DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

Octubre 2014

Índice

Introducción

La seguridad de la información en organizaciones tanto del sector público como del privado es importante para proteger su infraestructura crítica. En ambos sectores, la seguridad de la información permite, lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos. La interconexión de las redes públicas y privadas adicional a compartición de recursos de información aumenta la dificultad de lograr el control de los accesos. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Definir, realizar, mantener y mejorar la seguridad de la información, es esencial para mantener la competitividad, rentabilidad, cumplimiento de la normatividad aplicable e imagen ante los ciudadanos.

Establecer las Directrices de Seguridad de la Información para la Institución y Lineamientos para las áreas que hacen uso de información y de TIC dentro de las Unidades Administrativas Centrales y los Centros SCT, da cumplimiento al Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información (MAAGTICSI) en el acuerdo publicado en el Diario Oficial de la Federación el 8 de Mayo de 2014.

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

A todos los Servidores Públicos de la Institución, Terceros involucrados a través de servicios y/o contratos y a todos los que usen para sus funciones la Información y servicios de TIC de la Organización.

El presente documento está alineado con el Plan Nacional de Desarrollo, la Estrategia Digital Nacional, el propio MAAGTIC-SI y se dirigen a la armonización y homologación de las actividades en materia de Seguridad de la Información que deben apoyar el cumplimiento de metas, objetivos, servicios y programas de la Institución.

Responsables de la Aplicación

Las Subsecretarias, Unidades y Direcciones de Apoyo del Área del Secretario, Directores Generales, titulares de Unidad, Coordinadores, tanto se trate de autoridades directrices o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Directriz de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Directriz por parte de su personal y equipo de trabajo.

La Directriz de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Institución, cualquiera sea su situación de contratación, el área a la cual se encuentre adscrita o prestando sus servicios y cualquiera sea el nivel de las tareas que desempeñe.

Las altas autoridades de la Institución aprobaran esta Directriz y serán responsables de la autorización de sus modificaciones.

El **Grupo Trabajo de Seguridad de la Información** de la Institución, procederá a revisar y proponer a las autoridad de la SCT para su aprobación la Directriz de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información , de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la Institución y coordinar el proceso de administración de la continuidad de las actividades de la SCT.

DSI 1 Directriz de Seguridad de la Información de la SCT.

Proteger los activos y recursos de información de la Institución, así como la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta directriz, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Directriz de Seguridad de la Institución actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

DSI 1.1 Organización Interna

DSI 1.1-a) Asignación de responsabilidades y roles para la Seguridad de la Información.

La Institución identificara, definirá y asignara todas las responsabilidades y roles de seguridad de la información necesarios para el correcto cumplimiento de esta directriz.

DSI 1.1-b) Coordinación con las instituciones de Seguridad de la Información y Seguridad Nacional

La Institución mantendrá contacto con autoridades e instituciones para tratar cualquier tema relacionado con la Seguridad de la Información y Seguridad Nacional.

DSI 1.1-c) Contacto con Organismos Certificados en el manejo de la Seguridad de la Información

La Institución mantendrá contacto con grupos especialistas de intereses, foros de seguridad especializada y asociaciones profesionales de Seguridad de la Información para madurar sus procesos y conocer las tendencias en materia de Seguridad de la Información.

DSI 1.1-d) Equipos de Respuesta a Incidentes de la Institución

La Institución definirá y contara con un Equipo de Respuesta a Incidentes para la atención de problemas relacionados con la Seguridad de la Información en la Institución.

DSI 1.1-e) Administración de proyectos de Seguridad de la información.

Se cumplirá con la Seguridad de la Información en la administración de proyectos, con independencia del tipo y tema del proyecto.

DSI 1.2 Equipos Móviles

DSI 1.2-a) Uso de dispositivos móviles en la Institución

Se tendrá una directriz y el soporte a las medidas de seguridad adoptadas para administrar los riesgos generados por el uso de dispositivos móviles, a fin de garantizar que no se comprometa la información de la Institución.

DSI 1.2-b) Mecanismos Mínimos de Seguridad de la Información en Dispositivos Móviles

Se mantendrá un mínimo de contramedidas dentro de los dispositivos móviles o perimetral que garantice la Seguridad de la Información en contenida en estos y los de la Institución.

DSI 1.2-c) Acceso a la Red de Equipos Móviles

Se mantendrá en todo momento el control de los dispositivos integrados a la Red de la institución y la información que acceden mantenido separado los ambientes de pruebas, producción e invitados, que permita garantizar la Seguridad de la Información.

DSI 1.3 Acceso por Medios Externos

DSI 1.3-a) Administración y Operación Remota de usuarios
Se tendrá en todo momento la administración de los usuarios que acceden por medios externos a la infraestructura de la Institución que permita, identificar a los perfiles de los usuarios y la información a la que acceden.

