ESTADO DE SONORA

Gobierno del
Estado de Sonora

Secretaría **de la**
Contraloría General

Subsecretaría de **Desarrollo**
Administrativo y Tecnológico

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

NOVIEMBRE, 2017.

SONORA
UNIDOS LOGRAMOS MÁS

ÍNDICE

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

Introducción

La necesidad de prestar más y mejores servicios ha generado que los activos de información y los equipos informáticos sean recursos importantes y vitales de nuestra Dependencia o Entidad. El buen uso y la disponibilidad que se tenga de ellos hacen que nuestras actividades sean más eficientes y eficaces; es por tal razón que tenemos el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales. Por todo lo anterior, es necesario contar con políticas de seguridad informática que normen las actividades relacionadas con los sistemas de información.

Objetivo del Manual

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal, para que sea de su conocimiento y cumplimiento en el uso de los recursos informáticos asignados.

Alcance

El documento define las Políticas y Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos.

Sanciones por incumplimiento

El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política: Todo usuario de bienes y servicios informáticos se compromete a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos, así como el estricto apego al Manual de Políticas y informáticos cumplir las Políticas y Estándares de Seguridad Informática del presente manual.

1.1. Acuerdos de uso y confidencialidad. Todos los usuarios de bienes y servicios informáticos deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información, así como comprometerse a cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática.

1.2. Entrenamiento en Seguridad Informática. Todo empleado de nuevo ingreso deberá:

- Leer el Manual de Políticas y Estándares de Seguridad Informática, el cual se encuentra disponible en el portal de internet de esta Dependencia o Entidad, donde se dan a conocer las obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

- Firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas y Estándares de Seguridad; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

1.3. Acuerdos de uso y confidencialidad a externos.

- Cada Secretario, Director General, y Director debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas y Estándares de Seguridad Informática para el personal provisto por terceras partes, que realicen labores en o para la Dependencia o Entidad.

- Firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas y Estándares de Seguridad, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
- Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de la Dependencia o Entidad, quien será responsable del control y vigilancia del uso adecuado de la información y los bienes y servicios informáticos.

2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL.

Política: Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Dependencia o Entidad, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones de la Dependencia o Entidad.

La Dependencia o Entidad proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.
Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.
El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de tecnología de sistemas de información.

Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el responsable del área de tecnología de sistemas de información, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a la Mesa de Ayuda de las acciones ejecutadas.

2.1. Resguardo y protección de la información

2.1.1. Respaldo de la Información

La Dirección de Informática validará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Dirección de Informática,

encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, La Dirección de Informática velará porque los medios de almacenamiento que contienen la información crítica sean resguardados en diferentes sitios. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

2.1.2. **Copias de respaldo de la información**

2.1.2.1. La Dirección de Informática, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

2.1.2.2. La Dirección de Informática debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

2.1.2.3. La Dirección de Informática, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

2.1.2.4. La Dirección de Informática debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

2.1.2.5. Es responsabilidad de los usuarios de la plataforma tecnológica identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

2.1.2.6. El usuario deberá reportar de forma inmediata a la Dirección de Informática, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2.7. El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su resguardo, aun cuando no se utilicen y contengan información reservada o confidencial.

2.1.2.8. Es responsabilidad del usuario evitar en todo momento la fuga de la información que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

2.2. Controles de acceso físico de equipo

2.2.1. El resguardo de los equipos de cómputo deberá quedar bajo el área de Informática contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

2.2.2. Cualquier persona que tenga acceso a las instalaciones de la Dependencia o Entidad, deberá registrar en el Sistema de Ingreso (cuando sea implementado), el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Dependencia o Entidad, el cual podrán retirar el mismo día, sin necesidad de trámite alguno.

2.2.3. En caso de que el equipo que no es propiedad de la Dependencia o Entidad permanezca dentro de la institución más de un día hábil, es necesario que el responsable de la oficina en el que trabaja el dueño del equipo, elabore y firme oficio de autorización de salida.

2.3. Controles de acceso físico a la Infraestructura de Comunicaciones

2.3.1. Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por personal de la Dirección de Informática; no obstante, los visitantes siempre deberán estar acompañados durante su visita al centro de cómputo o los centros de cableado.

2.3.2. La Dirección de Informática debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

2.3.3. La Dirección de Informática debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

2.4. Infraestructura

2.4.1. Deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

2.4.2. Todo equipo de TI debe ser revisado, registrado y aprobado por la Dirección de Informática antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

2.4.3. La configuración de Routers, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Dirección de Informática.

2.4.4. La Dirección de Informática debe proveer las condiciones físicas y medioambientales necesarias para la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

2.4.5. La Dirección de Informática debe velar porque los recursos de la plataforma tecnológica ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

2.4.6. La Dirección de Informática debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

2.5. Seguridad Perimetral

2.5.1. La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

2.5.2. La Dirección de Informática implementará soluciones lógicas y físicas que garanticen la protección de la información de la Dependencia o Entidad de posibles ataques internos o externos.

- Rechazar conexiones a servicios comprometidos.
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

2.5.3. Firewall

- La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, ya sean clientes o servidores.
- Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- La Dirección de Informática establecerá las reglas en el Firewall necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.

