DIRECTRICES DE SEGURIDAD DE LA INFORMACION DE TIC

Versión 2

Octubre 2014

Tabla de contenido

Introducción

En este Manual se establecen las Directrices y Lineamientos para las áreas que hacen uso de las Tecnologías de Información y Comunicaciones dentro de las Unidades Administrativas Centrales y los Centros SCT dando 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

Objetivos

- Proporcionar la información general necesaria a los usuarios de la SCT, sobre las normas y mecanismos que deben cumplir para la protección de las TIC de la Institución, así como la información que es procesada y almacenada en estas.
- Consolidar la Seguridad de la Información en las TIC`s y en los procesos que se vinculan a esta

Ámbito de aplicación

Las Directrices y Lineamientos definidas en el presente documento están alineadas 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 TIC y de Seguridad de la Información que deben apoyar el cumplimiento de metas y programas de la SCT.

El desconocimiento del mismo, no exonera de responsabilidad alguna al usuario, ante cualquier eventualidad que involucre la seguridad de la información, los servicios tecnológicos y las TIC

Todos los Servidores Públicos de la SCT, Terceros involucrados a través de servicios y/o contratos y los usuarios directos de ésta deberán de apegarse a lo aquí establecido.

Definiciones

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
SIGTIC.- Sistema de Gestión de Tecnologías de Información y Comunicaciones

DIRECTRICES DE SEGURIDAD DE LA INFORMACION

DSITIC 1 Directriz de Seguridad de la Información de la SCT

La Información es el recurso más importante de la SCT después del Humano, por lo que la continuidad de los servicios y la salvaguarda de la información que los activos recolectan, procesan, transmiten y/o almacenen en la Institución, se mantendrá a un nivel acreditable, observando siempre la Confidencialidad, Integridad y Disponibilidad de la misma, siendo obligación de todos los empleados de la Secretaría ser garantes de la Seguridad de la Información de la Institución.

DSI 1

DSITIC1-a) Revisión y actualización de Directrices

Las directrices deben revisarse al menos una vez al año, con la finalidad de garantizar que se mantengan actualizadas para su aplicación en la Institución.

DSITIC 2 Grupo de Trabajo de Seguridad de la Información

El Grupo Estratégico de Seguridad de la Información en la SCT, evaluara los requerimientos en materia de Seguridad y formulara el plan de Seguridad de la Información, así como su programa de implementación, con la participación de los representantes informáticos de las Unidades Administrativas Centrales y Centros SCT.

DSI 1.1-a

DSITIC 2-a) Responsabilidades del Propietario de los Activos de Información

i. Identificar y categorizar los datos críticos que estén bajo su responsabilidad, incluyendo los requerimientos de confidencialidad, integridad y disponibilidad.
ii. Todos los activos de información deberán incluir la documentación de requerimientos de Seguridad de la información y éstas se presentaran al Grupo Estratégico de Seguridad de la Información para su revisión y validación
iii. Comunicar los requerimientos específicos de seguridad de información
iv. Definir el tiempo aceptable para recuperar su información (datos) y sistemas críticos además de identificar el impacto institucional en caso de una interrupción prolongada.
v. Definir la continuidad de los servicios de TIC institucional y requerimientos de recuperación en caso de desastre.
vi. Realizar una evaluación anual de riesgos para confirmar la confidencialidad, integridad y requerimientos de disponibilidad relacionados con su información y aplicaciones.
vii. Definir los requerimientos de seguridad de la información para que el área de sistemas de información sea capaz de proporcionar un nivel adecuado de seguridad a su Información(datos) y aplicaciones críticas
viii. Definir los requerimientos de seguridad física para la información, aplicaciones, cómputo y red.
ix. Revisar los registros y reportes de auditoria para asegurar el cumplimiento de las directrices de seguridad de Información (datos) y aplicaciones.
x. Participar en la solución de los incidentes relacionados con el acceso no autorizado o mal uso de Información (datos), incluyendo los incumplimientos a la seguridad, en la confidencialidad, disponibilidad e integridad de la Información (datos).

DSITIC 2-b) Responsabilidades de los Mandos Medios y Superiores con la Seguridad de la Información

i. Comunicar a sus empleados o subordinados las Directrices de Seguridad de Información y requerimientos relacionados con las TIC.
ii. Asegurar que los empleados comprendan que la violación de las Directrices de Seguridad de Información puede resultar en una acción disciplinaria y legal.
iii. Autorizar las solicitudes para que sus empleados accedan los recursos de SCT con base en las necesidades para realizar efectivamente las asignaciones de trabajo.

iv. Asegurar que todos los empleados que utilicen TIC en la SCT firmen un documento de responsabilidad para la seguridad y confidencialidad de la información (datos) y el documento se coloque en el archivo personal del empleado.
v. Notificar al departamento correspondiente del área de recursos humanos y a la UTIC de cualquier cambio al estado del empleado inmediatamente posterior a la transferencia o terminación de contrato.
vi. Revisar periódicamente las autorizaciones para que su área asegure que exista la justificación continua para el acceso a los recursos de TIC con los que se cuenta
vii. Asegurar que no se instalen en el área o proyecto bajo su cargo ningún software ni hardware informático o infraestructura de comunicaciones alguna, que no cuente con la revisión y aprobación de la UTIC.
viii. Reportar todas las violaciones de las Directrices a los responsables de la administración de la Seguridad de la información.
ix. Dar soporte a cualquier persona que reporte de buena fe una violación a las Directrices de Seguridad.
x. Contribuir y dar e apoyo necesario a los responsables de la seguridad de la información de la SCT, ante cualquier auditoría o revisión de los equipos, infraestructura y/o medio de almacenamiento de información que se encuentra en el área bajo su cargo.
xi. Asegurar que no se instalen ningún tipo de equipamiento o servicio de acceso a Internet dentro de las instalaciones de la SCT que no haya sido validado por la UTIC.

DSITIC 2-c) Responsabilidades de los Empleados

i. Comprender y cumplir con las Directrices de Seguridad de SCT.
ii. Utilizar los sistemas, aplicaciones y acceso a la red de SCT únicamente para propósitos de trabajo y no para uso personal o asuntos no autorizados.
iii. Mantener sus identificaciones de acceso de seguridad confidencialmente. (contraseñas o password).
iv. No se deberán compartir sus identificaciones (contraseñas o password) de acceso.
v. Comprender las directrices de protección de la información que se utilice, así como su responsabilidad respecto del uso, compartición y divulgación de Información sin autorización de la SCT.
vi. Instalar únicamente software aprobado por la UTIC que tenga licencia en su equipo de cómputo.
vii. No instalar software o hardware informático, infraestructura de comunicación alguna, que no haya sido validado por su Director de Área inmediato superior, el cual deberá contar con la validación de la UTIC.
viii. No instalar ningún tipo de equipamiento o servicio de acceso a Internet dentro de las instalaciones de la SCT que no haya sido validado por la UTIC.
ix. Utilizar los procedimientos apropiados para usar información obtenida fuera de las instalaciones de SCT.
x. Notificar a la UTIC inmediatamente. cualquier incidente o violación a la seguridad que descubra, incluyendo el mal uso de recursos, uso ilegal de software, virus o evidencia de actividad maliciosa.
xi. Responder por el buen uso e integridad de todos aquellos bienes e Información, propiedad de SCT, que utiliza en su actividad cotidiana y están bajo su resguardo.
xii. Responsable de la Información contenida en el equipo asignado propiedad de la SCT, que utiliza en su actividad cotidiana y deberá mantenerla respaldada.
xiii. Todo empleado al que se le asigna un equipo de cómputo debe firmar un resguardo del mismo.
xiv. No modificar equipos de cómputo a partir de la entrega de este o añadir Hardware (dispositivos o aditamentos) para mejorar la funcionalidad de algún equipo de la Institución por cualquier servidor público.

DSITIC 3 Contraseñas y claves de usuario

Todos los usuarios de sistemas, aplicaciones y en general de TIC deben controlar sus accesos a través de un usuario/contraseña (password) con la importancia de mantener la seguridad de información y de la responsabilidad que tienen con respecto a mantener controles de acceso efectivos.

Lineamientos:

DSITIC 3-a) Estándar de Contraseñas (Passwords) para usuarios

Las contraseñas para el acceso a los recursos de TIC deben cumplir con las siguientes características:

i. Deben tener una longitud mínima de 8 caracteres.
ii. Deben combinar caracteres alfanuméricos (al menos un número).
iii. Las contraseñas deben ser almacenadas en forma cifrada de tal forma que no puedan ser comprometidas con técnicas de análisis criptográfico.
iv. Las contraseñas deben viajar cifradas una vez que han sido introducidas en el recurso de procesamiento de información.
v. Si no es posible seguir con el estándar mencionado en los puntos anteriores porque la tecnología no lo permite, se deben tomar medidas alternas y estas medidas ser contempladas como adiciones o cambios a la presente directriz.

DSITIC 3-b) Gestión de usuario/contraseña (password)

Los usuarios/contraseña (password) de acceso a los sistemas, aplicaciones y servicios se gestionaran a través del SIGTIC.

DSITIC 3-c) Contraseñas (Passwords) de los usuarios

Todo usuario debe contar con un usuario/contraseña (password) de acceso y ésta será normada de acuerdo a cada plataforma, aplicación o servicios.

