguridad de la información que se definan e implementen, consideren los mecanismos establecidos en el factor crítico anterior, así como el análisis de riesgos que se indica en la actividad ASI 5.
4. Constatar que se efectúe la implementación del SGSI en la Institución y que se lleven a cabo revisiones al mismo en periodos no mayores a un año, a fin de verificar su cumplimiento.
5. Dar seguimiento a las acciones de mejora continua derivadas de las revisiones al SGSI.

ASI 3 Diseño del SGSI.

Descripción: Definir los objetivos y diseñar las directrices para establecer el SGSI en la Institución.

Factores Críticos:**El grupo estratégico de seguridad de la información deberá:**

1. Diseñar, en coordinación con las diferentes áreas y unidades administrativas de la Institución, la estrategia de seguridad de la información que será implementada al interior de la misma, así como efectuar su revisión al menos una vez al año. Dicha estrategia será la base para establecer el SGSI, cuyo diseño se efectuará atendiendo a lo siguiente:
 - a) Realizar un diagnóstico de los requerimientos de seguridad de la información de la Institución, considerando la participación de las unidades administrativas usuarias de la información para establecer adecuadamente el alcance del SGSI.
 - b) Definir el alcance del SGSI, de manera tal que establezca límites de protección desde la perspectiva institucional, para proporcionar la seguridad requerida a los activos de información.
 - c) Generar las estrategias específicas de seguridad de la información, que permitan cumplir con la misión, visión y objetivos de la Institución.
 - d) Desarrollar reglas técnicas para verificar que los controles de seguridad de la información que se definan operen según lo esperado.
 - e) Definir métricas para evaluar el grado de cumplimiento de los requerimientos de seguridad identificados para los activos de información.
 - f) Elaborar las reglas técnicas que contengan las acciones para la adecuada operación del SGSI.
2. Integrar, con la información del factor crítico anterior, el documento de definición del SGSI e incluir en éste el programa de implementación del SGSI que se desarrolle.

El responsable de la seguridad de la información de la Institución deberá:

3. Hacer del conocimiento del titular de la Institución el documento de definición del SGSI, que ya incluya el programa de implementación desarrollado.
4. Asegurarse de que se presente a la unidad administrativa responsable de la capacitación en la Institución, una propuesta para que se integren al programa de capacitación institucional, los cursos necesarios para difundir los conceptos e importancia de la seguridad de la información, así como la estructura y alcances del SGSI.
5. Dar a conocer el SGSI, y su programa de implementación, a los servidores públicos de la Institución involucrados con el mismo.

El grupo estratégico de seguridad de la información deberá:

6. Elaborar un programa de evaluaciones del SGSI, integrarlo al documento de definición del SGSI y difundirlo en la Institución.
7. Elaborar, probar y mantener actualizada una directriz rectora de respuesta a incidentes, en coordinación con el ERISC, la cual deberá contener al menos:
 - a) El rol y el servidor público asignado a éste, quien puede iniciar las tareas de respuesta a incidentes.
 - b) El mecanismo de notificación, escalamiento y atención de incidentes en la Institución.
 - c) Los mecanismos de interacción con otras Instituciones u organizaciones externas.
 - d) Los criterios técnicos de obtención de indicios, preservación de evidencias, e investigación de incidentes, considerando lo establecido en las disposiciones jurídicas aplicables.

El Responsable de la seguridad de la información de la Institución deberá:

8. Hacer del conocimiento del órgano interno de control en la Institución y/o, cuando corresponda, de las autoridades que resulten competentes, el incumplimiento al SGSI a efecto de que se determinen, en su caso, las responsabilidades que procedan en términos de los ordenamientos legales aplicables.

ASI 4 Identificar las infraestructuras críticas y los activos clave.

Descripción: Elaborar y mantener actualizado un catálogo de infraestructuras críticas, a fin de facilitar la definición de los controles que se requieran para protegerlas.

Factores Críticos:**El grupo estratégico de seguridad de la Información deberá:**

1. Establecer el equipo de trabajo de infraestructuras críticas, y designar a uno de sus integrantes como responsable del mismo y de las acciones realizadas por este equipo, debiendo asegurarse de que:
 - a) Se formalice el establecimiento del equipo y quede definido al menos conforme a lo siguiente: objetivos y responsabilidades del equipo; roles y responsabilidades de cada miembro, y funcionamiento del equipo (tipos de sesiones, levantamiento de minutas y seguimiento de acciones y acuerdos).
 - b) Se comunique la integración del equipo, así como los roles y responsabilidades de los integrantes del mismo.
 - c) El equipo que se constituya realice la identificación de infraestructuras críticas y activos clave, para la elaboración del catálogo de infraestructuras críticas de la Institución.
 - d) Los integrantes del equipo de trabajo tengan un concepto claro y uniforme con respecto a las acciones que en materia de Seguridad Nacional señala el artículo 3 de la Ley de Seguridad Nacional, así como sobre la forma en que las TIC apoyan los procesos sustantivos de la Institución y coadyuvan para garantizar la Seguridad Nacional.
 - e) Establecer, en caso de ser necesario, más de un equipo de trabajo de infraestructuras críticas, para efectuar el adecuado acopio de información y la integración de la totalidad de los datos del catálogo de infraestructuras críticas.

El equipo de trabajo de infraestructuras críticas, en la identificación de infraestructuras críticas y activos clave, deberá:

2. Identificar procesos críticos de la Institución, mediante la ejecución de las siguientes acciones:
 - a) Analizar los procesos existentes y determinar cuáles de éstos son críticos y enlistarlos, considerando como tales aquellos de los que depende la Institución para alcanzar sus objetivos, en los niveles de servicio que tenga establecidos, derivado de sus atribuciones. Dicho análisis se realizará considerando al menos los siguientes elementos:
 - i) Proveedores del proceso.
 - ii) Insumos del proceso.
 - iii) Eventos de inicio que disparan la ejecución del proceso.
 - iv) Subprocesos o actividades que lo conforman.
 - v) Actores que intervienen en su ejecución.
 - vi) Productos o servicios que genera.
 - vii) Evento de fin del proceso.
 - viii) Clientes o usuarios del proceso.
 - ix) Activos de información involucrados en el proceso.
 - b) Analizar los diagramas de los procesos, a fin de identificar las interdependencias que existan entre éstos así como con otros fuera de la Institución.
3. Identificar las actividades críticas de los procesos críticos ya enlistados, mediante la ejecución de las acciones siguientes:
 - a) Enlistar y describir las actividades de cada proceso crítico, así como los factores de éxito para que el proceso se lleve a cabo de manera adecuada.
 - b) Identificar y enlistar en esta misma relación, las actividades que resultan críticas para la operación del proceso.
4. Identificar, a partir de los procesos críticos identificados y enlistados en el factor crítico anterior, aquellos que se encuentren vinculados con la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo que señalan los artículos 3 y 5 de la Ley de Seguridad Nacional. En caso de no identificarse este tipo de procesos críticos, no será necesario atender los factores críticos 5 al 14 siguientes, debiendo iniciar la actividad ASI 5.

5. Identificar los activos de información involucrados en los procesos de Seguridad Nacional, mediante la ejecución de las acciones siguientes:
 - a) Elaborar una relación de los activos de información que soportan la generación, procesamiento, transmisión y almacenamiento de la información en los procesos, con apoyo de los responsables, según corresponda, de su desarrollo, mantenimiento, operación, uso y seguridad, así como de su administración y resguardo.
 - b) Incluir en la relación de los activos de información al responsable de su resguardo.
 - c) Clasificar los activos de información como activos primarios o de soporte, de acuerdo a su funcionalidad, alcance o impacto en el proceso.
 - d) Definir la nomenclatura para la identificación de los activos de información, a partir de dos campos: en el primero "Id. Activo" se asignará un número consecutivo que, relacionado con el segundo campo "Id. Proceso", correspondiente al proceso, provea una identificación única para cada activo.
6. Efectuar la valoración de los activos de información, en términos de la posible pérdida de su confidencialidad, integridad o disponibilidad, para identificar aquellos que deban considerarse como activos de información clave y registrar los resultados de la valoración efectuada, mediante matrices de infraestructuras críticas con respecto de sus activos clave.
7. Utilizar como parámetros para identificar la criticidad de una infraestructura, los tipos de impacto potencial que podrían ocurrir ante la presentación de un incidente. Éstos se deberán representar mediante matrices de impacto.
8. Determinar el nivel de criticidad de cada infraestructura mediante la identificación de su interdependencia y el nivel de impacto que tenga con cada una de las infraestructuras con las que se relacione.
9. Revisar los resultados obtenidos en los factores críticos anteriores.

El grupo estratégico de seguridad de la información deberá:

10. Verificar los resultados obtenidos en los factores anteriores, por el equipo de trabajo de infraestructuras críticas, y constatar que las infraestructuras críticas que se hubieren identificado efectivamente tengan ese carácter.

