SALUD
SECRETARÍA DE SALUD

Secretaría de Salud
Dirección General de Tecnologías de la Información

Guía de referencia para la Seguridad Informática en la Secretaría de Salud

MAAGTIC-SI

La Dirección General de Tecnologías de la Información elaboró el presente documento para promover el uso de la Seguridad Informática en la Secretaría de Salud.

Organización:
Dirección General de Tecnologías de la Información

1 INTRODUCCIÓN

Con fundamento en el Artículo 32 del Reglamento Interior de la Secretaría de Salud y en apego al Manual de Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información, publicado por la Secretaría de Función Pública, la Dirección General de Tecnologías de la Información elaboró la presente *"Guía de referencia para la Seguridad Informática en la Secretaría de Salud"*, con la finalidad de proteger la infraestructura computacional y todo lo relacionado con ésta, la cual incluye la información contenida.

2 OBJETIVO

Emitir las recomendaciones para el personal de ***"LA SECRETARÍA"*** en el manejo y utilización de equipo de cómputo, información, aplicaciones y sistemas de información durante la ejecución de sus funciones a fin de cumplir con los requerimientos de seguridad y de control establecidos por la Dependencia.

3 ABREVIATURAS Y DEFINICIONES

Abreviación o definición	Descripción
"LA SECRETARÍA"	Unidades Administrativas y Órganos Desconcentrados de la Secretaría de Salud.
"LA DGTI"	Dirección General de Tecnologías de la Información.
MAAGTIC-SI	Manual Administrativo de Aplicación General en las materias de Tecnologías de Información y Comunicaciones y Seguridad de la Información.
Activos de información	Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, deben ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
Personal	Los empleados de la Secretaría de Salud

4 GUÍA DE SEGURIDAD INFORMÁTICA

La presente guía recomienda acciones para la seguridad Informática de los activos de información de ***"LA SECRETARÍA"***.

4.1 ALCANCE

Esta guía está dirigida a todo el personal de ***"LA SECRETARÍA"*** que tenga acceso a cualquier activo de información de la Dependencia.

4.2 SEGURIDAD INFORMÁTICA

4.2.1 USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

- El personal protegerá y custodiará los activos de información que le son asignados para la ejecución de sus funciones y actividades.
- El personal utilizará los activos de información únicamente para los fines que le fueron asignados.
- El personal no utilizará los activos de información para fines personales.
- El personal no prestará activos de información a terceros ajenos a ***"LA SECRETARÍA"*** por parte del personal.
- El personal no almacenará, reproducirá, ejecutará ni transmitirá copias no autorizadas de software o información digital (incluyendo música, video y juegos) en los recursos de cómputo que les sean asignados.
- No alterará, la configuración de los programas precargados (software institucional) en los equipos de cómputo asignados al personal, asimismo, no podrán ser copiados a ningún otro medio.
- No utilizarán los activos de información de ***"LA SECRETARÍA"*** para almacenar, procesar, descargar o transmitir información (ej.: cadenas de correo electrónico) con la finalidad de promover actos y propaganda política, religiosa, racista, étnica, social, etc.
- No publicará información difamatoria o privada de alguna persona u organización sin su consentimiento, con o sin el fin de ocasionarle algún daño emocional, profesional, económico o de cualquier índole.
- No distribuirá fuera de ***"LA SECRETARÍA"*** artículos, documentos o cualquier otro material o información que sea identificado con registro de propiedad intelectual o que haya sido clasificada como reservada o confidencial (ej.: manuales, políticas, normas, planes estratégicos, documentación de procesos, entre otros).
- El personal de ***"LA SECRETARÍA"*** notificará a la Dirección General de Tecnologías de la Información cualquier evidencia o sospecha de mal uso

de los activos de información o violación a las recomendaciones establecidas en esta guía

- El personal no otorgará acceso a familiares, amigos, vecinos, clientes, proveedores, vendedores y otros visitantes desconocidos, a los servicios de red de ***"LA SECRETARÍA"*** mediante su cuenta institucional. En situaciones en las que se deba dar o requiera dar acceso a estas personas, el personal considerará los siguientes puntos:

  1. Verificar que las personas ajenas a **"LA SECRETARÍA"** cuando se encuentren dentro de las instalaciones de ésta, accedan a los activos de información con la supervisión y monitoreo del personal de la Dependencia.
  2. En caso de requerir transmitir información que se contengan en los activos de información, el personal de **"LA SECRETARÍA"** evaluará y bajo su consentimiento podrá otorgarle la información, misma que deberá verificar sea únicamente la aprobada para ser extraída.