DSI 1.3-b) Aseguramiento de equipos por accesos remotos (Home Office)
Se implementarán las medidas de Seguridad para proteger los activos e información consultada, procesada o almacenada, siempre que se acceda por medios externos para realizar actividades laborales.

DSI 2 Seguridad de la Información en los Recursos Humanos

Asegurar que los empleados de la institución, proveedores y todos aquellos externos que se vinculan directa o indirectamente con esta, comprenden, conocen y cumplen sus responsabilidades relacionadas a la Seguridad de la Información y estas coadyuvan con las funciones y actividades sustantivas para las que fueron contratados.

DSI 2.1 Requisitos para la Contratación

DSI 2.1-a) Investigar antecedentes de los prospectos.
Las áreas o Unidades Administrativas verificarán los antecedentes de todos los candidatos a empleo y se llevara de conformidad con las leyes, regulaciones y ética aplicable, siendo proporcional a los requerimientos de empleo, la clasificación de la información que accederá y los riesgos que esto implique.

DSI 2.1-b) Descripción de las actividades del personal en términos de Seguridad de la información del personal
Los contratos con los empleados y proveedores incluirán dentro de las descripciones de las funciones y actividades en la Institución, las responsabilidades relativas a la Seguridad de la Información.

DSI 2.1-c) Información al personal de nuevo ingreso de los términos de seguridad de la Información
Dentro de las actividades de inducción, debe integrarse el tema de Seguridad de la Información en la Institución para todo el personal de nuevo ingreso, proveedores y todos aquellos externos que se vinculan directa o indirectamente con esta.

DSI 2.2 Durante el tiempo de Contratación

DSI 2.2-a) Responsabilidades del personal (usuarios) de la Institución en la seguridad de la información
Se exigirá a todos los empleados y todos aquellos externos que se vinculan directa o indirectamente con la Institución, conocer, atender, vigilar y cumplir con la Seguridad de la Información de acuerdo con las directrices y procedimientos establecidos por la esta.

DSI 2.2-b) Programas de Difusión, Concientización y Cultura en Seguridad de la Información
Todos los empleados de la Institución y, los externos recibirán educación, capacitación y concientización sobre Seguridad de la Información, las directrices y sus procedimientos de forma periódica.

DSI 2.2-c) Programas de Capacitación
Se establecerán programas de capacitación enfocados a la Seguridad de la Información coordinados por las unidades rectoras de la capacitación en la Institución, con el involucramiento de todas las áreas para enriquecer los temas en esta materia.

DSI 2.2-d) Enterar al OIC sobre violaciones o desviaciones a las Directrices de Seguridad de la Información
Todas las violaciones o desviaciones a las directrices de Seguridad de la Información detectadas y documentadas, se enviaran al OIC de la Institución, para que aplique las medidas disciplinarias que establezca este Órgano de Control Interno.

DSI 2.3 Término y cambios de la relación laboral de los empleados

DSI 2.3-a) Responsabilidades al término de la Relación Laboral
Se comunicaran a los empleados, proveedores y todos aquellos externos que se vinculan directa o indirectamente con la Institución, las responsabilidades y deberes sobre la Seguridad de la Información que deberán de observar al término de la relación laboral con la Institución.

DSI 2.3-b) Responsabilidades en caso de cambio de funciones o puesto
Se comunicaran a los empleados, proveedores y todos aquellos externos que se vinculan directa o indirectamente con la Institución, las responsabilidades y deberes sobre la Seguridad de la Información que deberán de observar, acorde al cambio de funciones y actividades que desempeña para la Institución.

DSI 3 Control de Acceso

Controlar y delimitar el acceso a información e instalaciones de procesamiento, almacenamiento, alojamiento y consulta de información. Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios. Hacer responsables a los usuarios de proteger su información y de los métodos de autenticación que utilizan para prevenir el acceso no autorizado a las instalaciones, sistemas y aplicaciones de la Institución.

DSI 3.1 Requisitos de la Institución para el control de Accesos

DSI 3.1-a) Directriz de Control de Acceso
Se establecerá una directriz de control de acceso a las instalaciones e información basada en los requisitos de seguridad de la información y su clasificación en la Institución.

DSI 3.2 Responsabilidades del usuario

DSI 3.2-a) Manejo de Información confidencial
Todos los usuarios que usan la infraestructura y servicios de la Institución, están obligados a seguir las directrices y lineamientos establecidos para el uso de la información confidencial y servicios.

DSI 3.3 Administración de accesos de Usuarios

DSI 3.3-a) Administración y Registro de Usuarios
Se implementará un proceso sistematizado para el registro de usuarios que permita, controlar el perfilamiento de acceso a los aplicativos, sistemas, servicios e infraestructura de la Institución.

DSI 3.3-b) Administración de altas/bajas/cambios en el registro de usuarios
Se establecerá el proceso para el alta, baja y cambios de usuarios que permita la actualización de los registros de los usuarios.