- El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
- Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

2.5.4. **Sistemas de Detección de Intrusos (IDS)**

Un sistema de detección de intrusos (o IDS de sus siglas en inglés) es una aplicación usada para detectar accesos no autorizados a un computador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

- La Dirección de Informática implementará soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos.
- Detección de ataques en el momento que están ocurriendo o poco después.
- Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
- Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS.
- Análisis de comportamiento anormal, para revelar o descubrir una máquina comprometida o un usuario con su contraseña al descubierto o un sistema con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.

2.5.5. **Conectividad Remota - Redes Privadas Virtuales (VPN)**

La Dirección de Informática establecerá los requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Dependencia o Entidad; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

- La Dirección de Informática debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la Dependencia o Entidad.
- Los usuarios móviles y remotos de Dependencia o Entidad podrán tener acceso a la red interna desde cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por Dirección de Informática.
- La Dirección de Informática será la encargada de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.
- La Dirección de Informática debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a

personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Dependencia o Entidad y deben acatar las condiciones de uso establecidas para dichas conexiones.

2.5.6. **Conectividad a Internet**

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los usuarios tienen las mismas responsabilidades en cuanto al uso de Internet.
- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
- No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.
- Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

2.5.7. **Red Inalámbrica (WIFI)**

La red inalámbrica es un servicio que permite conectarse a la red de Datos e Internet sin la necesidad de algún tipo de cableado.

Las condiciones de uso definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.

2.5.7.1. ***Tecnología***

- La red inalámbrica usa el estándar 802.11b/g/n con cifrado WPA2. Por lo tanto, las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar y soportar los requerimientos descritos. Caso contrario se debe realizar algunas actualizaciones previas de tratarse de un computador portátil.
- A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA en ninguna forma el acceso desde cualquier punto fuera de cobertura.
- Sólo será soportado el protocolo TCP/IPV.4 en la red inalámbrica.
- La Dirección de Informática se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño

de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios.

- No se permiten la operación ni instalación de “puntos de acceso” (access points) conectados a la red cableada sin la debida autorización por parte La Dirección de Informática.
- No se permite configurar las tarjetas inalámbricas como “puntos de acceso” o la configuración de equipos como servidores adicionales.
- La Dirección de Informática, es la encargada de la administración, habilitación y/o bajas de usuarios en la red inalámbrica.

2.5.7.2. ***Identificación y activación***

- Para hacer uso de la red inalámbrica, el solicitante necesariamente deberá ser empleado la Dependencia o Entidad.
- Como primer paso para hacer uso de este servicio, se deben de registrar los usuarios que deseen la prestación del servicio mediante el llenado de un formulario, vía Mesa de Ayuda y presentando el dispositivo que se conectará a la red inalámbrica.
- Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos de comunicación.
- La activación de la cuenta se realizará por un periodo; salvo casos de fuerza mayor o anormalidades en el registro (usuarios inexistentes, apagones, fallas, etc.).
- Para conectarse a la red inalámbrica se deberá emplear autenticación tipo WPA2 para lo cual los nombres de usuarios y contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los usuarios.
- La Dirección de Informática, determinará las medidas pertinentes de seguridad para usar las redes inalámbricas.
- La Dirección de Informática, se reservan el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red.
- No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.
- Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a la Mesa de Ayuda para su respectiva baja del equipo de la red inalámbrica.

2.5.7.3. ***Restricciones/prohibiciones de acceso a Internet***

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (Peer to Peer).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
- Uso de JUEGOS "on line" en la red.

2.5.7.4. ***Excepciones***

- Entre las medidas de seguridad se encuentra configurado para restringir, algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad a la Mesa de Ayuda para que sea resuelta a la brevedad posible.
- En caso de eventos, cursos, talleres, conferencias, etc., se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos dos días hábiles.
- En el caso de estos eventos las restricciones para acceder podrán ser “anuladas” temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos dos días hábiles.

  Acceso a Invitados:
- La red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura.
- Los usuarios invitados no tendrán acceso a la Red de Las Empresas ni a ningún recurso de uso privado.
- La red inalámbrica es de tipo Portal Cautivo y se tendrá una lista de usuarios invitados con contraseñas que se actualizarán cada dos meses.

2.6. Servidores Configuración e instalación

2.6.1. La Dirección de Informática proveerá y supervisará la operación de los servidores físicos (Hosts) y su rendimiento.

2.6.2. La Dirección de Informática mantendrá actualizado las configuraciones de servidores físicos (Hosts) que componen el Centro de Datos Estatal que podrán ser utilizados por las dependencias y unidades administrativas siempre y cuando las capacidades de los mismos lo permitan.

2.6.3. El servicio de Aprovisionamiento de servidores será bajo el esquema de servidores virtuales.

2.6.4. En Caso de que los requerimientos de desempeño y capacidad de los servidores requeridos superen las configuraciones existentes, las dependencias o entidades podrán convenir con la Dirección de Informática la entrega de componentes necesarios para proveerles el servicio, tales como procesadores, memorias, discos duros y servicios de instalación de los mismos.

2.6.5. El Aprovisionamiento de servidores a externos deberá ser respaldada vía Oficio y solicitud debidamente llenada, con los requisitos de Hardware y Software, así como los requisitos de publicación de servicios vía Internet (IP pública, Dominio), y solicitud de acceso seguro vía VPN.

