Gobierno del
Estado de Sonora

Secretaría de Ganadería, Agricultura, Recursos Hidráulicos, Pesca y Acuacultura

Dirección General de Planeación, Administración y Evaluación

MANUAL DE POLITICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

Mayo, 2019

SONORA
UNIDOS LOGRAMOS MÁS

CONTENIDO

INTRODUCCIÓN

El presente manual fue elaborado debido a la necesidad de prestar un mejor servicio que garantice el uso correcto de los activos informáticos con los que actualmente cuenta la Dependencia. El buen uso de los mismos permitirá a la Secretaría alcanzar una mayor eficacia y eficiencia en nuestra relación laboral. Por tal motivo se deben tomar acciones apropiadas para mantenerlos, usarlos, mejorarlos y protegerlos de diferentes riesgos como: violación de privacidad, interrupción de servicios, accidentes y desastres naturales, mediante políticas que nos permitan normar las actividades relacionadas con los Sistemas de Información.

Con el establecimiento de las políticas y estándares de seguridad informática se busca garantizar que el material y los recursos de software de la Secretaría de Agricultura, Ganadería, Recursos Hidráulicos, Pesca y Acuacultura, se utilicen únicamente para los propósitos para los que fueron asignados y sean operados de una forma confiable. Esto permite una mayor integridad, confidencialidad y confiabilidad de la información que se genera en la Institución minimizando los riesgos de alteración o pérdida en el uso de las tecnologías de información.

OBJETIVO DEL MANUAL

El presente documento tiene por objetivo establecer y dar a conocer a todo el personal de la Secretaría, los mecanismos de control necesarios, para asegurar la integridad, confidencialidad y disponibilidad de la información electrónica de forma oportuna y confiable.

JUSTIFICACIÓN

El área de informática de la Secretaría está facultada para definir políticas y estándares en materia de informática; así como también para dar cumplimiento y seguimiento del mismo, para beneficio únicamente de la Dependencia.

ALCANCE

El presente documento establece los mecanismos de control que deberán aplicar de forma obligatoria los Servidores Públicos para el buen uso del equipo de cómputo, aplicaciones e información.

BENEFICIOS

Las políticas de seguridad e informática establecidas en este documento son la base para la protección de los activos tecnológicos e información de esta Secretaría.

SANCIONES POR INCUMPLIMIENTO

El incumplimiento del presente documento podrá derivar en responsabilidad administrativa y/o penal, según la naturaleza y/o gravedad, cuya sanción será aplicada por las autoridades correspondientes.

POLÍTICAS

1. POLÍTICAS Y ESTANDARES DE SEGURIDAD DEL PERSONAL

1.1. De los Usuarios

Todo usuario de la Dependencia, que maneje bienes y servicios informáticos asume el compromiso de operar bajo los principios de confidencialidad de la información y de uso adecuado de los recursos, así como el apego estricto a las políticas de seguridad informática del presente manual.

1.2. Inducción a los temas en Seguridad Informática.

Todo empleado de nuevo ingreso deberá:

- Leer Manual de Políticas de Seguridad Informática, donde se dan a conocer las obligaciones para los Servidores Públicos y las sanciones que pueden aplicarse en caso de incumplimiento.
- Firmar el documento "Aceptación de Políticas de Seguridad" del Manual de Políticas de Seguridad Informática; estos deben ser anexados a los demás documentos relacionados con su expediente personal.

1.3. Acuerdos de uso y confidencialidad a externos.

El Titular de la dependencia, Subsecretarios, Directores Generales y Directores de área, deberán verificar la existencia del documento de "Aceptación de Políticas de Seguridad" para el personal externo que realice labores en o para la Dependencia.

- Firmar "Aceptación de Políticas de Seguridad", del Manual de Políticas de Seguridad Informática; al momento de su acceso a las instalaciones de la Dependencia.
- Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de la Dependencia, quien será responsable del control y vigilancia del uso adecuado de la información y los bienes y servicios informáticos.

2. POLÍTICAS 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, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones de la Dependencia.

- La Dependencia implantará y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren sus instalaciones. 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 consideraran 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 y externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de informática.
- 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 informática y/o inventarios, a través de formatos de autorización de entrada/salida.
- La Dirección General de Planeación, Administración y Evaluación, notificará a las áreas correspondientes, las Altas y Bajas de usuarios, mediante formato establecido.

2.1. Resguardo y protección de la información

2.1.1 Respaldo de la Información.

El área de informática apoyará de ser necesario en la generación de copias de respaldo y almacenamiento de la información crítica, proporcionando los procedimientos para la realización de esta actividad. Cada Unidad Administrativa propietaria de la información, con el apoyo del área de informática, deberá realizar de manera periódica el respaldo de la información que considere de vital importancia para el desarrollo de las funciones, definiendo la estrategia a seguir y periodos de retención para el respaldo y almacenamiento de la información.

