# SECRETARIA DE LA FUNCION PUBLICA

**ACUERDO por el que se reforma y adiciona el diverso por el que se establecen las disposiciones administrativas en materia de tecnologías de la información y comunicaciones, y se expide el Manual Administrativo de Aplicación General en esa materia y en la de Seguridad de la Información.**

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

ALEJANDRO ALFONSO POIRE ROMERO, Secretario de Gobernación, y SALVADOR VEGA CASILLAS, Secretario de la Función Pública, con fundamento en lo dispuesto en los artículos 27, fracciones XII, XXIX y XXXII; 37, fracciones VI y XXVI de la Ley Orgánica de la Administración Pública Federal; 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 y 5, fracciones XIX, XXII, XXIV y XXXII del Reglamento Interior de la Secretaría de Gobernación; 1 y 6, fracciones I y XXIV del Reglamento Interior de la Secretaría de la Función Pública, y

## CONSIDERANDO

Que en cumplimiento a la instrucción del Ejecutivo Federal, para que la Secretaría de la Función Pública emitiera, por sí o con la participación de las dependencias competentes, disposiciones, políticas o estrategias, acciones o criterios de carácter general y procedimientos uniformes para la Administración Pública Federal y, en lo conducente, para la Procuraduría General de la República, en materia, entre otras, de tecnologías de la información y comunicaciones, el 13 de julio de 2010 se publicó en el Diario Oficial de la Federación el Acuerdo por el que se expidió el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y que contiene disposiciones administrativas en la materia;

Que el artículo octavo del Acuerdo que alude el considerando anterior, prevé que los procesos y procedimientos previstos en el respectivo Manual deberán revisarse, para efectos de sus actualización cuando menos una vez al año, motivo por el cual se publicó en el Diario Oficial de la Federación el 6 de septiembre pasado, el Acuerdo por el que se modifica el diverso por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones;

Que en la actualidad, y en virtud del desarrollo y utilización cada vez mayor de las tecnologías de la información y comunicaciones en la operación de los diferentes trámites y servicios públicos que proporciona la Administración Pública Federal, reviste particular importancia el establecimiento de procesos uniformes y de acciones y medidas coordinadas en materia de seguridad de la información, que permitan a partir de la identificación de la infraestructura de tecnologías de la información y comunicaciones y de aquélla otra vinculada o asociada con ésta que se considere crítica, fortalecer la gestión de la seguridad de la información, para lograr el uso seguro de equipos y servicios, así como una respuesta oportuna ante situaciones de emergencia, y contribuir a la seguridad de la nación ante amenazas materializadas a través del uso de tecnologías de la información y comunicaciones;

Que el Programa para la Seguridad Nacional 2009-2012, en su objetivo específico 1. "Fortalecer estructuralmente el sistema de seguridad nacional", en su línea estratégica 1.2. "Establecer un sistema integral de información para la preservación de la seguridad nacional", prevé como una de sus líneas de acción, la 1.2.4., "Desarrollar instrumentos y tecnología que garanticen la protección y confidencialidad de la información de seguridad nacional, así como su transmisión segura";

Que el Ejecutivo Federal acordó en el seno del Consejo de Seguridad Nacional, diversos lineamientos generales de seguridad de la Información; y su incorporación en el Acuerdo y en el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones;

Que en la definición de los procesos, acciones y medidas que en materia de seguridad de la información se contempla incorporar en las disposiciones del Acuerdo y del Manual en materia de tecnologías de la información y comunicaciones, ha tenido una participación preponderante el Grupo Técnico Intersecretarial Especializado en Seguridad de la Información establecido por el Consejo de Seguridad Nacional con objeto de coordinar los trabajos para el desarrollo de una política general de seguridad de la información, hemos tenido a bien expedir el siguiente

## ACUERDO

**ARTICULO PRIMERO.- Se REFORMAN** los Artículos Primero, en su primer párrafo; Segundo; Cuarto; Quinto; Sexto, en su primer párrafo; Séptimo y Octavo; y **se ADICIONA** el Capítulo III Bis y sus artículos Sexto Bis y Sexto Ter al Acuerdo por el que se expide el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, para quedar como sigue:

**"Artículo Primero**.- El presente Acuerdo tiene por objeto establecer las disposiciones administrativas en materia de tecnologías de la información y comunicaciones y de seguridad de la información, que deberán observar las dependencias y entidades de la Administración Pública Federal y la Procuraduría General de la República, así como expedir el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, que en términos del Anexo Unico de este Acuerdo, forma parte integrante del mismo.

...

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

I. **Centro:** el Centro de Investigación y Seguridad Nacional;

II. **Dependencias:** las secretarías de Estado, incluyendo a sus órganos administrativos desconcentrados y la Consejería Jurídica del Ejecutivo Federal, así como las unidades administrativas de la Presidencia de la República, conforme a lo dispuesto en la Ley Orgánica de la Administración Pública Federal. La Procuraduría General de la República será considerada con este carácter en lo que el presente Acuerdo y el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información, le resulten aplicables conforme a lo previsto en su Ley Orgánica;

III. **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;

IV. **Entidades:** los organismos públicos descentralizados, empresas de participación estatal mayoritaria 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;

V. **Infraestructura de TIC:** el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC;

VI. **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 aquéllas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional;

VII. **Manual:** el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información;

VIII. **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;

IX. **Seguridad nacional:** las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de lo dispuesto en el artículo 3 de la Ley de Seguridad Nacional;

X. **TIC:** las Tecnologías de la Información y Comunicaciones, y

XI. **Unidad:** la Unidad de Gobierno Digital de la Secretaría de la Función Pública.

**Artículo Tercero**.- ...

**Artículo Cuarto**.- Los titulares de las dependencias y entidades, en el ámbito de sus respectivas atribuciones, instruirán lo conducente para que se dejen sin efecto los acuerdos, normas, lineamientos, oficios circulares y demás disposiciones o procedimientos de carácter interno que se hubieren emitido en materia de TIC y de seguridad de la información que no deriven de facultades expresamente previstas en leyes y reglamentos.

**Artículo Quinto**.- La aplicación de las disposiciones contenidas en el presente Acuerdo y el Manual, corresponde a las áreas o unidades administrativas responsables de las TIC en las dependencias y entidades, así como a los servidores públicos cuyas atribuciones o funciones se vinculen con las TIC y con la seguridad de la información.

**Artículo Sexto**.- Con el propósito de armonizar y homologar las actividades que en materia de TIC y de seguridad de la información realizan las dependencias y entidades, en el Manual se identifican los procesos correspondientes que se regirán por lo dispuesto en las disposiciones jurídicas aplicables y el propio Manual.

...

**Capítulo III Bis**

**Disposiciones específicas para la seguridad de la información considerada de seguridad nacional**

**Artículo Sexto Bis**.- Las Instancias de seguridad nacional deberán observar las disposiciones específicas 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, 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 las atribuciones de las Instancias de seguridad nacional y de sus servidores públicos, cuya revelación no autorizada pueda actualizar o potenciar un riesgo o amenaza a la seguridad nacional en términos de la Ley de Seguridad Nacional, o bien, comprometer la operación de las propias Instancias, las condiciones de seguridad de sus instalaciones 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 la operación de las Instancias de seguridad nacional, las condiciones de seguridad de sus instalaciones 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, 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 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 la impresión o copiado no autorizados ni parcial o totalmente de su contenido;

   c) Se utilizarán mecanismos de firma electrónica y cifrado de llave pública y privada, que permitan la diseminación de la información únicamente al destinatario autorizado al que esté dirigida;

   d) Solicitar a los destinatarios la promesa de confidencialidad a que se refiere el artículo 53 de la Ley de Seguridad Nacional, y verificar su registro ante el Centro;

   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 firma electrónica y cifrado de llave pública y privada, así como abstenerse de compartir las llaves privadas;

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, y

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 trasladado será a cargo de servidores públicos de la Instancia 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.

Las dependencias y entidades que, aún 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 Trasparencia y Acceso a la Información Pública Gubernamental y demás disposiciones aplicables.

**Artículo Sexto Ter**.- Las dependencias y entidades 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.

**Artículo Séptimo**.- La interpretación del presente Acuerdo y del Manual, para efectos administrativos, así como la resolución de los casos no previstos en el mismo, corresponderá:

I. En materia de TIC y de seguridad de la información, a la Secretaría de la Función Pública, por conducto de la Unidad.

II. En materia de seguridad de la información considerada de seguridad nacional, a la Secretaría de Gobernación, a través del Centro.

**Artículo Octavo**.- Las disposiciones y los procesos contenidos en el Manual a que se refiere el presente Acuerdo deberán revisarse 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 Noveno**.- ..."

**ARTICULO SEGUNDO**.- **Se REFORMAN** la denominación del Anexo Uno; diversos numerales del Contenido; diversos términos y definiciones contenidos en el numeral 1, denominado "Definiciones y acrónimos"; los numerales 2 a 5; 5.1, en su denominación; 5.1.1.1; 5.1.1.2.1 en su actividad EMG-3, factor crítico 4; 5.1.1.4, en los numerales 1.2 a 1.4 de las reglas del proceso; 5.2, en su denominación y en sus

procesos 5.2.1 ASI– Administración de la seguridad de la información y 5.2.2, OPEC– Operación de controles de seguridad de la información y del ERISC; 5.4.1.2.1, en su actividad OSGP-2, factores críticos 1 y 2, inciso b); 5.5.1.2.1, en su actividad APT-3, en lo relativo al responsable de los factores críticos de la misma; 5.5.2.2.1, en su actividad ADTI-1, en lo relativo al responsable de los factores críticos 1 y 2; 5.6.2.2.1, en sus actividades DSTI-1, factores críticos 10 y 16, DSTI-4, en lo relativo al responsable de los factores críticos de la misma; DSTI-5, en lo relativo a su responsable y factor crítico 2, inciso a); 5.8.4.2.1, en su actividad ACNF-5, factor crítico 4; 5.9.2.2.1, en su actividad ANS-1, factor crítico 8; 5.11.1.2.1, en su actividad AO-1, factor crítico 1, inciso h); 5.11.2.2.1, en sus actividades AAF-1, en lo relativo al responsable de los factores críticos, AAF-2, en lo relativo al responsable del factor crítico 1 y en su inciso a), factor crítico 3, inciso a); 5.11.3.2.1, en su actividad MI-2, factores críticos 2, inciso g) y 4; **se DEROGAN** los numerales 5.9.3 a 5.9.3.4; y **se ADICIONAN** en el numeral 1, denominado "Definiciones y acrónimos", diversos términos en el orden alfabético que les corresponde; en el numeral 5.1.1.2.1, actividad EMG-3, los factores críticos 5 y 6, recorriéndose el actual factor crítico 5 para pasar a ser el 7; los numerales 5.1.4 a 5.1.4.4; en el numeral 5.11.2.2.1, un inciso e) en el factor crítico 2, de la actividad AAF-2; en el numeral 5.11.3.2.1, un inciso h) en el factor crítico 2 de la actividad MI-2; todos del Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones, para quedar como sigue:

**"ANEXO UNICO**

**MANUAL ADMINISTRATIVO DE APLICACION GENERAL EN MATERIA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES Y DE SEGURIDAD DE LA INFORMACION**

**CONTENIDO**

## 1. DEFINICIONES Y ACRONIMOS

Para efectos de este Manual se entenderá por:

| TERMINO | DEFINICION |
|---|---|
| **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, perdida, 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:** | ... |
| **Activos de información:** | Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, deben ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue. |
| **Activos de TIC:** | Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos. |
| **Activo de soporte:** | Aquél que apoya o complementa a un Activo primario en su función. |
| **Acuerdo de nivel de servicio SLA:** | ... |
| **Acuerdo de nivel operacional OLA:** | El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un servicio de TIC, que se deben 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:** | ... |
| **Amenaza:** | 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; efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas. |
| **Area técnica:** | ... |
| **Bitácora de seguridad:** | El registro continúo de eventos e incidentes de seguridad de la información que ocurren a los Activos de información. |
| **Centro de datos:** | El lugar físico en el que se ubican los Activos de TIC, desde donde se proveen los servicios de TIC. |
| **Confidencialidad**<br>a<br>**Cuadro de mando integral de la UTIC:** | ... |
| **Declaraciones de aplicabilidad:** | El documento que contiene los controles aplicados mediante el SGSI de la Institución como resultado del Análisis de riesgos. |

| | |
|---|---|
| **Directriz rectora:** | ... |
| **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. |
| **Disponibilidad** a **Entregable:** | ... |
| **Evento:** | Suceso que puede ser observado, verificado y documentado, en forma manual o automatizada, que puede llevar al registro de incidentes. |
| **Funcionalidad:** | ... |
| **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. |
| **Gobierno digital:** | ... |
| **Impacto:** | El grado de los daños y/o de los cambios sobre un Activo de información, por la materialización de una amenaza. |
| **Incidente:** | 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. |
| **Iniciativas de TIC:** | ... |
| **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. |
| **Infraestructura de TIC:** | ... |
| **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 aquéllas que tengan reconocido dicho carácter por Acuerdo tomado en el seno del Consejo de Seguridad Nacional. |
| **Institución** a **Integridad:** | ... |
| **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** a **Mapa estratégico de la UTIC:** | ... |
| **Marco rector de procesos:** | El conjunto de procesos tendientes a la homologación de la gestión de la seguridad de la información, así como de la gestión interna de las UTIC, que constituyen el presente Manual. |

| | |
|---|---|
| **Mesa de servicios**<br>a<br>**Recursos humanos en la UTIC:** | ... |
| **Reglas de adaptación:** | El documento que contiene los supuestos en que resulta factible adaptar alguno de los procesos del "Marco rector de procesos", cuando por las características particulares de la Institución así se justifique, conforme a lo previsto en el proceso OSGP- Operación del sistema de gestión y mejora de los procesos de la UTIC. |
| **Repositorio**<br>a<br>**Requerimientos funcionales:** | ... |
| **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. |
| **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. |
| **Seguridad nacional:** | Las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, conforme a lo dispuesto en el artículo 3 de la Ley de Seguridad Nacional. |
| **Sistema o aplicativo**<br>a<br>**Verificación:** | ... |
| **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. |
| **AA:** | El grupo de procesos de Administración de activos del "Marco rector de procesos". Agrupa los siguientes procesos: ADT, ACNC y APC. |
| **AAF:** | El proceso de Administración de ambiente físico, del "Marco rector de procesos". |
| **ACMB:** | El proceso de Administración de cambios, del "Marco rector de procesos". |
| **ACNC:** | El proceso de Administración del conocimiento, del "Marco rector de procesos". |
| **ACNF:** | El proceso de Administración de la configuración, del "Marco rector de procesos". |
| **AD:** | El grupo de procesos de Administración para el desarrollo de soluciones tecnológicas del "Marco rector de procesos". Agrupa los siguientes procesos: ATC, DST y CST. |
| **ADT:** | El proceso de Administración de dominios tecnológicos, del "Marco rector de procesos". |
| **ADTI:** | El proceso de Administración para las contrataciones de TIC, del "Marco rector de procesos". |

| | |
|---|---|
| **AE:** | El proceso de Administración de la evaluación, de TIC del "Marco rector de procesos". |
| **ANS:** | El proceso de Administración de niveles de servicio, del "Marco rector de procesos". |
| **AO:** | El proceso de Administración de la operación, del "Marco rector de procesos". |
| **AP:** | El grupo de procesos de Administración de procesos del "Marco rector de procesos". Está conformado por el proceso OSGP. |
| **APBS:** | El proceso de Administración de proveedores de bienes y servicios de TIC, del "Marco rector de procesos". |
| **APC:** | El proceso de Apoyo a la capacitación del personal de la UTIC, del "Marco rector de procesos". |
| **APP:** | El proceso de Administración del portafolio de proyectos de TIC, del "Marco rector de procesos". |
| **APS:** | El proceso de Administración del portafolio de servicios de TIC, del "Marco rector de procesos". |
| **APT:** | El proceso de Administración del presupuesto de TIC del "Marco rector de procesos". |
| **APTI:** | El proceso de Administración de proyectos de TIC, del "Marco rector de procesos". |
| **AR:** | El grupo de procesos de Administración de recursos, del "Marco rector de procesos". Agrupa los siguientes procesos: APT, APBS y ADTI. |
| **AS:** | El grupo de procesos de Administración de servicios, del "Marco rector de procesos". Agrupa los siguientes procesos: APS y DSTI. |
| **ASI:** | El proceso de Administración de la seguridad de la información, del "Marco rector de procesos". |
| **ATC:** | El proceso de Apoyo técnico para la contratación de soluciones tecnológicas de TIC, del "Marco rector de procesos". |
| **CST:** | El proceso de Calidad de las soluciones tecnológicas de TIC, del "Marco rector de procesos". |
| **DCSI:** | El grupo de procesos de Dirección y control de la seguridad de la información, del "Marco rector de procesos". Agrupa los siguientes procesos ASI y OPEC. |
| **DDT:** | El proceso de Determinación de la dirección tecnológica, del "Marco rector de procesos". |
| **DR:** | El grupo de procesos de Dirección y control de TIC del "Marco rector de procesos". Agrupa los siguientes procesos: EMG, PE, DDT y AE. |
| **DST:** | El proceso de Desarrollo de soluciones tecnológicas de TIC, del "Marco rector de procesos". |
| **DSTI:** | El proceso de Diseño de servicios de TIC, del "Marco rector de procesos". |
| **EMG:** | El proceso de Establecimiento del modelo del gobierno de TIC, del "Marco rector de procesos". |
| **ERISC:** | El Equipo de respuesta a incidentes de seguridad en TIC en la Institución. |
| **LE:** | El proceso de Liberación y entrega, del "Marco rector de procesos". |

| | |
|---|---|
| **MI:** | El proceso de Mantenimiento de infraestructura, del "Marco rector de procesos". |
| **OMS:** | El proceso de Operación de la mesa de servicios, del "Marco rector de procesos". |
| **OP:** | El grupo de procesos de Operaciones del "Marco rector de procesos". Agrupa los siguientes procesos: AO, AAF y MI. |
| **OPEC:** | El proceso Operación de controles de seguridad de la información y del ERISC, del "Marco rector de procesos". |
| **OS:** | El grupo de procesos de Operación de servicios del "Marco rector de procesos". Agrupa los siguientes procesos: OMS y ANS. |
| **OSGP:** | El proceso de Operación del sistema de gestión y mejora de los procesos de la UTIC, del "Marco rector de procesos". |
| **PE:** | El proceso de Planeación estratégica de TIC, del "Marco rector de procesos". |
| **PETIC:** | ... |
| **PR:** | El grupo de procesos de Administración de proyectos del "Marco rector de procesos". Agrupa los siguientes procesos: APP y APTI. |
| **SFP** a **SGSI:** | ... |
| **TE:** | El grupo de procesos de Transición y entrega del "Marco rector de procesos". Agrupa los siguientes procesos: ACMB, LE, THO y ACNF. |
| **THO:** | El proceso de Transición y habilitación de la operación, del "Marco rector de procesos". |
| **TIC** a **UTIC:** | ... |

## 2. OBJETIVOS

**General:**

Definir los procesos que en materia de TIC y de seguridad de la información, regirán a las Instituciones, con el propósito de regular y homologar su gestión, independientemente de la estructura organizacional con que éstas cuenten.

**Específicos:**

1. Proporcionar a las Instituciones procesos simplificados y homologados en materia de TIC y de seguridad de la información, así como las correspondientes regulaciones para cada proceso.
2. Establecer indicadores homologados que permitan a la SFP medir los resultados de la gestión de la UTIC, de manera que le sea posible definir estrategias de apalancamiento y apoyo a las Instituciones que lo requieran.
3. Contribuir a alcanzar una mayor eficiencia en las actividades y procesos institucionales, mediante la aplicación del "Marco rector de procesos", contenidos en el presente Manual.

## 3. AMBITO DE APLICACION

El presente Manual es de aplicación general en las Instituciones.