El grupo estratégico de seguridad de la información, con apoyo del equipo de trabajo de infraestructuras críticas, deberá:

11. Elaborar el catálogo de infraestructuras críticas, con base en la información verificada en el factor crítico anterior, y realizar las siguientes acciones:
 - a) Asignar, de acuerdo con la tabla que se contiene en el catálogo de infraestructuras críticas, el sector y subsector que corresponda a cada infraestructura crítica identificada.
 - b) Verificar que el catálogo de infraestructuras críticas incorpore los datos de identificación de las infraestructuras críticas, señalando su descripción, componentes, sector y subsector, Institución y ubicación y las matrices de la infraestructura con respecto de sus activos clave, y los impactos que le fueron determinados.
 - c) Incluir en el catálogo de infraestructuras críticas un mapa de localización geográfica, en donde se muestre la ubicación de las diversas infraestructuras críticas.
 - d) Incluir en el catálogo de infraestructuras críticas, la información de los miembros y roles del equipo de trabajo de infraestructuras críticas.

El responsable de la seguridad de la información de la Institución deberá:

12. Presentar a la aprobación del titular de la Institución, el catálogo de infraestructuras críticas elaborado.
13. Asegurarse de que se observe lo establecido en la Ley de Seguridad Nacional, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables, para la clasificación y resguardo de la información generada en esta actividad.

El grupo estratégico de seguridad de la información deberá:

14. Revisar, por lo menos una vez al año, el catálogo de infraestructuras críticas de la Institución e instruir, en su caso, al equipo de trabajo de infraestructuras críticas para que se efectúen los trabajos para su actualización.

ASI 5 Elaborar el análisis de riesgos.

Descripción: Identificar, clasificar y priorizar los riesgos para evaluar su impacto sobre los procesos y los servicios de la Institución, de manera que se obtengan las matrices de análisis de riesgos.

Factores Críticos:**El grupo estratégico de seguridad de la información deberá:**

1. Establecer la directriz de administración de riesgos, efectuando las siguientes acciones:
 - a) La definición de estrategias, metodologías y herramientas que se usarán para administrar los riesgos.
 - b) La integración del marco normativo que resulte aplicable a los riesgos identificados.
 - c) El establecimiento de las reglas para medir la efectividad de los controles en la gestión de los riesgos.
 - d) La definición de la forma y periodicidad con las que se informará a los grupos y equipos de trabajo, a las áreas y unidades administrativas de la Institución y externos involucrados, sobre los riesgos a los que se encuentran expuestos los procesos y servicios que utilizan.
 - e) La definición de consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas de la Institución.
 - f) Someter a consideración y aprobación del RSII, las definiciones efectuadas en los incisos anteriores.
2. Integrar el equipo de trabajo de análisis de riesgos y asegurar, al menos, lo siguiente:
 - a) La definición de los objetivos y responsabilidades del equipo; roles y responsabilidades de cada miembro, y el funcionamiento del mismo (tipos de sesiones, levantamiento de minutas y seguimiento de acciones y acuerdos).
 - b) La conformación del equipo se hará con servidores públicos que, preferentemente, deberán tener conocimientos en TIC, seguridad de la información y seguridad física; así como por aquellos que se considere puedan aportar mayor capacidad de análisis y alcance de objetivos.
 - c) Que los integrantes del equipo cuenten con al menos un año de experiencia y conocimientos en el área en la cual se desempeñan.
 - d) Se delimite el objetivo y alcance del análisis de riesgos que se efectuará por el equipo de trabajo.
 - e) Se seleccione al líder del equipo y se haga de su conocimiento que su rol será el de interpretar y difundir instrucciones, coordinar tareas y materializar resultados.
 - f) Integrar, en caso de ser necesario, más de un equipo de trabajo de análisis de riesgos, para efectuar el adecuado acopio de información e integración que deriva del análisis de riesgos que se efectúa en esta actividad.

El equipo de trabajo de análisis de riesgos, con el apoyo de las diversas áreas o unidades administrativas de la Institución involucradas, deberá:

3. Identificar los procesos críticos, recopilando la información siguiente:
 - a) La de aquellos procesos de los que la Institución dependa para alcanzar sus objetivos y niveles de servicio comprometidos, derivada de la identificación realizada conforme al factor crítico 2 de la actividad **ASI 4**, en los casos en que la Institución no hubiere identificado procesos críticos vinculados con la Seguridad Nacional.
 - b) La obtenida como resultado del desarrollo de la actividad **ASI 4**, por haberse identificado procesos críticos vinculados con la Seguridad Nacional.
4. Identificar los activos de información y consultar a los responsables de éstos, para identificar los elementos que se pretenden proteger ante la posible materialización de amenazas y elaborar una relación detallada con la información obtenida.
5. Identificar las vulnerabilidades, mediante las acciones siguientes:
 - a) Integrar, a la relación de activos de información, las características de los mismos que pudieran ser aprovechadas para poner en riesgo la confidencialidad, integridad y disponibilidad de éstos, considerando, asimismo, las características del ambiente y de la Institución en que se ubican.
 - b) Considerar como vulnerabilidad la ausencia y/o falla de controles.

- c) Integrar a los responsables de la administración, operación y, en su caso, resguardo de los activos de información en el proceso de identificación de vulnerabilidades.
6. Identificar las amenazas mediante las acciones siguientes:
- a) Registrar las posibles amenazas que, en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los activos de información que ya se tiene enlistados.
- b) Identificar y registrar los agentes que podrían materializar una amenaza, utilizando la lista de amenazas y agentes que se provee en el formato del producto “Documento de resultados del análisis de riesgos”.
7. Efectuar la identificación y evaluación de escenarios de riesgo, evaluando aquellos que se identifiquen y registrando los resultados obtenidos, considerando los datos recopilados en los factores críticos anteriores y efectuando las acciones siguientes:
- a) Definir los escenarios de riesgo, para lo cual es necesario efectuar los cálculos para establecer el valor del riesgo para cada escenario, utilizando la fórmula: $R=PI$; en la que “P” es la probabilidad de ocurrencia de la amenaza, e “I” es el impacto ocasionado por la materialización de la misma.
- b) Establecer las variables complementarias que se indican en el formato del producto “Documento de resultados del análisis de riesgos”, ya que éstas determinan el valor final del riesgo, utilizando la tabla denominada “Probabilidad de ocurrencia contra impacto”, que se encuentra en el formato de este mismo producto, e integrar en éste el resultado de la identificación y evaluación de los escenarios de riesgo.
- c) Definir la estrategia de seguridad para cada riesgo, seleccionando alguna de las establecidas en el citado formato: evitar, mitigar o reducir, financiar o asumir y transferir o compartir, debiendo evaluarse en este mismo orden.
- d) Obtener la relación de riesgos que requieren atención, su prioridad y estrategia de seguridad.
8. Elaborar el análisis del costo-beneficio de controles de seguridad, mediante las acciones siguientes:
- a) Elaborar la lista de escenarios de riesgo, cuya acción de seguridad implica el uso de controles o la modificación de un proceso para evitar, mitigar o reducir, financiar o asumir y transferir o compartir los riesgos.
- b) Comparar el costo del control que se proponga contra el impacto que se podría ocasionar por la materialización del riesgo.
- c) Verificar el costo-beneficio de controles de seguridad, debiendo definir los valores indicados en éste, para cada escenario de riesgo, e integrar los datos en el “Documento de resultados del análisis de riesgos”.
9. Elaborar el “Documento de resultados del análisis de riesgos”, mediante las acciones siguientes:
- a) Integrar la lista de controles recomendados, para un adecuado tratamiento de los riesgos detectados en el orden de prioridad establecido, indicando además los requerimientos para su implementación.
- b) Incluir, de ser el caso, el nivel de riesgo residual de cada escenario.
- c) Elaborar e integrar las declaraciones de aplicabilidad con los controles necesarios, de acuerdo a los resultados obtenidos de los factores críticos anteriores.
- d) Elaborar e incluir las propuestas para los programas de mitigación de riesgos, considerando los controles establecidos en las declaraciones de aplicabilidad.
- e) Elaborar e incluir en el “Documento de resultados del análisis de riesgos”, un programa de contingencia a los riesgos, considerando, de ser el caso, la intervención del ERISC.
10. Obtener del grupo estratégico de seguridad de la información, la aprobación del “Documento de resultados del análisis de riesgos” y enviarlo a los responsables de los procesos en las diversas áreas y unidades administrativas de la Institución para su revisión.
- Los responsables de los procesos en las diversas áreas y unidades administrativas de la Institución, con el apoyo del equipo de trabajo de análisis de riesgos, deberán:**
11. Seleccionar de entre los controles recomendados por el grupo estratégico de seguridad de la información, contenidos en el “Documento de resultados del análisis de riesgos”, aquéllos a implementar de acuerdo a las capacidades y recursos de las áreas y unidades administrativas involucradas.

12. Justificar ante el grupo estratégico de seguridad de la información las razones por las cuales existan controles recomendados no seleccionados.

El equipo de trabajo de análisis de riesgos, en coordinación con las áreas y unidades administrativas de la Institución involucradas, deberá:

13. Elaborar, e integrar en el “Documento de resultados del análisis de riesgos”, el programa de implementación para el manejo de riesgos, de acuerdo a los resultados de la selección efectuada conforme al factor crítico 11 de esta actividad. Dicho programa deberá incluir la asignación de responsables de la implementación de cada control, integrando éstas al “Documento de resultados del análisis de riesgos” y los datos necesarios para su implementación, así como documentarse conjuntamente con la implementación de las acciones y controles del SGSI.
14. En el programa de implementación para el manejo de riesgos se deberá establecer un responsable de la implementación de cada uno de los riesgos a manejar.
15. Obtener del grupo estratégico de seguridad de la información la aprobación del programa de implementación elaborado y verificar su adecuada integración con las demás actividades de implementación o mejora de los controles de seguridad y las acciones del SGSI.