DSITIC 3-d) Asignación de contraseñas (passwords) de acceso

Controlar la asignación de claves de acceso mediante un proceso de administración que:

i. Obtenga el compromiso de los usuarios para mantener la confidencialidad de las contraseñas (passwords) de acceso a los sistemas.
ii. Cuando se crea un nuevo usuario (USER-ID) con su contraseña (password) de acceso y esta contraseña es utilizada por primera vez, el sistema deberá solicitar el cambio automático de esta contraseña (password).
iii. Que existan elementos que obliguen a los usuarios a cambiar de manera inmediata sus contraseñas (passwords) iniciales de acceso.
iv. Notifique de manera segura las contraseñas (passwords) iniciales de acceso a los usuarios.
v. Se debe evitar la notificación de claves de acceso a terceras partes.
vi. Los usuarios deben confirmar la recepción de contraseñas (passwords) de acceso.
vii. La gestión de usuarios/contraseña (password) de acceso para acceder a los sistemas, aplicaciones o servicios, de acuerdo a su perfil, será de forma individual para cada usuario que lo requiera a través de su encargado o responsable Informática de cada área.
viii. La contraseña (password) inicial no debe de ser igual al nombre de usuario, por lo que el usuario tiene la responsabilidad de cambiar la contraseña (password) inicial inmediatamente después que le sea asignada. (atendiendo el punto iii anterior).

DSITIC 3-e) Compartir Contraseña (Password)

Está prohibido compartir la cuenta y contraseña (password) de usuario asignada, ya que éstas son de carácter personal e intransferible

DSITIC 3-f) Revocación de Usuario/Contraseña (Password)

La UTIC tiene la atribución de revocar cualquier cuenta de usuario, por lo que puede ser revocada bajo cualquiera de los siguientes supuestos

i. Violación de las Directrices y Lineamientos establecidos
ii. Cuando la relación laboral entre el usuario y la Secretaría se dé por finalizada

iii. El usuario pone en riesgo la operación de la red, servicios o aplicaciones, siendo esto un comportamiento doloso o no
iv. Cuando el Titular del área lo considere necesario,
v. Si la UTIC considera una afectación o daño a las aplicaciones o servicios de TIC de terceros que hacen uso de estos.

DSITIC 3-g) Usuarios/Contraseñas de Administración

Las cuentas de administración del fabricante, creadas por omisión en los equipos, sistemas operativos, aplicativos, etc. tales como root, administrador, entre otros, deben ser inhabilitadas y solo podrán ser utilizadas en casos especiales.

i. De no ser posible su desactivación las contraseñas deben ser cambiadas posterior a la instalación del producto.

DSITIC 3-h) Excepción de cuentas con privilegios

En caso de que un usuario tenga necesidad de "privilegios" especiales para un sistema o aplicación (por ej., un "administrador"), se debe crear un Usuario/Contraseña (Password) diferente al que ya ha sido asignado.

DSITIC 3-i) Usuario/contraseña (password) de invitado

No se permite ningún usuario tipo "guest" "invitado" o símil en los sistemas operativos, por lo que la UTIC deshabilitara cualquier cuenta de usuario de este tipo de todos los servidores, aplicaciones y sistemas operativos que lo contengan.

i. Los servicios y aplicaciones pueden contar con usuario/contraseña (password) "invitado" siempre y cuando cuente con la validación de la UTIC.
ii. Los usuarios/contraseñas (passwords) "invitado" deben ser limitadas en cobertura, capacidad y tiempo de acuerdo a el servicio que acceden, debiendo describir y justificar a detalle para la validación de la UTIC.

DSITIC 3-j) Responsabilidad de Usuario/Contraseña (password)

Los usuarios son responsables del resguardo y uso que se haga del usuario/contraseña (password de acceso que se les haya entregado para acceso a equipos, sistemas informáticos, correo electrónico institucional y en general de dispositivos y servicios de TIC

DSITIC 3-k) Restricciones de Usuario/contraseña (password)

Escribir y dejar los Usuarios/contraseñas (passwords) bajo su resguardo en lugares de fácil acceso físico y/o visual al público.

DSITIC 3-l) Periodo de Usuario/Contraseña (password) activo

Cualquier cuenta de usuario/contraseña (password) de los servicios, plataformas o aplicaciones, que se identifique inactiva en un periodo de 90 días, la UTIC procederá a la baja y eliminación de información contenida en esta, sin responsabilidad para la UTIC de realizar un respaldo o restituirla.

DSITIC 3-m) Baja de accesos por renuncia o Baja de la Institución

Es responsabilidad del Coordinador/Director Administrativo de cada Unidad Administrativa o Centro SCT, que a través del encargado o responsable de Informática gestionar por el sistema SIGTIC, la cancelación de usuario/contraseña (password) del personal que ha causado baja, que evite el mal uso de usuarios/contraseñas y accesos de los recursos o sistemas institucionales, en un plazo no mayor de 10 días hábiles de la fecha de renuncia del usuario.

DSITIC 3-n) Contraseñas (Passwords) por vía telefónica

De ninguna forma o excepción las contraseñas (passwords) se transmitirán, darán a conocer o comunicaran vía telefónica. Si una contraseña es revelada debe ser modificada inmediatamente.

DSITIC 3-o) Bloqueo de Cuentas de Usuario

Las cuentas de usuario pueden ser bloqueadas de manera automática o manual por los administradores de las TIC o servicios de acuerdo a los siguientes criterios:

i. La cuenta esta inactiva por 45 días.
ii. La cuenta se encuentre envuelta en un incidente de seguridad.

DSITIC 3-p) Desbloqueo de cuentas

Las cuentas bloqueadas por las situaciones mencionadas en el punto anterior, se reactivaran por los administradores de las TIC o servicios, con la aprobación por escrito del mando inmediato superior del usuario afectado y remitido este escrito a la UTIC.

DSITIC 3-q) Bitácoras de Auditoria de Usuarios/Contraseñas

Los sistemas, aplicaciones, plataformas y servicios de TIC, deben contar con una bitácora de registro en donde se almacenen los cambios de Usuarios/Contraseñas aplicados.

DSITIC 4 Tercerización (Outsourcing) de servicios de TIC

Garantizar mediante documentación que los requerimientos de Seguridad de la Información se cumplen, especialmente en aquellos casos en los que un determinado ambiente es confiado a un proveedor ya sea en instalaciones de SCT o en las suyas propias.

Lineamientos:

DSITIC 4-a) Identificar Riesgos y mitigación

i. Evaluar los riesgos de Seguridad de la Información asociados con la tercerización en general y en lo particular para aquellas funciones de la Secretaría a transferir.
ii. Identificar los ambientes, procesos e información críticos y sensitivos.
iii. Evaluar las prácticas de seguridad de la Información y estándares de los proveedores.
iv. Identificar las interdependencias entre la función tercerizada y el resto de las funciones de la UTIC.
v. Desarrollar una estrategia de continuidad de los servicios en relación con el proveedor para los casos de terminación temprana del acuerdo o contrato

DSITIC 4-b) Establecer Acuerdos con los Proveedores sobre Seguridad de Información

i. Cumplir con las buenas prácticas de seguridad de la información, incluyendo el manejo de información acorde a su Clasificación establecida por la UTIC.
ii. Proporcionar la información sobre los Incidentes de Seguridad
iii. Mantener la Confidencialidad de la información obtenida o recopilada en el transcurso del acuerdo o contrato
iv. Proteger la integridad de la información usada para asegurar que es completa, precisa y válida
v. Asegurar la disponibilidad de la información y los Sistemas proveyendo el equipo que garantice los tiempos SLA
vi. Limitar el acceso a los activos de la SCT solo al personal autorizado acordado entre la SCT y el proveedor
vii. Proteger la información que puede ser fácilmente identificable.
viii. Garantizar mediante convenios la Continuidad Operativa
ix. Asegurar el retorno y/o destrucción de la información, software o equipo según se establece en el procedimiento de borrado seguro.

DSITIC 4-c) Procedimientos de contacto para la Seguridad de la Información UTIC/Proveedor

Establecer procedimientos para el tratamiento confidencial de los problemas de seguridad con directivos del proveedor, adicional a los esquemas de escalación de incidentes establecidos con los proveedores.

DSITIC 4-d) Derechos de verificación y auditoria con el Proveedor

Establecer el derecho de auditar, monitorear y verificar el trabajo desarrollado por el proveedor, las licencias de uso, definir los derechos de propiedad intelectual y de los datos.

DSITIC 4-e) Contingencias del servicio del proveedor

Establecer convenios para los casos de indisponibilidad de servicios del proveedor.

DSITIC 4-f) Manejo de equipamiento de TIC con el proveedor

Para la entreguen o recolección de equipamiento de TIC el proveedor presentara la documentación que especifica el destino y procedencia de este.

DSITIC 5 Clasificación y Control de Activos

Identificar a los dueños de la información y asignar sus responsabilidades con respecto a estos activos, realizando un análisis para clasificar e identificar los riesgos asociados.

Lineamientos:

DSITIC 5-a) Registros de inventario de equipos de TIC

Los equipos de TIC propiedad de la Secretaría deben estar registrados en el inventario de mobiliario y equipo controlado por la Dirección General de Recursos Materiales.

i. Este inventario de equipamiento de TIC debe ser actualizado de acuerdo a los movimientos aplicados en cada Unidad Administrativa y reportado la DGRM.

DSITIC 5-b) Todo activo de información debe tener un propietario responsable

Identificados los activos y los sistemas de información asociados se identificara al dueño que tendrá la responsabilidad del activo.

DSITIC 5-c) Toda la información de la Secretaría debe tener clasificación de seguridad

La información se clasificara por lo menos en tres categorías para definir su nivel de importancia y seguridad: PUBLICA, USO INTERNO y CONFIDENCIAL (A, AA y AAA).

- CONFIDENCIAL (AAA): Información de uso únicamente dentro de la Secretaría. Su difusión no autorizada puede impactar muy seriamente a la Secretaria.
- USO INTERNO (AA): Información que se destina para uso interno al interior de la Secretaría.
- PUBLICA (A): Información que no se clasifica dentro de las categorías anteriores. La Secretaría, y los empleados, no tendrán ningún impacto adverso debido a la difusión de esta información.

