DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Buenas prácticas

CURSOS EN LÍNEA

Buenas prácticas

Proteger la información de nuestros sistemas es una tarea muy importante que requiere la vigilancia constante de un conjunto de actividades. A lo largo de los materiales se ha puesto énfasis en algunas configuraciones generales que permiten mejorar la seguridad de nuestros equipos.

Dada su importancia, en este documento se recuperan algunas de las acciones ya mencionadas, pero en las que se deberá asimilar que es necesaria una revisión periódica para asegurar su cumplimiento. Recuerde que la seguridad de la información implica una revisión constante en la configuración y procedimientos que se realiza en el tratamiento de datos en nuestros sistemas.

Revisiones períodicas

A continuación, se presenta un conjunto de revisiones periódicas a realizar para mantener la seguridad de la información en nuestros equipos.

Realizar una clasificación e inventario de la información

Para proteger la información debe establecerse un criterio para su clasificación. Típicamente, esto se realiza con base en su sensibilidad y el impacto que supondría de ser revelada a personas no autorizadas. Así que, para esta actividad podemos considerar dos ámbitos fundamentales, el ámbito laborar y el ámbito personal.

Ámbito laboral

Una clasificación de información comúnmente establecida para las organizaciones considera los siguientes tipos:

- Pública. Aquella información que al ser revelada no tiene ningún impacto en la organización. Este tipo de información es aquella expuesta por la misma organización en espacios comunes como su sitio web y plataformas de redes sociales.
- Privada. Este tipo de información es aquella que necesita ser protegida de acceso no autorizado, puede abarcar registros de personal, información de nómina, ganancias, etc. Es decir, esta información, debería ser conocida y utilizada solamente por la organización y su revelación puede afectar de manera considerable.
- Confidencial. Este tipo de información es aquella relacionada a los secretos de negocio, propiedad intelectual, y otro tipo de información que podría afectar de manera crítica el desarrollo de la organización si esta fuera revelada.

Los puntos mencionados representan solo una base de clasificación que podrían utilizar las organizaciones, sin embargo, cada una de ellas debería contar con una clasificación específica de acuerdo a sus necesidades y establecer políticas para su cumplimiento con base en la normativa de seguridad que aplique para su ramo particular.

Es su responsabilidad conocer las políticas de su organización y revisar de manera regular que cumple con la clasificación adecuada de la información para su tratamiento según sus actividades.

Ámbito personal

De manera personal se tendrá que realizar una clasificación que le permita identificar el tipo de información que podría suponer un riesgo para su integridad y establecer medidas de protección adecuadas con cada una de ellas. Por lo tanto, se requiere una revisión constante del tipo de información que mantiene en su sistema para clasificarla adecuadamente según sus necesidades particulares.

Figura 1. La correcta clasificación de la información es vital para tomar medidas apropiadas para su protección.

Una buena forma de comenzar una clasificación de información personal es considerar cuáles son datos personales y cuáles son datos personales sensibles. La Ley Federal de Protección de Datos Personales en Posesión de Particulares LFPDPPP los define de la siguiente manera:

Datos personales: "Cualquier información concerniente a una persona física identificada o identificable"[1]. Los datos personales incluyen:

- Datos de identificación. Por ejemplo, datos como el nombre, teléfono, dirección, CURP, INE, RFC.
- Datos laborales. Por ejemplo, teléfono institucional, referencias laborales, dirección de trabajo, nombramientos, entre otros.
- Datos patrimoniales. Por ejemplo, bienes inmuebles, historial crediticio, datos de ingreso, etc.
- Datos de actividades administrativas y jurídicas. Por ejemplo, información vinculada a procedimientos legales, estado civil, fiscal, mercantil…

[1] Ley Federal de Protección de Protección de Datos Personales en Posesión de Particulares. (2010). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Por otro lado, los **datos personales sensibles** se definen como "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste"[2]. En esta clasificación es posible considerar:

- Datos de salud. Se refieren a la información médica, abarcando aspectos como nuestro bienestar físico y mental. Esto incluye datos como historial, diagnósticos, tratamientos, intervenciones quirúrgicas, condiciones médicas, entre otros.
- Datos ideológicos. Estos datos abarcan la información relacionada a las creencias religiosas, afiliaciones políticas, etc.
- Datos de vida sexual. Estos datos están relacionados con las preferencias y prácticas sexuales del sujeto.
- Datos biométricos. Son todos aquellos datos relacionados a las características fisiológicas de las personas que permiten su identificación, como son la huella dactilar, características de retina e iris, entre otros.
- Datos electrónicos. Son los datos relacionados con las cuentas de correo, contraseñas, firma electrónica, dirección IP, entre otros, que permitan la identificación de nuestra actividad en internet y cualquier otro medio electrónico.