2.1.2 Copias de respaldo de la información.

2.1.2.1 Cada unidad administrativa será responsable del respaldo y resguardo de la información generada en el área, así como de la restauración, almacenamiento y tratamiento de la información, velando por su integridad y disponibilidad.

2.1.2.2 El área de Informática debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

2.1.2.3 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.

2.1.2.4 El usuario deberá reportar de forma inmediata al área 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.

2.1.2.5 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.

2.1.2.6 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 departamento de recursos materiales y bienes muebles, 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, deberá registrar el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la Dependencia, 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 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, deberá notificar la salida.

2.3. Controles de acceso físico a la infraestructura de comunicaciones.

2.3.1 Las solicitudes de acceso al centro de cableado deben ser aprobadas por el área de Informática; no obstante, los visitantes siempre deberán estar acompañados durante su visita al centro de cómputo.

2.3.2 El área de Informática debe registrar el ingreso de los visitantes a los puntos de cableado en una bitácora.

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 el área de Informática antes de conectarse a cualquier nodo de la Red y desconectar aquellos dispositivos que no estén aprobados.

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 el área de Informática.

2.4.4 El área de Informática debe proveer las condiciones físicas y medioambientales necesarias para la protección y correcta operación de los recursos ubicados en el centro de cómputo, el cual deberá ser de vidrio preferentemente transparente; 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 El área de Informática debe velar porque los recursos informáticos ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

2.4.6 El área 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. 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.

2.5.1 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.

2.5.2 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.
- El área 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.
- El área de Informática, es la encargada de la administración, habilitación y/o bajas de usuarios en la red inalámbrica.

2.5.2.1 Identificación y activación

- Para hacer uso de la red inalámbrica, el solicitante necesariamente deberá ser empleado la Dependencia.
- 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 al área de informática para su respectiva baja del equipo de la red inalámbrica.

2.5.2.2 **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.

2.5.2.3 **Excepciones**

- 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.

2.6. Protección y ubicación de los activos tecnológicos.

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

2.6.1 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.

2.6.2 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.

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

2.6.4 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 del área de informática, debiéndose solicitar a la misma en caso de requerir este servicio.

2.6.5 El departamento de recursos materiales y bienes muebles 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 Área de Informática.

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

2.6.7 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.

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

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

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

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

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

2.6.13 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.

2.7. Mantenimiento de activos informáticos e infraestructura

Personal autorizado para el mantenimiento se encargará de proporcionar de manera oportuna, los servicios que requiere la Dependencia en materia de mantenimiento

preventivo y correctivo a los activos informáticos y a la infraestructura mediante Bitácora de Mantenimiento.

2.7.1 Únicamente el personal autorizado por la Dirección General Planeación, Administración y Evaluación, a través del área 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.

2.7.2 El período para llevar a cabo el mantenimiento preventivo será determinado por la Dirección General Planeación, Administración y Evaluación.

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

2.7.4 En caso de ser necesario un mantenimiento correctivo de cualquier equipo de cómputo, deberá solicitarse mediante una orden de servicio.

2.7.5 Los tiempos de reparación dependerán del tipo de daño y de los tiempos del proveedor del servicio.

2.7.6 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.

2.7.7 Los usuarios no deberán utilizar medios de almacenamiento personales en los equipos de cómputo oficiales.

2.7.8 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.

2.8. Pérdida o transferencia de equipo

2.8.1 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.

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

2.8.3 El usuario deberá dar aviso de inmediato a la Dirección General de Planeación, Administración y Evaluación de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo, y dicha Unidad Administrativa a su vez al área de Informática.

2.8.4 El usuario notificará al área de informática, cuando por el cumplimiento de sus funciones, deba transferir o trasladar el equipo de cómputo a otra área, esto con la finalidad dar soporte y resguardar la integridad del equipo.

2.9. Uso de dispositivos especiales

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

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

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

2.10. 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 del accesorio, reparación y/o su reposición, para tal caso se determinará la causa de dicha descompostura.

3. POLÍTICA 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. 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 hacia redes externas como internet.

3.1. Uso de medios de almacenamiento.

3.1.1 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 al área de informática.

3.1.2 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.

3.2. Instalación de Software.

3.2.1. El área 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 cuando el software operativo es actualizado.

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

3.2.3. Los usuarios que requieran la instalación de software que no sea propiedad de la Dependencia, deberán justificar su uso y solicitar su autorización al área 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 área de Informática procederá de manera inmediata a desinstalar dicho software.

3.2.4. 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, que no esté autorizado por el área de Informática.

3.2.5. Del software propiedad de la Dependencia.

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

II. El área de Informática contará con un registro del software propiedad de la Dependencia, 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 del área de Informática se mantendrán como propiedad de la Dependencia respetando la propiedad intelectual correspondiente.
IV. Corresponderá al área de Informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas informáticos ubicados en los servidores.
V. El área de Informática administrará los diferentes tipos de licencias de software y vigilará su vigencia.