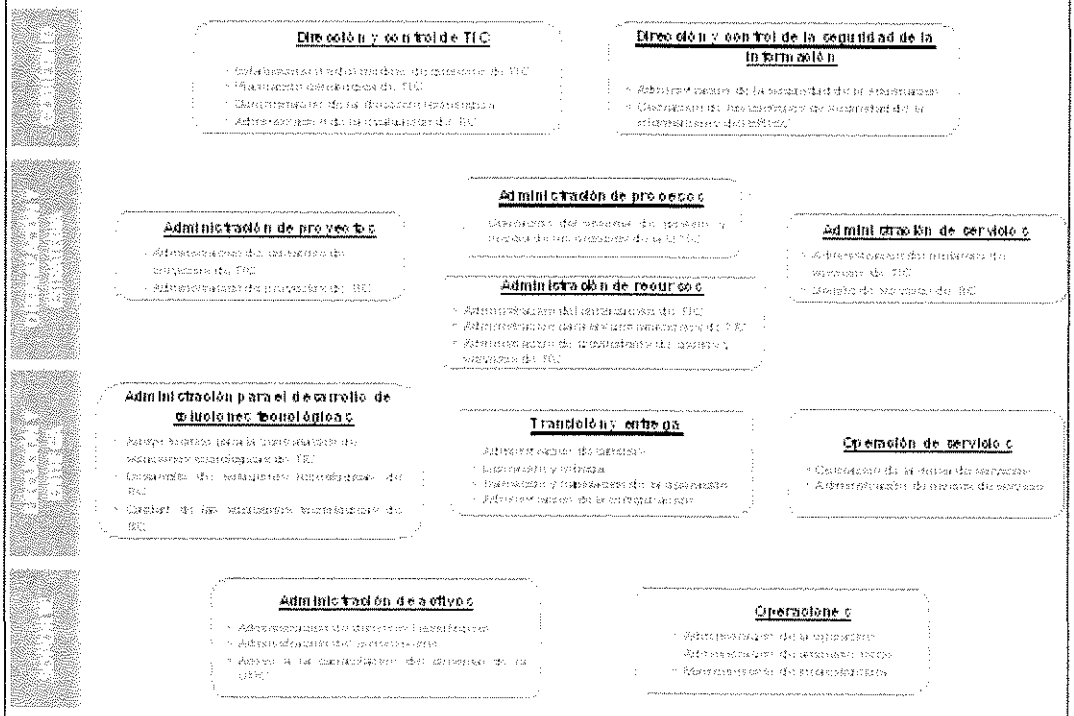
## 4. MARCO JURIDICO

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 Federal de las Entidades Paraestatales.
6. Ley Federal de Presupuesto y Responsabilidad Hacendaria.
7. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
8. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
9. Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
10. Ley Federal de Telecomunicaciones.
11. Ley General de Bienes Nacionales.
12. Ley de Seguridad Nacional.
13. Reglamento Interior de la Secretaría de Gobernación.
14. Reglamento Interior de la Secretaría de la Función Pública.
15. Reglamento de Ley Federal de las Entidades Paraestatales.
16. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.
17. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
18. Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional.
19. Plan Nacional de Desarrollo 2007-2012.
20. Programa Especial de Mejora de la Gestión en la Administración Pública Federal 2008-2012, publicado en el Diario Oficial de la Federación el 10 de noviembre de 2008.
21. Decreto que establece las medidas de austeridad y disciplina del gasto de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 4 de diciembre de 2006.
22. Lineamientos Específicos para la Aplicación y Seguimiento de las Medidas de Austeridad y Disciplina del Gasto de la Administración Pública Federal; publicado en el Diario Oficial de la Federación el 29 de diciembre de 2006.
23. Acuerdo por el que se adicionan y modifican los lineamientos específicos para la aplicación y seguimiento de las medidas de austeridad y disciplina del gasto de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 14 de mayo de 2007.
24. Lineamientos de Protección de Datos Personales, publicado en el Diario Oficial de la Federación el 30 de septiembre de 2005.
25. Recomendaciones sobre medidas de Seguridad aplicables a los Sistemas de Datos Personales, emitidos por el entonces Instituto Federal de Acceso a la Información.
26. Acuerdo por el que se da a conocer la Agenda de Gobierno Digital, publicado en el Diario Oficial de la Federación el 16 de enero de 2009.
27. Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011.

## 5. PROCESOS EN MATERIA DE TIC Y DE SEGURIDAD DE LA INFORMACION

El presente Manual contiene la estrategia para armonizar y homologar las actividades de las Instituciones en materia de TIC y de seguridad de la información, agrupadas en 29 procesos que conforman el Marco rector de procesos, el cual se muestra en la siguiente figura:




## 5.1 DR - DIRECCION Y CONTROL DE TIC

### 5.1.1 EMG – Establecimiento del modelo de gobierno de TIC

#### 5.1.1.1 Objetivos del proceso

**General:**

Establecer un modelo de gobierno de TIC en la Institución, mediante la conformación de dos grupos de trabajo para efectuar, entre otras acciones, el análisis de las oportunidades de aprovechamiento de las TIC y asegurar la adecuada organización al interior de la UTIC para la gestión de sus procesos.

**Específicos:**

1. Establecer un modelo de gobierno de TIC.
2. Establecer y mantener al interior de la UTIC los roles definidos en el "Marco rector de procesos".
3. Operar y mantener un modelo de gobierno de las TIC, a fin de:
   a) 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 servicios de TIC.
   b) Asegurar que la asignación de roles a quienes integran el Recurso humano en la UTIC, permita la gestión eficiente de los procesos indicados en el presente Manual.

| 5.1.1.2 | **Descripción del proceso** |
|---|---|

| 5.1.1.2.1 | **Descripción de las actividades del proceso** |
|---|---|

**EMG- 1** a

**EMG- 2** ...

| **EMG-3** | **Operar y mantener el modelo de gobierno de TIC** |
|---|---|
| **Descripción** | ... |
| **Factores críticos** | **El Grupo de trabajo para la dirección de TIC deberá:**<br>1. a 3. ...<br>4. Aprobar el sistema de gestión y mejora de los procesos de la UTIC, así como los indicadores del Cuadro de mando integral de la UTIC.<br>5. Establecer la coordinación necesaria con el Responsable de seguridad de la información para armonizar el gobierno de TIC, la administración de riesgos y el SGSI.<br>6. Conocer los criterios técnicos que proponga el Responsable de la seguridad de la información en la Institución para gestionar los riesgos.<br>**El Responsable de este proceso deberá:**<br>7. Informar al Titular de la Institución acerca de los resultados, recomendaciones y acuerdos del Grupo de trabajo para la dirección de TIC. |

**5.1.1.2.2** a

**5.1.1.3** ...

| **5.1.1.4** | **Reglas del proceso** |
|---|---|
| 1.1 | ... |
| 1.2 | Los roles que se señalan en cada uno de los procesos de este Manual, con excepción de los mencionados en los procesos ASI- Administración de la seguridad de la información y OPEC- Operación de los controles de seguridad de la información y del ERISC, serán asignados a los servidores públicos de la UTIC en este proceso. Para cualquier cambio en su asignación será necesario considerar los resultados del proceso OSGP- Operación del sistema de gestión y mejora de los procesos de la UTIC. |
| 1.3 | Los servidores públicos de la UTIC, así como los de otras áreas o 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 señalan para dichos roles. |
| 1.4 | El Grupo de trabajo para la dirección de TIC deberá apoyar la implantación, operación y mejora del SGSI, así como las acciones que realice el Grupo de trabajo estratégico de seguridad de la información. |

**5.1.2** a

**5.1.3.4** ...

| 5.1.4 | AE - Administración de la evaluación de TIC |
|---|---|

| 5.1.4.1 | Objetivos del proceso |
|---|---|

**General:**

Establecer mecanismos de seguimiento y evaluación de la ejecución de la planeación estratégica de TIC, así como acciones de mejora a partir de sus resultados.

**Específicos:**

1. Establecer un sistema que permita evaluar la operación y servicios de TIC, mediante la definición de indicadores y el seguimiento a éstos.
2. Proporcionar informes de resultados de la operación de los procesos y de los servicios de TIC, así como del avance en el cumplimiento de objetivos.
3. Establecer acciones de mejora para prevenir o corregir desviaciones, así como dar seguimiento a las mismas.

| 5.1.4.2 | Descripción del proceso |
|---|---|

| 5.1.4.2.1 | Descripción de las actividades del proceso |
|---|---|

| AE-1 | Establecer el sistema de evaluación de TIC |
|---|---|

| Descripción | Establecer los indicadores que integrarán el sistema de evaluación de TIC. |
|---|---|
| **Factores críticos** | **El Responsable del sistema de evaluación de TIC, con apoyo de los Responsables de los procesos del "Marco rector de procesos", deberá:**<br>1. Integrar el Documento de indicadores del sistema de evaluación de TIC, considerando los siguientes elementos:<br>a) Los indicadores de los procesos del Manual.<br>b) El diseño de indicadores para medir: proyectos y servicios de TIC; reducción de costos; satisfacción de los usuarios; niveles de servicio y cumplimiento de los Objetivos estratégicos de TIC.<br>c) Los insumos que este proceso requiere de los demás procesos del Manual y los productos a entregar al proceso OSGP- Operación del sistema de gestión y mejora de los procesos de la UTIC.<br>d) La forma de operar del sistema.<br>2. Obtener la aprobación del Responsable de este proceso para el establecimiento del sistema de evaluación de TIC.<br>3. Revisar, al menos una vez al año, el diseño de los indicadores y forma de operar del sistema de evaluación de TIC, de manera que se asegure su consistencia e integralidad.<br>4. Difundir el Documento de indicadores del sistema de evaluación de TIC entre el Recurso humano en la UTIC y usuarios involucrados.<br>5. Sensibilizar al Recurso humano en la UTIC y usuarios sobre la importancia de la evaluación de TIC a través de los indicadores establecidos. |

| AE-2 | **Alinear los insumos y las métricas** |
|---|---|
| **Descripción** | Establecer los insumos y las métricas de cada indicador de proyectos y servicios de TIC, de manera que sean consistentes con los indicadores de los procesos del presente Manual. |
| **Factores críticos** | **El Responsable del sistema de evaluación de TIC deberá:**<br>1. Identificar los insumos y las métricas de los indicadores.<br>2. Establecer, para cada métrica, su identificación y características: nombre, categoría, unidad de medida, periodicidad de recolección, valores máximos y mínimos; responsable del diseño de cada métrica e indicador, entre otros atributos de las métricas.<br>3. Especificar las fórmulas de cálculo de las métricas y los indicadores.<br>4. Establecer los valores máximos y mínimos de cada nivel de desempeño de los indicadores.<br>5. Integrar las definiciones de los factores anteriores en el Documento de métricas y fórmulas de cálculo del sistema de evaluación de TIC.<br>6. Obtener del Titular de la UTIC la aprobación del Documento de métricas y fórmulas de cálculo del sistema de evaluación de TIC.<br>7. Difundir el Documento de métricas y fórmulas de cálculo del sistema de evaluación de TIC entre el Recurso humano en la UTIC y usuarios involucrados.<br>8. Verificar la vigencia de las métricas al menos una vez al año. |

| AE-3 | **Especificar los mecanismos de recolección y almacenamiento** |
|---|---|
| **Descripción** | Identificar las fuentes de los datos que son insumo de las métricas y establecer cómo se obtienen y almacenan. |
| **Factores críticos** | **El Responsable del sistema de evaluación de TIC deberá:**<br>1. Integrar el Documento de mecanismos de recolección y almacenamiento de datos, con los elementos siguientes:<br>a) Identificación de las fuentes de los datos: el proceso que provee el dato, el responsable que provee el dato, la periodicidad con la que se provee el dato y la forma en que éste se entrega.<br>b) Definición e implantación de las Herramientas para la recolección y almacenamiento de datos.<br>2. Verificar que la totalidad de las métricas cuentan con una fuente de datos.<br>3. Obtener la aprobación del Titular de la UTIC del Documento de mecanismos de recolección y almacenamiento de datos.<br>4. Difundir el Documento de mecanismos de recolección y almacenamiento de datos, entre el Recurso humano en la UTIC y usuarios involucrados.<br>5. Revisar y, en su caso, actualizar métricas e indicadores al menos una vez al año. |