El grupo estratégico de seguridad de la información deberá:

16. Cuidar que el análisis de riesgos se realice o actualice conforme a los factores críticos de esta actividad, al menos una vez al año, o bien, en caso de un cambio en los procesos, activos de información o cuando se detecte una nueva amenaza o vulnerabilidad a la seguridad de la información y/o los activos de TIC que la soportan.
17. Asegurar que se ejecuten los factores críticos integralmente y se obtengan los productos de esta actividad debidamente actualizados. Asimismo, se documente la mejora continua que resulte necesaria, derivada del factor crítico anterior.

ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información.

Descripción: Definir los controles mínimos de seguridad de la información e integrarlos al SGSI, para su implementación a través de los diversos procesos de la UTIC y de aquellos procesos de la Institución que contengan activos de TIC, activos de información e infraestructuras críticas.

Factores Críticos:

El grupo estratégico de seguridad de la información, con apoyo de las áreas y unidades administrativas competentes de la Institución, deberá:

1. Definir los controles de seguridad necesarios para salvaguardar a los activos de TIC, los activos de información y las infraestructuras críticas de la Institución, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:
 - a) La definición, en términos de seguridad, de la viabilidad del software que se pretenda adquirir e instalar en los equipos de cómputo, dispositivos electrónicos o sistemas de información.
 - b) La designación de personal en las áreas relacionadas con el manejo, administración y gestión de los activos de información de la Institución, con apego a las disposiciones jurídicas aplicables y considerando los procedimientos que, en su caso, se tengan implementados en el área o unidad administrativa de que se trate.
 - c) La instalación y configuración del software, así como para la administración de la seguridad de las soluciones tecnológicas y servicios de TIC que se utilicen en la Institución.
 - d) El ingreso y salida de activos de información.
 - e) El borrado seguro de dispositivos de almacenamiento que por algún motivo necesiten ser reparados, reemplazados o asignados a otro usuario; y mantener evidencia auditable del proceso.
 - f) Evitar el daño, pérdida, robo, copia y acceso no autorizados a los activos de información.
 - g) Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a la información otorgados a servidores públicos de la Institución y de otras Instituciones, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo el nivel de privilegios de acceso asignado cambie.
 - h) Los criterios de asignación de usuarios y contraseñas permitidas para los diversos componentes de los dominios tecnológicos.
 - i) La configuración de las herramientas de protección implementadas en las redes institucionales.

j)	Las conexiones a redes públicas y privadas, así como para los dispositivos electrónicos que contengan información considerada como reservada o sensible para la Institución.
k)	La seguridad física y lógica que permita mantener, para los respaldos de información, su confidencialidad, integridad y disponibilidad.
l)	El uso del servicio de Internet en la Institución, el cual debe contar con herramientas de seguridad y de filtrado de contenido.
m)	El intercambio seguro de la información, ya sea de manera interna o hacia el exterior.
n)	Que la información clasificada o aquella que tiene valor para la Institución, sea respaldada y restaurada en el momento en que se requiera.
o)	Contar con registros de auditoría y bitácoras de seguridad en los sistemas identificados como críticos, así como con las condiciones de seguridad que impidan borrar o alterar éstos.
Los controles de seguridad que se establecen en este factor crítico aplicarán a los activos de TIC, activos de información e infraestructuras críticas que técnica y/o normativamente les corresponda, y de ser el caso, se deberá justificar la no aplicabilidad de los mismos. En aquellos que se haya definido la no aplicabilidad de los controles de este factor crítico, deberán definirse e implementarse los controles que deriven de la ejecución de la actividad ASI 5 .	
2.	Documentar los controles determinados conforme al factor crítico anterior, incluyendo su definición detallada e integrarlos al documento de definición del SGSI y elaborar conjuntamente con los responsables de los procesos institucionales involucrados, el programa de implementación del SGSI e integrarlo al mismo documento. El programa de implementación deberá incluir el nombre del responsable de la implementación de cada uno de los controles de seguridad del SGSI que se hayan establecido.

ASI 7 Mejorar el SGSI.

Descripción: Mejorar la seguridad de la información, a través de la aplicación de acciones preventivas y correctivas derivadas de las revisiones que se efectúen al SGSI.

Factores Críticos:

El grupo estratégico de seguridad de la información deberá:

1. Constatar, en coordinación con las áreas y unidades administrativas involucradas, que las actualizaciones de seguridad en todos los componentes de la infraestructura tecnológica de la Institución se apliquen, a fin de hacer del conocimiento del titular de la misma el cumplimiento de los controles de seguridad establecidos.
2. Obtener, de la evaluación del SGSI, los datos sobre su desempeño, a fin de definir y documentar las acciones correctivas y preventivas para ajustar el mismo, e integrarlas al documento de definición del SGSI.
3. Elaborar el documento de implementación de la mejora al SGSI e integrarlo al documento de definición del SGSI. El documento de implementación debe utilizarse para la planeación y el seguimiento de las acciones de mejora, ya sean preventivas o correctivas.
4. Comunicar las mejoras que deberán aplicarse al SGSI al responsable del grupo de trabajo para la implementación de la seguridad de la información, previsto en la actividad **OPEC 1**, por medio del documento de definición del SGSI, en lo relativo a los resultados de la evaluación del SGSI y la implementación al SGSI.
5. Vigilar y registrar las observaciones necesarias respecto a la implementación de las mejoras mediante un informe de seguimiento a las acciones de mejora al SGSI que deberá integrarse al documento de definición del SGSI.

Relación de Productos del proceso:

1. "Documento de integración y operación del grupo estratégico de seguridad de la información". Formato ASI F1.
2. "Catálogo de infraestructuras críticas". Formato ASI F2.
3. "Documento de resultados del análisis de riesgos". Formato ASI F3.
4. "Documento de definición del SGSI". Formato ASI F4.

5. "Directriz rectora de respuesta a incidentes". Formato ASI F5.

Indicador del proceso:

Nombre: Cumplimiento del Proceso de Administración de la Seguridad de la Información (ASI).

Objetivo: Obtener la eficiencia del proceso en base a su cumplimiento.

Descripción: Medir el cumplimiento en la implementación de los controles establecidos durante el proceso.

Fórmula: $\% \text{ de eficiencia} = (\text{controles implementados} / \text{controles programados para su implementación}) \times 100$.

Responsable: El responsable del Proceso de Administración de la Seguridad de la Información (ASI).

Frecuencia de cálculo: Anual.

III. PROCESOS DE ENTREGA

III.A. PROCESO DE ADMINISTRACIÓN DE PROYECTOS (ADP).

Objetivo General:

Administrar iniciativas, programas y proyectos de TIC, a fin de optimizar la aplicación de los recursos y obtener mayores beneficios para la Institución.

Objetivos Específicos:

1. Establecer la gobernabilidad del portafolio de proyectos de TIC.
2. Establecer una visión integral de los proyectos de TIC que genere sinergias y beneficios desde su planeación y durante su ejecución.
3. Establecer las directrices para administrar el portafolio de proyectos de TIC.

Reglas del proceso:

1. El responsable de este proceso es el administrador del portafolio de proyectos de TIC.
2. El administrador del portafolio de proyectos de TIC designará, para cada proyecto que se autorice, al administrador de proyecto, solicitando para ello autorización al titular de la UTIC.
3. Los administradores de proyecto deberán asegurarse de que todos los proyectos que administren cuenten con su documento de planeación del proyecto, así como los documentos de planeación subsidiarios, desde su inicio hasta su cierre, y de que éste se actualice en tiempo y forma de acuerdo a los avances de los proyectos hasta su cierre.
4. Los administradores de proyecto deben asegurarse que cualquier cambio a un proyecto que administren se realice mediante una solicitud de cambio autorizada por los involucrados.
5. El responsable de este proceso deberá asegurarse que en los proyectos de TIC se aplique la metodología de estimación de esfuerzo, de desarrollo o mantenimiento de sistemas, que se adopte por la UTIC con apego a la EDN, las políticas y disposiciones del Acuerdo por el que se expide este manual, así como a las metodologías, normas y mejores prácticas aplicables a los procesos de este manual, contenidas en el Apéndice IV.B.
6. Los responsables de proyecto deberán asegurarse que las metodologías y/o mejores prácticas que se adopten para los diversos tipos de proyectos, se documenten en cada uno de los proyectos que desarrolle la UTIC, debiendo seguirse la metodología o mejor práctica que se seleccione, en la amplitud necesaria para tener el gobierno de cada contratación, desarrollo, personalización, implementación, migración, mantenimiento y puesta en operación de aplicativos de cómputo, componentes y servicios de TIC de que se trate.

Roles del proceso:

1. Grupo de trabajo para la dirección de TIC.
2. Responsable del proceso y administrador del portafolio de proyectos de TIC.
3. Responsable de la administración de programas de proyectos.

4. Responsable de iniciativas de TIC.
5. Administradores de proyecto de TIC.

Actividades del Proceso.