2.6.6. La Dirección de Informática proporcionará acceso a través de una Virtual Private Network VPN.

2.6.7. La Dirección de Informática proporcionará las claves de acceso (**misma se solicita sea modificada al primer acceso**) y certificados de seguridad.

2.6.8. La Dirección de Informática, se limita al acceso al equipo, en el cual se encuentran instaladas las aplicaciones y Bases de Datos, propias de las dependencias y/o unidades administrativas.

2.6.9. El administrador del servidor será responsable de la administración del mismo en su totalidad (sistema operativo, antivirus, aplicaciones instaladas y respaldos).

2.6.10. El administrador del servidor deberá acreditar la propiedad del licenciamiento de los sistemas a instalar en el servidor.

2.6.11. La dependencia y/o unidad administrativa responsable de la administración deberá implementar los métodos o acciones necesarias para garantizar la seguridad a nivel de información y Sistema Operativo incluyendo cualquier vulnerabilidad reportada, parches y actualizaciones necesarias para el óptimo funcionamiento del mismo.

2.6.12. La Dirección de Informática en caso de que detecte alguna falla de seguridad, será puesto fuera de producción (cuarentena) con el fin de evitar brecha de seguridad hacia los demás servidores del Centro de Datos Estatal hasta la remediación de la falla por parte del Administrador responsable de la dependencia o Unidad Administrativa.

2.6.13. Los servidores que proporcionen servicios a través de la red e Internet deberán:
Funcionar 24 horas del día los 365 días del año.
Recibir mantenimiento anual que incluya la revisión de su configuración. Ser monitoreados.

2.6.14. La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:
Diariamente, información crítica.

2.6.15. Los servicios hacia Internet sólo podrán proveerse a los servidores autorizados por la Dirección de Informática.

2.7. Seguridad en Centro de Datos (Data Center)

El Centro de Datos es área restringida, por lo que sólo el personal autorizado por la Dirección de Informática puede acceder a él.

2.7.1. Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Dirección de Informática. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito de los responsables de la Dirección de Informática.

El Data Center deberá:

- Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.
- Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por la Dirección de Tecnología Informática.
- Recibir limpieza, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- Controles de humedad y temperatura. Mantener la temperatura a 21 grados centígrados.
- Los sistemas de Refrigeración deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Asignar un técnico para que realice un control diario temperatura y aires acondicionados y llevar un registro de estos controles.
- Sistemas de Detección y extinción de incendio.
- Los sistemas contra incendios deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Sistema de Vigilancia.
- Los sistemas de Vigilancia deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

2.8. Protección y ubicación de los activos tecnológicos

Los recursos tecnológicos, deben ser utilizados de forma ética y en cumplimiento de los reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación.

2.8.1. Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un usuario, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

2.8.2. Los recursos tecnológicos provistos a funcionarios y personal suministrado por terceras partes son proporcionados con el único fin de llevar a cabo las labores asignadas; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

2.8.3. El personal no debe utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

2.8.4. Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Mesa de Ayuda, debiéndose solicitar a la misma en caso de requerir este servicio.

2.8.5. La Dirección General de Administración y Control Presupuestal será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Dirección de Informática.

2.8.6. El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones asignadas al usuario.

2.8.7. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

2.8.8. Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.8.9. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.

2.8.10. Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.

2.8.11. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

2.8.12. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

2.8.13. Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados a la Mesa de Ayuda a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.8.14. Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

2.8.15. La Mesa de Ayuda en conjunto con la Dirección de Operaciones Tecnológicas, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica.

2.8.16. La Dirección de Operaciones Tecnológicas debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

2.8.17. La Dirección de Operaciones Tecnológicas es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.

2.8.18. La Dirección de Operaciones Tecnológicas es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores.

2.9. Uso de Dispositivos Móviles

2.9.1. La Dirección de Informática proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos.

2.9.2. La Dirección de Informática debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la Dependencia o Entidad.

2.9.3. La Dirección de Informática debe instalar un software de antivirus tanto en los dispositivos móviles institucionales, como en los personales que hagan uso de los servicios provistos por la Dependencia o Entidad.

2.9.4. Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

2.9.5. Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

2.9.6. Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

2.9.7. Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

2.9.8. Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

2.9.9. Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

2.10. Mantenimiento de Activos Informáticos e Infraestructura

El personal autorizado para el mantenimiento se encargará de proporcionar oportuna y eficientemente, los servicios que requiere la Dependencia o Entidad en materia de mantenimiento preventivo y correctivo a los activos informáticos y a la infraestructura, así como la contratación de servicios de proveedores externos, necesaria para el fortalecimiento y desarrollo de las actividades.

2.10.1. Únicamente el personal autorizado por la Dirección de Informática podrá llevar a cabo el mantenimiento preventivo y/o correctivo al equipo informático e infraestructura, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso.

2.10.2. El período para llevar a cabo el mantenimiento preventivo será determinado por la Dirección de Informática.

2.10.3. Queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no sea propiedad de la Dependencia o Entidad.

2.10.4. En caso de ser necesaria un mantenimiento correctivo de cualquier equipo de cómputo, deberá de solicitarse a través de la Mesa de Ayuda.