- No instalarán en los equipos de cómputo programas destructivos o maliciosos (ej.: virus, gusanos, caballos de troya, puertas traseras, y en general, herramientas de hacking) que puedan causar daños, interferencias con otros sistemas, accesos no autorizados o disminución en el desempeño de los sistemas de ***"LA SECRETARÍA".***

- El personal que tenga equipo de cómputo asignado, se responsabilizará de su uso y de la información contenida en los mismos, por lo que se recomienda no compartirlos y estar en cumplimiento de los requerimientos de seguridad física y lógica establecidos.

- El personal bloqueará sus pantallas o monitores cuando dejen desatendido su sistema de cómputo.

- En caso de que el personal tenga asignado un equipo de cómputo portátil (laptop, PDA, entre otros) y sea víctima de robo o pérdida, debe reportar a la brevedad el incidente.

- El personal de ***"LA SECRETARÍA"*** revisará todos los medios de almacenamiento removibles que sean introducidos o conectados a sus equipos de cómputo utilizando el programa antivirus instalado por "***LA SECRETARÍA".***

4.2.2 USO DE CONTRASEÑAS

- El personal es responsable de la custodia y manejo de sus identificadores de usuario y contraseñas (claves de acceso a los sistemas y aplicaciones).
- El personal es responsable de todas las actividades que se realicen con sus identificadores de usuario y contraseñas, incluyendo la recepción y transmisión de información, la ejecución de transacciones que se hagan entre los sistemas de información de ***"LA SECRETARÍA"*** y la ejecución de transacciones en las aplicaciones de ***"LA SECRETARÍA"***.
- Las contraseñas serán consideradas como información confidencial y no deben ser divulgadas por ningún medio a ninguna persona. Cuando, por requerimiento de algún proceso de ***"LA SECRETARÍA"***, requiera dar la contraseña, al término de su uso será cambiada de inmediato.
- El personal cambiará cada 60 días sus contraseñas como máximo o con la periodicidad que el sistema o aplicación se lo requiera.
- Las contraseñas utilizadas por los usuarios serán diferentes a las últimas 5 que se hayan utilizado.
- En caso de que el personal intente acceder al equipo de cómputo por más de 3 veces sin lograrlo y su cuenta sea bloqueada, lo notificará a su enlace informático y solicitar su reactivación.
- El personal seleccionará contraseñas diferentes para los distintos sistemas a los que tienen acceso autorizado.

- Las contraseñas iniciales sólo serán válidas para el primer acceso. Todo el personal es responsable de cambiarla después de acceder al sistema por primera vez.

- El personal utilizará una nomenclatura robusta, considerando los siguientes elementos:

1. Se utilizará una combinación de al menos 8 caracteres alfanuméricos.
2. Incluirá en la contraseña el uso de letras minúsculas, mayúsculas, caracteres especiales, espacios, puntuación y números.
3. No utilizará solo letras, solo números, solo mayúsculas o el mismo carácter repetido.
4. La mejor guía para seleccionar una contraseña es que ésta debe ser fácil de recordar para quien la selecciona pero prácticamente imposible adivinar por otra persona.
5. No se utilizará el nombre del identificador de usuario en ninguna forma (escrito al revés, doble, igual, etc.).
6. No utilizarán nombres o apellidos del usuario en ninguna forma.
7. No utilizarán el nombre del cónyuge, hijos, familiares, novias, mascotas, fechas, etc.
8. No utilizará información que pueda ser obtenida fácilmente como Registro Federal de Contribuyentes números telefónicos, placas de coches, dirección, etc.
9. No utilizarán palabras de diccionario (en cualquier idioma o de alguna disciplina específica como medicina, química, etc.).
10. Se recomienda utilizar un método para elaborar contraseñas que sea fácil de aprender y de recordar, ejemplos de estos métodos son:
    a) Seleccionar una o varias líneas de una canción o libro y formar la contraseña con la primera letra de cada palabra.
    b) Alternar entre una consonante y una o dos vocales, produciendo una palabra que sea pronunciable y de esta forma fácil de recordar.

