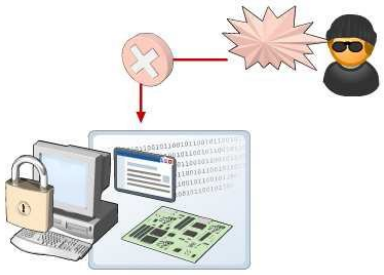
Castillo Navarro Adolfo y González Bello Edgar Oswaldo (2010). Antología de aspectos de seguridad en el uso de la computadora [Adaptación].México: Universidad de Sonora.

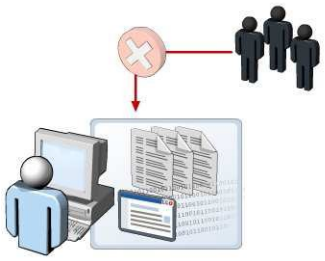
Aspectos de Seguridad en el uso de la computadora

Cualquier factor que pueda dañar la computadora o los datos que contiene supone una amenaza para ella. Existen distintos tipos de amenazas para las computadoras. Los desastres naturales, tales como terremotos o huracanes, pueden causar un daño físico generalizado. También puede ocurrir que el usuario u otra persona elimine por error archivos importantes, lo que puede causar el mal funcionamiento de la computadora. Si la computadora está conectada a una red, se volverá incluso más vulnerable a las amenazas.

Existen varias medidas que puede tomar para reducir estas amenazas y la posibilidad de sufrir pérdidas causadas por un daño. Por ejemplo, puede restringir el acceso a su computadora y crear copias de seguridad de los datos importantes, que podría usar si éstos se eliminan o alteran. Siguiendo algunas instrucciones básicas, puede minimizar los riesgos de que se produzcan daños en su computadora, y garantizar su seguridad y privacidad.

Seguridad de la computadora	
El hardware de la computadora puede sufrir daños a causa de un error humano o desastres naturales, como terremotos, inundaciones y huracanes. Asimismo, es necesario proteger los datos y el software de la computadora ante posibles pérdidas y alteraciones, ya sean accidentales o intencionadas. La seguridad de la computadora está relacionada con las medidas que se pueden tomar para evitar estos daños, tanto en la computadora como en sus datos.	

(Microsoft Corporation, 2006 p.14)

Privacidad de la computadora	
En la computadora se almacenan documentos o archivos personales que no desearía que nadie leyera. La privacidad de la computadora implica que ninguna persona sin permiso puede obtener acceso a sus datos, tales como mensajes de correo electrónico y archivos personales. La privacidad de la computadora está relacionada con las medidas que puede tomar para restringir el acceso a sus datos. También implica tener especial cuidado a la hora de proporcionar cualquier información personal a través de Internet. Podría hacerse un mal uso de ella para obtener acceso a cuentas personales, como cuentas bancarias o de correo electrónico.	

(Microsoft Corporation, 2006 p.15)

Amenazas naturales o ambientales

Elemento	Descripción
Categoría	Algunas de las principales amenazas naturales y ambientales para las computadoras son las siguientes: • **Desastres naturales, como inundaciones, terremotos y huracanes**: estos desastres pueden llegar a causar una destrucción masiva. Las computadoras de la zona afectada pueden sufrir importantes daños físicos, incluyendo generalmente la pérdida total de los datos. • **Incendios**: los incendios pueden dañar las computadoras de manera permanente. Incluso si el fuego no alcanza directamente a la computadora, el calor provocado es suficiente para fundir los delicados componentes de su interior. Además, el humo contiene unas partículas diminutas que pueden dañar la computadora, especialmente el disco duro. • **Calor o frío extremos**: la mayoría de los componentes internos de una computadora están diseñados para funcionar dentro de un intervalo específico de temperatura. En el caso de producirse calor o frío excesivos, es posible que algunos de ellos empiecen a funcionar incorrectamente y sea necesario sustituirlos. Si la computadora estuvo en el exterior y se expuso a temperaturas extremas, deje que vuelva a adquirir la temperatura ambiente antes de encenderla. • **Problemas de voltaje (sobre voltaje/picos)**: el sobre voltaje o los picos son un aumento repentino del voltaje de alimentación que puede dañar permanentemente algunos de los componentes de la computadora. Por ejemplo, un aumento repentino del voltaje puede destruir la placa base de la computadora. El sobre voltaje puede producirse por un rayo que cae con una gran cantidad de carga eléctrica. Esta carga se transmite por las líneas telefónicas