2.10.5. El tiempo de reparación dependerá del nivel de daño o tipo de problema presentado en el equipo y en caso de ser necesario, se enviará a reparación especializada fuera de esta Dependencia o Entidad.

2.10.6. Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal de la Dirección de Informática.

2.11. Pérdida o transferencia de equipo

2.11.1. El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo con la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.11.2. El resguardo para las laptops tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.11.3. El usuario deberá dar aviso de inmediato a la Dirección General de Administración y Control Presupuestal de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo, y dicha Unidad Administrativa a su vez a la Dirección de Informática.

2.12. Uso de periféricos y medios de almacenamiento

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica la Dependencia o Entidad será reglamentado por la Dirección de Informática, considerando sus necesidades de uso.

2.12.1. La Dirección de Informática, debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica, de acuerdo con los lineamientos y condiciones establecidas.

2.12.2. La Dirección de Informática debe aplicar lineamientos para la disposición segura de los medios de almacenamiento del instituto, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

2.12.3. El personal de la Dependencia o Entidad y personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Informática.

2.12.4. El personal de la Dependencia o Entidad y personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Informática.

2.12.5. El personal de la Dependencia o Entidad es responsable por la custodia de los medios de almacenamiento asignados.

2.12.6. El personal de la Dependencia o Entidad y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica.

2.13. Uso de dispositivos especiales

2.13.1. El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen.

2.13.2. La asignación de este tipo de equipo será previa justificación por escrito y autorización del titular o jefe inmediato correspondiente.

2.13.3. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.13.4. Los módems internos deberán existir solo en las computadoras portátiles y no se deberán utilizar dentro de las instalaciones de la institución para conectarse a ningún servicio de información externo, excepto cuando lo autorice la Dirección de Informática.

2.14. Daño del equipo.

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso se determinará la causa de dicha descompostura.

3. POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO.

Política: Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura de la Dependencia o Entidad. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la Dependencia o Entidad o hacia redes externas como internet.

Los usuarios que hagan uso de equipo de cómputo deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir a la Mesa de Ayuda para solicitar asesoría.

3.1. Uso de medios de almacenamiento.

3.1.1. Toda solicitud para utilizar un medio de almacenamiento de información compartido deberá contar con la autorización del jefe inmediato del usuario y del titular del área dueña de la información.

3.1.2. Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, el documento se presentará con sello y firma del titular de área a la Dirección de Informática.

3.1.3. Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la Mesa de Ayuda, para que dichos asesores determinen el medio en que se realizará dicho respaldo.

3.1.4. En caso de que por el volumen de información se requiera algún respaldo en CD, este servicio deberá solicitarse por escrito al Titular de la Dirección de Informática, y deberá contar con la firma del titular del área de adscripción del solicitante.

3.1.5. Los servidores públicos deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita el Instituto de Transparencia y Acceso a la Información del Estado de Sonora, en términos de Ley de Acceso a la Información Pública y Protección de Datos Personales del Estado de Sonora, y demás criterios y procedimientos establecidos en esta materia.

3.1.6. Las actividades que realicen los usuarios en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

3.2. Instalación de Software

3.2.1. La Dirección de Informática debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software, así como monitorear dichas actualizaciones.

3.2.2. La Dirección de Informática debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

3.2.3. En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente.

3.2.4. Los usuarios que requieran la instalación de software que no sea propiedad de la Dependencia o Entidad, deberán justificar su uso y solicitar su autorización a la Dirección de Informática, a través de un oficio firmado por el titular del área de su adscripción, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software.

Si el dueño del software no presenta la factura de compra del software, el personal asignado por la Dirección de Informática procederá de manera inmediata a desinstalar dicho software.

3.2.5. Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Dependencia o Entidad, que no esté autorizado por la Dirección de Informática.

3.2.6. Del software propiedad de la Dependencia o Entidad.

I. Todo programa o sistema adquirido por compra, donación o cesión es propiedad de la Dependencia o Entidad y mantendrá los derechos que la ley de propiedad intelectual le confiera.

II. La Dirección de Informática contará con un registro del software propiedad de la Dependencia o Entidad, por lo que es responsabilidad de las áreas informar sobre posibles adquisiciones extemporáneas.

III. Los sistemas informáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos de la Dirección de Informática se mantendrán como propiedad de la Dependencia o Entidad respetando la propiedad intelectual correspondiente.

IV. Corresponderá a la Dirección de Informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas informáticos ubicados en los servidores.

V. La Dirección de Informática propiciará la gestión de patentes y derechos de creación de software propiedad de la Dependencia o Entidad.

VI. La Dirección de Informática administrará los diferentes tipos de licencias de software y vigilará su vigencia.

3.2.7. La Dirección de Informática es la responsable de realizar revisiones periódicas para asegurar que sólo programas con licencia estén instalados en las computadoras de la Dependencia o Entidad.

3.3. Identificación del incidente.

3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo a la Dirección, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar al titular de su adscripción.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la Dependencia o Entidad, debe ser reportado a la Dirección de Informática.

3.4. Administración de la configuración.

Los usuarios de las áreas de la Dependencia o Entidad no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red, sin la autorización por escrito de la Dirección de Informática.