DSITIC 5-d) Etiquetas en los medios de almacenamiento de información

La información almacenada en cualquier medio (físico, magnético, portable o impresa), debe ser etiquetada con la categoría correspondiente. En caso de que los archivos contengan información de varios tipos, ésta debe etiquetarse con la clasificación más alta de cualquier elemento de información contenida.

DSITIC 5-e) Responsables de los activos críticos

Identificar a los funcionarios responsables por activo o aplicación de información crítico que maneja. Este funcionario debe conducir un ejercicio de análisis de riesgo cada año como mínimo para asegurar la integridad, disponibilidad y confidencialidad de la información.

DSITIC 5-f) Propietario único en caso de duplicidad

Si hubiera más de un propietario potencial para la información, la unidad administrativa propietaria designara la responsabilidad a un solo individuo preferentemente quien tenga mayor jerarquía sobre ella.

DSITIC 5-g) Propiedad de información operacional y de red

Con la excepción de la información operacional o de la red, la UTIC no es dueña de ningún activo de información de la SCT.

DSITIC 5-h) Definición de los controles de seguridad en los activos

No serán delegadas a un proveedor de servicio externo a la Secretaria las responsabilidades que tiene un propietario designado de información, para especificar los controles apropiados para la Seguridad de la misma

DSITIC 5-i) Frecuencia de los análisis de riesgo de los activos críticos

Debe realizarse por lo menos un análisis de riesgos al año, que permita identificar el nivel de exposición a que están sujetos los activos críticos de información, especialmente en casos de tercerización.

DSITIC 5-j) Revisión del Propietario de la Información sobre el acceso de los usuarios

El acceso de los usuarios a recursos protegidos deberá ser revisado al menos una vez por mes por el dueño de la información con el objeto de asegurarse que los accesos siguen siendo válidos y que los privilegios asociados con los accesos siguen siendo requeridos.

DSITIC 5-k) Asignación de Activos de los usuarios

Con excepción de los servidores públicos con nivel jerárquico de mando medio o superior, no se le permite la asignación de más de un equipo de TIC por persona, a menos que por el desempeño de sus funciones y el uso esté justificado o autorizado por su Jefe Inmediato, y se cuente con el equipo disponible.

DSITIC 6 Directriz de Seguridad para el Personal

La UTIC debe asegurarse que los empleados de la SCT comprenden y se comprometen con directrices, lineamientos y procedimientos de seguridad.

Lineamientos:

DSITIC 6-a) Las descripciones de puestos incluyen responsabilidades de Seguridad de la Información

Incluir dentro de las descripciones de puestos, las responsabilidades relativas a la seguridad de los activos dentro de la organización, y el cumplimiento de los procedimientos de seguridad.

DSITIC 6-b) La responsabilidad de seguridad de la información

La seguridad de la información es responsabilidad de todos los usuarios y empleados de SCT.

DSITIC 6-c) Incumplimiento de las Directrices de Seguridad

Todos los empleados regulares, eventuales y terceros deberán firmar el acuerdo de desempeñar su trabajo conforme a las Directrices de seguridad.

DSITIC 6-d) Acuerdo de confidencialidad se refrendan al menos una vez por año

Todo el personal involucrado en el alcance de SGSI debe contar con un acuerdo firmado de confidencialidad y no exposición de la información con la UTIC.

DSITIC 6-e) Difusión y concientización de las Directrices de Seguridad

Establecer un programa de concientización de seguridad dirigido a todo el personal, con respecto a la importancia de los procesos de seguridad de la información.

DSITIC 6-f) Identificación de personal Externo

Los proveedores, personal de limpieza, personal de vigilancia, y personal de servicio social o prácticas profesionales deben identificarse mediante una credencial de la empresa o cualquier otra identificación oficial antes y durante todo el tiempo que permanezcan en las instalaciones de la UTIC o en su momento portar el gafete institucional para su acceso.

DSITIC 6-g) Involucrados ante incumplimiento o violación de Directrices de Seguridad

En caso de cometerse una violación a las Directrices de Seguridad de SCT, se hará un seguimiento en el que estarán involucradas las áreas del OIC, Recursos Humanos hasta su completa aclaración. Las faltas en el cumplimiento de las Directrices de Seguridad, pueden resultar en acciones disciplinarias y en algunos casos hasta la aplicación del Código Penal Federal.

DSITIC 6-h) Renuncia de Personal

Restringir el acceso físico, así como quitar los privilegios otorgados a equipos ó sistemas institucionales a los que acceso el personal que fue despedido o renuncio a la SCT.

DSITIC 7 Directriz de Seguridad Física

Instrumentar reglas administrativas, procedimientos y mecanismos físicos para garantizar la protección de los activos.

Lineamientos:

DSITIC 7-a) Perímetros Seguros

Implementar barreras y controles (Perímetro seguro) para proteger los activos o servicios críticos de información, que delimiten el acceso a personal no autorizado.

DSITIC 7-b) Controles para proteger las áreas seguras

Las áreas seguras contaran con los controles de entrada para limitar solo al personal autorizado el acceso. Todo objeto que se introduzca a las áreas restringidas, estará sujeto a una revisión detallada para minimizar riesgos de sabotaje y destrucción.

i. Toda oficina, salas de juntas, auditorios o almacenes en donde se encuentre documentación sensible, confidencial y equipamiento de TIC se mantendrá bajo llave.
ii. En caso de que el personal de SCT o Terceros se ausente de su oficina, área o lugar de trabajo se asegurar que la documentación y equipo de TIC están asegurados bajo llave

DSITIC 7-c) Acceso a áreas restringidas

El acceso a los centros de Datos, áreas en las que se procese ó maneje información confidencial, de uso Interno, conmutador y equipos de comunicaciones, estarán estrictamente controlados y restringidos.

DSITIC 7-d) Responsables de las áreas restringidas

Se asignara un responsable(s) de la seguridad del sitio(s) o área(s) restringidas; cuyas funciones son, y que no son limitativas:

iii. Otorgar la autorización de acceso al sitio
iv. Verificar y validar que la Bitácora de acceso físico al sitio se tenga a la vista y disponible para el registro de acceso
v. Ingresar o sustraer cualquier tipo de dispositivo de almacenamiento de información sin previo registro y revisión de su contenido y con autorización por escrito por el responsable del mismo.
vi. Ingreso o sustracción de cualquier tipo de equipo de cómputo, dispositivo, herramienta, etc., sin previo registro y revisión de su contenido y con autorización por escrito por el responsable del sitio.
vii. Autorizar cualquier asunto que requiera atención para la seguridad del área

DSITIC 7-e) Protección a equipos de soporte (faxes y copiadoras)

Los equipos de soporte como copiadoras y faxes deberán estar en sitios seguros, con el fin de minimizar el riesgo de que usuarios no autorizados tengan acceso a información confidencial.

DSITIC 7-f) Protección a cables de energía y comunicación

Los cables de energía y las líneas de comunicaciones deben estar protegidos contra daños e intercepciones.

DSITIC 7-g) Área de carga y descarga de los Centros de Datos

Las áreas de carga, descarga de material y equipo de los Centros de Datos estarán aisladas. Esta área deberá estará restringida solamente al personal autorizado.

DSITIC 7-h) Protección a los documentos de la SCT

El personal guardará cualquier documento y cualquier información en el medio en que se encuentre, para reducir el riesgo de pérdida y daño a la información, especialmente fuera del horario normal.

DSITIC 7-i) Bóvedas para respaldos de información

Los medios magnéticos que contienen respaldos de información crítica, serán protegidos contra robo y estarán guardadas en una bóveda externa al centro de datos (de SCT o de terceros).

DSITIC 7-j) Protección de bóvedas

El acceso a las bóvedas externas deberá estar debidamente controlado, y existirá un control estricto de entrada y salida de objetos.

DSITIC 7-k) Evacuación en casos de contingencias

Se deberá contar con planes documentados y probados para evacuación del personal en caso de cualquier contingencia.

DSITIC 7-l) Protección de los servidores

Los servidores centrales y remotos estarán ubicados en un ambiente seguro. Se tomarán medidas para limitar el acceso físico al servidor, los servidores estarán ubicados en un armario (rack) o sitio cerrado y sólo personal autorizado tendrá acceso al mismo.

DSITIC 7-m) Salida de equipo de las instalaciones

Ningún equipo, datos o software podrán ser retirados de las instalaciones de SCT sin la debida autorización por escrito.

DSITIC 7-n) Evitar daños de Equipo de protección a los activos de información

Las áreas seguras deberán contar con el equipo apropiado de Seguridad Física para evitar daños tanto a la información como a los equipos de hardware y se deberá instruir al personal sobre el uso y funcionamiento de los equipos.

DSITIC 7-o) Suministro ininterrumpido de energía

Los equipos que efectúan las operaciones críticas de SCT contarán con equipo UPS para suministros de energía en caso de falla en la corriente eléctrica.

DSITIC 7-p) Protección de robo de partes de los equipos

Las estaciones de trabajo, las computadoras personales y los servidores estarán protegidos contra el robo de partes, de tal forma que no puedan ser abiertos. Las llaves para las estaciones de trabajo serán controladas por la administración de los departamentos.

DSITIC 7-q) Protección del equipo en áreas usuarias

Cada área deberá analizar las protecciones de seguridad que requiera el equipo personal, que será utilizado fuera de las instalaciones de la Secretaría.

DSITIC 7-r) Revisión obligatoria al desechar medios de información

Todos los dispositivos removibles tales como discos, cintas o memorias deberán ser revisados, para asegurar que no contengan información confidencial o software con licencia antes de ser desechados.