| AE-4 | **Especificar los métodos de análisis** |
|---|---|
| **Descripción** | Especificar los métodos para el análisis y reporte de los datos del sistema de evaluación de TIC. |
| **Factores críticos** | **El Responsable del sistema de evaluación de TIC deberá:**<br>1. Seleccionar métodos y herramientas para el análisis de datos e integrarlos en el Documento de Métodos de análisis del sistema de evaluación de TIC, considerando:<br>a) La naturaleza de los datos que serán insumo del sistema, de manera que permitan el cálculo y análisis de métricas e indicadores.<br>b) La forma y plazos en que se revisarán los métodos seleccionados.<br>c) Que las Herramientas de análisis de datos permitan una elaboración ágil de los Informes de medición y análisis.<br>2. Especificar y priorizar los requerimientos de información y reportes que deban generarse.<br>3. Definir el contenido y formato de la información requerida por los métodos de análisis seleccionados.<br>4. Efectuar, al menos una vez al año, la revisión de métricas, indicadores, informes y de la forma para evaluar los resultados del análisis de datos, así como de los informes establecidos. |

| AE-5 | **Establecer el Repositorio de métricas** |
|---|---|
| **Descripción** | Establecer y mantener actualizado el Repositorio de métricas del sistema de evaluación de TIC. |
| **Factores críticos** | **El Responsable del sistema de evaluación de TIC deberá:**<br>1. Determinar las necesidades de almacenamiento y recuperación de métricas.<br>2. Diseñar e implantar el Repositorio de métricas como un componente del sistema de conocimiento, de acuerdo al proceso ACNC- Administración del conocimiento.<br>3. Especificar la forma en que se almacenarán, actualizarán y recuperarán las métricas y la información para interpretarlas y evaluarlas.<br>4. Mantener disponible y actualizado el Repositorio de métricas, con la información que se genere por las actividades del presente proceso.<br>5. Revisar, al menos una vez al año, la integridad de la información contenida en el Repositorio de métricas. |

| AE-6 | **Recolectar y revisar los datos insumo para las métricas** |
|---|---|
| **Descripción** | Obtener los datos que son insumo para las métricas y analizar e interpretar los mismos. |
| **Factores críticos** | **El Analista de evaluación de TIC deberá:**<br>1. Extraer del Repositorio de métricas los datos de insumo para las métricas.<br>2. Revisar la integridad y exactitud de los datos de insumo.<br>3. Analizar e interpretar los datos.<br>4. Almacenar datos e información de acuerdo con lo señalado en las actividades AE-3 y AE-5 de este proceso.<br>5. Integrar el Reporte de resultados de la revisión, el cual deberá contener la lista de verificación de los datos insumo para la totalidad de las métricas, de acuerdo a los |

| | |
|---|---|
| | resultados del análisis y la interpretación de los datos. |
| **AE-7** | **Elaborar Informes de medición y análisis** |
| **Descripción** | Elaborar los informes de resultados de la evaluación de la ejecución de la planeación estratégica de TIC. |
| **Factores críticos** | **El Analista de evaluación de TIC deberá:**<br>1. Elaborar los Informes de medición y análisis de manera que muestren:<br>a) El resultado del análisis de los datos de insumo para las métricas y el cálculo de indicadores.<br>b) Los riesgos relacionados con la capacidad de desarrollo de soluciones tecnológicas, la entrega de servicios de TIC y el nivel de cumplimiento de los objetivos de los procesos.<br>c) La interpretación de los resultados.<br>d) Las conclusiones de la medición efectuada, incluyendo el impacto en los servicios de TIC, los activos de TIC y los procesos.<br>2. Desarrollar, en caso de ser necesario, análisis complementarios, preparar los resultados e integrar éstos a los Informes de medición y análisis.<br>3. Obtener el visto bueno del Responsable del sistema de evaluación de TIC, para su presentación a los Responsables de los procesos del presente Manual. |

| | |
|---|---|
| **AE-8** | **Comunicar resultados a los grupos de trabajo y al Recurso humano en la UTIC involucrado** |
| **Descripción** | Mantener informados al Grupo de trabajo para la dirección de TIC y a los grupos de trabajo de la UTIC, de los resultados de la evaluación de la ejecución de la planeación estratégica de TIC. |
| **Factores críticos** | **El Analista de evaluación de TIC deberá:**<br>1. Consolidar los datos relevantes que muestren el grado en el que se están cumpliendo los proyectos y servicios de TIC, en informes ejecutivos de evaluación de TIC, que reflejen el impacto de la gestión.<br>2. Integrar los controles y acciones realizadas para la mitigación de los riesgos identificados en la UTIC.<br>3. Mostrar en el Cuadro de mando integral de la UTIC los resultados de los indicadores.<br>4. Obtener del Responsable del sistema de evaluación de TIC, la aprobación de los resultados consolidados de los informes ejecutivos.<br>**El Responsable del sistema de evaluación de TIC deberá:**<br>5. Elaborar las conclusiones finales sobre el impacto a los procesos, proyectos, recursos y servicios de TIC.<br>6. Dar a conocer, en forma oportuna y confiable los Informes ejecutivos de evaluación de TIC, a los Responsables de los procesos de la UTIC y a los miembros de los |

| | |
|---|---|
| | grupos de trabajo establecidos en cada proceso, así como las acciones que se realizaron para mitigar los riesgos que se materializaron. |

| **AE-9** | **Implementar acciones de mejora** |
|---|---|
| **Descripción** | Identificar desviaciones y oportunidades de mejora en los proyectos y servicios de TIC, con base en los Informes ejecutivos de evaluación de TIC, para definir e implementar las acciones correctivas y preventivas. |
| **Factores críticos** | **El Responsable del sistema de evaluación de TIC deberá:**<br>1. Identificar desviaciones y oportunidades de mejora, con base en los Informes ejecutivos de evaluación de TIC.<br>2. Determinar, con la participación del Recurso humano en la UTIC involucrado, las acciones correctivas y preventivas e integrarlas en el Programa de mejora, incorporando actividades para revisiones periódicas.<br>3. Definir los resultados esperados de la implementación del Programa de mejora.<br>4. Coordinar a los involucrados en la ejecución del Programa de mejora.<br>5. Evaluar los resultados del Programa de mejora y comunicar al Titular de la UTIC y a los responsables de proyectos y servicios de TIC dichos resultados y su evaluación, que incluirá:<br>a) El comparativo de los resultados esperados y de los obtenidos.<br>b) Las lecciones aprendidas.<br>c) Las conclusiones documentadas. |

| **5.1.4.2.2** | **Relación de productos** |
|---|---|
| 1.1 | "Documento de Indicadores del sistema de evaluación de TIC", formato sugerido: anexo 4, formato 1. |
| 1.2 | "Documento de métricas y fórmulas de cálculo del sistema de evaluación de TIC", formato sugerido: anexo 4, formato 2. |
| 1.3 | "Documento de mecanismos de recolección y almacenamiento de datos", formato sugerido: anexo 4, formato 3. |
| 1.4 | "Herramientas para la recolección y almacenamiento de datos", definidas por la Institución. |
| 1.5 | "Documento de métodos de análisis del sistema de evaluación de TIC", conforme al formato que defina la Institución. |
| 1.6 | "Herramientas de análisis de datos", definidas por la Institución. |
| 1.7 | "Repositorio de métricas", definido por la Institución. |
| 1.8 | "Reporte de resultados de la revisión", formato sugerido: anexo 4, formato 4. |
| 1.9 | "Informes de medición y análisis", formato sugerido: anexo 4, formato 5. |
| 1.10 | "Informes ejecutivos de evaluación de TIC", formato sugerido: anexo 4, formato 6. |
| 1.11 | "Programa de mejora", formato sugerido: anexo 4, formato 7. |

| **5.1.4.2.3** | **Relación de roles** |
|---|---|

| | |
|---|---|
| 1.1 | Responsable del proceso AE- "Administración de la evaluación de TIC". |
| 1.2 | Responsable del sistema de evaluación de TIC. |
| 1.3 | Analista de evaluación de TIC. |
| **5.1.4.3** | **Indicadores del proceso** |

| Nombre | Objetivo | Descripción | Clasificación | Fórmula | Responsable | Frecuencia de cálculo |
|---|---|---|---|---|---|---|
| Resultado del sistema de evaluación de TIC. | Conocer la eficiencia con la que está operando el sistema de evaluación de TIC. | Medir las desviaciones y oportunidades de mejora resueltas por medio del sistema de evaluación de TIC. | Dimensión: Eficiencia.<br>Tipo:<br>De gestión. | % de eficiencia= (Desviaciones y oportunidades de mejora resueltos por medio del sistema de evaluación de TIC / Desviaciones y oportunidades de mejora identificados por medio del sistema de evaluación de TIC) X 100 | El Responsable del sistema de evaluación de TIC. | Semestral. |

| | |
|---|---|
| **5.1.4.4** | **Reglas del proceso** |
| 1.1 | El Titular de la UTIC es el Responsable de este proceso. |
| 1.2 | El Responsable de este proceso, a través del Responsable del sistema de evaluación de TIC deberá asegurarse que el sistema de evaluación de TIC sea consistente con los demás sistemas de evaluación de la Institución. |

| | |
|---|---|
| **5.2** | **DCSI – DIRECCION Y CONTROL DE LA SEGURIDAD DE LA INFORMACION** |

| | |
|---|---|
| **5.2.1** | **ASI – Administración de la seguridad de la información** |

| | |
|---|---|
| **5.2.1.1** | **Objetivos del proceso** |

**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.

**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.<br>7. Fomentar una cultura de Seguridad de la información en la Institución. |

| | |
|---|---|
| **5.2.1.2** | **Descripción del proceso** |

| | |
|---|---|
| **5.2.1.2.1** | **Descripción de las 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 implantación y adopción del modelo de gobierno de seguridad de la información en la Institución. |
| **Factores críticos** | **Al Titular de la Institución le corresponderá:**<br>1. Designar al Responsable de la seguridad de la información en la Institución, quien deberá tener nivel jerárquico mínimo de Director General o equivalente.<br>**El Responsable de la seguridad de la información en la Institución deberá:**<br>2. Establecer el Grupo de trabajo estratégico de seguridad de la información, 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 de trabajo estratégico de seguridad de la información, y asegurarse de que:<br>a) 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.<br>b) Se comuniquen los roles y responsabilidades de los integrantes del Grupo de trabajo estratégico de seguridad de la información.<br>3. Encabezar el Grupo de trabajo estratégico de seguridad de la información y dar seguimiento a las acciones establecidas en el mismo. |