4.2.3 USO DE INTERNET

- El personal no publicará ningún tipo de información de ***"LA SECRETARÍA"*** en Internet.
- El personal notificará a la Dirección General de Tecnologías de la Información en forma inmediata cualquier actividad sospechosa o evidencia de violaciones a la seguridad relacionadas con la conectividad hacia Internet (acceso no autorizado a la red, telecomunicaciones o sistemas de cómputo; transmisión aparente o real de un virus o gusano a través de la red, sabotaje aparente o real de cualquier archivo para el que el personal haya definido un usuario y contraseña).
- No se transmitirá información confidencial y reservada a través de Internet sin un mecanismo apropiado como encripción y sin autorización.
- El uso de los servicios de Internet se limita a las actividades necesarias para ***"LA SECRETARÍA"***.
- No usará servicios de mensajería electrónica (ej.: Microsoft Messenger, Yahoo Messenger, AOL Messenger, ICQ, Trillian, entre otros) en los recursos de cómputo asignados al personal.
- El personal no utilizará los servicios de Internet para fines ilegales, en caso de no estar seguro de la legalidad de sus acciones, solicitará información al personal de ***"LA DGTI".***
- El personal no puede levantar servidores (ej.: servidores de web, dhcp, dns, entre otros) en los recursos de cómputo que no fueron asignados para ese fin.

4.2.4 USO DE CORREO ELECTRÓNICO

El uso de correo electrónico será considerado conforme a lo estipulado en al "*Guía de referencia para el uso del correo electrónico institucional*".

4.2.5 ESTÁNDARES Y NORMAS PARA ASEGURAR LA INFORMACIÓN

El conjunto de las medidas de seguridad y protección de la información y de disciplina informática constituirán la Seguridad Informática, que comprende medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo o constituyan una amenaza para la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías informáticas y de comunicaciones; así como el correcto uso y conservación de las mismas.

Para la correcta administración de la seguridad de la información, se mantendrán acciones para cumplir con los tres requerimientos de mayor importancia para la información, estos son:

Confidencialidad: Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.

Integridad: Busca asegurar:

- Que no se realicen modificaciones por personas no autorizadas a los datos o procesos.
- Que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos.
- Que los datos sean consistentes tanto interna como externamente.

Disponibilidad: Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado.

Tipos de Amenazas: Las amenazas se pueden clasificar principalmente como:

Tipos de Amenaza	Ejemplos
Suplantación	Falsificar mensajes de correo electrónico
Alteración	Alterar datos durante la transmisión Cambiar datos en archivos
Repudio	Eliminar un archivo esencial y denegar este hecho

	Adquirir un producto y negar posteriormente que se ha adquirido
Divulgación de información	Exponer la información en mensajes de error Exponer el código de los sitios Web
Denegación de servicio	Inundar una red con diversas peticiones por ejemplo solicitudes de acceso a una pagina web institucional logrando saturarla y que se encuentre sin servicio.
Elevación de privilegios	Explotar vulnerabilidades para obtener privilegios en el sistema Obtener privilegios de administrador de forma ilegítima

4.2.6 ENTRENAMIENTO Y CONCIENCIACIÓN

- Todo el personal que maneje activos de información asistirá a los programas de entrenamiento y concienciación en el tema de seguridad de la información provistos por ***"LA SECRETARÍA"***, cuando así se requiera.

4.2.7 MONITOREO DE USUARIOS

- ***"LA SECRETARÍA"*** a través de ***"LA DGTI"*** podrá reservarse el derecho de monitorear el correo electrónico, los directorios personales de archivos y otra información almacenada en los equipos de ***"LA SECRETARÍA"*** en cualquier momento y sin previo aviso, aún y cuando éstos contengan información personal, dar cumplimiento al marco legal y regulatorio vigente en materia.

- Los sistemas de ***"LA SECRETARÍA"*** y toda la información contenida en ellos, (incluyendo archivos, mensajes de correo electrónico y correo de voz, registros de acceso a Internet, etc.) son propiedad de ***"LA SECRETARÍA"*** y son auditables. La información contenida en los sistemas puede ser revisada, divulgada o interceptada por ***"LA SECRETARÍA"*** en cualquier momento y sin previo aviso para propósitos de revisión.