DSITIC 7-s) Controles en el manejo de Información confidencial o reservada

Con la premisa de evitar que información clasificada como confidencial o reservada sea extraída de los equipos de la Secretaria, ningún componente de cómputo o electrónico, sin importar su tamaño o valor, puede ser retirado de las instalaciones de la SCT sin autorización expresa mediante un documento oficial autorizado por el área o responsable designado.

DSITIC 7-t) Reutilización de Medios de Información

Toda vez que no sean requeridos los medios removibles (Cintas, Memorias USB, CD, diskettes, etc.) debe borrarse todo su contenido por medio seguro para evitar que la información pueda ser recuperada y/o expuesta a personas no sean autorizadas o externas a la Institución, aplicando el "procedimiento de borrado seguro establecido".

DSITIC 7-u) Controles de Seguridad Física de la Institución

Todos los funcionaros de la Secretaria, proveedores, personal de servicio social y toda aquella persona que ingresa a las instalaciones de la SCT independientemente de un asunto relacionado con las TIC, deberá acatar las disposiciones de Seguridad Física que se tienen implementadas en la institución, por el área encargada de la Seguridad Física de la SCT.

DSITIC 8 Directriz de Operación de Cómputo

Asegurar la operación eficiente de los equipos de cómputo, mediante los procedimientos de administración, operación y monitoreo de los equipos de cómputo.

Lineamientos:

DSITIC 8-a) Acceso a los equipos de cómputo

Se debe contar con un sistema de administración de passwords que garantice la calidad de los mismos, es decir, que sean passwords fuertes, de acuerdo a lo establecido por la UTIC como es:

i. longitud mínima
ii. caracteres alfanuméricos
iii. tiempo de vida, etc.

DSITIC 8-b) Procedimientos de acción inmediata para incidentes de seguridad

Establecer procedimientos para el manejo de incidentes de seguridad que permitan una respuesta rápida y efectiva.

DSITIC 8-c) Manejo de los incidentes y problemas de seguridad

Los incidentes y problemas de la Seguridad de la Información se manejaran por la UTIC incluyendo las situaciones de tercerización.

DSITIC 8-d) Programa Institucional de Protección contra Virus

El programa institucional de Protección contra Virus en los equipos de cómputo contara con las actividades de concientización involucrando a todo el personal.

DSITIC 8-e) Nueva Aplicación a Producción

Todos los aplicativos se apegaran al proceso de Gestión de Cambios para aceptar una nueva aplicación en el ambiente de producción en todas las plataformas.

DSITIC 8-f) Procedimientos de respaldo y recuperación de información

Los procedimientos de respaldo y recuperación de la información contaran con los procedimientos de recuperación de respaldos de acuerdo a los requerimientos.

DSITIC 8-g) Continuidad de Servicios

Definir la estrategia de recuperación a nivel Secretaría que permita contar con un centro de datos alterno en casos de desastre.

DSITIC 8-h) Facilidades de Seguridad de los Sistemas Operativos

El uso y operación de los Recursos de los Sistemas Operativos, para la administración de la seguridad será función exclusiva de la UTIC o de quien designe esta, como responsable en la Unidad Administrativa o Centro SCT de estos recursos.

DSITIC 8-i) Retención de registros de seguridad

Se registrarán y conservarán los accesos y cambios en la Seguridad; el periodo a retener de los registros será definido en función de la necesidad del área administrativa y la plataforma.

DSITIC 8-j) Manejo de medios magnéticos

Se aplicaran los procedimientos específicos para el manejo de dispositivos como cintas, disquetes, cassettes, reportes impresos, incluyendo su distribución, transferencia, etiquetado y almacenamiento que aseguren el manejo seguro de la información y de autorización para el retiro de los dispositivos fuera de la organización.

DSITIC 8-k) Respaldo de Información confidencial

Toda información en formato electrónico clasificada como reservada o confidencial, será respaldada con la periodicidad que su criticidad lo demande.

DSITIC 8-l) Autenticación en operaciones con terceros

Todas las operaciones de archivos entre SCT y terceros deben autenticarse y asegurarse.

DSITIC 8-m) Correo electrónico

Los controles aplicados en el correo electrónico mantendrán la integridad, confidencialidad y autenticación de la información en los equipos de cómputo que la contienen para su tratamiento, transmisión o almacenamiento.

DSITIC 8-n) Auditorias de Seguridad

Todos los sistemas de información en producción (Hardware y Software) deberán sujetarse a una evaluación para determinar el mínimo de controles, necesarios para reducir al mínimo los riesgos.

DSITIC 8-o) Carpetas compartidas

Los usuarios utilizaran las herramientas que permiten asegurar el acceso a carpetas compartidas mediante al menos un usuario/password.

DSITIC 8-p) Prohibiciones en equipos de Cómputo

Las actividades que están prohibidas en el uso de equipos de cómputo incluyen, más no limitan:

i. Desinstalar, desactivar o dejar de actualizar el software antivirus institucional.
ii. Instalar software de antivirus diferente al institucional.
iii. Descargar software directamente de Internet sin autorización de la UTIC.
iv. Realizar, con cualquier tipo de herramienta de software, cualquier acción que vulnere la seguridad de la información de SCT, tales como escaneo de puertos, pruebas de vulnerabilidad, etc.
v. Realizar cambios a cualquier parámetro de los equipos de cómputo, tales como comunicaciones, operación, administración del sistema operativo y sus aplicaciones.
vi. Abrir equipos de cómputo, reparar equipos de cómputo, insertar o sustraer cualquier dispositivo de los equipos de cómputo de la Institución.

DSITIC 8-q) Servidores

Todos los servidores en cualquiera de sus modalidades de arrendamiento, comodato, adquisición, préstamo, outsorcing que contengan, procesen, respalden, etc. información deberán estar ubicados en el Centro de Datos de la SCT.

DSITIC 8-r) Ambiente de Producción aislado

Las áreas de Desarrollo de Sistemas no accederán, modificaran o respaldaran información de los ambientes de Producción. Los cambios al ambiente productivo, se realizarán sola y exclusivamente con el proceso de Gestión de Cambios.

DSITIC 8-s) Antivirus y código malicioso

Todos los equipos de cómputo de la SCT deben tener instalado, actualizado y activado el software de antivirus institucional, incluyendo los servidores cuyo sistema operativo así lo permita, para la eliminación de virus y código malicioso.

DSITIC 8-t) Baja de Servicios por renuncia o Baja de la Institución

El encargado o responsable de Informática gestionara mediante el Sistema de Gestión de Tecnologías de Información y Comunicaciones (SIGTIC), la baja de los servicios del personal que ha causado baja, que evite el mal uso de los recursos o sistemas institucionales.

DSITIC 8-u) Mantenimientos preventivos y correctivos de equipo de cómputo

Los calendarios de mantenimiento preventivo se deben acordar entre el proveedor y la UTIC, evitando al máximo que interfiera con el horario de oficina de los usuarios. La UTIC debe confirmar con el Administrativo o al usuario, la fecha y hora en la cual debe estar disponible su equipo para el servicio de mantenimiento preventivo.

DSITIC 8-v) Verificar componentes del equipo de cómputo

Durante los mantenimientos preventivos, se debe verificar que los componentes del equipo, el software instalado, su ubicación física y los servicios que estén utilizando, concuerden con los registros de informática, en caso contrario se debe reportar la anomalía a la UTIC.

DSITIC 8-w) Autorizados para apertura de cubiertas del equipo de cómputo

El personal designado para el mantenimiento preventivo y correctivo del equipo de cómputo, es el único que está autorizado para abrir los gabinetes o las cubiertas de las computadoras o periféricos.

DSITIC 8-x) Reporte de fallas

Las fallas o mal funcionamiento de los equipos de cómputo, deben ser reportadas a la Mesa de Ayuda de la UTIC. En ningún caso debe intentar reparar equipo de cómputo, el personal no autorizado.

DSITIC 9 Directriz de Operación Red

Asegurar la operación eficaz y eficiente de la red de comunicaciones mediante los procedimientos de administración, operación y monitoreo de la red de comunicaciones

Lineamientos:

DSITIC 9-a) Configuraciones de Red

Los componentes de la red deben de contar con las configuraciones adecuadas de seguridad y con la actualización de parches y versiones indicadas por el proveedor.

DSITIC 9-b) Procedimientos de acción inmediata para incidentes de seguridad de red

Establecer procedimientos para el manejo de incidentes de seguridad de red que permitan una respuesta rápida y efectiva, por parte de la UTIC incluyendo las situaciones de tercerización.

DSITIC 9-c) Procedimientos de respaldo y recuperación de información

Los procedimientos de respaldo y recuperación de la información se conformaran de acuerdo a los requerimientos del dueño de la información, siempre y cuando se cuente con los recursos de TIC para cubrir el requerimiento.

DSITIC 9-d) Retención de registros de seguridad

Se registrarán y conservarán los accesos y cambios en la Seguridad; el periodo a retener de los registros será definido en función de la necesidad del área administrativa y la plataforma.

DSITIC 9-e) Controles de información en la red

Se actualizarán por lo menos una vez por año los controles que vigilan la integridad y confidencialidad de los datos que viajan por la red, así como los controles que vigilen los accesos a los servicios conectados.

DSITIC 9-f) Expansión o ampliación de alcance de la red

Se deben tomar las medidas necesarias cuando se lleve a cabo cualquier expansión de la red para asegurar la protección de la misma y de la información almacenada procesada y transmitida.