La clasificación de la información representa el primer paso en su protección. La revisión periódica del tipo de información almacenada ayudará a identificar cuál es aquella en la que se tiene que tener especial cuidado para su tratamiento.

Por otro lado, y sea cual sea la clasificación que decida adoptar, recuerde que esta debe aplicarse de manera consistente para asegurar que las medidas de protección se lleven a cabo de manera uniforme.

Actualizaciones y parches de software y sistemas operativos

Mantener el software actualizado permitirá la protección y corrección de errores que los desarrolladores han identificado. Por lo tanto, se recomienda aplicar las actualizaciones y parches de seguridad tanto en los programas como en el sistema operativo del equipo. Si no es posible contar con la última versión del sistema operativo o software, al menos, se debería contar con la última actualización o parches disponibles.

En el ámbito laborar esta tarea es responsabilidad del área de sistemas correspondiente. Sin embargo, en un equipo personal deberá asegurarse de que el sistema cuenta con la característica de actualización activada.

Revisión del software instalado en el sistema

Resulta conveniente realizar una inspección periódica de los programas instalados en nuestro sistema para saber si son necesarios o se pueden eliminar. Como sugerencia, elimine todos aquellos programas que no utilice o que ya no utilizará, pues no solo liberará espacio de almacenamiento, sino que evitará contar con programas no deseados que pudieran representar un peligro latente.

[2] Ibidem

Recuerde que es importante instalar software de distribuidores autorizados. En el ámbito laboral se recomienda que solicite la instalación y remoción de software al personal autorizado.

Actualización y aplicación de los sistemas de seguridad

Revise y compruebe su sistema Antivirus

Al igual que para el software, se requiere de la actualización constante de los sistemas antimalware para que estos ofrezcan una mejor protección. Los sistemas antimalware combaten al software malicioso por medio del análisis de sus firmas digitales mismas que compara con aquellas de su base de datos. Si un sistema antivirus detecta que la firma digital de un software malicioso coincide con aquella de su base de datos, emitirá una alerta para informar su presencia. Es por esta razón que los sistemas antimalware deben estar actualizados de manera regular, pues día a día aparecen nuevas amenazas, así que resulta necesario que la base de datos se encuentre al día para poder contenerlas.

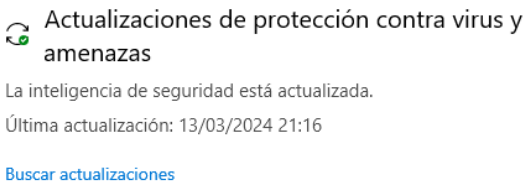

Figura 2. Revise de manera periódica que el antivirus se encuentra actualizado.

Revisión del sistema Firewall activado

Se sugiere revisar de manera periódica que el sistema Firewall se encuentra activado y cuenta con las configuraciones recomendadas según la política de seguridad de la organización. El sistema Firewall es una de las principales medidas de seguridad para el sistema. Funciona por medio de la inspección de paquetes que atraviesan por la tarjeta de red del equipo. El Firewall analiza estos paquetes y los compara con lo especificado en sus reglas de funcionamiento para permitir o frenar su avance. De manera predeterminada, Windows cuenta con el Windows Defender Firewall y corresponde a usted como usuario asegurarse de que este sistema se encuentre activado para su protección. Por otro lado, en un ámbito laboral corresponderá al administrador de sistemas configurar las reglas de acuerdo a las políticas de la organización.

Uso responsable de internet

Asegúrese de ingresar a páginas protegidas que cuenten con un certificado de seguridad. No visite sitios web que representen un riesgo. Se recomienda que mantenga una actitud profesional y utilice las computadoras de su espacio de trabajo solamente para sus actividades laborales.

Ajustar las configuraciones de seguridad del navegador en los niveles más altos

Se recomienda que revise de manera periódica que las configuraciones de seguridad del navegador que utiliza se encuentran activadas.