| | |
|---|---|
| **ASI-2** | **Operar y mantener el modelo de gobierno de seguridad de la información** |
| **Descripción** | Institucionalizar prácticas para asegurar la implantación, seguimiento y control de la seguridad de la información en la Institución. |
| **Factores críticos** | **El Grupo de trabajo estratégico de seguridad de la información deberá:**<br>1. Coordinar la elaboración y actualización del Catálogo de infraestructuras críticas de la Institución.<br>2. Establecer, conjuntamente con los Responsables de los grupos de procesos PR, AS, TE, OS, AA y OP, así como en su caso con los servidores públicos que administren Activos de información, los mecanismos para garantizar la protección de las Infraestructuras críticas que éstos tengan bajo su responsabilidad.<br>3. Vigilar que los controles de seguridad de la información que se definan e implanten, consideren los mecanismos establecidos en el factor crítico anterior, así como el Análisis de riesgos que se realiza en la actividad ASI-6.<br>4. Constatar que se efectúe la implantación de 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.<br>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 de trabajo estratégico de seguridad de la información deberá:<br>1 Diseñar, en coordinación con las diferentes áreas y unidades administrativas de la Institución, la Estrategia de seguridad de la información que será implantada 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:<br>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.<br>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.<br>c) Generar las estrategias específicas de seguridad de la información, que permitan cumplir con la misión, visión y objetivos de la Institución.<br>d) Desarrollar reglas técnicas para verificar que los controles de seguridad de la información que se definan operen según lo esperado.<br>e) Definir métricas para evaluar el grado de cumplimiento de los requerimientos de seguridad identificados para los Activos de información.<br>f) Elaborar las reglas técnicas que contengan las acciones para la adecuada operación del SGSI.<br>2. Integrar, con la información del factor crítico anterior, el Documento de definición del SGSI y el Programa de implantación del SGSI.<br>El Responsable de la seguridad de la información de la Institución deberá:<br>3. Someter a la consideración del Titular de la Institución el Documento de definición del SGSI y su Programa de implantación.<br>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.<br>5. Dar a conocer el SGSI y su programa de implantación a los servidores públicos de la Institución involucrados con el mismo.<br>El Grupo de trabajo estratégico de seguridad de la información deberá:<br>6. Elaborar el Programa de evaluaciones del SGSI y difundirlo en la Institución.<br>7. Elaborar, probar y mantener actualizada una Directriz rectora de respuesta a incidentes, en coordinación con el ERISC, ésta deberá contener al menos:<br>a) El rol y el servidor público asignado a éste, quien puede iniciar las tareas de respuesta a incidentes.<br>b) El mecanismo de notificación, escalamiento y atención de incidentes en la Institución.<br>c) Los mecanismos de interacción con otras instituciones o entidades externas.<br>d) Los criterios técnicos de obtención de indicios, preservación de evidencias, e investigación de incidentes, considerando lo establecido en las disposiciones jurídicas aplicables.<br>e) Los elementos del Programa de contingencia a los Activos de información que son sustantivos para el cumplimiento de la misión, visión y los objetivos institucionales.<br>8. Asegurarse de que la información obtenida de los factores críticos anteriores se integre en el Documento de definición del SGSI y éste se mantenga actualizado.<br>El Responsable de la seguridad de la información de la Institución deberá:<br>9. Hacer de conocimiento del órgano interno de control de la Institución y/o, cuando corresponda, de las autoridades que resulten competentes, el incumplimiento al SGSI para el 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 de trabajo estratégico de seguridad de la información deberá:<br>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 éste, debiendo asegurarse de que:<br>a) Se formalice el establecimiento del Equipo, mediante el Documento de integración del equipo de trabajo de infraestructuras críticas, y que éste contenga al menos: los objetivos y responsabilidades del Equipo; roles y responsabilidades de cada miembro, así como el funcionamiento del mismo.<br>b) Se comunique la integración del Equipo así como los roles y responsabilidades de los integrantes del mismo.<br>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.<br>d) Los integrantes del Equipo de trabajo tengan un concepto claro y uniforme con respecto de 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.<br>El Equipo de trabajo de infraestructuras críticas, en la identificación de Infraestructuras críticas y Activos clave, deberá:<br>2. Identificar procesos críticos de la Institución, mediante las ejecución de las siguientes acciones:<br>a) Analizar los procesos existentes y determinar cuáles de éstos son críticos, 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:<br>i. Proveedores del proceso.<br>ii. Insumos del proceso.<br>iii. Eventos de inicio que disparan la ejecución del proceso.<br>iv. Subprocesos o actividades que lo conforman.<br>v. Actores que intervienen en su ejecución.<br>vi. Productos o servicios que genera.<br>vii. Evento de fin del proceso.<br>viii. Clientes o usuarios del proceso.<br>ix. Activos de información involucrados en el proceso.<br>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.<br>3. Identificar, a partir de los procesos críticos determinados en el factor crítico anterior, aquéllos 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 4 a 15 restantes, debiendo dar inicio a la actividad ASI-5. |

4. Obtener un listado de los procesos críticos de la institución e integrar la información de los factores críticos 2 y 3 anteriores en el Documento de identificación de infraestructuras críticas.

5. Identificar las actividades críticas de los procesos contenidos en el Documento de identificación de infraestructuras críticas, 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) Determinar las actividades que resultan críticas para la operación del proceso.

   c) Integrar en el Documento de identificación de infraestructuras críticas, los datos obtenidos de los incisos anteriores.

6. 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.

   e) Registrar los datos obtenidos de los incisos anteriores en el Documento de identificación de infraestructuras críticas.

7. Efectuar la valoración de los Activos de información, en términos de la posible pérdida de su confidencialidad, integridad o disponibilidad, para identificar aquéllos que deban considerarse como Activos de información clave y registrar los resultados de la valoración efectuada en el documento de Matrices de infraestructuras críticas y activos clave.

8. Utilizar como parámetros para identificar la criticidad de una infraestructura, los tipos de impacto potencial que podrían ocurrir ante la presentación de un incidente. Estos se deberán representar en las matrices de impacto que forman parte del documento denominado Matrices de infraestructuras críticas y activos clave.

9. 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, en el documento de Matrices de infraestructuras críticas y activos clave.

10. Revisar los resultados obtenidos y los documentos generados en los factores críticos anteriores.

El Grupo de trabajo estratégico de seguridad de la información deberá:

11. Verificar los resultados obtenidos y documentos generados por el Equipo de trabajo de infraestructuras críticas, y constatar que las infraestructuras críticas que se hubieren identificado efectivamente tengan ese carácter.

| | |
|---|---|
| | El Grupo de trabajo estratégico de seguridad de la información, con apoyo del Equipo de trabajo de infraestructuras críticas, deberá:<br>12. Elaborar el Catálogo de infraestructuras críticas, con base en la información contenida en el Documento de identificación de infraestructuras críticas y en el de Matrices de infraestructuras críticas y activos clave, y realizar las siguientes acciones:<br>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.<br>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.<br>c) Incluir en el Catálogo de infraestructuras críticas un mapa de localización geográfica, en donde se muestre la ubicación de las diversas infraestructuras críticas.<br>El Responsable de la seguridad de la información de la Institución deberá:<br>13. Presentar a la aprobación del Titular de la Institución, el Catálogo de infraestructuras críticas.<br>14. 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.<br>El Grupo de trabajo estratégico de seguridad de la información deberá:<br>15. 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 | Establecer la Directriz rectora para la administración de riesgos |
| Descripción | Definir y difundir la Directriz rectora para la administración de riesgos. |
| Factores críticos | El Grupo de trabajo estratégico de seguridad de la información, deberá:<br>1. Elaborar la Directriz rectora para la administración de riesgos, mediante las siguientes acciones:<br>a) Integrar los antecedentes y demás elementos que justifiquen la necesidad de implantar la administración de riesgos en la Institución.<br>b) Definir metodologías y herramientas que se usarán para administrar los Riesgos.<br>c) Integrar el marco normativo que resulte aplicable a los Riesgos identificados.<br>d) Establecer las reglas para medir la efectividad de los controles en la gestión de los riesgos.<br>e) Establecer 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.<br>f) Establecer consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas de la Institución. |

| | |
|---|---|
| | 2. Verificar que la Directriz rectora para la administración de riesgos permanezca actualizada, mediante las siguientes acciones:<br>a) La revisión de su adecuada alineación con el Modelo de gobierno de seguridad de la información.<br>b) La evaluación de las acciones adoptadas por incumplimientos detectados en la administración de los riesgos.<br>c) La revisión de los formatos de los reportes de ASI-6, al menos cada seis meses.<br>El Responsable de la Seguridad de la Información deberá:<br>3. Autorizar la Directriz rectora para la administración de riesgos.<br>4. Difundir la Directriz rectora para la administración de riesgos y sus actualizaciones a los involucrados y a los integrantes del Grupo de trabajo para la dirección de TIC, a fin de que sea conocida por los mismos.<br>El Grupo de trabajo estratégico de seguridad de la información, deberá:<br>5. Establecer el Repositorio de riesgos e integrar la información de la Directriz rectora para la administración de riesgos. |

| | |
|---|---|
| ASI-6 | 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 de trabajo estratégico de seguridad de la información deberá:<br>1. Integrar el Equipo de trabajo de análisis de riesgos, mediante la elaboración del Documento de integración del equipo de trabajo de análisis de riesgos, y asegurarse de que:<br>a) El Documento contenga, al menos: los objetivos y responsabilidades del Equipo de trabajo, los roles y responsabilidades de cada miembro así como el funcionamiento del Equipo.<br>b) El Equipo se conforme con un número de entre 5 y 10 integrantes, quienes preferentemente deberán ser servidores públicos con conocimientos en materia de TIC, de seguridad de la información, de seguridad física y por aquéllos que se considere puedan aportar al Equipo mayor capacidad de análisis y alcance de objetivos.<br>c) Los integrantes del Equipo cuenten con al menos un año de experiencia y conocimientos en el área en la cual se desempeñan.<br>d) Se delimite el objetivo y alcance del Análisis de riesgos que se efectuará por el Equipo de trabajo.<br>2. Seleccionar al líder del Equipo y hacer de su conocimiento que su rol será el de interpretar y difundir instrucciones, coordinar tareas y materializar resultados.<br>3. Integrar la información de los factores críticos anteriores en el Documento de integración del equipo de trabajo de análisis de riesgos. |

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

4. Elaborar el Documento de identificación de procesos críticos, integrando en éste la información siguiente:

   a) La de aquellos procesos de los que la Institución depende 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.