DSITIC 9-g) Seguridad en la red Wireless

El uso de redes inalámbricas debe ser bajo un estricto control de configuración de seguridad, por el riesgo que representan

DSITIC 9-h) Seguridad en dispositivos móviles

Siempre que se usen equipos móviles se asegurara que la información de SCT no se comprometa, teniendo en cuenta aspectos de seguridad física, control de acceso lógico, respaldos de la información contenida en el equipo, protección contra virus, código móvil, entre otros

DSITIC 9-i) Equipos de Comunicaciones (Telecomunicaciones)

Se protegerá su configuración, a través de usuario/password robustos para los atributos de administración. Todos los intentos de traspasar o evadir las medidas de seguridad del acceso de la red institucional, se consideran como una falta grave que se debe reportar al responsable de seguridad.

DSITIC 9-j) Plan de Direccionamiento

La SCT utilizará un esquema de direccionamiento único para todos los sitios a nivel nacional, el cual será determinado por la UTIC.

i. **Plan de Direccionamiento con Terceros**
La conexión con redes externas a la SCT, la UTIC analizará el esquema de conexión y definirá el direccionamiento que se aplicará. No se permitiendo el uso o expansión de direccionamiento IP que no haya sido aprobado por la UTIC.

ii. **Direccionamiento para equipos críticos**
Se asignaran segmentos específicos para los equipos críticos o sensibles de la SCT.

DSITIC 9-k) Respaldo de Información confidencial

Toda información en formato electrónico clasificada como reservada o confidencial, será respaldada con la periodicidad que su criticidad lo demande.

DSITIC 9-l) Autenticación en operaciones con terceros

Todas las operaciones de archivos entre SCT y terceros deben autenticarse y asegurarse.

DSITIC 9-m) Intercambio de datos y software con terceros

Los intercambios de software o datos con terceros requerirán de un acuerdo formal por escrito. En el acuerdo mencionado se deberán especificar los términos del intercambio, así como la manera con la cual el software y los datos serán manejados y protegidos.

DSITIC 9-n) Auditorias de Seguridad

Todos los sistemas de información en producción (Hardware y Software) deberán sujetarse a una evaluación para determinar el mínimo de controles, necesarios para reducir al mínimo los riesgos.

DSITIC 9-o) Protección de información confidencial en la red

La información confidencial a ser transmitida sobre la red se cifrara con los estándares y procedimientos establecidos.

DSITIC 9-p) Internet

Se debe proteger toda la información clasificada como reservada o confidencial que pase sobre redes públicas como Internet, así mismo debe controlarse el uso de Internet tomando en cuenta el flujo de datos, el monitoreo de la información transmitida por este medio y las implicaciones legales aplicables.

DSITIC 9-q) Mantenimientos preventivos y correctivos de TIC

Los calendarios de mantenimiento preventivo se deben acordar entre el proveedor y la UTIC, evitando al máximo que interfiera con el horario de oficina de los usuarios y sus servicios.

DSITIC 10 Directriz de Acceso a Sistemas

Se controlara el acceso a los servicios y sistemas de la SCT y en las instalaciones de terceros que brindan a la Institución un servicio.

Lineamientos:

DSITIC 10-a) Identificación de Usuario

Todos los Usuarios que requiera acceder a los sistemas institucionales, aplicaciones, etc., se le asignara una identificación de usuario personal única e irrepetible.

DSITIC 10-b) Funcionalidad de los programas de seguridad

Todos los recursos de los sistemas serán protegidos por programas de seguridad. Dentro de la funcionalidad con que se debe contar para estas herramientas de protección de acceso, están las de notificación en caso de ser detectada alguna violación de seguridad.

i. Identificar y verificar la identidad y si es necesario conocer hasta la identificación y localización de la terminal o estación de trabajo de cada usuario autorizado.
ii. Registrar los accesos exitosos y fallidos al sistema.
iii. Proveer un sistema de administración de claves de acceso que asegure la calidad de las mismas.
iv. Restringir el tiempo de conexión de los usuarios.

DSITIC 10-c) Controles de Acceso al Sistema y monitoreo

Establecerse controles que prevengan el acceso no autorizado a la información. Estableciendo un proceso de monitoreo con el fin de registrar intentos de acceso no autorizados a los recursos protegidos.

DSITIC 10-d) Registro de Usuarios para acceso al sistema y servicios

El acceso a los servicios y aplicaciones se controlara mediante un procedimiento de registro que contemple dar de baja usuarios inexistentes. El procedimiento de registro de usuarios deberá contemplar los siguientes elementos:

i. Verificar que el usuario tiene la autorización del dueño de la información para acceder a esta.
ii. Verificar que los accesos asignados al usuario son congruentes con sus responsabilidades y con los objetivos de la SCT.
iii. Entregar al usuario por escrito los accesos concedidos y obtener la firma de éste.
iv. Asegurar que no se proporciona el acceso a los servicios hasta que el procedimiento de autorización ha terminado.
v. Mantener un registro formal de todas las personas registradas para usar los servicios.
vi. Dar de baja los usuarios que han cambiado sus responsabilidades.
vii. Establecer un procedimiento para aquellos empleados que son dados de baja por cualquier motivo, Recursos Humanos informará al área de seguridad para cancelar en forma inmediata todo tipo de acceso a los recursos de TI.
viii. Mensualmente se deberá verificar que no existen usuarios que han dejado de laborar en SCT.
ix. Mantener un registro de los perfiles registrados para el uso de sistemas aplicaciones o servicios.

DSITIC 10-e) Herramientas automatizadas

La UTIC contara con herramientas tecnológicas que permitan a la Secretaría controlar costos y necesidades de cómputo, aumentar la eficiencia y demostrar el cumplimiento de licenciamiento, así como responder de manera oportuna a los requerimientos de auditoria y de planeación. Dicha herramienta deberá detectar y monitorear automáticamente dispositivos de cómputo conectados a la RDM de la Secretaria, manteniendo a detalle el inventario de Hardware y Software en uso, así como mantener actualizada la CMDB de la Secretaría.

DSITIC 10-f) Asignación de privilegios

La asignación de privilegios de acceso a la información, deberá ser controlada mediante un proceso de autorización. Este proceso deberá:

i. Identificar los privilegios asociados con cada programa producto del sistema y el perfil al cual se deberá asignar.
ii. Asignar privilegios únicamente a quien por sus funciones así lo requiera.
iii. Estar basado en un proceso de autorización y registrar todos los privilegios asignados.

DSITIC 10-g) Autorización del Propietario de la Información

Los usuarios deberán tener la autorización del dueño o propietario de la información de utilizar los recursos que se requieran para el desempeño de sus funciones.

DSITIC 10-h) Protección de acceso en línea desde Internet

Los sistemas de información de la SCT que accedan desde Internet, deben contar con los mecanismos de seguridad apropiados para evitar que los sistemas y la información se vean comprometidas, los mecanismos de acceso pueden ser tales como una VPN.

DSITIC 10-i) Disponibilidad de los servicios de seguridad

Los servicios de seguridad deben estar disponibles siempre que los sistemas de SCT sean utilizados.

DSITIC 10-j) Perfiles reservados para auditoria

Contar con perfiles especiales para ser usados por la función de auditoria.

DSITIC 10-k) Notificación a Propietarios de Activos en casos de violación de seguridad

Los dueños o Propietarios de los activos de información serán notificados tan rápido como sea posible de cualquier incidente de violación de seguridad.

DSITIC 10-l) Auditoria de acceso de los usuarios

Mantener un control efectivo en el acceso a la información y a los servicios, por lo que el administrador de seguridad, en coordinación con los dueños de información, deberá realizar una de revisión de los accesos de los usuarios.

DSITIC 10-m) Inhibición de terminales de trabajo

Todos los equipos personales y terminales de trabajo deberán contar con claves que inhiban el acceso a la información cuando éste es encendido o cuando es desatendido por un periodo determinado.

DSITIC 10-n) Participación de Propietarios en controles de acceso

Los requerimientos de SCT referentes al control de acceso a la información deberán ser definidos y documentados por los Propietarios de ésta.

DSITIC 10-o) Autenticación de usuarios y terminales

Asegurar que los usuarios conectados a los servicios de cómputo no comprometan la seguridad de cualquier otro servicio, es necesario establecer un estricto control de acceso sobre toda conexión, autenticando usuarios y terminales

i. Un empleado no tendrá más de un user-ID o identificación de usuario para acceder a un sistema.
ii. Los empleados usarán la misma identificación de usuario para todas las plataformas y aplicaciones que utilicen

DSITIC 10-p) Procedimientos de login de usuarios

Los procedimientos de LOGIN serán diseñados de acuerdo a las funciones desarrolladas por el usuario, con el objeto de evitar accesos no autorizados; Considerando:

i. No desplegar información del sistema o identificación de la aplicación hasta que el procedimiento de LOGIN haya terminado.
ii. Desplegar un mensaje que indique que los servicios serán utilizados únicamente por usuarios autorizados.
iii. Validar la información de entrada al procedimiento de LOGIN hasta que se hayan tecleado todos los datos.
iv. Limitar el número de intentos de LOGIN.
v. No prestar ayuda en línea, si existe un error durante el procedimiento de LOGIN.
vi. Limitar el tiempo máximo y mínimo del procedimiento de LOGIN.
vii. Desplegar información de fecha y hora del último LOGIN exitoso.
viii. Detallar los intentos de LOGIN fallidos después del último LOGIN exitoso.

DSITIC 10-q) Conexión desatendida

Inactivar las conexiones a los servicios utilizados desde una terminal después de un periodo de desatención (Time out).

DSITIC 10-r) Acceso a utilerías del software de sistema operativo

Se aplicaran restricciones de acceso a las utilerías de software de sistema operativo y únicamente el personal técnico autorizado tendrá el acceso a este previo aplicación. Cada vez que se lleguen a utilizar, se deberá de registrar en alguna bitácora protegida. La bitácora deberá ser revisada con oportunidad por el responsable de la operación del sistema.