ADP 1 Establecer directrices para la gobernabilidad y evaluación del portafolio de proyectos de TIC.

Descripción: Definir las directrices para la asignación y uso de los recursos en proyectos de TIC.

Factores Críticos:

El grupo de trabajo para la dirección de TIC deberá:

1. Tomar acuerdos respecto a la gobernabilidad del portafolio de proyectos de TIC que le presente el titular de la UTIC:
 - a) Autorizar la fijación de prioridades de las iniciativas y los proyectos que las integran.
 - b) Confirmar la asignación de presupuesto a las iniciativas, programas de proyectos y proyectos de TIC y en su caso, a las modificaciones a que haya lugar.
 - c) Verificar la alineación de las inversiones en proyectos de TIC con las necesidades y objetivos de la Institución.
 - d) Autorizar nuevas iniciativas de TIC; la suspensión, cambios o cancelación de programas de proyectos y de proyectos de TIC, o la reasignación de recursos entre programas y proyectos de TIC.

El administrador del portafolio de proyectos de TIC, con apoyo del responsable de la planeación estratégica de TIC y de los administradores de proyecto, deberá:

2. Definir proyectos a partir de las iniciativas de TIC que se autoricen.
3. Analizar las iniciativas de TIC y sus proyectos, con el propósito de definir aquéllos susceptibles de conformarse en programas de proyectos.
4. Integrar el portafolio de proyectos, definiendo los diversos programas de proyectos, así como los proyectos de TIC que contendrá cada uno de dichos programas, y asociar los programas de proyectos, y los proyectos a las iniciativas de las que derivan e identificar los proyectos que se administrarán individualmente.
5. Difundir el estado que guarda el portafolio de proyectos de TIC, por medio de un tablero de control de proyectos.
6. Priorizar y equilibrar el portafolio de proyectos de TIC, a efecto de optimizar el uso de los recursos.
7. Dar seguimiento al portafolio, a fin de prever riesgos y desviaciones.

El titular de la UTIC deberá:

8. Presentar el portafolio de proyectos de TIC al grupo de trabajo para la dirección de TIC, para su aprobación y autorizaciones procedentes.

ADP 2 Identificar y documentar iniciativas de TIC.

Descripción: Dar seguimiento a las iniciativas de TIC durante su ciclo de vida.

Factores Críticos:

El administrador del portafolio de proyectos de TIC deberá:

1. Mantener actualizado el registro de las iniciativas de TIC y sus proyectos, así como el de los programas de proyectos a los que éstas pertenezcan.
2. Identificar e integrar las iniciativas de TIC, incluyendo:
 - a) Aquellas identificadas en el Proceso de Planeación Estratégica (PE).
 - b) Las provenientes de las necesidades de desarrollo de nuevos servicios de TIC o de ajustes a los servicios ya existentes.

- c) Las relativas a la continuidad de los servicios de TIC.
 - d) Las que deriven del mantenimiento necesario a la infraestructura tecnológica y el soporte.
3. Integrar, para cada iniciativa de TIC, la información mínima siguiente:
 - a) Identificación (nombre, unidad administrativa solicitante y en su caso, unidad administrativa que la promueve).
 - b) Alcance de alto nivel (objetivos de la iniciativa de TIC, alcance, cronograma de alto nivel, objetivos estratégicos a los que contribuye la iniciativa de TIC, beneficios cuantitativos y cualitativos, riesgos, recursos requeridos y entregables).
 - c) Organización de gobernabilidad sugerida para la ejecución de la iniciativa de TIC.
 - d) Responsables de la iniciativa de TIC en la UTIC y en la unidad administrativa solicitante.
 - e) La relativa a su seguimiento (el estado que guarda y los cambios aprobados a la iniciativa de TIC).
4. Verificar que se elaboren los estudios de factibilidad con información suficiente para evaluar, seleccionar y priorizar las iniciativas, que contengan además la justificación técnica y económica del servicio de TIC, así como el valor que proveerá.
5. Verificar, al menos una vez durante el ciclo de vida de las iniciativas de TIC, que se mantengan alineadas y actualizadas con respecto a la planeación estratégica institucional y el programa de tecnología.
6. Presentar al grupo de trabajo para la dirección de TIC, la información de impacto respecto a los cambios en las iniciativas de TIC a fin de que evalúe y en su caso, apruebe, si se continúa con la ejecución de las mismas.

ADP 3 Priorizar, equilibrar y autorizar el portafolio de proyectos de TIC.

Descripción: Priorizar las iniciativas de TIC que estén seleccionadas para su aprobación.

Factores Críticos:**El administrador de portafolio de proyectos de TIC deberá:**

1. Evaluar las iniciativas de TIC que serán propuestas al grupo de trabajo para la dirección de TIC para su priorización y, en su caso, autorización. Para llevar a cabo la evaluación deberá considerar, cuando menos, los análisis relativos a:
 - a) Los objetivos estratégicos y beneficios que sustentan la iniciativa de TIC.
 - b) Las funciones sustantivas que sustentan la iniciativa de TIC.
 - c) La capacidad de recursos humanos.
 - d) La capacidad financiera y/o presupuestaria.
 - e) La capacidad de activos e infraestructura de TIC.

El grupo de trabajo para la dirección de TIC, respecto de las iniciativas de TIC deberá:

2. Revisar y analizar el resultado de la evaluación de las iniciativas de TIC y su prioridad.
3. Autorizar las iniciativas de TIC, sin perjuicio del cumplimiento de las disposiciones jurídicas aplicables a la contratación de los bienes y/o servicios requeridos para su implementación.

El administrador del portafolio de proyectos de TIC deberá:

4. Establecer y mantener actualizado el portafolio de proyectos de TIC.
5. Mantener el equilibrio de los recursos del portafolio de proyectos de TIC, mediante la revisión a los informes de rendimiento de los programas de proyectos y, de ser el caso, sugerir al grupo de trabajo para la dirección de TIC, un cambio de prioridad o la continuación, suspensión o cancelación de iniciativas, de programas de proyectos, y de proyectos de TIC.
6. Someter a la autorización del grupo de trabajo para la dirección de TIC, los ajustes al portafolio de proyectos de TIC y preparar las justificaciones de cada ajuste.
7. Designar responsables para cada iniciativa, programa de proyectos o proyecto de TIC, autorizados.
8. Generar con la información recopilada de las actividades de este proceso el documento de planeación y acta de constitución del proyecto para su registro.

- | |
|---|
| 9. Actualizar el tablero de control de proyectos de TIC y difundirlo. |
|---|

ADP 4 Administrar programas de proyectos y proyectos de TIC.

Descripción: Administrar programas de proyectos, así como proyectos de TIC, en los que se integran las iniciativas de TIC, orientando las acciones a una coordinación optimizada de las actividades de administración de los mismos.

Factores Críticos:
El responsable de la administración de cada programa de proyectos deberá:

1. Revisar la información de la iniciativa de TIC que se integre al programa de proyectos de TIC, para lo cual:
 - a) Identificará y evaluará las alternativas establecidas en los estudios de factibilidad.
 - b) Justificará la selección que efectúe.
2. Determinar los proyectos que integrarán un programa de proyectos de TIC para la realización de una o más iniciativas de TIC y elaborar su justificación.
3. Elaborar un cronograma ejecutivo para el programa de proyectos de TIC de las iniciativas de TIC, que muestre la duración y las fechas de inicio y fin de cada proyecto, e incluya hitos de control y riesgos potenciales.
4. Asegurarse de que se cuente con las asignaciones y autorizaciones necesarias para el inicio de un programa de proyectos de TIC y sus proyectos.
5. Elaborar la estrategia para administrar y concretar los beneficios, de cada programa de proyectos, en la que se deberá definir:
 - a) Las líneas de acción para el logro de los beneficios esperados.
 - b) El responsable de cada resultado clave del programa de proyectos de TIC, la fecha estimada de obtención del resultado y el mecanismo de seguimiento.
 - c) Los beneficios esperados para cada resultado clave del mismo, los riesgos para el cumplimiento de los resultados y las acciones de mitigación correspondientes.
6. Dar seguimiento al programa de proyectos de TIC, desde su inicio y hasta su conclusión.
7. Administrar las eventualidades que se presenten en la ejecución del programa de proyectos de TIC, tales como: cambios controlados, incidentes o riesgos que se materialicen.
8. Elaborar el análisis comparativo entre el avance real y el planeado, así como los beneficios obtenidos.
9. Elaborar el análisis del programa de proyectos, el cual deberá incluir la medición de su desempeño e indicadores, así como la de los proyectos que lo conforman.
10. Actualizar el tablero de control de proyectos, de manera que permita identificar niveles críticos y apoyar la definición de acciones correctivas a la estrategia del programa de proyectos.

ADP 5 Monitorear el desarrollo de los proyectos de TIC y sus programas.

Descripción: Mantener un monitoreo constante del estado que guardan los proyectos de TIC, así como su repercusión en los resultados del programa de proyectos, con el fin de identificar y controlar las desviaciones y las eventualidades.