DSI 3.3-c) Administración de los Perfiles de acceso
Se establecerá un proceso, para asignar o revocar los permisos o derechos de acceso de los perfiles de usuario que acceden a los aplicativos, sistemas, servicios e infraestructura de la Institución.

DSI 3.3-d) Administración de los Perfiles de accesos con privilegiados y especiales
Se establecerá un control restrictivo para la asignación y uso de los perfiles o accesos privilegiados, de administrador, especiales y excepciones.

DSI 3.3-e) Administración de la información confidencial de autenticación
El encargado de Seguridad de la Información de la Institución mantendrá la administración de la asignación de información confidencial, para la autenticación o acceso a la infraestructura y servicios, mediante procesos plenamente identificados y formalizados.

DSI 3.3-f) Borrado y eliminación de los Perfiles de acceso
Sin excepción todos los permisos o perfiles de acceso a los aplicativos, sistemas, servicios e infraestructura de la información de los empleados, proveedores y todos aquellos externos que se vinculan directa o indirectamente con la Institución, serán eliminados por factoreś como, el NO uso de estos por un tiempo mayor a 120 dias naturales, licencia, al término de su contrato, acuerdo o relación laboral con la institución, por presentar un riesgo a la seguridad de la Información, por uso inadecuado, por solicitud de un área de mando superior o a solicitud del encargado de Seguridad de la Información de la Institución y se ajustaran por el cambio de funciones, responsabilidades o puesto.

DSI 3.3-g) Auditorias de los Perfiles de acceso
Se mantendrá en todo momento la supervisión y auditoria, de los permisos y perfiles de acceso de los activos e infraestructura de la Institución, para mantener un control y actualización de los registros de estos.

DSI 3.4 Control de acceso a TIC

DSI 3.4-a) Restricciones de Acceso a la Información
El acceso a la información, utilidades, aplicativos y herramientas de los sistemas se limitaran mediante perfiles de acceso para la autenticación de los usuarios

DSI 3.4-b) Procedimiento de inicio de sesión segura
El acceso a los sistemas y aplicaciones de la Institución será controlado en todo momento por un procedimiento de inicio de sesión seguro.

DSI 3.4-c) Control de utilidades para la administración de activos
Se restringirá y controlaran las utilidades de administración de los activos e infraestructura de la Institución, que se utilizan para manipular o controlar el funcionamiento de los mismos.

DSI 4 Administración de los Activos

Identificar los activos de la Institución, así como, definir las responsabilidades de resguardo de estos, garantizando que la información cuenta con un nivel de protección acorde a su importancia.

Prevenir la modificación, divulgación o transmisión no autorizada, eliminación o destrucción de la información de la Institución, almacenada o contenida en todo tipo de medio.

DSI 4.1 Responsabilidad sobre los Activos

DSI 4.1-a) Inventario de activos
Todos los activos identificados y relacionados con la manipulación, generación, procesamiento, almacenamiento o respaldo de información de la institución se integraran en un inventario y este se mantendrá siempre actualizado.

DSI 4.1-b) Resguardos y encargados de los activos
El inventario de los activos identificados derivado de la directriz anterior, tendrá en todo momento asociado e identificado al dueño o resguardante del activo, quien será responsable de este.

DSI 4.1-c) Sistematización de la administración de los activos
Se desarrollara e implementara la sistematización de la información de activos de la institución, a fin de tener la posibilidad de procesarla, consultarla, almacenarla y respaldarla con ayuda de las TIC

DSI 4.1-d) Uso aceptable de los activos
Se documentarán e implementarán reglas y procedimientos de uso aceptable de los activos con el fin de mantener siempre su operación óptima.

DSI 4.1-e) Devolución de activos
Los empleados, proveedores y todos aquellos externos que se vinculan directa o indirectamente con la Institución, tienen como responsabilidad final, devolver los activos de la Institución que a lo largo de su vida laboral se les asigno una vez que se da por concluida toda relación laboral.

DSI 4.2 Clasificación de la Información

DSI 4.2-a) Clasificación de la Información
Toda la información de la Institución será clasificada en términos de sus requisitos legales, el valor para la Institución, criticidad, características de seguridad, sensibilidad de divulgación, modificación no autorizada y las definidas en el MAAGTICSI.

DSI 4.2-b) Rotulación y Etiquetado de la Información
Se desarrollaran e implementaran los procedimientos para la rotulación y etiquetado de la información acorde al establecido por la institución y la clasificación que se indica en la directriz anterior.

DSI 4.3 Manejo de almacenamiento de información

DSI 4.3-a) Administración de los medios de almacenamiento removibles
Se aplicaran procedimientos para la administración de los medios extraíbles de acuerdo con el esquema de clasificación adoptado por la Institución.

DSI 4.3-b) Borrado o eliminación segura de los medios de almacenamiento removibles
Todos los medios de almacenamiento y comunicación removibles serán eliminados de forma segura cuando sea necesario de acuerdo con el esquema de clasificación adoptado por la Institución y utilizando procedimientos formalmente establecidos.