	o eléctricas hasta la computadora y daña sus componentes internos.
Solución	Las computadoras requieren condiciones ambientales óptimas para funcionar correctamente. Éstas son algunas de las medidas que puede tomar para proteger su computadora de las amenazas naturales y ambientales, y minimizar los daños causados por éstas: • **Realizar copias de seguridad de los datos**: implica crear varias copias de los datos. Los desastres, como inundaciones y terremotos, pueden producirse sin aviso. Los datos siempre son únicos e insustituibles. Si crea una copia de seguridad, podrá recuperar los datos en caso de que se pierdan. Para disponer de una mayor capacidad de recuperación, intente mantener una copia de los datos importantes en una ubicación física distinta, como otro edificio o ciudad. • **Instalar las computadoras en ubicaciones seguras**: instale la computadora en un lugar donde no sea probable que sufra daños por factores ambientales. Por ejemplo, evite instalarla en salas que estén expuestas a un exceso de polvo o humedad. • **Controlar el entorno operativo**: debe mantener un nivel de temperatura y humedad óptimo para garantizar el correcto funcionamiento de la computadora. Puede hacerlo si instala determinados dispositivos, como aparatos de aire acondicionado o controladores de humedad. • **Protección contra sobre voltaje y acondicionamiento de la línea**: use determinados dispositivos, como protectores contra sobre voltaje y acondicionadores de línea, que conectan la computadora con la fuente de alimentación. Esta conexión ofrece protección ante el sobre voltaje o los picos de la línea eléctrica. No obstante, si se produce un fuerte sobre voltaje, sigue existiendo el riesgo de que se produzcan daños y, por lo tanto, es

	fundamental mantener copias de seguridad de los datos importantes. Si hay una fuerte tormenta, debe apagar la computadora y desconectarla de la red eléctrica para evitar posibles daños causados por un rayo. • **Sistema de alimentación ininterrumpida (SAI)**: instale dispositivos, como un SAI, que puedan proporcionar una alimentación ininterrumpida a la computadora. Un SAI ofrece una batería de reserva en caso de que se produzca una interrupción del suministro eléctrico. De este modo, se evitan posibles daños en el software a causa de un apagado repentino de la computadora. Un SAI también ofrece características integradas de protección contra sobre voltaje y acondicionamiento de la línea.

(Microsoft Corporation, 2006 p. 16)

Amenazas humanas (malintencionadas)

Elemento	Descripción
Categoría	A continuación, se enumeran algunos ejemplos de amenazas humanas malintencionadas: • **Empleados descontentos**: un empleado de su oficina que esté descontento puede intentar deliberadamente alterar o destruir los datos de su computadora. • **Piratas informáticos**: un *pirata informático* es una persona que intenta obtener acceso de forma ilegal a su computadora cuando se conecta a Internet. Una vez que logra obtener acceso, puede robar o dañar los datos almacenados en ella. • **Robo físico**: cualquier persona puede robar su computadora o sus componentes si tiene acceso a ella. Con la popularidad adquirida por las computadoras portátiles, el robo físico de

	computadoras se convirtió en un hecho muy habitual. • **Robo virtual**: puede llegar a convertirse en una víctima del robo virtual, algo también más común en el caso de computadoras conectadas a Internet. Un ejemplo de robo virtual es el *robo de identidad*, donde un pirata informático puede robar su información personal para usurpar su identidad. Con esta identidad falsa, el pirata informático puede obtener acceso a sus recursos financieros o realizar alguna actividad ilegal. Otro ejemplo de robo virtual es la *piratería de software*, que hace referencia al robo de un programa o diseño informático. También puede hacer referencia a la distribución y el uso no autorizados de un programa informático.
Programa	Ciertas personas malintencionadas pueden dañar los datos almacenados en su computadora mediante programas creados especialmente para este fin. Algunos ejemplos de estos programas son los siguientes: • **Malware.** El malware (del inglés malicious software, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y/o dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano hasta un spyware (Colaboradores de Wikipedia, 2010f). • **Virus informático.** Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador,

aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos por que no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil. (Colaboradores de Wikipedia, 2010k)

- **Troyano.** En informática, se denomina troyano o caballo de Troya (traducción literal del inglés Trojan horse) a un software malicioso que bajo una apariencia inofensiva se ejecuta de manera oculta en el sistema y permite el acceso remoto de un usuario no autorizado al sistema.