5. Identificar los Activos de información e incluirlos en una relación detallada que se incorporará en el Documento de identificación de activos de información.

6. Consultar a los responsables de los Activos de información, para identificar los elementos que se pretende proteger ante la posible materialización de Amenazas e integrar la información obtenida en el Documento de identificación de activos de información.

7. Identificar las Vulnerabilidades, mediante las acciones siguientes:

   a) Elaborar una relación de las características de los Activos de información, así como del ambiente y de la Institución en que se ubican los mismos, que pudieran ser aprovechadas para poner en riesgo la confidencialidad, integridad y disponibilidad de estos.

   b) Considerar como vulnerabilidad la ausencia y 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.

8. Identificar Amenazas, mediante las acciones siguientes:

   a) Elaborar el Documento de identificación de amenazas, registrando las posibles Amenazas que, en caso de materializarse, tendrían efectos negativos sobre la seguridad en uno o varios de los Activos de información contenidos en el Documento de identificación de activos de información.

   b) Identificar y registrar en el documento del inciso anterior, los agentes que podrían materializar una Amenaza, utilizando la Lista de amenazas y agentes que se provee en el formato del mismo.

9. Elaborar el Documento de identificación y evaluación de escenarios de riesgo, en el que se deberán registrar y evaluar los escenarios de riesgo que se identifiquen, mediante las acciones siguientes:

   a) Definir los escenarios, 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) Integrar las variables complementarias que se indican en el formato del Documento de identificación de amenazas y sus ponderaciones, ya que éstas determinan el valor final del Riesgo, utilizando la tabla denominada "Probabilidad de ocurrencia contra impacto", que se contiene en el formato del documento mencionado.

   c) Definir la estrategia de seguridad para cada Riesgo, seleccionando alguna de las establecidas en el formato del Documento de identificación de amenazas: 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.

10. Elaborar el Análisis de 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) Utilizar el Documento de análisis de costo-beneficio de controles de seguridad, debiendo definir los valores indicados en éste, para cada escenario de riesgo

11. 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 implantación.

    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 obtenidas.

    e) Elaborar e incluir en el Documento de resultados del análisis de riesgos, la propuesta de Programa de contingencia a los riesgos, considerando, de ser el caso, la intervención del ERISC.

12. Obtener del Grupo de trabajo 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:

13. Seleccionar de entre los controles recomendados por el Grupo de trabajo estratégico de seguridad de la información, contenidos en el Documento de resultados del análisis de riesgos, aquéllos a implantar de acuerdo a las capacidades y recursos de las áreas y unidades administrativas involucradas

14. Justificar ante el Grupo de trabajo 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:

15. Elaborar el Programa de implantación para el manejo de riesgos, de acuerdo a los resultados de la selección efectuada conforme al factor crítico 13 de esta actividad. Dicho Programa deberá incluir la designación de responsables de la implantación de cada control, de acuerdo al Documento de resultados del análisis de riesgos y los datos necesarios para su implantación, así como documentarse conjuntamente con la implantación de las acciones y controles del SGSI.

16. Obtener del Grupo de trabajo estratégico de seguridad de la información la aprobación del Programa de implantación para el manejo de riesgos y verificar su adecuada integración con las demás actividades de implantación o mejora de los controles y acciones del SGSI.

| | |
|---|---|
| | El Grupo de trabajo estratégico de seguridad de la información deberá:<br>17. 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.<br>18. Asegurar que se obtengan los productos de esta actividad actualizados y se documente, en caso de ser procedente, la mejora continua que se efectúe derivada del factor crítico anterior.<br>19. Vigilar que se actualice el Repositorio de riesgos. |

| | |
|---|---|
| **ASI-7** | **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 implantación a través de los diversos procesos del Manual. |
| **Factores críticos** | El Grupo de trabajo estratégico de seguridad de la información, con apoyo de las áreas y unidades administrativas competentes de la Institución, deberá:<br>1. Definir los controles de seguridad necesarios para salvaguardar a los Activos de TIC, las Infraestructuras críticas y los Activos de información de la Institución, proporcionales a su valor e importancia, siendo como mínimo los necesarios para:<br>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.<br>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 implantados en el área o unidad administrativa de que se trate.<br>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.<br>d) El ingreso y salida de Activos de información.<br>e) El borrado seguro de dispositivos de almacenamiento que por algún motivo necesiten ser reparados, reemplazados o asignados a otro usuario.<br>f) Evitar el daño, pérdida, robo, copia y acceso no autorizados a los Activos de información.<br>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.<br>h) Los criterios de asignación de Usuarios y contraseñas permitidas para los diversos componentes de los dominios tecnológicos.<br>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.<br>k) La seguridad física y lógica que permita mantener la confidencialidad, integridad y disponibilidad de los respaldos de información.<br>l) El uso del servicio de Internet en la institución, el cual debe contar con herramientas de seguridad y de filtrado de contenido.<br>m) El intercambio seguro de la información, ya sea de manera interna o hacia el exterior.<br>n) Que la información clasificada o aquélla que tiene valor para la institución, sea respaldada y restaurada en el momento en que se requiera.<br>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.<br>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 implantación del SGSI. |

| | |
|---|---|
| **ASI-8** | **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 de trabajo estratégico de seguridad de la información deberá:<br>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.<br>2. Obtener, del Informe de 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 Acciones preventivas y correctivas al SGSI.<br>3. Elaborar el Documento de implantación de la mejora al SGSI. Este documento debe utilizarse para la planeación y el seguimiento de las acciones de mejora, ya sean preventivas o correctivas.<br>4. Comunicar las mejoras que deberán aplicarse al SGSI al Responsable del grupo de trabajo para la implantación de la seguridad de la información, previsto en la actividad OPEC-1, por medio de los productos: Acciones preventivas y correctivas al SGSI y el Documento de implantación al SGSI.<br>5. Vigilar la implantación de las mejoras mediante el informe de seguimiento a las acciones de mejora al SGSI. |

| | |
|---|---|
| **5.2.1.2.2** | **Relación de productos** |
| 1.1. | "Documento de integración y operación del grupo de trabajo estratégico de seguridad de la información", formato sugerido: anexo 5, formato 1. |
| 1.2 | "Directriz rectora para la administración de riesgos", formato sugerido: anexo 5, formato 2. |
| 1.3 | "Documento de integración del equipo de trabajo de infraestructuras críticas", formato sugerido: anexo 5, formato 3. |

| | |
|---|---|
| 1.4 | "Documento de identificación de infraestructuras críticas", formato sugerido: anexo 5, formato 4. |
| 1.5 | "Matrices de infraestructuras críticas y activos clave", formato sugerido: anexo 5, formato 5. |
| 1.6 | "Catálogo de infraestructuras críticas", formato sugerido: anexo 5, formato 6. |
| 1.7 | "Documento de integración del equipo de trabajo de análisis de riesgos", formato sugerido: anexo 5, formato 7. |
| 1.8 | "Documento de identificación de procesos críticos", formato sugerido: anexo 5, formato 8. |
| 1.9 | "Documento de identificación de activos de información", formato sugerido: anexo 5, formato 9. |
| 1.10 | "Documento de identificación de amenazas", formato sugerido: anexo 5, formato 10. |
| 1.11 | "Documento de identificacion y evaluación de escenarios de riesgo", formato sugerido: anexo 5, formato 11. |
| 1.12 | "Documento de análisis de costo-beneficio de controles de seguridad", formato sugerido: anexo 5, formato 12. |
| 1.13 | "Declaraciones de aplicabilidad", formato sugerido: anexo 5, formato 13. |
| 1.14 | "Programas de mitigación de riesgos", formato sugerido: anexo 5, formato 14. |
| 1.15 | "Programa de contingencia a los riesgos", formato sugerido: anexo 5, formato 15. |
| 1.16 | "Documento de resultados del análisis de riesgos", formato sugerido: anexo 5, formato 16. |
| 1.17 | "Programa de implantación para el manejo de riesgos", formato sugerido: anexo 5, formato 17. |
| 1.18 | "Documento de definición del SGSI", formato sugerido: anexo 5, formato 18. |
| 1.19 | "Programa de implantación del SGSI", formato sugerido: anexo 5, formato 19. |
| 1.20 | "Programa de evaluaciones del SGSI", formato sugerido: anexo 5, formato 20. |
| 1.21 | "Directriz rectora de respuesta a incidentes", formato sugerido: anexo 5, formato 21. |
| 1.22 | "Informe de evaluación del SGSI", formato sugerido: anexo 5, formato 22. |
| 1.23 | "Acciones preventivas y correctivas de mejora al SGSI", formato sugerido: anexo 5, formato 23. |
| 1.24 | "Informe de seguimiento a las acciones de mejora al SGSI", formato sugerido: anexo 5, formato 24. |
| 1.25 | "Documento de implantación de la mejora al SGSI", formato sugerido: anexo 5, formato 25. |

| 5.2.1.2.3 | Relación de roles |
|---|---|
| 1.1 | Responsable de la seguridad de la información en la institución o RSII. |
| 1.2 | Grupo estratégico de seguridad de la información o GESI. |
| 1.3 | Equipo de trabajo de infraestructuras críticas. |
| 1.4 | Equipo de trabajo de análisis de riesgos. |
| 1.5 | Equipo de respuesta a incidentes de seguridad o ERISC. |

| 5.2.1.3 | Indicadores del proceso |
|---|---|

| Nombre | Objetivo | Descripción | Clasificación | Fórmula | Responsable | Frecuencia de cálculo |
|---|---|---|---|---|---|---|
| Cumplimiento del proceso ASI-Administración de la seguridad de la información. | Obtener la eficiencia del proceso en base a su cumplimiento. | Medir el cumplimiento en la implantación de los controles establecidos durante el proceso. | Dimensión: Eficiencia. Tipo: Estratégico. | % de eficiencia= (Controles implantados / Controles programados para su implantación) * 100 | El Responsable del proceso ASI-Administración de la seguridad de la información. | Anual. |

| 5.2.1.4 | Reglas del proceso |
|---|---|
| 1.1 | El Responsable de la seguridad de la información en la institución es el responsable de este proceso. |
| 1.2 | En los casos en que el Titular de la institución tenga un nivel jerárquico equivalente o inferior a Director General, el servidor público que éste designe como Responsable de la seguridad de la información en la Institución deberá tener un nivel inmediato inferior al del Titular. |
| 1.3 | El Responsable de este proceso se deberá asegurar de 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. |
| 1.4 | En caso de que la institución cuente con Infraestructuras críticas que impactan 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 contrario que dicho análisis se oriente a sus Activos de información clave. |
| 1.5 | 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 asegurase de que éstos conozcan las reglas de operación del mismo, así como la Guía técnica de atención a incidentes. |
| 1.6 | El Responsable de la seguridad de la información de cada Institución será quien mantendrá comunicación con el Centro de Investigación y Seguridad Nacional 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. |
| 1.7 | 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. |
| 1.8 | El Grupo de trabajo estratégico de seguridad de la información deberá asegurarse de 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. |

| | |
|---|---|
| 1.9 | El Grupo de trabajo 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. |
| 1.10 | 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. |
| 1.11 | El Grupo de trabajo 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. |
| 1.12 | El Grupo de trabajo estratégico de seguridad de la información deberá coordinarse con los Responsables de los grupos de procesos PR, AD y TE, para que se implanten 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. |
| 1.13 | El Grupo de trabajo estratégico de seguridad de la información deberá coordinarse con los Responsables de los grupos de procesos PR y AD, para que se implanten 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. |
| 1.14 | El Grupo de trabajo estratégico de seguridad de la información deberá constatar que, como parte de los mecanismos que se establezcan para el ambiente operativo, se implante un control para elaboración y conservación de Bitácoras de seguridad para los sistemas identificados como parte de una infraestructura crítica, en éstas 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. |
| 1.15 | El Grupo de trabajo 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. |

| | |
|---|---|
| 5.2.2 | OPEC - Operación de los controles de seguridad de la información y del ERISC |

| | |
|---|---|
| 5.2.2.1 | Objetivos del proceso |

General:

Implantar y operar los controles de seguridad de la información de acuerdo al Programa de implantación del SGSI, así como los correspondientes a la capacidad de respuesta a incidentes.

Específicos:

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

| | |
|---|---|
| 5.2.2.2 | Descripción del proceso |

| | |
|---|---|
| 5.2.2.2.1 | Descripción de las actividades del proceso |

| | |
|---|---|
| OPEC-1 | Establecer el grupo de implantación de la seguridad |
| Descripción | Conformar un grupo de trabajo para la ejecución de: Programa de implantación para el manejo de riesgos y del Programa de implantación del SGSI. |
| Factores críticos | El Responsable de la seguridad de la información, en coordinación con los Titulares de las unidades administrativas para las que se hayan definido controles de seguridad de la información, deberá:<br>1. Establecer el Grupo de trabajo para la implantación de la seguridad de la información, mediante el Documento de integración del mismo, y asegurarse de que éste contenga:<br>a) El alcance, objetivos, roles y responsabilidades del Grupo de trabajo y de sus miembros, así como el funcionamiento del Grupo.<br>b) Al servidor público responsable del Grupo de trabajo, quien será propuesto por los titulares de las unidades administrativas involucradas y aprobado por el Responsable de la seguridad de la información.<br>c) A los Responsables de los procesos de la UTIC en los cuales se deban implantar los controles que les sean indicados.<br>2. Asegurarse de que se comunique a los involucrados, el establecimiento del grupo de trabajo.<br>El Responsable del grupo de trabajo para la implantación de la seguridad de la información, deberá:<br>3. Mantener actualizada la información del Repositorio de riesgos, con la siguiente información:<br>a) La información de la Directriz rectora para la administración de riesgos.<br>b) El Programa de implantación para el manejo de riesgos y el Programa de implantación del SGSI, así como 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 deberá:<br>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 o entidades externas, en concordancia con la Directriz rectora de respuesta a incidentes, incluyendo al menos, los relativos a:<br>a) Los canales de comunicación, que deberán ser seguros.<br>b) Los relativos a la Diseminación de datos de los incidentes.<br>El ERISC deberá:<br>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 al menos los siguientes apartados:<br>a) Detección de los incidentes.<br>b) Priorización de los Incidentes.<br>c) Investigación técnica de los incidentes. |

| | |
|---|---|
| | d) Criterios técnicos de contención de los incidentes, de acuerdo a la criticidad de los Activos de TIC.<br>e) Obtención, preservación y destino de los indicios de los incidentes.<br>f) Erradicación de los incidentes.<br>g) Recuperación de la operación.<br>h) Documentación de las lecciones aprendidas.<br>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.<br>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 del grupo de trabajo para la implantación de la seguridad de la información, deberá:<br>1. Definir las acciones de atención a los incidentes con apoyo de la Guía técnica, respecto del incidente que se haya presentado.<br>2. Ejecutar la solución necesaria.<br>3. Registrar los datos del incidente y su solución.<br>4. Asegurar que se comunique el incidente y su solución, al Grupo de trabajo estratégico de seguridad de la información y a los Responsables de los dominios tecnológicos involucrados, así como a los usuarios afectados.<br>5. Integrar los datos del incidente y su solución a los repositorios de la UTIC y, en su caso, a los repositorios de la Institución que determine el Grupo de trabajo estratégico de seguridad de la información. |

| | |
|---|---|
| OPEC-4 | **Implantar los controles de mitigación de riesgos y los controles del SGSI** |
| **Descripción** | Asegurar que los controles de mitigación de riesgos y del SGSI se implanten y operen de acuerdo a su definición. |
| **Factores críticos** | El Grupo de trabajo para la implantación de la seguridad de la información, deberá:<br>1. Ejecutar el Programa de implantación para el manejo de riesgos y el Programa de implantación del SGSI, con apoyo de los titulares de las unidades administrativas en las cuales se implantarán los controles.<br>2. Dar seguimiento a la ejecución del Programa de implantación del SGSI y actualizar su estado.<br>El Responsable del grupo de trabajo para la implantación de la seguridad de la información, deberá:<br>3. Elaborar el Informe de resultados de la implantación del SGSI.<br>4. Asegurar que los controles de seguridad se hayan implantado de acuerdo a lo previsto en el Documento de definición del SGSI y el Programa de implantación del SGSI.<br>5. Elaborar los informes correspondientes a las desviaciones en la implantación y/o en la operación de los controles de seguridad.<br>6. Integrar los resultados de los factores críticos 3, 4 y 5 anteriores e incorporarlos, para efectos de su actualización, en el Programa de implantación para el manejo de riesgos y en el Programa de implantación del SGSI, y enviarlos al Grupo de trabajo estratégico de seguridad de la información. |

| | |
|---|---|
| OPEC-5 | **Implantar 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 de trabajo estratégico de seguridad de la información para su integración al SGSI, así como que se efectúe su implantación y se operen de acuerdo a su definición. |
| Factores críticos | El Responsable del proceso ADT- Administración de los dominios tecnológicos, con apoyo de los responsables de cada dominio tecnológico, deberán:<br>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.<br>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.<br>3. Implementar mecanismos de TIC para impedir la conexión a redes inalámbricas externas que se encuentren al alcance de los dispositivos electrónicos institucionales.<br>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 de trabajo estratégico de seguridad de la información.<br>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.<br>6. Instalar en los componentes de los servicios de correo electrónico, herramientas actualizadas de protección contra correos electrónicos no deseados o no solicitados.<br>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 aquellas necesarias para prevenir ataques por la vulnerabilidad que el uso de estos equipos conlleva.<br>8. Instalar mecanismos de cifrado de datos en los dispositivos electrónicos móviles que contengan información considerada como reservada o sensible para la Institución.<br>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.<br>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.<br>11. Adicionalmente al factor crítico anterior, integrar a toda solución tecnológica o servicio de TIC, adquirida o desarrollada, un módulo de control de acceso lógico que solicite como mínimo, un nombre de usuario y contraseña, cuya definición deberá aprobarse por el Grupo de trabajo estratégico de seguridad de la información. |

| | |
|---|---|
| | El Responsable del proceso ADT- Administración de los dominios tecnológicos, deberá: |
| | 12. Obtener de 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 de trabajo 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 implantado de acuerdo a lo establecido en esta actividad. |
| | 15. Dar a conocer a los Responsables de cada dominio tecnológico, la actualización que se realice al Programa de implantación para el manejo de riesgos y al Programa de implantación 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 del grupo de trabajo para la implantación de la seguridad de la información, 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 de trabajo estratégico de seguridad de la información. |
| | 2. Medir la efectividad de los controles de seguridad implantados. |
| | 3. Efectuar, con base en el Programa de evaluaciones del SGSI, la evaluación del SGSI. |
| | 4. Registrar la información de los intentos, exitosos y no exitosos, de violaciones e incidentes de seguridad, 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 informe de revisión del SGSI y enviarlo al Grupo de trabajo estratégico de seguridad de la información. |

| OPEC-7 | Aplicar al SGSI las mejoras definidas por el Grupo de trabajo 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 consecuentes, definidas por el Grupo de trabajo estratégico de seguridad de la información. |
| Factores críticos | El Grupo de trabajo para la implantación de la seguridad de la información, mediante el Documento de implantación de la mejora al SGSI, deberá: |
| | 1. Aplicar las acciones correctivas y preventivas a los controles de seguridad de la información, indicados por el Grupo de trabajo 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. |
| | El Responsable del grupo de trabajo para la implantación de la seguridad de la información, deberá: |
| | 4. Verificar el contenido del Informe de seguimiento a las acciones de mejora al SGSI; actualizar el Programa de evaluaciones del SGSI y enviarlos al Grupo estratégico de seguridad de la información para su revisión. |

| 5.2.2.2.2 | Relación de productos |
|---|---|
| 1.1 | "Documento de integración del Grupo de trabajo para la implantación de la seguridad de la información", formato sugerido: anexo 5, formato 26. |
| 1.2 | "Programa de implantación para el manejo de riesgos", formato sugerido: anexo 5, formato 12. |
| 1.3 | "Documento de definición del SGSI", formato sugerido: anexo 5, formato 17. |
| 1.4 | "Programa de implantación del SGSI", formato sugerido: anexo 5, formato 18. |
| 1.5 | "Programa de evaluaciones del SGSI" formato sugerido: anexo 5, formato 19. |
| 1.6 | "Directriz rectora de respuesta a incidentes", formato sugerido: anexo 5, formato 20. |
| 1.7 | "Informe de revisión del SGSI", formato sugerido: anexo 5, formato 27. |
| 1.8 | "Informe de seguimiento a las acciones de mejora al SGSI", formato sugerido: anexo 5, formato 23. |
| 1.9 | "Documento de implantación de la mejora al SGSI" formato sugerido: anexo 5, formato 24. |
| 1.10 | "Repositorio de riesgos de TIC", definido por la institución. |

| 5.2.2.2.3 | Relación de roles |
|---|---|
| 1.1 | Grupo de trabajo para la implantación de la seguridad de la información. |
| 1.2 | Responsable del Grupo de trabajo para la implantación de la seguridad de la información. |
| 1.3 | ERISC |