DSI 4.3-c) Seguridad de los medios de almacenamiento reubicados
Todos los medios extraíbles que contienen información de la Institución estarán protegidos contra el acceso no autorizado, mal uso o corrupción durante su movimiento o transporte.

DSI 5 Cifrado

Establecer el uso efectivo de la criptografía que permita mantener la confidencialidad, autenticidad e integridad de la información de la Institución.

DSI 5.1 Controles criptográficos

DSI 5.1-a) Directriz de uso de los controles criptográficos
Se implementará una directriz de los controles criptográficos para la protección de la información de la Institución, alineado a lo establecido en el MAAGTICSI.

DSI 5.1-b) Administración de Claves Criptográficas
Se establecerá una administración y control sobre la protección y la duración de las claves de cifrado usadas por la institución a través de su ciclo de vida.

DSI 6 Seguridad Física y Ambiental

Prevenir la pérdida, daño, extracción no autorizada, accesos no autorizados, vulneración de los activos y la interrupción de las operaciones de la Institución.

DSI 6.1 Áreas Seguras

DSI 6.1-a) Perímetros de Seguridad física
Se definirán y asignaran perímetros de seguridad física para proteger las áreas, activos e instalaciones de la Institución que alojen o contengan información sensible o crítica.

DSI 6.1-b) Asegurar activos, oficinas e instalaciones
Los activos, áreas e infraestructuras de la Institución se protegerán mediante controles de acceso, a fin de asegurar que ingresa únicamente el personal identificado y autorizado.

DSI 6.1-c) Áreas y zonas seguras de trabajo
Se diseñaran y asignaran áreas de trabajo en la Institución con procedimientos para mantenerlas aseguras.

DSI 6.1-d) Zonas de carga y descarga
Se controlaran y aislaran los puntos de acceso, zonas de carga/descarga y otros puntos contiguos o cercanos a las áreas, activos e instalaciones de la Institución que alojen o contengan información sensible o crítica a fin de evitar accesos no autorizados.

DSI 6.1-e) Amenazas internas, externas y ambientales
Se diseñaran, aplicaran y mantendrán controles, procedimientos y acciones de protección para la contención, manejo y control de amenazas tales como accidentes, ataques maliciosos, desastres naturales y todo aquel elemento interno y externo que pueda representar una amenaza.

DSI 6.1-f) Desalojo de áreas y zonas seguras en casos de contingencias
Se diseñaran, aplicaran y mantendrán controles, procedimientos y acciones de desalojo de áreas y zonas seguras en casos de contingencias de todo tipo, a fin de mantener en lo posible seguras a las personas, los activos e instalaciones de la Institución.

DSI 6.2 Seguridad de los equipos

DSI 6.2-a) Ubicación y protección de los equipos
Los equipos de la Institución estarán ubicados y protegidos a fin de reducir o eliminar, los riesgos, amenazas ambientales y no ambientales, así como de accesos no autorizados.

DSI 6.2-b) Procedimientos contra fallas e interrupciones eléctricas
Se implementaran procedimiento para que los equipos de la Institución a fin de mantenerlos protegidos contra fallas de energía eléctrica y otras interrupciones ocasionadas por elementos de los servicios externos.

DSI 6.2-c) Mantenimiento de los equipos
Se dará mantenimiento preventivo a todo el equipo de la Institución a fin de garantizar su disponibilidad e integridad en todo momento.

DSI 6.2-d) Seguridad de los equipos y activos fuera de las instalaciones
Se aplicaran los controles de seguridad necesarios a los equipos y activos fuera de las instalaciones de la Institución, contemplando los diferentes escenarios de riesgo fuera de sus instalaciones.

DSI 6.2-e) Baja o Reutilización de equipos
Se asegurara que todos los equipos que contienen, almacenan o alojan información y software con licenciamiento de la Institución en cualquier medio, se elimine de forma segura antes de su baja o reutilización.

DSI 6.2-f) Seguridad en equipos de usuarios desatendidos.
Los usuarios de la Institución, se aseguraran de proteger su equipo, sesiones de trabajo o exposición de información, cuando no se utilice, estén ausentes en su oficina, área o zona de trabajo.

DSI 6.2-g) Directriz de Escritorio limpio
Se adoptará una directriz Institucional que coadyuve a mantener los escritorios libres de papel y dispositivos, así mismo de pantalla limpia o protector de pantalla Institucional en todos los equipos cómputo, consolas y dispositivos de TIC.

DSI 7 Seguridad en las Operaciones

Asegurar la óptima y segura operación de las actividades de la Institución mediante herramientas, procedimientos, dispositivos que registren evidencia de todas las operaciones fisicas y lógicas de la Institución, teniendo en todo momento el cuidando de que estas herramientas y actividades de auditoria no afecten, impacten o alteren el óptimo desempeño de la operaciones.