Factores Críticos:
El administrador del portafolio de proyectos de TIC, con apoyo de los administradores de proyectos, deberá:

1. Verificar y evaluar de manera continua el estado que guarda cada uno de los proyectos de TIC, de acuerdo a sus hitos y puntos de control, para determinar su contribución al portafolio de proyectos de TIC y a los programas de proyectos a los que pertenezcan, y actualizar el tablero de control de proyectos.
2. Mantener permanentemente informado al grupo de trabajo para la dirección de TIC, por medio del tablero de control de proyectos de TIC, el cual deberá contener, al menos, la información sintetizada

del avance del portafolio de proyectos, el resultado de los indicadores del desempeño del portafolio de proyectos y, en su caso, de las eventualidades o riesgos que se hayan presentado.

ADP 6 Cerrar iniciativas y proyectos de TIC.

Descripción: Concluir las iniciativas de TIC, mediante la elaboración y presentación de un informe final que contenga la evaluación de los resultados y los beneficios obtenidos.

Factores Críticos:

El administrador de portafolio de proyectos de TIC deberá:

1. Revisar los resultados y la documentación de los programas de proyectos y de los proyectos de TIC asociados a la iniciativa de TIC que se pretenda cerrar.
2. Evaluar los beneficios de los programas de proyectos de la iniciativa de TIC, mediante revisiones que se podrán efectuar una vez implementados los productos y servicios obtenidos de la iniciativa de TIC.
3. Elaborar la descripción de las lecciones aprendidas del desarrollo de la iniciativa de TIC.
4. Preservar y mantener disponible la información del desarrollo de la iniciativa de TIC.

Relación de Productos del proceso:

1. "Tablero de control de proyectos de TIC" (formato de acuerdo a la plataforma tecnológica y recursos de aplicativos de cómputo de la UTIC).
2. "Acta de constitución del proyecto". Formato ADP F1.
3. "Acta de aceptación de entregables". Formato ADP F2.
4. "Acta de cierre de proyecto". Formato ADP F3.

Indicador del proceso:

Nombre: Cumplimiento de los beneficios de iniciativas y programas de proyectos.

Objetivo: Conocer la eficiencia de acuerdo a las estrategias de realización de beneficios.

Descripción: Medir la eficiencia del proceso por los beneficios alcanzados.

Fórmula: $\% \text{ de eficiencia} = (\text{número de beneficios alcanzados con la administración de los programas del portafolio} / \text{número total de beneficios establecidos en las iniciativas y los programas de proyectos del portafolio de proyectos de TIC}) \times 100$.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Semestral.

III.B. PROCESO DE ADMINISTRACIÓN DE PROVEEDORES (APRO).

Objetivo General:

Establecer un mecanismo que permita verificar el cumplimiento de las obligaciones derivadas de los contratos celebrados para la adquisición, arrendamiento o servicios de TIC.

Objetivos Específicos:

1. Identificar hallazgos, desviaciones y riesgos en el cumplimiento de los contratos en materia de TIC.
2. Proponer acciones preventivas y correctivas que propicien el adecuado cumplimiento del proveedor a sus obligaciones contractuales.

Reglas del proceso:

1. El responsable de este proceso deberá ser asignado por el titular de la UTIC.
2. Este proceso deberá ejecutarse con apego a las disposiciones que en materia de adquisiciones y arrendamientos de bienes muebles y contratación de servicios resulten aplicables, así como al Acuerdo por el que se expide el MAAGMAASSP.
3. El responsable de este proceso designará a los administradores de contratos de bienes y servicios de TIC y solicitará para ello el visto bueno del titular de la UTIC.

4. Este proceso deberá ejecutarse con apego, en lo que respecta a la administración de contratos, a lo que dispongan las políticas, bases y lineamientos en materia de adquisiciones, arrendamientos y servicios de cada Institución.

Roles del proceso:

1. Responsable del Proceso de Administración de Proveedores (APRO).
2. Administradores de contratos.

Actividades del Proceso.**APRO 1 Generar lista de verificación de obligaciones.**

Descripción: Elaborar una lista de verificación, conforme al contrato celebrado, que sirva como base para dar seguimiento al desarrollo de las obligaciones pactadas.

Factores Críticos:**El responsable de este proceso deberá:**

1. Apoyar técnicamente a los administradores de contratos de bienes y servicios de TIC en el seguimiento a las obligaciones adquiridas mediante los contratos celebrados por la UTIC.

El responsable del proceso, para cada contrato suscrito, con apoyo de los administradores de contrato, deberá:

2. Elaborar, de conformidad con el contrato de que se trate, una lista de apoyo para la verificación y seguimiento de las obligaciones contractuales, la cual deberá contener al menos, lo siguiente:
 - a) La totalidad de las obligaciones asumidas por el proveedor y la Institución.
 - b) Los supuestos en que se aplicarán penalizaciones al proveedor.
 - c) Las fechas de entrega de los bienes o de prestación de los servicios contratados y en su caso, el calendario de entrega de los productos o entregables.
 - d) Los datos del enlace o de los enlaces o responsables, designados por el proveedor.
3. En los casos en que participen diversos proveedores en un contrato, será necesario identificar qué obligaciones corresponden a cada uno.

APRO 2 Monitorear el avance y desempeño del proveedor.

Descripción: Verificar que el avance de los compromisos y actividades del proveedor se realicen como se especifica en el contrato.

Factores Críticos:**El responsable de este proceso deberá:**

1. Solicitar a cada uno de los administradores de contrato, la información relativa a los aspectos siguientes:
 - a) Cumplimiento de las obligaciones asumidas por el proveedor en el contrato.
 - b) Los avances del proveedor y el desempeño al que éste se encuentre obligado.
 - c) La identificación de los incumplimientos del proveedor y las penas convencionales o deductivas que se hubieren aplicado o que deban aplicarse.

El responsable del proceso, con la información obtenida de los administradores del contrato, coadyuvará para:

2. Establecer la coordinación necesaria con el enlace, enlaces o responsables designados por el proveedor, para el cumplimiento de sus obligaciones.
3. Elaborar un reporte de avance sobre el cumplimiento de obligaciones, con el fin de:
 - a) Identificar, analizar y registrar hallazgos, desviaciones y riesgos, y proponer al administrador del

proyecto, así como a la unidad administrativa solicitante o a los responsables de los procesos involucrados, las acciones preventivas y/o correctivas correspondientes.

- b) Dar seguimiento a las acciones preventivas y/o correctivas que se determinen hasta su cierre.

APRO 3 Apoyo para la verificación del cumplimiento de las obligaciones de los contratos.

Descripción: Coadyuvar, con el área requirente, el área técnica y/o el administrador del contrato, para corroborar que el proveedor de cada contrato, cumpla con las obligaciones estipuladas en el mismo.

Factores Críticos:

El responsable de este proceso deberá realizar las siguientes actividades:

1. Apoyar en la revisión del cumplimiento de las obligaciones contractuales del proveedor, principalmente para la aceptación de los bienes o servicios objeto de la contratación.
2. Confirmar, cuando proceda, que los accesos a los activos o servicios de TIC proporcionados al proveedor, para el cumplimiento del contrato, han sido retirados al darse por finiquitado el mismo.
3. Actualizar el reporte de avance sobre el cumplimiento de obligaciones con la información final, y comunicar cualquier incidente o desviación que se detecte al administrador de proyecto y, en su caso, a la unidad administrativa solicitante o a los responsables de los procesos involucrados, así como a la unidad administrativa facultada en la Institución para efecto de dar por concluidas las obligaciones contractuales, en términos de las disposiciones aplicables.

Relación de Productos del proceso:

1. "Reporte de avance sobre el cumplimiento de obligaciones". Formato APRO F1.

Indicador del proceso:

Nombre: Cumplimiento del proceso.

Objetivo: Conocer el grado de cumplimiento del proceso.

Descripción: Medir el cumplimiento del proceso por medio de la actividad de revisión sobre contratos.

Fórmula: % de eficiencia= (número de revisiones de avance y conclusión ejecutadas / número de revisiones de avance y conclusión programadas) X 100.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Semestral.

III.C. PROCESO DE ADMINISTRACIÓN DE LA OPERACIÓN (AOP).

Objetivo General:

Entregar a los usuarios los servicios de TIC, conforme a los niveles de servicio acordados y con los controles de seguridad definidos.

Objetivos Específicos:

1. Establecer mecanismos para administrar y operar la infraestructura y servicios de TIC, de manera que puedan resistir fallas, ataques deliberados o desastres y, se recuperen los servicios de TIC de manera ágil y segura.
2. Asegurar la estabilidad y continuidad de la operación de la infraestructura de TIC en la aplicación de cambios y la solución de problemas e Incidentes, la implementación de aplicativos de cómputo, soluciones tecnológicas y nuevos servicios de TIC.

Reglas del proceso:

1. El responsable de este proceso estará a cargo de la operación del centro de cómputo y comunicaciones, o bien, del enlace con los responsables de los servicios de cómputo y comunicaciones que se encuentren contratados.
2. El responsable de este proceso deberá revisar y en su caso, aprobar los cambios a los elementos o componentes del ambiente operativo.
3. El responsable de este proceso, en coordinación con cada responsable de dominio tecnológico, se asegurará de que los servidores de cómputo de la red institucional, así como los componentes del ambiente operativo que manejen fecha y hora en sus sistemas operativos, se encuentren sincronizados a la hora oficial para los Estados Unidos Mexicanos generada por el Centro Nacional de Metrología, en los husos horarios establecidos en la Ley del Sistema de Horario en los Estados Unidos Mexicanos, para lo cual hará uso del servicio que dicho centro proporciona de manera gratuita.
4. El responsable de este proceso se deberá asegurar que se realicen oportunamente las evaluaciones, para determinar la efectividad de los controles de seguridad implementados.
5. El responsable de este proceso deberá verificar que se siguen en todo momento los controles de seguridad establecidos en el SGSI.
6. El titular de la UTIC deberá asignar al Responsable del mantenimiento de la infraestructura.