DSITIC 10-s) Control de la Bibliotecas de Programas

El control sobre las bibliotecas de programas fuentes contendrá las siguientes medidas:

i. Cada aplicación deberá contar con una biblioteca propia.
ii. Los programas bajo desarrollo o mantenimiento no deberán estar en el ambiente productivo.
iii. Los programas fuente deberán estar en un ambiente seguro.
iv. Deberá existir un LOG de auditoria que mantenga todos los accesos a las bibliotecas de programas fuente.
v. Las versiones anteriores deberán ser copiadas a otro medio magnético y borradas de la copia actual.

vi. El mantenimiento a los programas fuente deberá ser controlado por un proceso de gestión de cambios.

DSITIC 10-t) Verificación de acceso

Los procedimientos indicaran como se verificara a los usuarios que acceden a las funciones habilitadas, tomando en cuenta al menos los eventos:

i. Mensajes de falla de acceso.
ii. Revisión de los patrones de LOGIN buscando indicaciones de terminación anormal.
iii. Seguimiento de accesos a los usuarios con accesos privilegiados.
iv. Verificación de uso de los recursos sensitivos.
v. Seguimiento de transacciones identificadas como sensitivas.

DSITIC 10-u) Sincronización de los relojes de los sistemas

La sincronización de los relojes en los sistemas será única, con el fin de facilitar las tareas de auditoria y seguimiento de evidencias legales.

DSITIC 10-v) Información de los proveedores de SCT

Toda la información confidencial o propietaria que haya sido confiada a SCT por un proveedor externo, deberá de ser asegurada y manejada como si fuera información confidencial. Así mismo toda información confiada a un proveedor externo deberá ser asegurada y manejada en forma confidencial por el mismo.

DSITIC 10-w) Vigencia de acceso de nuevos usuarios

Las cuentas nuevas de usuario generadas, tendrán dos días de vigencia, por lo que de no ser usada se dará de baja siendo obligación y responsabilidad del usuario gestionar la asignación de una cuenta nueva.

DSITIC 10-x) Protectores de pantalla

Si el sistema de cómputo está conectado a la red o contiene una aplicación crítica o confidencial, los usuarios deberán desconectar o apagar su sistema antes de salir de su área de trabajo o en su caso optara por utilizar un protector de pantalla que se active por tiempo transcurrido de no uso y se active el acceso a la sesión del equipo por contraseña.

DSITIC 10-y) Gestión de accesos y permisos

Los accesos y permisos a los sistemas o aplicaciones se gestionaran a través del SIGTIC.

DSITIC 11 Directriz para la Seguridad en el Desarrollo y Mantenimiento de Sistemas

Se deben considerar los requerimientos de seguridad de la información desde la etapa de análisis del sistema incluyendo las necesidades de respaldo y deberán ser justificados como parte de un análisis de factibilidad.

Lineamientos:

DSITIC 11-a) Catálogo de Sistemas

Las solicitudes de desarrollo, compra y uso de software especial deben dirigirse al Titular de la Unidad, con una explicación detallada de cómo se va a utilizar, los beneficios que se esperan con su implementación, y en qué equipo o equipos se deberá instalar, para que dictamine la procedencia y se integre al catálogo de Sistemas de la SCT

DSITIC 11-b) Controles de Seguridad en los nuevos sistemas o actualización de anteriores

Los nuevos sistemas para los requerimientos de SCT así como las mejoras de los sistemas ya existentes deberán contemplar los controles de seguridad. Estos controles tenderán a cubrir los aspectos de confidencialidad, integridad y disponibilidad de la información. Los elementos a considerar son los siguientes:

i. Desarrollos a la Medida y Desarrollos Comerciales, con recursos propios o a través de terceros, deben estar dictaminadas por la UTIC
ii. Se almacenaran elementos auditables para eventos relevantes.

iii. Se verificara y protegerá la integridad de la información.
iv. Se protegerá la información contra accesos de usuarios no autorizados.
v. Se protegerá la toma de respaldos de información.
vi. Establecer planes de recuperación.
vii. Cubrir los requerimientos legales incluyendo la producción de reportes especiales con fines específicos.

DSITIC 11-c) Liberación de sistemas a producción

Cualquier sistema de información que sea liberado a producción deberá ser plenamente identificado y documentado para su administración.

DSITIC 11-d) Consideraciones de Seguridad en todo el ciclo del desarrollo

Para todas las aplicaciones comerciales, las medidas de seguridad deberán ser consideradas desde la primera etapa del diseño hasta las últimas etapas del ciclo estándar del desarrollo de aplicaciones.

DSITIC 11-e) Cifrado de la información clasificada

La información confidencial debe ser encriptada cuando se vaya a transmitir, respaldar y almacenar

DSITIC 11-f) Autenticación de mensajes en aplicaciones sensibles

La autenticación de mensajes deberá ser considerada para las aplicaciones, considerando vital proteger la integridad del contenido del mensaje.

DSITIC 11-g) Restricción al personal de desarrollo en el ambiente de producción

Por ningún motivo el personal de desarrollo de sistemas debe llevar a cabo la función de pasar la aplicación al ambiente de producción. Se deberán considerar los siguientes controles:

i. La actualización de bibliotecas de producción sólo podrá ser realizada por usuarios autorizados.
ii. Establecer un procedimiento de emergencia para la actualización de bibliotecas de producción para situaciones que así lo requieran.
iii. Ningún código ejecutable pasara al ambiente de producción sin haber sido probado exhaustivamente y autorizado por el usuario.
iv. Deberá mantenerse una bitácora de los cambios a las bibliotecas del ambiente productivo.
v. Se deberán mantener versiones previas de software como medida de contingencia.

DSITIC 11-h) Aislamiento del ambiente de producción a las pruebas

La información de producción no deberá estar disponible para las pruebas de las aplicaciones nuevas o de modificaciones a las ya existentes.

DSITIC 11-i) Protección de datos de prueba

Los datos de prueba deben ser protegidos y deben considerando los siguientes aspectos:

- Deberá existir una autorización cada vez que se trasmiten datos del ambiente de producción al ambiente de desarrollo.
- Los datos de prueba deberán ser protegidos al mismo nivel que los datos de producción.
- Deberá mantenerse una bitácora de la copia de datos de prueba con el fin de contar con pistas de auditoria.

DSITIC 11-j) Protección de los sistemas en ambiente de producción

Al personal que no tiene actividades en el área de producción, no se le permitirá actualizar o modificar la información de los sistemas en producción.

DSITIC 11-k) Liberar aplicaciones solamente cuando tengan la seguridad ya implantada

Las aplicaciones no pueden ser liberadas antes de contar con la seguridad mínima establecida en estas directrices para el desarrollo aplicativo.

DSITIC 11-l) Validación de datos de entrada

Los datos de entrada deberán ser validados para asegurar el correcto procesamiento de la información, considerando las siguientes validaciones:

i. Detectar valores fuera de rango, campos con caracteres inválidos, datos incompletos, límites dentro de los valores, información inconsistente.
ii. Revisar periódicamente los campos llaves para confirmar su validez.
iii. Inspeccionar documentos de entrada para detectar cambios no autorizados
iv. Procedimientos para responder a los eventos de validación.
v. Definir responsabilidades en las tareas de captura de información.

DSITIC 11-m) Validación de integridad de la información

Las aplicaciones deberán incorporar validaciones que permitan detectar si la información es correcta y no está corrupta.

DSITIC 11-n) Los sistemas son propiedad de la SCT

Sin ninguna excepción, todos los programas y documentación generados o elaborados por los empleados, consultores y personal contratado por honorarios para SCT son propiedad exclusiva de ésta. Se contara con carta compromiso firmada de este lineamiento con los antes mencionados.

DSITIC 11-o) Acceso a bases de datos por interfaces autorizadas

Las Interfaces aplicativas para acceder las bases de datos deben de ser el único vehículo mediante el cual se acceda a la Información.

DSITIC 11-p) Monitoreo de intentos de actualización de información no autorizados

Establecer controles que prevengan la actualización no autorizada de la información. Mediante un proceso de monitoreo con el fin de registrar intentos de actualización no autorizados a los recursos protegidos.

DSITIC 11-q) Proceso de Pruebas

Los sistemas aplicativos deben ser probados en forma exhaustiva, antes de ser liberados a producción, en ambientes controlados de pruebas. El proceso de pruebas (como parte de la disciplina de control de cambios), debe llevar un control estricto en los puntos que debe cumplir la nueva aplicación y realizar un reporte a desarrollo del resultado de la prueba.

DSITIC 11-r) Pruebas en ambiente Preproducción

Los sistemas aplicativos deben ser probados por un grupo especializado en esta función y en un ambiente de pruebas semi-real.

DSITIC 11-s) Producción autoriza ingreso de nuevo código al ambiente

Solamente el área de producción contará con la capacidad de autorizar el movimiento de código de los ambientes de prueba a los ambientes de producción. Deberá existir un registro detallado de los cambios realizados utilizando el Proceso de Control de Cambios.

DSITIC 11-t) El código migrado a Producción debe ser fuente

Los módulos en formato ejecutable no se deben pasar directamente desde las bibliotecas de prueba a las bibliotecas de producción. Los módulos se deberán volver a compilar y revisar sujetándolos a una prueba completa para pasarlos entonces a las bibliotecas de producción. Estas actividades de revisión y de volver a compilar deberán de ser realizadas por el personal autorizado y no por el personal de Desarrollo de Sistemas.

DSITIC 11-u) DSITIC 10-y) Falla en pruebas en producción

Siempre que no sea completado satisfactoriamente un proceso de transferencia de información se deberá notificar esta situación mediante el proceso gestión de problemas.

DSITIC 11-v) Controles para bibliotecas

La función de control de bibliotecas de Sistema Operativo, Programas Producto y Programas Fuente debe establecerse con el objeto de mantener integridad sobre los ambientes de prueba y producción; por medio del proceso de Gestión de Cambios.