DSI 7.1 Procedimientos de operación

DSI 7.1-a) Registro de los procesos operativos
Se documentarán y generara un registro de los procedimientos operativos de la Institución para su publicación y difusión al interior de la Institución.

DSI 7.1-b) Administración de Cambios
Se documentaran y controlaran todos los cambios en la Institución, que incluyen mas no limitan a los procesos, activos, instalaciones, sistemas, operaciones fisicas y lógicas, procesamiento de información que afecten o puedan afectar la seguridad de información.

DSI 7.1-c) Administración de cambios con proveedores
De la misma forma que lo establecido en la directriz anterior, se documentaran y controlaran todos los cambios que los proveedores y todos aquellos externos que se vinculan directa o indirectamente con la Institución, apliquen o hallan aplicado en procesos, activos, instalaciones, sistemas, operaciones fisicas y lógicas, procesamiento de información bajo su resguardo, administración y operación, que afecten o puedan afectar la seguridad de información de la Institución.

DSI 7.1-d) Administración de las Capacidades
Se mantendrán monitoreados los recursos, activos, infraestructura, operaciones fisicas, lógicas y todas aquellas que se juzguen necesarias, que permitan determinar los ajustes, cambios a las necesidades de capacidad de la Institución en actuales y futuras proyecciones a fin de asegurar el rendimiento y capacidades de los activos, infraestructura, instalaciones, sistemas, entre otros.

DSI 7.1-e) Separación de los ambientes de desarrollo, prueba y producción
Se mantendrán separados los entornos y ambientes de desarrollo, prueba y producción a fin de reducir al minimo los riesgos o cambios al entorno operativo.

DSI 7.2 Protección Contra Código Malicioso

DSI 7.2-a) Controles contra Código Malicioso
Se implementaran los controles y herramientas que permitan la detección, prevención y recuperación de un incidente de Código Malicioso, a fin de proteger los activos e infraestructura contra este tipo de códigos.

DSI 7.2-b) Difusión de información contra código malicioso
La directriz anterior será complementada y se combinara con la capacitación e información a los empleados, proveedores y todos aquellos externos que se vinculan directa o indirectamente con la Institución, referente a las implicaciones del código malicioso.

DSI 7.3 Respaldos de Información

DSI 7.3-a) Respaldo de la Información
Se establecerán, aplicaran y validaran con regularidad respaldos y copias de seguridad de software, imágenes de sistemas e información sensible de la Institución.

DSI 7.4 Bitácoras y Registros y Monitoreo

DSI 7.4-a) Registro y Bitácoras de eventos
Se registraran, almacenaran y revisarán todos los eventos de las actividades de los usuarios de la Institución, fisicas y lógicas en materia de seguridad de la información.

DSI 7.4-b) Protección de los Registros y Bitácoras de información
Se proveerán de los elementos de seguridad que permitan proteger y asegurar las ubicaciones que contienen o concentran los registros, bitácoras e información de eventos, con el fin de evitar su manipulación y acceso no autorizado.

DSI 7.4-c) Sincronización de Relojes
Todos los sistemas de procesamiento de información, de aplicaciones, servicios y todos aquellos que utilizan un reloj para registrar o generar eventos de todo tipo, se sincronizaran mediante una sola fuente de tiempo de referencia establecido por la Institución.

DSI 7.5 Administración y Control de software

DSI 7.5-a) Instalación de software
Se implementaran procedimientos, herramientas y controles para administrar y controlar la instalación de software, en los sistemas operativos de los equipos y dispositivos de la Institución.

DSI 7.6 Administración de Vulnerabilidades

DSI 7.6-a) Administración de las Vulnerabilidades
Se establecerán procedimientos y utilizaran herramientas que permitan obtener de forma oportuna, la Información referente a las vulnerabilidades presentes en los sistemas de información, que permitan evaluar y determinar la exposición de la Institución, para aplicar las medidas que permitan manejar los riesgos asociados.

DSI 7.7 Auditorías de los sistemas de información

DSI 7.7-a) Controles de Auditoria en los sistemas de información
Se planificaran, acordaran requisitos y actividades de auditoria, relacionadas con la verificación de los sistemas información con el fin de reducir al mínimo las interrupciones de los procesos operativos de la Institución.

DSI 8 Seguridad en las Comunicaciones

Garantizar la protección de la información que se trafica en las redes e instalaciones que soportan el procesamiento de la misma. Mantener la seguridad de la información fluye, transita o se transfiere al interior de la Institución y con entidades o proveedores externos.

DSI 8.1 Administración de la Seguridad en las Redes de Telecomunicaciones

DSI 8.1-a) Controles de Red
Se administraran y aplicaran controles en las Redes Telecomunicaciones de la Institución a fin de garantizar la protección de la información que transita, comparte, trafica y transfiera por estas.