3.4.1. Seguridad de la red. Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Dirección de Informática en la cual los usuarios realicen la exploración de los recursos informáticos en la red, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

3.4.2. Del control de acceso local a la Red institucional:

I. Corresponde a la Dirección de Informática proporcionar a los usuarios el acceso a los recursos informáticos, mediante la asignación de cuentas personalizadas, con un nivel de privilegios acorde a sus funciones.

II. Dado el carácter unipersonal de la cuenta de acceso a la red, el uso que se haga de esta es responsabilidad de cada usuario y deberá apegarse a los lineamientos establecidos en este manual.

3.4.3. Del acceso a los sistemas administrativos:

I. Tendrá acceso a los sistemas administrativos solo el personal de la Dependencia o Entidad que sea responsable de esa herramienta o bien tenga la autorización del responsable de la misma, si se tratará de personal de apoyo administrativo o técnico.

II. La información administrativa que se considere de uso restringido deberá ser protegida mediante los mecanismos apropiados con el objeto de garantizar su integridad.

3.4.4. De la supervisión y evaluación.

I. Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse a las políticas emitidas por la Dirección de Informática.

II. La Dirección de Informática está facultada para realizar monitoreo de red, aplicaciones y servicios que se consideren necesarios para garantizar la seguridad o rendimiento de dichos recursos.

III. Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

3.5. Uso del correo electrónico.

3.5.1. El Departamento de Recursos Humanos es la responsable de solicitar el alta y baja de correos, de acuerdo con la relación de personal con la que se cuenta.

3.5.2. La asignación de cuentas de correo se hará en base a las funciones del cargo que desempeña, solo en caso de requerir el uso de cuenta personal es necesario realizar la solicitud por Memorándum a la Dirección de Informática.

3.5.3. Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.

3.5.4. Con el propósito de contar con niveles de seguridad apropiados, es responsabilidad del usuario manejar la contraseña de acceso al correo electrónico con privacidad.

3.5.5. La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, (Números, Letras Mayúsculas/Minúsculas, Caracteres especiales).

3.5.6. Cuando un servidor público de la Dependencia o Entidad sea dado de baja, la Dirección de Recursos Humanos de la Instancia, deberá informar a la Dirección de Informática, para el bloqueo de la cuenta de correo correspondiente.

3.5.7. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Dependencia o Entidad (si es propiedad de la Dependencia o Entidad es información pública). Los mensajes de correo electrónico

deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.5.8. Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la Dirección de Informática.

3.5.9. La Dependencia o Entidad, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad violando políticas de Seguridad Informática de la Dependencia o Entidad o realizado acciones no autorizadas.

3.5.10. Como la información del correo electrónico institucional es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

3.5.11. El usuario debe de utilizar el correo electrónico de la Dependencia o Entidad, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

3.5.12. La asignación de una cuenta de correo electrónico externo deberá solicitarse por escrito a la Dirección de Informática, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área que corresponda.

3.5.13. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.5.14. El usuario es responsable de la información enviada o reenviada desde su buzón de correo electrónico, sujetándose a los siguientes requisitos:

I. Comprimir, en la medida de lo posible, los archivos anexos en caso de que excedan de 15 MB. Evitar el envío de correos mayores a 20 MB.

II. Verificar, antes de cualquier envío, que los archivos anexos no contengan ningún virus informático que ponga en riesgo los bienes de la Dependencia o Entidad.

III. Depurar continuamente los correos para evitar saturación.

3.5.15. El usuario final de este servicio deberá mantener una imagen y comportamiento profesional cuando haga uso del correo electrónico, deberá abstenerse de realizar cualquiera de las actividades que a continuación se describen:

I. Enviar correos masivos no oficiales a todo el personal de esta Dependencia o Entidad.

II. Enviar o reenviar cadenas de mensajes a un grupo de usuarias(os), ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas.

III. Compartir o divulgar números de cuenta, claves de acceso y número de identificación personal u otra información confidencial o sensible para la Dependencia o Entidad.

IV. Enviar mensajes con contenido multimedia (audio, video, etc.).

V. Utilizar el servicio de correo electrónico institucional para fines diferentes a los objetivos de la Dependencia o Entidad.

VI. Transmitir por correo cualquier material que transgreda la Ley Federal de Derechos de Autor y la Ley de Acceso a la Información Pública y de Protección de Datos Personales del Estado de Sonora.

VII. Enviar o promover dentro o fuera de la Dependencia o Entidad o hacia su personal, material que vaya contra la moral y las buenas costumbres, o que constituya o fomente un comportamiento que dé lugar a responsabilidades civiles, administrativas o penales.

3.6. Controles contra código malicioso

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque que involucre controles humanos, técnicos y administrativos, que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso y como control mínimo, las estaciones de trabajo deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.

3.6.1. La Dirección de Informática debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada por el usuario.

3.6.2. La Dirección de Informática podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual en el desempeño.

3.6.3. La Dirección de Informática debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

3.6.4. La Dirección de Informática debe validar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

3.6.5. La Dirección de Informática, a través de sus funcionarios, debe asegurarse que los usuarios de la Dependencia o Entidad o personal externo no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

3.6.6. Los usuarios de la Dependencia o Entidad no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la

Dirección de Informática; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en los diferentes medios de almacenamiento, considerando al menos memorias USB, discos flexibles, CD´s, y estos mismo se encuentren libres de cualquier tipo de código malicioso.