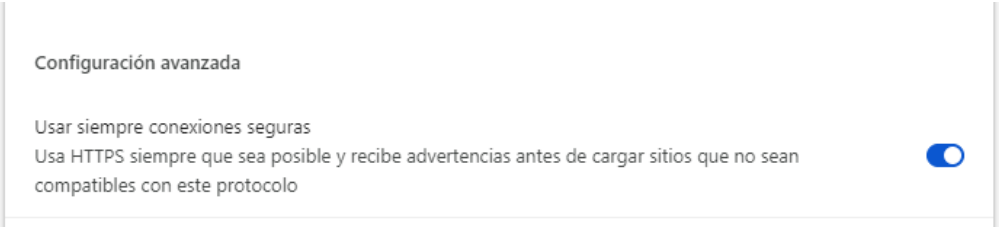

Figura 3. Compruebe que se cuenta con las configuraciones de seguridad en su navegador.

Revisión del espacio de trabajo

Diariamente, usted deberá asegurarse de mantener su área de trabajo limpia, sin información confidencial expuesta a la vista de terceros. Sea cuidadoso en el manejo de documentos con información confidencial, contraseñas, así como en el uso memorias u otros dispositivos de almacenamiento que permitan que otras personas puedan tomarlos u observarlos.

Sea profesional y mantenga en buen estado su espacio de trabajo. Existen personas maliciosas que pueden sacar provecho de su falta de organización.

Figura 4. La política de escritorio limpio es parte de muchos estándares de seguridad de la información.

Revisión en la configuración del bloqueo, cierre de sesión y apagado del equipo

Será necesario comprobar que se ha implementado el bloqueo de sesión. Como se ha mencionado, el dejar el equipo y su información a la vista de los demás supone un riesgo a la seguridad. Por lo tanto, asegúrese de que la configuración de bloqueo está activada y de preferencia, actívelo usted mismo de manera manual cada vez que sea necesario alejarse de su espacio de trabajo.

En Windows se puede utilizar la combinación de teclas CONTROL + L para bloquear el equipo.

De igual manera, deberá verificar que usted cierra su sesión de trabajo y apaga correctamente el equipo cuando haya finalizado la jornada laboral. Cerrar su sesión protegerá la información y apagar el equipo aumentará la vida útil del hardware y permitirá al software mantenerse estable.

Revisión del hardware

Revise de manera periódica el estado del hardware del equipo. Esto incluye la limpieza de sus componentes y que no tenga daños físicos notorios. Deberá revisar de manera periódica que el hardware se encuentre libre de polvo y que las conexiones eléctricas estén aisladas de manera adecuada. En caso de observar algo fuera de lo normal es su responsabilidad informar al personal especializado de su organización para que le brinde soporte técnico, en el ámbito personal usted deberá contactar con un profesional para evitar provocar daños en el equipo.

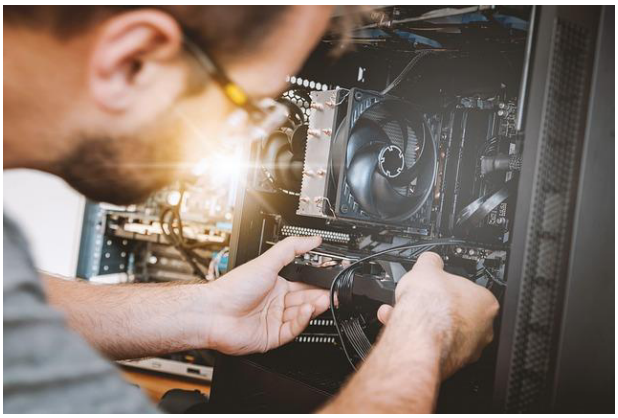

Figura 5. El área de soporte es la responsable de la revisión técnica de los equipos.

Por otro lado, recuerde que todo el hardware utilizado en sus actividades debe ser aprobado por el área de TIC. Si usted necesita adquirir un producto de hardware para sus actividades laborales, se sugiere que se acerque al área correspondiente para que le ofrezcan ayuda y orientación.

Esto aplica también en el ámbito personal, se recomienda que se adquiera hardware de distribuidores autorizados para evitar posibles daños en el correcto funcionamiento del equipo.

Existen dispositivos de hardware capaces de servir como medios espía y robar su información o, incluso, realizar acciones en el hardware que pueden poner en peligro su integridad. Esta es una razón más para adquirir productos de distribuidores autorizados y confiables.

Revisión del uso de memorias y discos extraíbles

Se sugiere que, en la medida de lo posible, NO se utilicen memorias USB o discos extraíbles en al ámbito laboral, pues son fáciles de perder y es posible que estos medios se infecten de algún tipo

de virus si se conectan en otras computadoras que no cuenten con las medidas de seguridad apropiadas.

Si no existe otra alternativa, el área responsable de tecnologías debería proveerle el dispositivo y usted debería hacer un uso responsable utilizándolo solamente en computadoras en las que tenga autorización. De igual manera, debería realizar una revisión periódica con un sistema antivirus para asegurarse que se encuentre libre de malware.