Roles del proceso:

1. Responsable del Proceso de Administración de la Operación (AOP).
2. Responsable del mantenimiento de la infraestructura.

Actividades del Proceso.**AOP 1 Establecer el mecanismo de operación de los sistemas, aplicaciones y servicios de TIC.**

Descripción: Establecer las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación de los sistemas, aplicaciones y servicios de TIC.

Factores Críticos:**El responsable de este proceso deberá:**

1. Desarrollar, implementar y mantener un mecanismo de operación de TIC para los sistemas, aplicaciones y servicios de TIC, que contemple las acciones a seguir para la programación, ejecución y seguimiento de las tareas de la operación, mantenimiento y respaldo; considerando al menos, lo siguiente:
 - a) El cumplimiento de lo establecido en los programas de capacidad, de disponibilidad y de continuidad.
 - b) Las tareas de entrega en turno (actividades, estado, actualizaciones finalizadas y en curso, problemas e incidentes de operación y de mesa de servicios, escalamientos y reportes sobre tareas relevantes pendientes de ejecutar o en seguimiento).
 - c) Las actividades rutinarias que se deben ejecutar en cada activo de TIC, así como las que, en su caso, se deberán realizar de requerirse algún cambio en las actividades habituales.
 - d) La elaboración de programas de ejecución de tareas para la operación de TIC, conforme a las necesidades de operación de la infraestructura y servicios de TIC.
 - e) Los tiempos máximos permitidos para que un activo de TIC permanezca fuera de operación, por incidentes en la ejecución de tareas de la operación de TIC.
 - f) Controles para el registro y seguimiento de incidentes en la ejecución de tareas de la operación de TIC.
 - g) La identificación y aprobación de las salidas de las tareas de la operación de TIC.

- h) El manejo de excepciones, eventos e incidentes y cambios administrados, así como de controles de seguridad conforme al Proceso de Administración de la Seguridad de la Información (ASI) y al Proceso de Operación de Controles de Seguridad de la Información y del ERISC (OPEC).

El responsable de este proceso, con apoyo del titular de la UTIC, deberá:

2. Definir e implementar, en la medida de lo posible y conforme a las necesidades y recursos de la UTIC, herramientas tecnológicas para notificar y rectificar fallas críticas en las tareas de la operación, así como para monitorear el estado y operación de los dispositivos dentro de los límites aceptables, con la finalidad de prevenir fallas en la operación.

AOP 2 Programar y ejecutar las tareas de la operación de los sistemas, aplicaciones y servicios de TIC.

Descripción: Efectuar la programación de las tareas de la operación de los sistemas, aplicaciones y servicios de TIC, con base en el mecanismo de operación de TIC.

Factores Críticos:

El responsable de este proceso deberá:

1. Elaborar, conforme al mecanismo de operación de TIC, los programas de ejecución de tareas para la operación de TIC, que incluyan de manera detallada y calendarizada: las tareas a desarrollar, por día y turno; el nombre de los responsables; los componentes y elementos de la configuración involucrados; el manejo de excepciones, eventos e incidentes y cambios.
2. Coordinar la ejecución diaria de las tareas programadas para la operación de los sistemas, aplicaciones y servicios de TIC que se hubiere elaborado.
3. Constatar que el personal a su cargo:
 - a) Ejecute las tareas contenidas en el programa de ejecución de tareas para la operación de TIC que les corresponda desarrollar y documentarlas en una bitácora de operación.
 - b) Registre y dé trámite a las solicitudes de cambio que deriven de la ejecución de las tareas de operación y efectuar tales cambios de manera administrada, estableciendo controles de seguridad en cada caso.
 - c) Registre y dé el trámite que corresponda a cualquier solicitud de servicio con motivo de incidentes de operación que deriven de la ejecución de las tareas de operación, y efectuar el seguimiento de la solicitud de manera administrada, estableciendo controles de seguridad en cada caso.
4. Revisar las bitácoras de operación, para constatar que las tareas ejecutadas coinciden con las tareas programadas.

AOP 3 Monitorear la infraestructura de TIC en operación.

Descripción: Monitorear en los diferentes dispositivos de la infraestructura y de los servicios de TIC, la ejecución de las tareas de la operación, con el propósito de identificar eventos para prevenir o solucionar fallas e incidentes.

Factores Críticos:

El responsable de este proceso deberá:

1. Elaborar y mantener un listado de la información de la infraestructura y de los servicios de TIC cuya operación requiera monitorearse, con base en la información de los datos de los elementos de configuración correspondientes.
2. Revisar que se registre cualquier tarea ejecutada como parte de la operación, a efecto de contar con registros que permitan identificar la causa raíz de incidentes, así como confirmar la ejecución satisfactoria de las tareas de la operación.
3. Identificar los eventos que se presenten en la operación de la infraestructura y de los servicios de TIC, considerando al menos los eventos siguientes:
 - a) Alertas relacionadas con niveles máximos y mínimos de operación.
 - b) Alertas derivadas de alguna excepción en la secuencia de las tareas de operación.

- c) Alertas por operación o comportamiento inusual.
- 4. Verificar que se hayan registrado en la bitácora de operación, los incidentes de la operación detectados, con base en los factores críticos 2 y 3 de esta actividad, en el momento en que se presentaron.
- 5. Dar seguimiento a los eventos e incidentes que se presenten en la operación y registrar aquellos que aporten experiencia y conocimiento, con el propósito de apoyar el análisis para la solución de problemas o la prevención de incidentes, así como la mejora de las tareas de operación en la Institución y estar en posibilidad de transmitirlos a otras Instituciones.

AOP 4 Implementar y verificar que se cumplan los controles de seguridad física en el centro de datos.

Descripción: Implementar, de acuerdo con el SGSI, los controles de seguridad física en el centro de datos, así como para el acceso al propio centro y a los componentes o elementos del ambiente operativo, ubicados en el mismo.

Factores Críticos:

El responsable del proceso, con apoyo del responsable del Proceso de Administración de la Seguridad de la Información (ASI), deberá:

1. Definir un sistema de seguridad física en el centro de datos, en el que se incorporen, de acuerdo con el SGSI, los controles de seguridad para:
 - a) Los riesgos de seguridad física identificados en el Proceso de Administración de la Seguridad de la Información (ASI).
 - b) Limitar el acceso a la información sensible del centro de datos.
 - c) Efectuar el retiro, transporte y almacenamiento de activos de TIC, de forma segura.
 - d) El borrado seguro de la información de los dispositivos de almacenamiento fijos, removibles y externos, que sean retirados del ambiente operativo, por daño o reemplazo.
 - e) El registro de incidentes sobre la seguridad del ambiente físico, mediante la solicitud de servicio respectiva.
2. Integrar al sistema de seguridad física en el centro de datos a que se refiere el factor crítico anterior, los controles de seguridad que de acuerdo con el SGSI se requieran para el acceso físico a las áreas reservadas de la UTIC, los cuales deberán considerar al menos los siguientes accesos:
 - a) Normal u ordinario.
 - b) Restringido.
 - c) Entrada o salida en caso de emergencia.
 - d) A equipos con datos sensibles.
 - e) A proveedores o visitantes.
3. Integrar al sistema de seguridad física en el centro de datos, a que se refiere el factor crítico 1 anterior, los controles de seguridad que de acuerdo con el SGSI sean necesarios para hacer frente a los riesgos ambientales, considerando para ello:
 - a) Los riesgos por fenómenos naturales, identificados en el Proceso de Administración de la Seguridad de la Información (ASI).
 - b) Los activos de TIC, incluyendo el equipo móvil y el que esté fuera del centro de datos.
 - c) Los dispositivos que detectan amenazas ambientales, para responder a las alarmas y a otras notificaciones.
4. Difundir al interior de la UTIC los controles de seguridad implementados y verificar su cumplimiento.
5. Registrar los incidentes del ambiente físico que se presenten y administrarlos hasta su solución.

AOP 5 Elaborar y dar seguimiento al programa de aprovisionamiento de la infraestructura tecnológica.

Descripción: Elaborar y dar seguimiento al programa de aprovisionamiento de la infraestructura tecnológica, para mantener la continuidad de la operación de los servicios de TIC.

Factores Críticos:

El responsable del mantenimiento de la infraestructura, deberá:

1. Elaborar un programa de aprovisionamiento de la infraestructura tecnológica, el cual contendrá al menos:

- a) Los componentes que requiere y la justificación de los mismos, con base en el programa de tecnología y los servicios de TIC que soportará o complementará.
- b) La estimación de costos, beneficios, vida útil, disponibilidad de soporte técnico y/o mantenimiento, periodo de permanencia en el mercado, y apego a estándares tecnológicos.
- c) La fecha estimada en que se requerirá contar con cada componente.