3.6.7. Los usuarios de la Dependencia o Entidad deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

3.6.8. Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

3.6.9. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que, a través de ella, se tome las medidas de control correspondientes.

3.6.10. Ningún usuario ni empleado de la Dependencia o Entidad o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Dirección de Informática.

3.6.11. Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil será responsable de solicitar de manera periódica a la Mesa de Ayuda las actualizaciones del software de antivirus.

3.6.12. Debido a que algunos virus son extremadamente complejos, ningún usuario debe intentar erradicarlos de las computadoras, lo indicado es llamar a la Mesa de Ayuda para su atención.

3.7. Permisos de uso de Internet.

3.7.1. El acceso a internet provisto a los usuarios es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo con lo que determine la Dirección de Responsabilidades.

3.7.2. La asignación del servicio de internet deberá solicitarse por escrito a la Dirección de Informática, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del titular del área correspondiente.

3.7.3. Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por la Dependencia o Entidad.

3.7.4. La Dirección de Informática es el responsable de administrar los servicios WWW que ofrece a la Dependencia o Entidad. Es decir, sólo se permiten servidores Web implementados por dicha Unidad Administrativa.

3.7.5. Los usuarios con acceso a Internet tienen que reportar todos los incidentes de seguridad informática a la Mesa de Ayuda, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.7.6. Toda programación mediante la tecnología Web deberá estar supervisada por la Dirección de Informática.

3.7.7. El usuario con servicio de navegación en internet al utilizar el servicio acepta que:

- Deberán cumplirse todas las normas específicas dictadas por la Dirección de Informática.
- Dichas normas se comunicarán por los diferentes medios disponibles, e incluso directamente a los interesados.
- Deberá comunicarse a la Mesa de ayuda cualquier deficiencia o funcionamiento anómalo que se observe.
- Está estrictamente prohibido cualquier uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral que dio origen a la habilitación del servicio.
- Todo usuario deberá comunicar a la Dirección de Informática cualquier incumplimiento de estas normas que lleguen a su conocimiento.
- Está prohibido transmitir cualquier material en violación de cualquier regulación de la Dependencia o Entidad. Esto incluye: derechos de autor, amenazas o material obsceno, o información protegida por secreto comercial.
- No es aceptable el uso para actividades comerciales. Está prohibido el uso para propaganda de productos o propaganda política.
- El contenido de la información que a través de este medio se obtenga, será responsabilidad del usuario.
- Se autoriza el acceso a cualquier página de Internet, excepto a las que se encuentran clasificadas dentro de las categorías listadas en la siguiente tabla. A solicitud del titular del área, vía memorándum autorizado por el titular de la Dependencia o Unidad Administrativa, los usuarios podrán ser movidos de perfil estándar al perfil avanzado.
- La navegación en la red y la obtención de software a través de la misma deberá apegarse estrictamente a los sistemas de protección aplicados por la Dirección de Informática.
- Todas las actividades que los usuarios realicen dentro de Internet serán susceptibles de monitoreo y ser registradas en archivos históricos y serán consideradas como información confidencial de auditoría.
- La información desde o hacia Internet que los usuarios manejen, será protegida mediante los procedimientos, herramientas y lineamientos de seguridad lógica

que al respecto determine la Dirección de Informática; ésta misma impedirá el acceso a sitios no relacionados con las funciones.

- No se permite descargar Software o instalar aplicaciones que no estén plenamente justificadas con las funciones del usuario; no se permite descargar, ver o escuchar en línea archivos de música, archivos de video, multimedia, etc., provenientes de Internet, que represente un riesgo legal sobre derechos de autor para la Dependencia o Entidad.
- El acceso a las redes de comunicación para la conexión a Internet será a través de los esquemas que para el efecto se definan por la Dirección de Informática; en ningún caso los usuarios podrán modificarlos, ni serán permitidos medios personales para acceso a conexiones de Internet sin autorización del Titular de la unidad Administrativa y la Dirección de Informática.
- Los enlaces a través de líneas telefónicas, módem, enlaces inalámbricos o celulares que generen puentes hacia Internet o sistemas externos, no están permitidos, con excepción de los expresamente autorizados por razones plenamente justificadas y aprobadas por la Dirección de Informática; en cuyo caso se definirán los momentos y las condiciones aplicables.
- La Dirección de Informática determinará qué servicios y puertos de conexión de los servidores estarán disponibles en Internet.

3.7.8. Queda estrictamente prohibido:

I. La descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

II. El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

III. El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Whatsapp, Skype, Twitter, P2P y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias.

IV. La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

V. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet.

VI. Navegar en Internet a excepción, de cuando las actividades propias del puesto así lo requieran.

3.7.9. Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea son:

NIVEL 1: Sin restricciones: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

NIVEL 2: Internet restringido y mensajería instantánea: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea, aplicándose las políticas de seguridad y navegación.

NIVEL 3: Internet restringido y sin mensajería instantánea: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación.

NIVEL 4: El usuario no tendrá acceso a Internet ni a servicios de mensajería instantánea.