DSI 8.1-b) Controles de Seguridad asociados a los servicios de Red
Se identificaran e incluirán en los contratos y acuerdos de servicios, mecanismos de seguridad, niveles de servicio y requerimientos de administración de seguridad de los servicios de Red, provistos por la Institución o proporcionados por proveedores o terceros.

DSI 8.1-c) Segmentación de las Redes
Se implementara una administración de segmentación de las Redes de la Institución, a través de grupos de servicios de información, usuarios, sistemas y todos aquellos que permitan separar e identificar los flujos de información, para asegurar el tránsito de la información de forma segura.

DSI 8.2 Intercambio de información

Procedimientos de intercambio de información
Se implementaran directrices, procedimientos y controles que permitan identificar y garantizar que se realizan transferencias de información de forma segura en la Institución, y con ello mantener la seguridad de la información a través de cualquier tipo de servicios de comunicaciones utilizado.

DSI 8.2-a) Acuerdos para el Intercambio de Información
Se realizaran acuerdos que garanticen la transferencia segura de la información entre la Institución y todas aquellas instituciones, ciudadanos, organizaciones, entes y en general, que requieran de intercambio o transferencia de información.

DSI 8.2-b) Mensajería Electrónica
Se implementaran los procedimientos y controles que permitan garantizar la Seguridad de la Información que involucra la transferencia de Información a través de mensajería electrónica.

DSI 8.2-c) Acuerdos de Confidencialidad y no Divulgación
Se identificaran, revisaran y documentaran regularmente los requisitos para los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la Institución para la protección de la información.

DSI 8.2-a) Servicios Accesibles por Redes Públicas
Se identificaran y documentaran todos los servicios que se acceden a través de Redes Públicas, para implementar los controles y mecanismos de Seguridad que permitan, garantizar la Seguridad de la Información de los servicios expuestos por estos medios.

DSI 9 Desarrollo, Soporte y Adquisición de Sistemas de Información

Garantizar que la Seguridad de la Información sea parte integral de los Sistemas y Aplicativos de Información durante todo su ciclo de vida. Además de incluir requerimientos mínimos para los sistemas de información que otorgan servicios a través de redes públicas.

Garantizar la protección de los datos utilizados para las pruebas.

DSI 9.1 Requisitos de Seguridad de los Sistemas de Información

DSI 9.1-a) Especificaciones y Requerimientos de Seguridad de la Información en Sistemas
Asegurar que todos los nuevos Sistemas, así como, las actualizaciones o mejoras a los ya existentes incluyen especificaciones y requerimientos mínimos de Seguridad de la Información.

DSI 9.1-b) Actualizar Controles de Seguridad en Sistemas Legados
Se generaran actividades y procedimientos especificos para actualizar los mecanismos y controles de seguridad de los Sistemas y Aplicativos legados, a fin de actualizarlos y contar con un mínimo de Seguridad de la Información de los estos.

DSI 9.1-c) Aseguramiento de las transacciones de los Sistemas y Aplicaciones
Garantizar que la Información de la Institución relacionada con actividades transaccionales de los Sistemas y Aplicaciones es segura, a fin de prevenir su transmisión incompleta, errores de enrutamiento, modificación no autorizada, divulgación no autorizada, duplicación de información no autorizados o reproducción de mensajes.

DSI 9.2 Seguridad en el Proceso de desarrollo y soporte

DSI 9.2-a) Directriz de desarrollo de sistemas seguros
Se desarrollaran y establecerán directrices para el desarrollo seguro de sistemas y de software de la Institución.

DSI 9.2-b) Procedimientos de Control de Cambios a los sistemas
Se establecerán procedimientos de Control de Cambios para la implementación y aplicación de cambios en los Sistemas dentro del ciclo de vida de desarrollo.

DSI 9.2-c) Validación técnica de aplicaciones después de Cambios en el Ambiente de Operación
Se revisaran y probaran los cambios a las aplicaciones, sistemas y plataformas operativas críticas de la Institución, a fin de asegura que no existen impactos negativos en las operaciones o la seguridad.

DSI 9.2-d) Restricciones a cambios en Aplicativos de Software
Se limitaran las modificaciones a los aplicativos de software, aplicando las actualizaciones y modificaciones de forma programada y con estricto control.

DSI 9.2-e) Seguridad en los Ambientes de Desarrollo
Se establecerán los controles, procedimientos y mecanismos de seguridad en los Ambientes de Desarrollo para su realización e integración a los Sistemas durante todo el ciclo de vida del Desarrollo del Sistema.

DSI 9.2-f) Desarrollo de Sistemas por Terceros
La Institución y generara procedimientos para controlar y supervisar todas las actividades del ciclo de vida del Desarrollo de Sistemas Tercerizados.

DSI 9.2-g) Pruebas de seguridad a los sistemas
Se llevaran a cabo pruebas de funcionalidad, estrés y seguridad durante el Desarrollo de los Sistemas.