DSITIC 11-w) Control de implantaciones en producción

Con el proceso de Control de Cambios se analizaran los cambios que se implantarán en el ambiente de producción.

DSITIC 11-x) Cambios de versión del sistema operativo y/o software del sistema

El cambio de versión del sistema operativo y de los programas producto pueden provocar problemas severos en las aplicaciones en producción.

i. Revisar las nuevas facilidades que contiene el nuevo software y verificar las implicaciones en las aplicaciones.
ii. Asegurar que las áreas afectadas conocen las implicaciones y han sido avisadas con tiempo a manera de tomar las precauciones adecuadas.

DSITIC 11-y) Modificaciones a software adquirido

El software adquirido no será modificado por personal que labora en SCT, si el producto requiere una modificación ésta será solicitada al proveedor.

DSITIC 12 Directriz de Continuidad de la SCT

Establecer el plan de continuidad completo y probado para todos los procesos administrativos que se hayan identificado como críticos por su importancia para los servicios de la SCT.

Lineamientos:

DSITIC 12-a) Estrategia recuperación

La estrategia de recuperación para las diferentes plataformas, así como desarrollar, documentar, probar y mantener los planes de recuperación que conduzcan a la restauración de los sistemas críticos de información de SCT será permanente.

DSITIC 12-b) Resguardo del plan de recuperación

Una copia del plan de recuperación deberá estar en algún sitio previamente definido fuera de las instalaciones centrales, en conjunto con los respaldos de la información crítica.

DSITIC 12-c) Plan de Continuidad y responsables

El plan de continuidad de SCT deberá especificar claramente las condiciones de su activación, así como los responsables de ejecutar cada componente del plan considerando los procedimientos, de emergencia, recuperación, retorno y prueba.

DSITIC 12-d) Pruebas periódicas del plan

El plan de continuidad de SCT deberá probarse por lo menos 1 vez al año.

DSITIC 12-e) Cambios al plan

El plan de continuidad de SCT deberá actualizarse cuando un cambio en el medio ambiente impacta su funcionalidad.

DSITIC 12-f) Recuperación para procesos de auditoria

Se debe contar con un plan de recuperación en caso de desastre que contemple los archivos requeridos por los procesos de auditoria.

DSITIC 13 Directriz de Monitoreo y Auditoria

Generar informes de auditoría de rutina describiendo las actividades del sistema, generando alertas sobre intentos o violaciones a la seguridad con pistas de auditoria para rastrear las actividades y demostrar el nivel de cumplimiento sobre las Directrices de Seguridad.

Lineamientos:

DSITIC 13-a) Licencias del software utilizado

Todo el software instalado en las computadoras propiedad de SCT deberá ser desarrollado internamente o estar de acuerdo a los compromisos de licencias, las leyes de protección de copia y los acuerdos de compra.

DSITIC 13-b) Software no autorizado

La SCT deberá usar software de detección y eliminación de virus. La UTIC deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la Secretaría. Además de verificar el cumpliendo con los requisitos de contratos de licencia de software y de hardware.

DSITIC 13-c) Sospecha de software malicioso

La Mesa de Servicio debe informar a la UTIC, reportes de software que no esté operando de acuerdo a las especificaciones, presente un comportamiento inestable y tener la sospecha que la inestabilidad o comportamiento se debe a software malicioso.

DSITIC 13-d) Identificación de información retenida

Para cubrir las necesidades de auditoria se identificará la información que será retenida y el periodo por conservar de acuerdo a las regulaciones.

DSITIC 13-e) Protección de la información

Toda información contenida y procesada en una computadora deberá ser protegida.

DSITIC 13-f) Auditorias

Realizar auditorías periódicas para verificar el cumplimiento de las Directrices de Seguridad, que permitan tomar acciones correctivas en su caso.

DSITIC 13-g) Revisiones técnicas de los controles de seguridad

Establecer revisiones técnicas periódicas para evaluar el grado de adecuación y cumplimiento con los controles de la Seguridad de la Información.

DSITIC 13-h) Precauciones de auditoria sistemas operativos

Las actividades de auditoria que involucren actividades de revisión al sistema operativo, deberán ser acordadas y cuidadosamente planeadas para minimizar el riesgo de interrupciones en los procesos de básicos de SCT.

i. Los requerimientos de auditoria deberán ser acordados con la administración de Sistemas.
ii. El alcance de las revisiones será acordado y controlado por las áreas involucradas.
iii. Los accesos para las revisiones serán solo de lectura.
iv. Los recursos necesarios para las revisiones deberán ser identificados y acordados con los proveedores de servicios.
v. Todos los accesos deberán ser monitoreados y registrados.
vi. Todos los procedimientos, requerimientos y responsabilidades, deberán ser documentados.

DSITIC 13-i) Participación de dueños o propietarios de la información

Los dueños o propietarios de la Información deberán participar en el proceso de auditoría.

DSITIC 13-j) Documentar auditoria de incidentes de seguridad

Desarrollar un proceso para la conducción de la auditoria de incidentes de seguridad, (violaciones a las Directrices de Seguridad) que ayudarán a identificar a los que violan la seguridad y a tomar acciones correctivas.

DSITIC 13-k) Reportes para identificar violaciones

Definir los reportes que ayudarán a identificar las violaciones a la seguridad, estos reportes deberán contener la siguiente información:

i. Utilización de los recursos del sistema.
ii. Los privilegios asociados con los usuarios, programas y recursos de grupo.

DSITIC 13-l) Registros completos de auditoria

Los registros de auditoria deberán contener los elementos de información que se consideren necesarios para poder dar un completo seguimiento a un incidente de seguridad.

DSITIC 13-m) Identificación de Usuarios con acceso a sistemas

Las aplicaciones deben operar con base en la identificación del usuario que accede al Sistema.

DSITIC 13-n) Reportes para auditoria

Se aplicaran los procedimientos técnicos que permitan obtener los reportes en forma periódica y que serán utilizados por el personal de auditoria.

DSITIC 13-o) Recolección de información para auditoria

Existirá un solo punto de recolección y manejo de la información de auditoria del control de acceso.

DSITIC 13-p) Auditoria constante a usuarios privilegiados

Los usuarios catalogados como con funciones especiales en los sistemas deben ser auditados trimestralmente.

DSITIC 13-q) Protección de herramientas de auditoria

Las herramientas utilizadas con propósitos de auditoria así como los archivos generados por éstas, deberán ser protegidas contra el acceso a usuarios no autorizados.

DSITIC 13-r) Reporte anual al Grupo Estratégico de Seguridad de la Información

Generar un análisis anual de los problemas y violaciones a la seguridad de la información, para presentarse al Grupo Estratégico de Seguridad de la Información.

DSITIC 13-s) Definición de puntos críticos de auditoria

El área de Seguridad definirá puntos críticos con el fin de monitorear el funcionamiento de los procesos de Seguridad. Los procesos de Alerta y auditoria serán elementos para la toma de decisiones y apoyarán a mejorar y retroalimentar a estos procesos.

DSITIC 13-t) Captar y escuchar informes de usuarios sobre seguridad

Implantar un mecanismo de comunicación formal para permitir a los empleados informar acerca de violaciones al sistema de seguridad, así como de actividades inseguras y que permita tomar decisiones correctivas o legales según corresponda.

DSITIC 14 Directriz de Servicios de Internet

La UTIC provee el servicio de Internet con fines estrictamente laborales. El contenido de la información que a través de este medio se obtenga, es responsabilidad del usuario.

Lineamientos:

DSITIC 14-a) Monitoreo y registros de actividad del servicio de Internet

Dado que el servicio de Internet hace uso de los recursos de la SCT, la actividad de los usuarios puede ser monitoreada y registrada en archivos históricos que son considerados como información confidencial de auditoria, lo anterior no generará alguna obligación, por lo que los usuarios no pueden esperar que se mantenga privacidad sobre el servicio.

DSITIC 14-b) Seguridad de Navegación de Internet

La información desde o hacia Internet que los usuarios manejen, es protegida mediante los procedimientos, herramientas y lineamientos de seguridad lógica que al respecto determine la UTIC.

DSITIC 14-c) Cuentas de acceso para acceso a Servicio de Internet

Todos los usuarios que requieran navegar en Internet deben contar con una cuenta de Active Directory para la activación del Servicio.

DSITIC 14-d) Filtrado de Contenido en el servicio de Internet

Se aplicaran filtros y otras técnicas para restringir el acceso a sitios de Internet que no tengan fines estrictamente laborales en todos los dispositivos, equipos, móviles o TIC que hagan uso del Internet que proporciona la SCT.

DSITIC 14-e) Actividades de Navegación Prohibidas

Las actividades que se prohíben cuando se hace uso de la conexión a Internet incluyen las siguientes categorías o apartados:

i. Material pornográfico, desnudos o sexo
ii. Drogas
iii. Apuestas, juegos
iv. Asuntos ilegales o cuestionables
v. Grupos extremistas
vi. Racismo
vii. Alcohol y tabaco
viii. Citas y anuncios personales
ix. Violencia y armas
x. Y, en general, todo aquello que no contribuya a su productividad laboral.
xi. Descarga de software o aplicaciones que representen una vulnerabilidad o riesgo a la Información de la SCT.
xii. Descarga de software o instalar aplicaciones que no estén plenamente justificadas con las funciones del usuario.
xiii. Descarga de archivos de música, de video, multimedia, etc. que representen un riesgo legal sobre derechos de autor para la Secretaría y/o que representen una vulnerabilidad para la seguridad de la información de la SCT.
xiv. Redes sociales o mensajería instantánea (Chat) en horarios oficiales de trabajo.