3.3. Administración de la configuración.

Los usuarios de las áreas de la Dependencia 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.

3.3.1. Del acceso a los sistemas administrativos:

I. Tendrá acceso a los sistemas administrativos solo el personal de la Dependencia 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. 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 el área de Informática.
II. El área 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 área de Recursos Humanos notificará al área de informática las altas y bajas de personal que manejen correos oficiales de la Dependencia.

3.5.2. La asignación de cuentas de correo se hará en base a las funciones del cargo que desempeña.

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 manejarla contraseña de acceso al correo electrónico con privacidad.

3.5.5. Cuando un servidor público de la Dependencia sea dado de baja, el área de Recursos Humanos deberá informar al área de Informática, para el bloqueo de la cuenta de correo correspondiente.

3.5.6. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Dependencia. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.5.7. 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 se le proporcionó.

3.5.8. El usuario debe de utilizar el correo electrónico institucional 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.

3.5.9. El usuario es responsable de la información enviada o reenviada desde su buzón de correo electrónico.

3.5.10. El Servidor Público 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:

- Enviar correos masivos no oficiales.

- 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.
- Compartir o divulgar números de cuenta, claves de acceso y número de identificación personal u otra información confidencial o sensible para la Dependencia.
- Utilizar el servicio de correo electrónico institucional para fines diferentes a los objetivos de la Dependencia.
- 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.
- Enviar o promover dentro o fuera de la Dependencia, 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.

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

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al área de Informática, para que, a través de ella, se tome las medidas de control correspondientes.
- Ningún usuario ni empleado de la Dependencia o personal externo podrá bajar o descargar software de sistemas, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de Informática.
- Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil será responsable de solicitar de manera periódica a Informática las actualizaciones del software de antivirus.
- Debido a que algunos virus son extremadamente complejos, ningún usuario debe intentar erradicarlos de las computadoras, lo indicado es realizar una orden de Servicio 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/o función que desempeña. En caso de daño a la imagen de la institución se dará vista al Órgano Interno de Control, a fin de evaluar de acuerdo a la gravedad del daño causado, según lo establecido en la Ley Estatal de Responsabilidades y el Código de Ética de las personas servidoras públicas de la administración pública estatal conforme al principio de transparencia y resguardo de la información y/o documentación gubernamental que tiene bajo su responsabilidad.

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

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

- Deberán cumplirse todas las normas específicas dictadas por el área de Informática.
- Deberá comunicarse al área de informática 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 al área 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. 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.
- 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 el área 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.
- 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.
- 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.

3.8. Queda estrictamente prohibido*:*

- 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.
- 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.
- 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.
- 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.

- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet.
- Navegar en Internet a excepción, de cuando las actividades propias del puesto así lo requieran.

3.9. Atención a usuarios de servicios tecnológicos.

- La atención por parte de Informática se realizará previo informe de incidencia y según sea el caso se solicitará la elaboración de una orden de servicio para enviar el equipo con un especialista externo.
- Se podrá resolver telefónicamente dudas operativas y funcionales con respecto a las herramientas utilizadas en aplicaciones, sistemas operativos, etc.
- Se hará el soporte solicitado vía remota o en sitio, según sea considerado por el área de informática.

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

3.9.2. El área de informática tendrá 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 al Director General de Planeación, Administración y Evaluación los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

3.9.3. El área de Informática no es responsable por el contenido de datos ni por el tráfico que circule en la red, la responsabilidad recae directamente sobre el usuario que los genere.

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

4. POLÍTICAS DE CONTROLES DE ACCESO LÓGICO

El usuario no debe proporcionar información a personal externo de los mecanismos de acceso a las instalaciones e infraestructura tecnológica de la dependencia; así mismo tiene prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña, será responsabilidad exclusiva al usuario al que pertenecen, salvo prueba de que le fueron usurpados esos controles.

4.1. Acceso a redes y recursos de red

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

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

4.1.3. 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.

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

4.2. Equipo desatendido

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

5. POLÍTICAS DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Política: El área 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.

5.1. Derechos de la 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.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte del área de informática, o sea coordinado por ésta, son propiedad intelectual de la Dependencia.

5.1.3. El material que aparezca en la página Internet de la Dependencia deberá ser supervisado por el área 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. Cualquier instalación de software que sea realizada sin autorización o supervisión del área 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. El área de Informática realizará acciones de verificación del cumplimiento del Manual de Políticas y de Seguridad Informática.

5.2.2. El área de Informática podrá implementar mecanismos de verificación y 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 General de Planeación, Administración y Evaluación.

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 del área de Informática.

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

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 Reemplazar por la Ley Estatal de Responsabilidades Administrativas.

6. DISPOSICIONES GENERALES

6.1. Este Manual de Políticas 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.

6.2. 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.