4.2.8 VIRUS Y CÓDIGO MALICIOSO

- No podrá el personal obtener archivos de Internet directamente de un servidor o equipo de producción. Los archivos obtenidos de Internet se colocarán en un ambiente aislado o en medios de almacenamiento de sólo lectura para ser revisados por el software antivirus antes de ser colocados en los directorios de trabajo.
- No abrirá cualquier archivo adjunto de correos electrónicos provenientes de una fuente desconocida, sospechosa o no confiable. Estos correos se borrarán inmediatamente del buzón de correo electrónico.
- Todos los archivos adjuntos (incluyendo el contenido de archivos comprimidos) que se reciban vía correo electrónico serán revisados a través de las herramientas que ***"LA DGTI"*** implemente para detectar la presencia de virus y de otros programas destructivos antes de ser abiertos o almacenados en los equipos o sistemas de ***"LA SECRETARÍA"***.
- El personal revisará todos los medios de almacenamiento removibles con el software antivirus antes de ser utilizados y de acceder a la información contenida en ellos.
- El personal no modificará la configuración, eliminar, desactivar o forzar por alguna otra manera el software antivirus.
- El personal utilizará el software antivirus autorizado e instalado por ***"LA SECRETARÍA"***. y no podrá instalar cualquier software antivirus diferente a éste.
- El personal reportará en forma inmediata todos los incidentes de virus o código malicioso (detectados por el software antivirus instalado).
- El personal evitará compartir información de sus equipos con acceso de lectura/escritura a menos que sea absolutamente necesario por requerimientos de trabajo, en tal caso, se revisará ambos equipos con el software antivirus de ***"LA SECRETARÍA"*** antes de compartir recursos.

- El personal borrará el correo electrónico no solicitado (basura, cadenas, etc.).

4.2.9 HERRAMIENTAS DE HACKEO

- El personal no realizará hackeo y actividades relacionadas o similares a éstas. El hackeo incluye, pero no está limitado a las siguientes actividades: acceso ilegal o no autorizado a computadoras, redes, cuentas y otros sitios restringidos, o intento de evadir medidas de seguridad y zonas restringidas en la red.
- No descargará, instalará o ejecutará herramientas de hackeo, como son sniffers, caballos de troya, herramientas de interrogación de puertos y vulnerabilidades, entre otros.

4.2.10 PORNOGRAFÍA

- El personal no introducirá, almacenará, desplegará, anunciará, procesará ó transmitirá material pornográfico en cualquier activo de información de ***"LA SECRETARÍA"***.
- No accederá a sitios de material pornográfico en Internet o a sitios relacionados.

4.2.11 RESPALDOS

- El personal respaldará periódicamente sus archivos con información clasificada como confidencial o reservada.
- El personal mantendrá organizada su información en carpetas electrónicas para facilitar el respaldo y recuperación de la misma.

4.2.12 USO DE MEDIOS REMOVIBLES

- El personal no utilizará medios removibles que sean propiedad del personal para descargar, almacenar o transmitir información de ***"LA SECRETARÍA"***.

4.2.13 DECÁLOGO DE SEGURIDAD

1. Es responsabilidad de cada usuario el uso de su cuenta y contraseña con la que tiene acceso a los equipos y Servicios Institucionales
2. La configuración de los equipos de cómputo institucionales no podrá ser modificada, no descargará programas ajenos a las actividades laborales.
3. El servicio de Internet es para fines laborales, por lo que no se accederá a sitios o descargará programas (juegos, música, vídeo, etc.).
4. La información considerada como confidencial se almacenará y transmitirá de forma segura, y cada usuario es responsable de la información que maneja, por lo que es importante realizar los respaldos.
5. El uso del correo electrónico sólo será a través del servicio institucional y para propósitos laborales, no se emplearán cuentas personales.
6. El uso de equipo de Comunicación de voz (teléfonos fijos, móviles, terminales cifradas, radiocomunicación) es responsabilidad de cada usuario para fines institucionales.
7. La impresión de documentos se limitará a lo indispensable y es responsabilidad de cada usuario, empleando los esquemas que la Institución proporciona.
8. Se recomienda que todo documento que se considere como inservible sea evaluada su destrucción en su totalidad a través del triturado de papel y conforme a la Ley Federal de Archivos.
9. Se recomienda al personal dejar libre de documentos su escritorio o estaciones de trabajo cuando no estén siendo ocupadas.

10. Cada documento que circule por la institución se siguiere que sea manejado de manera responsable y de acuerdo a su clasificación.