Algunas de las operaciones que se pueden llevar a cabo en el ordenador remoto son:

- Utilizar la máquina como parte de una botnet (por ejemplo para realizar ataques de denegación de servicio o envío de correo no deseado).
- Instalación de otros programas (incluyendo otros programas maliciosos).
- Robo de información personal: información bancaria, contraseñas, códigos de seguridad.
- Borrado, modificación o transferencia de archivos (descarga o subida).
- Ejecutar o terminar procesos.
- Apagar o reiniciar el equipo.
- Monitorizar las pulsaciones del teclado.
- Realizar capturas de pantalla.

- Ocupar el espacio libre del disco duro con archivos inútiles (Colaboradores de Wikipedia, 2010j).
- **Spyware.** Un programa espía, traducción del inglés spyware, es un programa, dentro de la categoría malware, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en ella. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

Principales síntomas de infección son:

- Cambio de la página de inicio, error en búsqueda del navegador web.
- Aparición de ventanas "pop-ups", incluso sin estar conectados y sin tener el navegador abierto, la mayoría son temas pornográficos y comerciales (por ejemplo, la salida al mercado de un nuevo producto).
- Barras de búsquedas de sitios como la de Alexa, Hotbar, MyWebSearch, FunWeb, etc.. que no se pueden eliminar.
- Modificación de valores de registro.
- La navegación por la red se hace cada día más lenta, y con más problemas.
- Aumento notable en el tiempo que toma el computador en iniciar, debido a la carga requerida por el spyware que se ejecuta en ese momento, alterando el registro con el fin de que el spyware se active a cada inicio.
- Al hacer clic en un vínculo el usuario retorna de nuevo a la misma página que el software espía hace aparecer.
- Etc. (Colaboradores de Wikipedia, 2010i)

	• **Adware.** Un programa de clase adware es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad web al computador después de instalado el programa o mientras se está utilizando la aplicación. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en inglés. • **Spam.** Se llama spam o correo basura a los mensajes no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. • **Fraudes en Internet**: cuando se usa Internet se pueden recibir algunas ofertas atractivas a través de mensajes de correo electrónico o conversaciones de salones de chat. Debe tener mucho cuidado a la hora de aceptar alguna de estas ofertas, ya que pueden formar parte de fraudes planeados que pueden causarle pérdidas económicas. • **Depredadores en línea**: son individuos que atraen a cualquier persona que esté en línea para mantener relaciones inapropiadas y poco éticas. El usuario o su familia pueden convertirse en víctimas de los depredadores en línea. Estos depredadores establecen contacto con sus víctimas mediante el correo electrónico o los salones de chat.
Solución	A continuación, se enumeran algunas medidas que puede tomar para minimizar los riesgos asociados con amenazas humanas malintencionadas: • **Almacenamiento de datos en ubicaciones seguras**: guarde sus datos en ubicaciones seguras que tengan acceso limitado para otras personas. De este modo, minimizará la posibilidad de robo o alteración de los datos.

- **Protección contra virus y spyware**: existen algunas medidas básicas que se pueden tomar para reducir la amenaza de virus y de spyware. Debe tener precaución al abrir un archivo adjunto de un mensaje de correo electrónico o instalar un programa de software desde un sitio Web. La forma más eficaz de instalar software antivirus y anti spyware es hacerlo mediante un proveedor de confianza. Estos programas de software permiten comprobar la existencia de virus y de spyware en la memoria de la computadora, además de evitar la entrada de otros nuevos. También es necesario actualizar el software antivirus y anti spyware con regularidad para que pueda reconocer nuevos virus y spyware. La mayoría de este tipo de software ofrecen actualizaciones automáticas que instalan automáticamente la versión actualizada del software en la computadora.
- **Firewall**: la instalación de un firewall es otra medida eficaz que puede tomar para proteger su computadora de amenazas malintencionadas. Un *firewall* permite filtrar el tráfico de Internet antes de que llegue a una computadora o una red privada. Ofrece asimismo protección adicional contra amenazas, como piratas informáticos y virus. Un firewall ayuda además a garantizar la privacidad de la computadora, ya que restringe el acceso externo a la computadora por parte de algún usuario no autorizado.