DSI 9.2-h) Pruebas de aceptación de sistemas
Se establecerán procedimientos, criterios y pruebas de aceptación para actualizaciones y nuevas versiones de los sistemas de información, cuidando en todo momento la funcionalidad y la Seguridad de la Información.

DSI 9.3 Datos de Prueba

DSI 9.3-a) Protección de datos de prueba
Todos los datos de prueba estarán invariablemente identificados y controlados, consecuentemente se deberán mantener protegidos y asegurados por los controles de Seguridad necesarios.

DSI 10 Relación con Proveedores

Garantizar la Seguridad de la Información de los activos e infraestructura de la Institución que se consulta y accede por proveedores.

Mantener la Seguridad de la Información en altos niveles, a través de los acuerdos establecidos con los proveedores, siempre alineado a lo establecido en el MAAGTICSI.

DSI 10.1 Seguridad de la Información en la relaciones con los proveedores.

DSI 10.1-a) Directriz de Seguridad de la Información en la interacción con proveedores

Se establecerán y documentaran acuerdos de los requisitos mínimos en materia de Seguridad de la Información, que contribuyan al manejo y mitigación de los riesgos, asociados al acceso y uso de los activos de la Institución por parte de los proveedores.

DSI 10.1-b) Requerimientos de Seguridad de la información en los contratos con Proveedores.

Se establecerán en los contratos con proveedores, los requisitos de Seguridad de la Información mínimos a fin de que puedan acceder, procesar, almacenar, comunicar, utilizar, agregar componentes, mejorar entre otros, a los activos e infraestructura Institución.

DSI 10.1-c) Administración de Riesgos de Seguridad de la Información con proveedores

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las directrices, procedimientos y controles de seguridad de la información existentes, se realizaran, teniendo en cuenta la criticidad de la información de la Institución, los sistemas y los procesos involucrados y una re-evaluación de los riesgos.

DSI 10.2 Auditoria de servicios a proveedores

DSI 10.2-a) Seguimiento y revisión de los servicios de los proveedores.

Generar procedimientos y controles que permitan realizar y aplicar verificaciones, revisiones y auditorias a los proveedores sobre la atención y prestación de servicios en la Institución.

DSI 11 Administración de Incidentes de la Seguridad de la Información

Garantizar un enfoque coherente y eficaz para la administración de incidentes de Seguridad de la Información, incluyendo la comunicación de eventos de seguridad y vulnerabilidades.

DSI 11.1 Administración de Incidentes de Seguridad de la Información y mejoras

DSI 11.1-a) Responsables y Procedimientos de atención

Se establecerán las responsabilidades y procedimientos de administración a fin de asegurar una respuesta rápida, eficaz y ordenada a los incidentes de Seguridad de la Información.

DSI 11.1-b) Informe de Análisis de Riesgos

Generar y aplicar los Análisis de Riesgos de los Activos e Infraestructura de la Institución e informar al responsable de la Seguridad de la información en la Institución de los resultados obtenidos en estos.

DSI 11.1-c) Reportar Incidentes de Seguridad de la Información

Se reportaran los eventos de Seguridad de la Información, a través de los canales de comunicación establecidos, al responsable de la Seguridad la Información en la Institución tan pronto como sea posible, para su conocimiento y atención.

DSI 11.1-d) Informe de vulnerabilidades de Seguridad de la Información
Los empleados y externos que utilizan los sistemas y servicios de información de la Institución, están obligados a reportar cualquier debilidad de seguridad de información observada o que se sospeche en los sistemas o servicios.

DSI 11.1-e) Evaluación y clasificación de Incidentes de Seguridad de la Información
Se implementara y aplicara un procedimiento para evaluar los eventos de Seguridad de la Información y clasificarlos, a fin de dar la atención acorde a su clasificación.

DSI 11.1-f) Respuesta a los Incidentes de Seguridad
Se establecerán procedimientos y actividades, para la atención de los Incidentes de Seguridad de la Información.

DSI 11.1-g) Bases de Conocimiento sobre Incidentes de Seguridad de la Información
El aprendizaje adquirido a partir de atender, analizar, mitigar, manejar y resolver Incidentes de Seguridad de la información se concentraran en una Base de Conocimientos, que tendrá como finalidad la búsqueda y consulta de eventos de Seguridad de la Información atendidos y resueltos que permitan reducir los tiempos de atención e impacto de incidentes similares futuros.

DSI 11.1-h) Evidencias y resguardo
La Institución definirá y aplicara procedimientos para la identificación, recopilación, adquisición, conservación y resguardo de la información, que puede servir como evidencia.

DSI 12 Seguridad de la Información en la Continuidad de las Actividades Sustantivas de la Institución

Garantizar y asegurar que la Seguridad de la Información está integrada y coadyuva a la continuidad de las funciones y actividades sustantivas de la Institución.

Asegurar la disponibilidad de la información en los activos e instalaciones sustantivas de la Institución.