4.2.14 SEGURIDAD EN EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Todas las aplicaciones desarrolladas para ***"LA SECRETARÍA"***, considerarán la seguridad como un aspecto a cubrir por los involucrados en el desarrollo de sistemas en todas sus fases.

Antes de adquirir o desarrollar una aplicación, ***"LA SECRETARÍA"*** especificará claramente los requerimientos mínimos de seguridad con que contará la aplicación.

Las diferentes alternativas serán revisadas con los desarrolladores o proveedores para obtener un balance adecuado entre los requerimientos de seguridad y la funcionalidad (facilidad de uso, simplicidad operativa, actualizaciones, costos, entre otros). Buscando mantener la confidencialidad, integridad y disponibilidad de las información.

La aceptación de nuevas soluciones tecnológicas, actualizaciones, reconfiguraciones y cambios a nuevas versiones, tendrán una base de criterios de aceptación, tomando en consideración los siguientes puntos:

- Requerimientos de capacidad y desempeño de los equipos.
- Procedimientos para recuperación de errores y planes de contingencia.
- Revisión de procedimientos operativos de rutina.
- Manuales de procedimientos.
- Controles de seguridad.
- Evidencia de que la adquisición, actualización, reconfiguración y cambios de versiones, no afectan la operación normal ni la seguridad de la organización.
- Capacitación en la operación y uso de nuevos sistemas.

Ambientes de desarrollo, prueba y producción

Las herramientas para el desarrollo de sistemas o aplicaciones serán accesibles solo para los miembros autorizados de desarrollo de sistemas.

Las herramientas para el desarrollo de sistemas o aplicaciones se propone eliminarse de cualquier equipo de cómputo que no sea utilizado para el desarrollo de sistemas, o bien, justificar su uso mediante la elaboración de un análisis de riesgos.

Los ambientes de desarrollo y pruebas, estarán separados de los de producción, tomando en consideración la parte física y de redes. Al no ser posible esta separación de ambientes por que los sistemas no lo permitan, se llevará a cabo separaciones lógicas de redes, directorios y archivos.

No se instalarán herramientas de desarrollo en los ambientes de producción o pruebas, y en caso de ser necesario, se implantarán los controles adecuados de seguridad aprobados por las áreas responsables de realizar el desarrollo.

Estándar de seguridad para prueba y liberación de aplicaciones

Se realizarán pruebas a los controles de seguridad y de código antes de ser liberada la aplicación por parte de los involucrados en el desarrollo de sistemas.

Se llevarán a cabo pruebas de estrés y pruebas de carga para asegurar que la aplicación cumple con los requisitos de disponibilidad.

Se recomienda que bajo ninguna circunstancia, el código fuente de la aplicación se copie, y mucho menos se modifique, en el ambiente de pruebas.

No se liberará ningún sistema o aplicación sin antes haber realizado las pruebas pertinentes (pruebas de funcionalidad, de estrés, de seguridad, entre otras).

Estándar de seguridad para el mantenimiento de sistemas

Se recomienda disponer de procedimientos para el mantenimiento de los sistemas, los cuales especificarán las actividades a realizar con base a la clasificación del sistema.

Las modificaciones a los sistemas serán probadas antes de entrar a los ambientes de producción.

Todos los cambios a los sistemas se llevarán a cabo bajo procedimientos establecidos y revisados por las áreas responsables de realizar el desarrollo.

5 BITÁCORA DE CONTROL DE CAMBIOS

Descripción del Cambio	Impacto	Fecha de evaluación	Aprobador	Aceptado /Rechazado	Fecha de aplicación
N/A	N/A	N/A	N/A	N/A	N/A

Versión: V1 Fecha: Noviembre-2012	Descripción: Guía de referencia para la Seguridad Informática en la Secretaría de Salud.		
Documentó	**Calidad**	**Revisó**	**Aprobó**
Nombre: Lic. Silvia Conde Arreaga. **Subdirectora de Control de Gestión.**	**Nombre: Lic. Elizabeth Grace Jiménez Vázquez** **Jefa de Departamento de Gestión y Acceso a la Información Pública.**	**Nombre: Lic. Rubén Jáuregui Vázquez** **Director General Adjunto de Tecnologías de la Información**	**Nombre: Lic. Pedro Valencia Santiago** **Director General de Tecnologías de la Información**
Firma:	**Firma:**	**Firma:**	**Firma:**