Por otro lado, se sugiere que el dispositivo se encuentre cifrado, de tal manera que se necesite una contraseña para poder acceder a los archivos. El área responsable de TIC debe hacerse cargo de este proceso, pero en su defecto, asegúrese de que usted hace un uso sensato de estos medios.

Participación y capacitación en seguridad

De manera periódica, usted debería tener participación en sesiones formativas de concientización y capacitación en seguridad de la información. Como se ha mencionado, las actividades de seguridad se deben realizar de manera constante. Cada día existen nuevos peligros y es importante mantenerse al tanto y actualizado para poder mitigar riesgos.

Figura 6. La capacitación y entrenamiento es muy importante para mejorar la postura de seguridad en nuestras actividades.

Respaldo periódico de información personal

Resguardar y respaldar los datos son tareas que debemos llevar a cabo de manera periódica para tener nuestra información segura. Existen varias **técnicas de seguridad** para la información, César Lozano, en el número 10 de la revista "Seguridad UNAM"[3] publicó un listado con algunas recomendaciones entre las que destacan las siguientes:

- **Organizar los archivos y carpetas** colocando nombres claros, precisos y que hagan referencia al contenido.

[3] Medidas preventivas para resguardar la información: https://revista.seguridad.unam.mx/numero-10/medidas-preventivas-para-resguardar-la-informacion

- **Elegir el medio de almacenamiento**:
  - USB o unidades Flash: se recomiendan en caso de que solo se manejen archivos de texto, hojas de cálculo, presentaciones o documentos PDF, o cualquier tipo de información en cantidades menores.
  - Discos duros externos: son recomendados para el manejo de grandes cantidades de información.
  - Discos ópticos: en ellos podemos respaldar fotografías, imágenes, música o videos; ya que es información que no cambia constantemente y puede ser preservada por mucho tiempo con el debido cuidado. Aunque estos medios

Figura 7. Existen diferentes opciones de unidades de almacenamiento cuya selección dependerá de nuestras necesidades particulares de respaldo.

- **Establecer tiempos de respaldo**: es necesario dedicar el tiempo requerido para resguardar la información, más aún cuando se maneja información crítica y de constante actualización. Si le es posible respaldar su información diariamente, hágalo.
- **Controlar los medios de almacenamiento**: no importando el medio de almacenamiento que eligió para resguardar su información etiquételo y lleve un control con fechas y tipo de información respaldada.

Figura 8. Control de información respaldada.

- **Utilizar el mayor espacio posible del medio**: al respaldar la información es muy probable que quede un pequeño espacio libre en la unidad de almacenamiento. Registre este espacio en su control de respaldos, este espacio puede ser utilizado posteriormente con archivos más pequeños.
- **Comprimir la información**: utilice un software de compresión (Winrar, 7zip) para acoplar toda la información en un solo archivo. Entre las ventajas de este proceso se encuentran que puede colocarle una contraseña y que se utilizará menos espacio al momento de almacenarlo.
- **Optar por alternativas virtuales de almacenamiento**: en caso de no contar con un dispositivo de almacenamiento a la mano y se requiera respaldar información al momento; puede optar por utilizar los espacios que ofrecen los servidores de correo electrónico como Gmail, o bien, inclinarse por proveedores de alojamiento de espacio virtual como Dropbox.
- **Verificar respaldos cada determinado tiempo**: ya que se han realizado los respaldos, no se olvide de ellos, revíselos al cumplir 6 meses y como máximo 1 año, esto con la finalidad de verificar que la información se encuentre en buenas condiciones, también puede realizar simulacros de restauración para comprobar el estado de la información.
- **Manejar adecuadamente los medios de almacenamiento**: las unidades de almacenamiento deben estar alejadas de las altas temperaturas, sol, humedad y polvo. Recuerde utilizar estuches para su almacenaje. Evite que sufran caídas o golpes, o que sean retirados/desconectados de manera repentina mientras son utilizados.

Figura 9. El resguardo de los medios de almacenamiento es una tarea muy importante que puede llegar a ser crítica dependiendo del tipo de información que se desee recuperar.

- **Realizar al menos dos copias**: una copia no es suficiente, ya que un respaldo no está exento a sufrir algún daño, diversifique sus medios de almacenamiento. Por ejemplo, si tiene un respaldo en un CD, realice el otro en un servicio en la nube.

AUTORES

ELIER EMANUEL LÓPEZ BASILIO

YAZMÍN SARAÍ SANJUAN CARREÑO