DSI 12.1 Continuidad de las Actividades Sustantivas de la Institución

DSI 12.1-a) Planeación de la Continuidad de las Actividades Sustantivas de la Institución
Se tendrán identificados los elementos que dan sustento a la continuidad de Actividades Sustantivas de la Institución, en situaciones adversas, de crisis o desastre, siempre en coordinación con el responsable de Seguridad de la Información de la Institución, que permitan planear las actividades de continuidad de las Actividades Sustantivas de esta y el regreso a la operación normal.

DSI 12.1-b) Implementación de la Continuidad Actividades Sustantivas de la Institución
La Institución establecerá, documentara, implementara y mantendrá los procesos, procedimientos y controles necesarios que garanticen la Continuidad de las Actividades Sustantivas de la Institución durante una situación adversa.

DSI 12.1-c) Evaluación, actualización y mejora de los planes de Continuidad de Actividades Sustantivas
La Institución verificara en intervalos regulares a los procesos, procedimientos, controles y planes establecidos para la Continuidad de las Actividades Sustantivas de la Institución, con el fin de asegurar que son adecuados y eficaces en situaciones adversas.

DSI 12.2 Respaldo

DSI 12.2-a) Disponibilidad de las Instalaciones para el procesamiento de la información
Se establecerán e implementaran Instalaciones de procesamiento de la información con redundancia para atender la disponibilidad y continuidad de los servicios de la Institución.

DSI 13 Auditoria

Evitar incumplimientos de las obligaciones legales, reglamentarias y contractuales en materia de Seguridad de la Información y de los requerimientos mínimos de Seguridad.

Verificar y asegurar que la Seguridad de la Información opera de acuerdo a las directrices, procedimientos y controles implementados por la Institución.

DSI 13.1 Cumplimiento de leyes y contratos

DSI 13.1-a) Identificación de la legislación aplicable y los requerimiento contractuales
La Institución identificara y documentara, todos los requerimientos legales, contractuales, leyes regulatorias y marco normativo, con el fin de alinearse y cumplir con estos.

DSI 13.2-b) Derechos de Propiedad intelectual DPI
Se implementaran procedimientos y controles para garantizar el cumplimiento de requerimientos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietario.

DSI 13.1-c) Protección de los registros de la Institución
Se protegerán los registros y bitácoras de información contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requerimientos legales, reglamentarios y contractuales de la Institución.

DSI 13.1-d) Privacidad y Protección de los datos personales
Se garantizara la privacidad y protección de los datos personales como lo requiere la legislación y la regulación aplicable vigente.

DSI 13.2 Revisión de la Seguridad de la Información

DSI 13.2-a) Revisión Institucional de la Seguridad de la Información
El tratamiento Institucional sobre la gestión la Seguridad de la Información y su aplicación será revisado de forma independiente en intervalos planificados o cuando se produzcan cambios significativos a esta.

DSI 13.2-b) Cumplimiento de las directrices y procedimientos de la Seguridad de la Información
Los administradores observaran y garantizaran el cumplimiento en su ámbito de responsabilidad, los procedimientos y directrices de seguridad Institucionales vigentes.

DSI 14 Sanciones Previstas por Incumplimiento

El incumplimiento a la presente Directriz de Seguridad de la Información, generaran un proceso para determinar y aplicar las sanciones que correspondan por parte del Órgano Interno de Control de la Institución.

DSI 14.1 Enterar al OIC

Se envira un reporte documentado al OIC de la Institución, de los incumplimientos a las Directrices de Seguridad detectadas para que este, aplique las medidas que juzgue necesarias, a los empleados y externos que incurrieron en este supuesto.

Glosario

Política.- Directriz u ordenamiento específico en un tema que requiere una definición para decidir el curso de las acciones ante varias alternativas. -Equivalente a Directriz Rectora que solicita el MAAGTICSI en sus diferentes procesos y factores críticos.-
Lineamiento.- Pautas que deben seguirse para aplicar y dar cabal cumplimiento a una política
SCT.- Secretaría de Comunicaciones y Transportes, también puede ser simplemente la Secretaría
UTIC.- Unidad de Tecnologías de Información y Comunicaciones
SLA.- El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (Service Level Agreement, por sus siglas en inglés).
MAAGTICSI.- Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información.
Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.
Para ello es necesario considerar aspectos tales como:
Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
No repudio: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.

Referencias

Acuerdo de las Politicas de TIC y del MAAGTICSI: http://cidge.gob.mx/menu/normatividad-2/maagticsi/

Tecnologia de la información - Técnicas de seguridad - Código de conducta para los controles de seguridad de la información: http://www.iso.org/iso/catalogue_detail?csnumber=54533

Aprobó	Revisó	Elaboró
Ignacio Edmundo Funes Maderey Titular de la UTIC	Norma Gabriela Medina Galindo Directora Adjunta de Estrategia en TIC	Juan Pablo Sánchez Gómez Subdirector de Seguridad Informática y Servicios de Voz
FIRMA	FIRMA	FIRMA