3.7.10. El diseño de las páginas WEB de la Dependencia o Entidad deberá apegarse a los Lineamientos de Imagen Institucional para el Desarrollo de Portales de Internet del Estado de Sonora, emitidos por la Oficina de Imagen Institucional adscrita al Ejecutivo Estatal.

3.8. Atención a usuarios de servicios tecnológicos.

3.8.1. La atención por parte de la Dirección de Informática se realizará previo reporte de incidencias, mismas que serán registradas por el usuario, a través del sistema de Mesa de Ayuda.

3.8.2. La Mesa de Ayuda podrá resolver telefónicamente dudas operativas y funcionales con respecto a las herramientas utilizadas en aplicaciones, sistemas operativos, etc.

3.8.3. Se utilizará la herramienta de Acceso Remoto, para poder brindar una mejor atención, en tiempo real según sea la necesidad y problemática del usuario.

3.8.4. Se hará el soporte solicitado vía remota o en sitio, según sea considerado por el especialista de la Mesa de Ayuda.

3.8.5. Aquellas peticiones de soporte que por su naturaleza dependan de otras áreas, serán canalizadas a estas de forma inmediata, informando de esta determinación al usuario que realizó la solicitud.

3.8.6. El acceso al sistema de atención a usuarios será de acuerdo con el procedimiento y la herramienta vigente.

3.8.7. Para proporcionar estos servicios la Dirección de Informática deberá de contar con un procedimiento de levantamiento de incidentes, debidamente documentado, el cual se pueda consultar a través de la página institucional.

3.8.8. Debido al carácter confidencial de la información a la cual tiene acceso por motivo de sus labores de soporte técnico, el personal de la Dirección de Informática deberá de conducirse de acuerdo con los códigos de ética, normas y procedimientos establecidos.

3.8.9. Los Ingenieros de Soporte tendrán las siguientes atribuciones y/o responsabilidades:

- Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
- Utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.
- Realizar respaldos de la información de los recursos de cómputo, siempre y cuando se cuente con dispositivos de respaldo.
- Actualizar la información de los recursos de cómputo, cada vez que adquiera e instale equipos o software nuevo.
- Registrar cada máquina en el inventario de control de equipos de cómputo y red.
- Auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extras que pongan en riesgo la seguridad de la información.
- Reportar a la Dirección de Informática los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

4. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Política: Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica, por lo cual deberá mantenerlo de forma confidencial.

4.1. Controles de acceso lógico

4.1.1. El acceso a la infraestructura tecnológica para personal externo debe ser autorizado al menos por un titular de área, quien deberá notificarlo por oficio a la Dirección de Informática, quien lo habilitará.

4.1.2. Los recursos disponibles a través de la Red institucional serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la Dependencia o Entidad, por lo que está prohibido que los usuarios utilicen la infraestructura tecnológica para obtener acceso no autorizado a la información u otros sistemas de información del Poder Ejecutivo del Estado de Sonora.

4.1.3. Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.4. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Dirección de Informática antes de poder usar la infraestructura tecnológica de la Dependencia o Entidad.

4.1.5. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica, a menos que se tenga autorización de la Dirección de Informática.

4.1.6. Cada usuario que accede a la infraestructura tecnológica de la Dependencia o Entidad debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

4.1.7. Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

4.1.8. Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

4.2. Administración de privilegios.

4.2.1. Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica, deberán ser notificados por escrito o vía correo electrónico a la Dirección de Informática con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.2.2. Corresponde a la Dirección de Informática, administrar, mantener y actualizar la infraestructura de la red institucional.

4.2.3. La Dirección de Informática, administrará y supervisará el uso y funcionamiento del correo electrónico institucional.

4.2.4. La Dirección de Informática es la responsable de emitir y dar seguimiento al presente manual, para el uso adecuado de la red institucional.

4.3. Acceso a redes y recursos de red

4.3.1. La Dirección de Informática no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

4.3.2. Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

4.3.3. No se permite el uso de los servicios de la red cuando no cumplan con las labores propias del área.

4.3.4. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

4.3.5. El uso de analizadores de red es permitido única y exclusivamente por la Dirección de Informática, para monitorear la funcionalidad de las redes.

4.3.6. No se permitirá el uso de analizadores para monitorear o censar redes ajenas y no se deberán realizar análisis de la Red desde equipos externos.

4.3.7. Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

4.4. Equipo desatendido.

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por la Dirección de Informática) como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

4.5. Administración y uso de contraseñas.

4.5.1. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

4.5.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito a la Mesa de Ayuda, indicando si es de acceso a la red o a módulos de sistemas

desarrollados por la Dirección de Informática, para que se le proporcione una nueva contraseña.

4.5.3. La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la Dirección de Informática como empleado de la Dependencia o Entidad.

4.5.4. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

4.5.5. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos.
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10); Estos caracteres deben ser alfanuméricos, o sea, números y letras.
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.5.6. La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

4.5.7. Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.

4.5.8. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

4.6. Control de accesos remotos.

4.6.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la Dirección de Informática.

4.6.2. La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por la Dirección de Informática.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política: La Dirección de Informática, es la encargada de fijar las bases de la política informática que permitan conocer y planear el desarrollo tecnológico al interior de la Dependencia o Entidad.