El titular de la UTIC deberá:

- 2. Obtener del grupo de trabajo para la dirección de TIC la aprobación del programa de aprovisionamiento de la infraestructura tecnológica, y enviarlo al responsable del Proceso de Administración del Presupuesto y las Contrataciones (APCT), para su trámite.

El responsable del mantenimiento de la infraestructura deberá:

- 3. Dar seguimiento al avance del programa de aprovisionamiento de la infraestructura tecnológica.
- 4. Efectuar revisiones periódicas a la infraestructura tecnológica e identificar las posibles actualizaciones o mejoras a la misma, para efectos de que sean incluidas al programa de aprovisionamiento de la infraestructura tecnológica.
- 5. Evaluar la eficiencia de los resultados del programa de aprovisionamiento de la infraestructura tecnológica e integrar la evaluación al propio programa.

AOP 6 Mantener los recursos de infraestructura tecnológica y su disponibilidad.

Descripción: Elaborar, ejecutar y dar seguimiento al programa de mantenimiento de la infraestructura tecnológica, e integrar controles de seguridad en la configuración, instalación y mantenimiento de componentes en la infraestructura.

Factores Críticos:**El responsable del mantenimiento de la infraestructura deberá:**

- 1. Elaborar un programa de mantenimiento de la infraestructura tecnológica que contenga acciones de carácter preventivo para evitar fallas a los componentes de dicha infraestructura, y difundirlo a los responsables de los procesos de la UTIC que estén involucrados.
- 2. Aplicar los controles de mitigación de riesgos establecidos en el Proceso de Administración de la Seguridad de la Información (ASI), relativos a componentes de infraestructura.
- 3. Asegurar que el programa de mantenimiento de la infraestructura tecnológica se ejecute por medio de cambios administrados.
- 4. Implementar, en la realización de las tareas de instalación y mantenimiento de la infraestructura tecnológica, los controles de seguridad del SGSI, que consideren cuando menos:
 - a) La protección de los componentes que serán instalados o que recibirán mantenimiento.
 - b) Efectuar el respaldo y protección de los datos almacenados en la infraestructura tecnológica, así como del software que se encuentre instalado.
 - c) Verificar que el ambiente de desarrollo y pruebas sea el adecuado para efectuar las tareas de instalación o de mantenimiento a la infraestructura tecnológica.
 - d) Verificar que el ambiente de desarrollo y pruebas a que se refiere el inciso anterior esté separado del ambiente operativo.
 - e) Comprobar la funcionalidad, seguridad, disponibilidad e integridad de los componentes instalados o en mantenimiento, con el propósito de que operen adecuadamente y se cumpla con los acuerdos de niveles de servicio SLA establecidos.
 - f) Modificar, en los componentes instalados, las contraseñas originales, configuraciones y parámetros que puedan afectar la seguridad y suprimir los accesos temporales utilizados en la instalación.
 - g) Verificar que la instalación de software se efectúe de acuerdo con las especificaciones del mismo y que cualquier desviación sea identificada para evaluar su impacto, así como incluir la instalación de las actualizaciones de seguridad disponibles.
 - h) Verificar que el software sea instalado con los privilegios mínimos necesarios a usuarios y administradores del software, así como que se hayan aplicado las recomendaciones de seguridad emitidas por el fabricante y por el SGSI para el fortalecimiento de la seguridad del software instalado.
- 5. Evaluar la efectividad de los controles de seguridad aplicados en la instalación de los componentes y en las tareas de mantenimiento.
- 6. Registrar y dar seguimiento a los incidentes de mantenimiento, con el propósito de analizar y eliminar las vulnerabilidades dentro de la infraestructura tecnológica.

7. Informar de los incidentes de mantenimiento a los responsables de los dominios tecnológicos involucrados.
8. Diseñar el ambiente que permita la creación y simulación de pruebas de concepto y prototipos para verificar la viabilidad de componentes de infraestructura y de soluciones tecnológicas.
9. Establecer y mantener el ambiente diseñado, mediante cambios administrados.
10. Efectuar en el ambiente a que se refiere esta actividad, las pruebas de factibilidad a componentes de infraestructura y de soluciones tecnológicas.
11. Registrar el resultado de las pruebas realizadas y mantenerlas disponibles como información de conocimiento.

Relación de Productos del proceso:

1. "Mecanismo de operación de TIC" (formato de acuerdo a las necesidades de la UTIC).
2. "Programa de aprovisionamiento de la infraestructura tecnológica". Formato AOP F1.
3. "Programa de mantenimiento de la infraestructura tecnológica". Formato AOP F2.

Indicador del proceso:

Nombre: Incidentes en el ambiente operativo.

Objetivo: Medir la eficiencia en el proceso.

Descripción: Obtener el número de Incidentes en la operación resueltos mediante la aplicación del mecanismo de operación de TIC.

Fórmula: % de eficiencia = (incidentes en la operación resueltos / incidentes que se presentaron en el ambiente operativo) X 100.

Responsable: El responsable de este proceso.

Frecuencia de cálculo: Semestral.

III.D. PROCESO DE OPERACIÓN DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y DEL ERISC (OPEC).
Objetivo General:

Implementar y operar los controles de seguridad de la información de acuerdo al programa de implementación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.

Objetivos Específicos:

1. Implementar y operar los controles de seguridad de la información.
2. Definir y aplicar la planeación para la mitigación de riesgos por incidentes.
3. Implementar las mejoras recibidas del Proceso de Administración de la Seguridad de la Información (ASI), para el fortalecimiento del SGSI, tanto de sus guías técnicas como de los controles de seguridad de la información en operación.

Reglas del proceso:

1. El responsable de este proceso estará a cargo de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos.
2. Los servidores públicos de la UTIC y los usuarios están obligados a operar en un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información, de acuerdo a lo previsto en el presente manual.
3. El responsable de este proceso se deberá asegurar que las acciones y los productos obtenidos de la ejecución del presente proceso sean consecuentes con lo previsto en el Acuerdo por el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno, publicado en el Diario Oficial de la Federación el 12 de julio de 2010, y su reforma de fecha 27 de julio de 2012, en lo relativo a la administración de riesgos y la seguridad de la información, y de que los mismos se comuniquen al coordinador de control interno de la Institución que se designe conforme a lo establecido en dicho ordenamiento.
4. El responsable de este proceso, con apoyo de la totalidad de los responsables de los procesos de la UTIC, deberá verificar que se implementen los controles que se definan en el SGSI, en los proyectos, procesos y en todas aquellas operaciones en las que el SGSI y el propio Proceso de Administración

- de la Seguridad de la Información (ASI), lo indiquen, así como en los servicios de TIC a fin de garantizar la seguridad de la información de la Institución, debiendo constatar que se conserve la evidencia de la implementación y aplicación de dichos controles.
5. El responsable de este proceso deberá tomar como insumos del proceso los productos que se generan en el Proceso de Administración de la Seguridad de la Información (ASI), y sobre tales productos deberá efectuar las actualizaciones que deriven de la ejecución de los factores críticos de las actividades del presente proceso.
 6. El personal de la UTIC deberá asegurarse de integrar la totalidad de la información que se muestra en los formatos de los productos de este proceso, que se integran en el Apéndice IV.A de este manual, considerando que el orden de la información que se presenta en los formatos de los productos es sugerido.

Roles del proceso:

1. Responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos.
2. Responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos.
3. ERISC.

Actividades del Proceso.

OPEC 1 Designar un responsable de la supervisión de la implementación de los controles de seguridad definidos en el SGSI y en el análisis de riesgos.

Descripción: Designar a un servidor público como responsable de la supervisión de la adecuada implementación de los controles de seguridad de la información definidos en el SGSI y de aquellos resultantes del análisis de riesgos.

Factores Críticos:

El responsable de la seguridad de la información en la Institución deberá:

1. Asignar a un servidor público que será responsable de supervisar que los responsables de implementar controles de seguridad del SGSI y controles para el manejo de riesgos, lleven a cabo su tarea en tiempo y forma, con apego a la definición del control de seguridad correspondiente.
2. Comunicar la asignación a todos los involucrados.

El responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberá:

3. Mantener actualizada la información del "Documento de resultados del análisis de riesgos y el programa de implementación del SGSI, incluyendo su avance.

OPEC 2 Establecer los elementos de operación del ERISC.

Descripción: Establecer la operación del ERISC, así como la guía técnica de atención a incidentes.

Factores Críticos:

El responsable de la seguridad de la información en la Institución deberá:

1. Establecer las reglas de operación del ERISC, en las que se preverán los mecanismos de coordinación del ERISC al interior de la Institución o con otros ERISC u organizaciones externas, en concordancia con la directriz rectora de respuesta a incidentes, incluyendo al menos, los relativos a:
 - a) Los canales de comunicación, que deberán ser seguros.
 - b) Los relativos a la diseminación de datos de los incidentes.

El ERISC deberá:

2. Elaborar, de acuerdo a lo establecido en la directriz rectora de respuesta a incidentes, la guía técnica de atención a incidentes, de acuerdo a la criticidad de los activos de TIC afectados, considerando en su elaboración al menos los siguientes apartados:
 - a) Detección y registro de los incidentes.
 - b) Priorización de los incidentes.
 - c) Investigación técnica de los incidentes.