DSITIC 14-f) Solicitudes de servicio de Internet

El servicio de Internet es gestionado a través del SIGTIC por el encargado de Informática de cada Unidad Administrativa Central y Centro SCT.

DSITIC 14-g) Interconexión de servicio de Internet

El acceso a las redes de comunicación para la conexión a Internet, es a través de los esquemas que para el efecto sean definidos por la UTIC; en ningún caso los usuarios pueden modificarlos.

DSITIC 14-h) Excepciones de interconexión de Internet

La interconexión al servicio de Internet o sistemas externos distintos de los dispuestos por la UTIC, no están permitidos, con excepción de los expresamente autorizados por razones plenamente justificadas y aprobadas por la UTIC, en cuyo caso se deben definir los momentos y las condiciones aplicables.

DSITIC 14-i) Puertos lógicos de Comunicación para Internet

La UTIC determinara qué puertos lógicos de protocolos de comunicación serán habilitados para la operación del servicio de Internet, vigilando en todo momento la seguridad de la información de la SCT

DSITIC 15 Directriz de Servicios de Correo Electrónico

El uso del correo electrónico está permitido únicamente para fines estrictamente laborales, por lo que toda la información transmitida por este medio debe controlarse a fin de evitar exposición no autorizada de información reservada y/o confidencial.

Lineamientos:

DSITIC 15-a) Solicitudes de servicio de Correo Electrónico

El servicio de Correo Electrónico es gestionado a través del SIGTIC por el encargado de Informática de cada Unidad Administrativa o Centro SCT.

DSITIC 15-b) Transferencia de información no autorizada

La transferencia no autorizada de información clasificada como confidencial a otros empleados, personas ajenas u otras instituciones, es una falta grave que debe de reportarse al responsable de la seguridad.

DSITIC 15-c) Baja de cuentas por fin de actividades laborales en la Institución

Es responsabilidad del Encargado de Informática de las Unidades Administrativas o Centros SCT que cada vez que un servidor público cause baja en la SCT, se solicite la baja de la cuenta y se elimine del servidor de Correo Electrónico.

DSITIC 15-d) Listas de Distribución

El empleo de listas de distribución es de uso exclusivo del Administrador de la lista de distribución quien tiene facultad de agregar, modificar o eliminar destinatarios o permitir recibir mensajes de miembros ajenos a la Lista de distribución.

DSITIC 16 Directriz de Atención de Incidentes de seguridad

Todos los empleados, contratistas y terceros que laboren o presten algún tipo de servicio para la SCT deben reportar cualquier evento, debilidad o incidente de seguridad de información que se detecte por medio de los canales establecidos para tal efecto, a fin de que éstos puedan ser atendidos en tiempo y forma para mitigar, contener o eliminar el posible impacto de los mismos.

Lineamientos:

DSITIC 16-a) Incidentes de Seguridad relevantes

Siempre que el incidente amerite una investigación, debe recabar toda la evidencia posible, siempre y cuando este adentro del marco legal y normativo aplicable.

i. Ante un incidente de seguridad de la información, los empleados deben registrar, capturar, mantener y enviar la evidencia de tal acción a la UTIC.

DSITIC 16-b) Acciones ante incidentes de seguridad

Las acciones que la Unidad debe llevar a cabo ante la ocurrencia de incidentes de seguridad son:

i. Análisis e identificación de la causa del incidente ocurrido.
ii. Planeación e implementación para prevenir la recurrencia de incidentes.
iii. Obtención de evidencias para efectos de auditoría.
iv. Comunicación entre los responsables de los servicios.
v. Reporte a las autoridades legales apropiadas.

DSITIC 16-c) Reporte de incidentes de seguridad

Todos los funcionarios públicos, proveedores y terceros tienen la obligación de reportar al área correspondiente cualquier incidente de seguridad que sea de su conocimiento, entre otros se encuentra lo siguientes casos:

i. Pérdida de servicios de TIC.
ii. Sustracción, robo o pérdida de equipos de cómputo.
iii. Incumplimiento a las directrices de seguridad de la información.
iv. Brechas en los controles de seguridad existentes.
v. Accesos no autorizados a las instalaciones.
vi. Accesos no autorizados a los centros de datos.
vii. Accesos no autorizados a sistemas, aplicativos y/o servicios de TIC.
viii. Virus (detección o sospecha).
ix. Desastres.
x. Fallas de suministro eléctrico.
xi. Spam.

DSITIC 16-d) Registros de incidentes de seguridad

Los registros del reporte de los incidentes de seguridad de la información debe incluir al menos la siguiente información:

i. Nombre del incidente.
ii. ID del incidente.
iii. Usuario asociado.
iv. Hora del reporte.
v. Descripción del incidente.
vi. Estatus del incidente.

DSITIC 16-e) Acuerdos con terceros

Se deben establecer acuerdos de no divulgación y de confidencialidad antes de involucrar a una persona ajena a la SCT en respuesta a un incidente de seguridad.

DSITIC 17 Directriz de Eliminación de Información

Todos los funcionarios públicos, proveedores y terceros involucrados en el almacenamiento, procesamiento y resguardo de la información de la SCT catalogados como dueños de la información, deben definir las acciones necesarias para la eliminación de información de acuerdo al medio de almacenamiento y a su propiedad de confidencialidad definida en la directriz de clasificación de la información:

- Publica
- Reservada
- Confidencial

Lineamientos:

DSITIC 17-a) Destrucción de información en Equipo de Cómputo y Dispositivos de Almacenamiento.

Asegurar la eliminación de la información clasificada como reservada y/o confidencial que contiene el equipo de cómputo, dispositivos de almacenamiento y documentos físicos (papel), además, se debe proveer una protección continua, incluso previo a su eliminación.

i. La información en equipo de cómputo y dispositivos almacenamiento debe ser eliminada de acuerdo a su clasificación de confidencialidad.
ii. La eliminación de la información en equipo de cómputo y dispositivos almacenamiento puede ser realizada por personal interno de la SCT o por un proveedor. A continuación se describe la técnica a utilizar:

Clasificación	Medio de almacenamiento	Eliminación
Confidencial	• Dispositivos de almacenamiento removibles (USB, ZIP). • Cinta magnética. • CD-ROMS, DVD.	• Destrucción física.
	• Discos duros en PC, servidores, etc.	• Desmagnetización electrónica • Mediante utilería, sobre escribir el disco duro en repetidas ocasiones con información aleatoria.
Reservada	• Dispositivos de almacenamiento removibles (USB, ZIP). • Cinta magnética • CD-ROMS, DVD.	• Destrucción física.
	• Discos duros en Pc, Servidores, etc.	• Desmagnetización electrónica. • Mediante utilería sobre escribir el disco duro en repetidas ocasiones con información aleatoria.
Publica	• Dispositivos de almacenamiento removibles (USB, ZIP. • Cinta magnética • CD-ROMS, DVD	• No se requiere acción alguna, sin embargo en los casos donde se pueda reutilizar el dispositivo y sea factible, un simple formateo bastará.
	• Discos duros en Pc, servidores, etc.	• Formateo simple.

DSITIC 17-b) Eliminación programada.

La existencia de un gran volumen de dispositivos con información a eliminar

i. La información propuesta a eliminar debe ser revisada y aprobada por la Subdirección de Seguridad Informática y Servicios de Voz.
ii. En caso que se decida contratar a un proveedor para efectuar está actividad, esto debe ser autorizado por la Subdirección de Seguridad Informática y Servicios de Voz.
iii. Por cada evento en que se elimine información, se debe elaborar una acta que avale el proceso de eliminación, como mínimo el acta debe contener:
    - Fecha de la eliminación.
    - Descripción de la información a eliminar.
    - Descripción de la técnicas y herramientas utilizadas en el proceso
    - Testigos del proceso (de acuerdo al procedimiento "borrado seguro")
    - Anexar fotos del proceso de eliminación.

DSITIC 17-c) Eliminación del día a día.

Se habilitara a un funcionario de cada unidad para que aplique la eliminación de la información que se da día con día observado lo siguiente:

i. Contar con conocimientos en la materia.
ii. Recibir capacitación en las herramientas y técnicas utilizadas.
iii. Contar con los procedimientos que lo orienten en su labor de eliminación.
iv. Llevar un registro de los dispositivos que fueron sujetos a la eliminación.

DSITIC 17-d) Eliminación de documentos Físicos.

Los documentos físicos (papel) con clasificación reservada y/o confidencial deben ser eliminados por personal interno de la SCT o por un proveedor,

Confidencialidad	Eliminación
Pública	No necesaria
Reservada	Por medio de trituradoras
Confidencial	Por medio de trituradoras

En caso de que sea aplicada esta eliminación por un proveedor, se sujetara a lo indicado en las eliminaciones programadas para equipo de cómputo y dispositivos de almacenamiento realizadas por un proveedor

i. Cuando la eliminación es realizada por personal interno, este debe:
    - Recibir capacitación en las herramientas y técnicas utilizadas.
    - Llevar un registro de los documentos que fueron sujetos a la eliminación.
ii. El dueño de la información será el responsable de realizar la eliminación de este tipo de documentos.
iii. Deben existir procedimientos que guíen al dueño de la información en su labor de eliminación.
iv. El tipo de herramientas y utilerías requeridas en la eliminación deben ser autorizadas por la Subdirección de Seguridad Informática y Servicios de Voz.

DSITIC 18 Incumplimiento y Sanciones

Se deben evitar acciones en contra de las normas de Seguridad establecidas y en su caso aplicar sanciones correspondientes.

Lineamientos:

DSITIC 18-a) Enterar al OIC

Se envira un reporte al OIC de las violaciones a las Directrices de Seguridad detectadas y documentadas para que este OIC, aplique las medidas que juzgue necesarias a los funcionarios que incurrieron en la violación de las Directrices de Seguridad Establecidas

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