5.1. Derechos de Propiedad Intelectual.

5.1.1. Está prohibido por las leyes de derechos de autor, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Dependencia o Entidad.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte de la Dirección de Informática, o sea coordinado por ésta, son propiedad intelectual de la Dependencia o Entidad.

5.1.3. El material que aparezca en la página de Intranet e Internet de la Dependencia o Entidad deberá ser supervisado por la Dirección de Informática, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

5.1.4. Corresponde a la Dirección de Informática garantizar que todo el software instalado en la Red institucional cumpla con la ley de propiedad intelectual.

5.1.5. Cualquier instalación de software que sea realizada sin autorización o supervisión de la Dirección de Informática, es y será responsabilidad del resguardante del equipo de cómputo en el que sea instalado.

5.2. Revisiones del cumplimiento.

5.2.1. La Dirección de Informática realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.

5.2.2. La Dirección de Informática podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

5.3. Violaciones de seguridad informática.

5.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la Dirección de Informática.

5.3.2. Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información.

Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación de la Dirección de Informática.

5.3.3. Ningún usuario de la Dependencia o Entidad debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Dirección de Informática.

5.3.4. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para auto replicarse, dañar, afectar el desempeño, acceso a las computadoras, redes e información de la Dependencia o Entidad.

5.3.5. Cualquier infracción a las políticas emitidas en este manual en las que se comprometa la seguridad de la Red institucional será sancionada de conformidad a lo que dispone la Ley de Responsabilidades de los Servidores Públicos del Estado y de los Municipios.

6. DISPOSICIONES GENERALES

6.1.1. Este Manual de Políticas y Estándares de Seguridad Informática deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la plantilla de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.

6.1.2. El presente Manual empezará a surtir sus efectos legales a partir de su autorización, el cual deberá ser difundido en todas las áreas para su conocimiento y aplicación.

Para los efectos del presente manual, se escribe el presente glosario de términos:

(A)

Acceso: Es el privilegio de una persona para utilizar un objeto o infraestructura.

Acceso Físico: Es la actividad de ingresar a un área.

Acceso Lógico: Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.

Acceso Remoto: Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.

Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.

Área Crítica: Es el área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de la Dependencia o Entidad.

Ataque: Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.

(B)

Base de datos: Es un conjunto de datos interrelacionados que cumple con ciertos parámetros estructurales y de organización a la cual se puede acceder a través de programas específicos.

(C)

Confidencialidad: Se refiere a la obligación de los servidores judiciales a no divulgar información a personal no autorizado para su conocimiento.

Contraseña: Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

Control de Acceso: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

Copyright: Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida.

(D)

Disponibilidad: Se refiere a que la información esté disponible en el momento que se necesite.

DataCenter (Centro de Datos)
Oficina con equipos de cómputo, telecomunicaciones y servidores que prestan servicios a todas Las Empresas con las características físicas y ambientales adecuadas para que los equipos alojados funcionen sin problema.

(E)

Estándar: Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

Equipo de Telecomunicaciones: Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Equipo de Computo: Dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles .

(F)

Falta administrativa: Acción u omisión contemplada por la normatividad aplicable a la actividad de un servidor judicial, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.

FTP: Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.

(G)

Gusano: Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

(H)

Hardware: Se refiere a las características técnicas y físicas de las computadoras.

Herramientas de seguridad: Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica.

(I)

Identificador de Usuario: Nombre de usuario (también referido como UserID) único asignado a un servidor público para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.

Impacto: Magnitud del daño ocasionado a un activo en caso de que se materialice.

Incidente de Seguridad: Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.

Integridad: Se refiere a la pérdida ó deficiencia en la autorización, totalidad ó exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.

Internet: Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes (world wide web) en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.

Intrusión: Es la acción de introducirse o acceder sin autorización a un activo.

(M)

Maltrato: Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad del Gobierno del Estado. Se contemplan dentro de éste al descuido y la negligencia.

Malware: Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, spyware, troyanos, rootkits, backdoors, adware y gusanos.

Mecanismos de seguridad o de Control: Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir a probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Medios de almacenamiento magnéticos: Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD´s, DVD´s, etc.)

Mesa de Ayuda:

Módem: Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de

la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.

(N)

“Necesidad de saber” principio: Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades.

Normatividad: Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.

(P)

Password: Véase Contraseña.

(R)

Red institucional: Es un sistema de comunicación de datos que enlaza dos o más ordenadores y dispositivos o periféricos. La Red institucional es un conjunto de PC's y otros dispositivos que se conectan entre sí, para comunicarse entre ellos, con el fin de compartir información y recursos, haciendo que todas las personas o departamentos de esta Dependencia o Entidad, estén trabajando unidos, sin duplicar la información, transmitiéndola en forma rápida y eficaz.

Respaldo: Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Riesgo: Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.

(S)

Servidor: Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura clienteservidor.

Sitio Web: El sitio web es un lugar virtual en el ambiente de internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.

Software: Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.

Software Libre: es la denominación del software que respeta la libertad de los usuarios y por tanto, una vez obtenido, puede ser usado, copiado, estudiado, modificado y redistribuido libremente.

Spyware: Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraer información sin la autorización del propietario.

(U)

UserID: Véase Identificador de Usuario.

Usuario: Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).

(V)

Virus: Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.

Vulnerabilidad: Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

(W)

WWW (World Wide Web): Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma fácilmente accesible.