- d) Criterios técnicos de contención de los incidentes, de acuerdo a la criticidad de los activos de TIC.
 - e) Obtención, preservación y destino de los indicios de los incidentes.
 - f) Erradicación de los incidentes.
 - g) Recuperación de la operación.
 - h) Documentación de las lecciones aprendidas.
3. Establecer el mecanismo de registro de los incidentes de seguridad de la información, que incluya un repositorio para contener los datos de éstos y crear una base de conocimiento.
 4. Reportar al responsable de la seguridad de la información, los incidentes de seguridad de la información que se presenten.

OPEC 3 Operación del ERISC en la atención de incidentes.

Descripción: Ejecutar las acciones necesarias para atender un incidente de seguridad de la información de acuerdo a la guía técnica elaborada.

Factores Críticos:

El ERISC, en coordinación con el responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberá:

1. Definir las acciones de atención a los incidentes con apoyo de la guía técnica de atención de incidentes, respecto del incidente que se haya presentado.
2. Asegurarse que los responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos, ejecuten las acciones siguientes:
 - a) Apliquen la solución necesaria.
 - b) Registren los datos del incidente y su solución.
 - c) Comuniquen el incidente y su solución al grupo estratégico de seguridad de la información y a los responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados.
3. Integre los datos del incidente y su solución a los repositorios con los que cuente la UTIC y en su caso, a los repositorios de la Institución que determine el grupo estratégico de seguridad de la información.

OPEC 4 Implementar los controles de mitigación de riesgos y los controles del SGSI.

Descripción: Asegurar que los controles de mitigación de riesgos y del SGSI, se implementen y operen de acuerdo a su definición.

Factores Críticos:

Los responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberán:

1. Ejecutar los programas de implementación para el manejo de riesgos y de implementación del SGSI, de acuerdo a lo que se establece en el documento de definición del SGSI, y con apoyo de los titulares de las unidades administrativas en las cuales se implementarán los controles.
2. Dar seguimiento a la ejecución del programa de implementación del SGSI y actualizar el avance del mismo.

El responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberá:

3. Elaborar un informe de resultados de la implementación del SGSI e integrarlo al documento de definición del SGSI.
4. Asegurar que los controles de seguridad se hayan implementado de acuerdo a lo previsto en el documento de definición del SGSI y su programa de implementación del SGSI.
5. Elaborar los informes correspondientes a las desviaciones en la implementación y/o en la operación de los controles de seguridad.
6. Integrar los resultados de los factores críticos 3, 4 y 5 anteriores e incorporarlos, para efectos de su actualización, en el documento de definición del SGSI y enviarlos al grupo estratégico de seguridad de la información.

OPEC 5 Implementar los controles del SGSI relacionados con los dominios tecnológicos de TIC.

Descripción: Asegurar que los controles de seguridad para los dominios tecnológicos de TIC se definan y aprueben por el grupo estratégico de seguridad de la información para su integración al SGSI, así como que se efectúe su implementación y se operen de acuerdo a dicha definición.

Factores Críticos:

Los responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos, con el apoyo del responsable de este proceso, deberán:

1. Mantener los componentes de los dominios tecnológicos con el software de seguridad y de administración y monitoreo, actualizado y en operación; incluyendo software para evitar vulneraciones y accesos no autorizados.
2. Reforzar, con mecanismos de TIC, las conexiones de la red institucional con redes públicas o privadas, de manera que se tenga control del acceso a los servicios autorizados, así como monitorear, detectar, prevenir e impedir ataques o intrusiones.
3. Implementar mecanismos de TIC para impedir la conexión a redes inalámbricas externas que se encuentren al alcance de los dispositivos electrónicos institucionales.
4. Definir y establecer las conexiones remotas que den acceso a la red y a los servicios de TIC institucionales, tanto para usuarios internos como a proveedores, determinando si éstas se establecen a través de canales cifrados de comunicación que aseguren técnicamente la seguridad de los datos. Para estas conexiones se deberá obtener autorización expresa del grupo estratégico de seguridad de la información.
5. Asegurar que los servidores y estaciones de trabajo, cuenten con software actualizado para detección y protección contra programas para vulnerar la seguridad de los dispositivos de TIC, así como su información y los servicios que proveen. El software debe emitir reportes sobre el estado de actualización de los componentes sobre los que tienen cobertura.
6. Instalar en los componentes de los servicios de correo electrónico, herramientas actualizadas de protección contra correos electrónicos no deseados o no solicitados.
7. Instalar en los equipos de cómputo de los usuarios, incluyendo los móviles que se conecten a la red de datos, las herramientas antivirus y aquéllas necesarias para prevenir ataques por la vulnerabilidad que el uso de estos equipos conlleva.
8. Instalar mecanismos de cifrado de datos en los dispositivos electrónicos móviles que contengan información considerada como reservada o sensible para la Institución.
9. Establecer el mecanismo para garantizar la eliminación o modificación de los privilegios de acceso a la información del personal interno y proveedores de servicios, cuando terminen su relación contractual o cuando por algún motivo el nivel de privilegios de accesos asignados cambie.
10. Establecer, para cada componente de los dominios tecnológicos, los elementos de control de acceso lógico que, como mínimo, soliciten un nombre de usuario y contraseña, y lleven el registro de estos accesos.
11. Adicionalmente al factor crítico anterior, integrar al aplicativo de cómputo o servicio de TIC, adquirido o desarrollado, un módulo de control de acceso lógico que solicite como mínimo, un nombre de usuario y contraseña, cuya definición deberá aprobarse por el grupo estratégico de seguridad de la información.

El responsable del Proceso de Administración de Servicios (ADS), deberá:

12. Obtener del titular de la UTIC, la aprobación de los controles definidos conforme a los factores críticos 1 a 11 de esta actividad.
13. Obtener, con apoyo del titular de la UTIC, la aprobación del grupo estratégico de seguridad de la información, para la integración al SGSI, de los controles a que se refiere el factor crítico anterior.
14. Asegurar que los controles de seguridad se hayan implementado de acuerdo a lo establecido en esta actividad.
15. Dar a conocer a los responsables de los servicios de TIC, la actualización que se realice al programa de implementación para el manejo de riesgos y al programa de implementación del SGSI.

OPEC 6 Revisar la operación del SGSI.

Descripción: Efectuar la revisión de la operación de los controles de mitigación de riesgos y de seguridad, así como obtener mediciones de la misma.

Factores Críticos:

El responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberá:

1. Obtener los datos necesarios para verificar la eficiencia y eficacia de los controles implementados, de acuerdo al programa de evaluaciones del SGSI recibido del grupo estratégico de seguridad de la información.
2. Medir la efectividad de los controles de seguridad implementados.
3. Efectuar, con base en el programa de evaluaciones del SGSI, la evaluación del SGSI.
4. Registrar la información de los intentos de violaciones e incidentes de seguridad, hayan sido exitosos o no, así como efectuar el análisis y evaluación de dicha información.
5. Documentar las acciones de revisión del SGSI que hayan resultado de los factores críticos anteriores, mediante la elaboración de un informe de revisión del SGSI, integrarlo al documento de definición del SGSI y enviarlo al grupo estratégico de seguridad de la información.

OPEC 7 Aplicar al SGSI las mejoras que defina el grupo estratégico de seguridad de la información.

Descripción: Mejorar el SGSI, a través de la aplicación de acciones preventivas y correctivas derivadas de las revisiones efectuadas al mismo, así como de las acciones de mejora que defina el grupo estratégico de seguridad de la información.

Factores Críticos:**Los responsables de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberán:**

1. Aplicar las acciones correctivas y preventivas a los controles de seguridad de la información, indicados por el grupo estratégico de seguridad de la información.
2. Documentar el resultado de la aplicación de la mejora, para cada uno de los controles de seguridad de la información que resultaron impactados, incluyendo las mejoras del SGSI aplicadas.
3. Actualizar el informe de seguimiento a las acciones de mejora al SGSI e integrarlo en el documento de definición del SGSI.

El responsable de la supervisión de la implementación de los controles de seguridad de la información y de manejo de riesgos, deberá:

4. Verificar el contenido del informe de seguimiento a las acciones de mejora al SGSI; actualizar el programa de evaluaciones del SGSI, integrarlo en el documento de definición del SGSI y enviar éste al grupo estratégico de seguridad de la información para su revisión.

Relación de Productos del proceso:

Este proceso utiliza para su operación, consulta y actualización los productos del Proceso de Administración de la Seguridad de la Información (ASI).

Indicador del proceso:

Nombre: Cumplimiento de la administración de riesgos.

Objetivo: Medir la eficiencia de la gestión del proceso.

Descripción: Medir el cumplimiento en la implementación de los controles para la mitigación de riesgos establecidos durante el proceso.

Fórmula: % de eficiencia = (controles implementados en operación de acuerdo a su definición / controles implementados) X 100.

Responsable: El responsable del proceso.

Frecuencia de cálculo: Anual.

IV. APÉNDICES

IV.A Formatos para los productos de los procesos.

IV.B Matriz de metodologías, normas y mejores prácticas aplicables a la gestión de las TIC.

IV.C Diagramas de actividades de los procesos.

Disponibles en http://www.normateca.gob.mx/NF_Secciones_Otras.php?Subtema=61