| 5.2.2.3 | Indicadores del proceso |
|---|---|

| Nombre | Objetivo | Descripción | Clasificación | Fórmula | Responsable | Frecuencia de cálculo |
|---|---|---|---|---|---|---|
| Cumplimiento de la administración de riesgos | Medir la eficiencia de la gestión del proceso. | Medir el cumplimiento en la implantación de los controles para la mitigación de riesgos establecidos durante el proceso. | Dimensión: Eficiencia.<br>Tipo:<br>De gestión. | % de eficiencia= (Controles implantados / Controles programados para su implantación) X 100 | El Responsable del proceso. | Anual. |
| Resultados del proceso OPEC-Operación de los controles de seguridad de la información y del ERISC | Medir la eficiencia del proceso. | Medir la eficiencia del proceso, mediante las mejoras que hayan sido implantadas a los controles. | Dimensión: Eficiencia.<br>Tipo:<br>De gestión. | % de eficiencia = Número de Acciones de mejora a los controles implantadas/ Número de acciones de mejora definidas) X 100 | El Responsable del proceso OPEC-Operación de los controles de seguridad de la información y del ERISC. | Anual. |

| | |
|---|---|
| 5.2.2.4 | Reglas del proceso |
| 1.1 | El Responsable del grupo de trabajo para la implantación de la seguridad de la información es el Responsable de este proceso. |
| 1.2 | Los servidores 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. |
| 1.3 | El Responsable de este proceso se deberá asegurar de 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, 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. |
| 1.4 | El Responsable de este proceso, con apoyo de la totalidad de los Responsables de los procesos de la UTIC, deberá verificar que se implanten los controles que se definan en el SGSI, en los proyectos, procesos y servicios de TIC y de la UTIC a fin de garantizar la seguridad de la información de la Institución. Asimismo, deberá constatar que se conserve la evidencia de la implantación de dichos controles. |

5.3 a

5.4.1.2 ...

| | |
|---|---|
| 5.4.1.2.1 | Descripción de las actividades del proceso |

OSGP-1 ...

| | |
|---|---|
| OSGP-2 | Establecer Reglas de adaptación |
| Descripción | ... |
| Factores críticos | El Responsable de este proceso podrá:<br>1. Elaborar y someter a la autorización del Titular de la UTIC, Reglas de adaptación que permitan no observar uno o más factores críticos de alguna actividad o, una o más actividades de un proceso, cuando tal adaptación responda a necesidades específicas de la Institución y no se afecte la consistencia y cohesión del proceso o la interrelación de éste con los demás procesos del "Marco rector de procesos".<br>El Titular de la UTIC deberá:<br>2. ...<br>a) ...<br>b) En ningún caso los procesos de los grupos: DR, DCSI y AP serán objeto de dichas Reglas.<br>c) ...<br>d) ...<br>3. a 4. ... |

OSGP-3 a

OSGP-6 ...

5.4.1.2.2 a

5.5.1.2 ...

| | |
|---|---|
| 5.5.1.2.1 | **Descripción de las actividades del proceso** |

APT-1 a

APT-2 ...

| | |
|---|---|
| **APT-3** | **Apoyar en la elaboración del anteproyecto anual de presupuesto en materia de TIC** |
| **Descripción** | ... |
| **Factores críticos** | **El Responsable del seguimiento del presupuesto, con apoyo de los Responsables de los procesos de los grupos DR, DCSI, PR, AS, AA y OP, deberá:**<br>1. a 5. ... |

5.5.1.2.2 a

5.5.2.2 ...

| | |
|---|---|
| 5.5.2.2.1 | **Descripción de las actividades del proceso** |

| | |
|---|---|
| **ADTI-1** | **Establecer un programa para las contrataciones de TIC** |
| **Descripción** | ... |
| **Factores críticos** | El Responsable de este proceso, con apoyo del Responsable del proceso APT-Administración del presupuesto de TIC y de los Responsables de los procesos de los grupos DR, DCSI, PR, AA y OP, deberá:<br>1. a 6. ... |

ADTI-2 a

ADTI-3 ...

5.5.2.2.2 a

5.6.2.2 ...

| | |
|---|---|
| 5.6.2.2.1 | **Descripción de las actividades del proceso** |

| | |
|---|---|
| **DSTI-1** | **Diseñar soluciones de servicio de TIC** |
| **Descripción** | ... |
| **Factores críticos** | ...<br>1. a 9. ...<br>10. Verificar que la solución para el servicio de TIC que se hubiere seleccionado, cumpla con los controles previstos en el proceso ASI- Administración de la seguridad de la información.<br>11. a 15. ...<br>16. Integrar el Paquete de diseño del servicio de TIC, con la información obtenida en los factores críticos anteriores. El Paquete de diseño del servicio de TIC es un insumo para los grupos de procesos AD, TE, OS y OP.<br>17. ... |

**DSTI-2** a

**DSTI-3** ...

| | |
|---|---|
| **DSTI-4** | **Administrar la disponibilidad de servicios de TIC** |
| **Descripción** | ... |
| **Factores críticos** | **El Responsable del diseño integral de los servicios de TIC, con apoyo del Grupo de trabajo de arquitectura tecnológica y de los Responsables de los procesos de los grupos DCSI, OS y OP, deberá:**<br>1. a 6. ... |

| | |
|---|---|
| **DSTI-5** | **Administrar la continuidad de servicios de TIC** |
| **Descripción** | ... |
| **Factores críticos** | **El Responsable de diseño del servicio de TIC, con apoyo del Grupo de trabajo de arquitectura tecnológica y de los Responsables de los procesos de los grupos DCSI, OS y OP, deberá:**<br>1. ...<br>2. ...<br>...<br>a) Los resultados del Análisis de impacto al negocio y la estrategia de recuperación determinada en el proceso ASI- Administración de la seguridad de la información.<br>b) a e) ...<br>3. a 13. ... |

**5.6.2.2.2** a

**5.8.4.2** ...

| | |
|---|---|
| **5.8.4.2.1** | **Descripción de las actividades del proceso** |

**ACNF-1** a

**ACNF-4** ...

| | |
|---|---|
| **ACNF-5** | **Desarrollar y controlar los almacenes y librerías de configuraciones** |
| **Descripción** | ... |
| **Factores críticos** | ...<br>1. a 3. ...<br>4. Implantar controles para la seguridad de los repositorios señalados, en congruencia con lo establecido en el SGSI, previsto en el proceso ASI- Administración de la seguridad de la información. |

**5.8.4.2.2** a

**5.9.2.2** ...

| | |
|---|---|
| **5.9.2.2.1** | **Descripción de las actividades del proceso** |

| | |
|---|---|
| **ANS-1** | **Definir y actualizar los acuerdos de niveles de servicio y operacionales** |
| **Descripción** | ... |
| **Factores críticos** | ...<br>1. a 7. ...<br>...<br>8. Comunicar a los Responsables de los procesos DSTI- Diseño de los servicios de TIC y ADT- Administración de los dominios tecnológicos, los Acuerdos de nivel de servicio SLA y los Acuerdos de nivel operacional OLA que se establezcan conforme al previsto en esta actividad, para que los mismos sean considerados en la elaboración de los programas de continuidad y de contingencia, así como al Responsable del proceso ASI- Administración de la seguridad de la información, para su conocimiento. |

**ANS-2** a

**ANS-4** ...

**5.9.2.2.2** a

**5.9.2.3** ...

**5.9.3** a

**5.9.3.4** **Derogado**

**5.10** a

**5.11.1.2** ...

| | |
|---|---|
| **5.11.1.2.1** | **Descripción de las actividades del proceso** |

| | |
|---|---|
| **AO-1** | **Establecer el Mecanismo de operación de TIC** |
| **Descripción** | ... |
| **Factores críticos** | ...<br>1. ...<br>a) a g) ...<br>h) El manejo de excepciones, Eventos e Incidentes y cambios, así como de controles de seguridad conforme a los procesos ACMB- Administración de cambios, OMS- Operación de la mesa de servicios y OPEC- Operación de los controles de seguridad de la información y del ERISC.<br>...<br>2. ... |

**AO-2** a

**AO-3** ...

**5.11.1.2.2** a

**5.11.2.2** ...

| | |
|---|---|
| **5.11.2.2.1** | **Descripción de las actividades del proceso** |

| | |
|---|---|
| **AAF-1** | **Diseñar el centro de datos** |
| **Descripción** | ... |
| **Factores críticos** | **El Responsable del ambiente físico, con apoyo de los Responsables de los procesos del Manual, deberá:**<br>1. a 2. ... |

| | |
|---|---|
| **AAF-2** | **Implementar controles de seguridad física en el centro de datos** |
| **Descripción** | ... |
| **Factores críticos** | **El Responsable del ambiente físico, con apoyo del Responsable del proceso ASI-Administración de la seguridad de la información, deberá:**<br>1. ...<br>a) Los riesgos de seguridad física identificados en el proceso ASI- Administración de la seguridad de la información.<br>b) a e) ...<br>...<br>2. ...<br>a) a d) ...<br>e) A proveedores o visitantes.<br>3. ...<br>a) Los riesgos por fenómenos naturales, identificados en el proceso ASI-Administración de la seguridad de la información.<br>b) a c) ...<br>4. ... |

**AAF-3** ...

**5.11.2.2.2** a

**5.11.3.2** ...

| | |
|---|---|
| **5.11.3.2.1** | **Descripción de las actividades del proceso** |

**MI-1** ...

| | |
|---|---|
| **MI-2** | **Mantener los recursos de infraestructura tecnológica y su disponibilidad** |
| **Descripción** | ... |
| **Factores críticos** | ...<br>1. ...<br>2. ...<br>a) a f) ...<br>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.<br>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.<br>3. ...<br>4. Aplicar los controles de mitigación de riesgos establecidos en el proceso ASI-Administración de la seguridad de la información, relativos a componentes de infraestructura.<br>5. a 7. ... |

**MI-3** ...

**5.11.3.2.2** a

**5.12** ..."

TRANSITORIOS

**Primero.-** El presente Acuerdo entrará en vigor el día 2 de enero de 2012.

**Segundo.-** En la fecha de entrada en vigor del presente Acuerdo, las dependencias y entidades deberán comunicar al Centro los datos de los servidores públicos designados como responsables de la seguridad de la información y de los enlaces responsables a los que se refiere el artículo Sexto Ter del presente ordenamiento.

Sufragio Efectivo. No Reelección.

México, Distrito Federal, a los veinticinco días del mes de noviembre de dos mil once.- El Secretario de Gobernación, **Alejandro Alfonso Poiré Romero**.- Rúbrica.- El Secretario de la Función Pública, **Salvador Vega Casillas**.- Rúbrica.