(Microsoft Corporation, 2006 p. 17)

Amenazas humanas (no malintencionadas)

Elemento	Descripción
Categoría	A continuación, se enumeran algunos ejemplos de amenazas humanas no malintencionadas: • **Errores humanos**: muchas veces, los daños producidos en una computadora se deben a un error humano no intencionado. Por ejemplo, puede que elimine por error un archivo importante que provoque el mal funcionamiento de la computadora. • **Daños en el hardware**: debido a que los componentes de la computadora son muy delicados, corren el riesgo de sufrir daños por algún descuido. Por ejemplo, si la computadora portátil se cae accidentalmente, podría causar daños a los componentes de hardware, como la placa base o el CD ROM. En consecuencia, perdería los datos almacenados en la computadora.
Solución	A continuación, se describen las medidas que puede tomar para proteger su computadora de las amenazas humanas no malintencionadas y minimizar los daños causados por éstas: • **Proteger el hardware de daños accidentales y ambientales**: puede tomar varias medidas para evitar cualquier daño no intencionado en la computadora. Coloque la computadora en una zona sin polvo ni vibraciones y que esté fuera del alcance de posibles golpes. El lugar donde coloque la computadora debe estar bien ventilado para evitar cualquier daño debido al calor. Mantenga la computadora alejada de cualquier sustancia magnética, agua o descarga estática. Por ejemplo, no coloque la computadora en el suelo ni sobre una alfombra. Use un regulador de voltaje para evitar daños eléctricos. Evite comer y beber cerca del teclado, y use una funda protectora para protegerlo de posibles derrames. La mesa o estante de la computadora debe ser firme y estable para evitar que la computadora se caiga,

	incluso si recibe un golpe. • **Realizar copias de seguridad de los datos**: realice copias de seguridad de los datos importantes de la computadora con regularidad. Si crea varias copias de los datos, podrá protegerlos de posibles pérdidas causadas por borrado o destrucción accidentales.

(Microsoft Corporation, 2006 pp. 17-19)

Protección de la computadora y los datos

Para tener acceso a su caja de seguridad del banco, necesita proporcionar su identificación. Esta identificación sirve para garantizar que nadie más pueda tener acceso a sus pertenencias.

De igual modo, es posible implementar distintas medidas de seguridad para minimizar la amenaza a la que se enfrenta la computadora y los datos que contiene. Esta lección es una introducción a algunas recomendaciones comunes que le ayudarán a proteger el sistema operativo, el software y los datos de su computadora (Microsoft Corporation, 2006 p. 26).

Protección del entorno operativo y los datos de la computadora

Establecer un nombre de usuario y contraseña
Del mismo modo, puede aumentar la seguridad y limitar el acceso no autorizado a la computadora si configura un nombre de usuario y una contraseña. En casi todas las oficinas, cada empleado tiene un nombre de usuario y una contraseña exclusivos que deben proporcionar para tener acceso a las computadoras.

(Microsoft Corporation, 2006 p.27)

Mantener las contraseñas seguras

Una contraseña actúa como una clave para poder usar una computadora. Por lo tanto, cualquier persona que conozca la contraseña podrá tener acceso a la computadora y alterar los datos.

La contraseña debe permanecer segura. Tenga cuidado al escribir la contraseña para evitar que otros puedan verla, y no la comparta con otras personas.

No anote la contraseña ni la deje sobre la computadora o el escritorio. Si cree que la contraseña ya no es segura, cámbiela de inmediato antes de que cualquiera haga un mal uso de ella.

(Microsoft Corporation2006, p. 28)

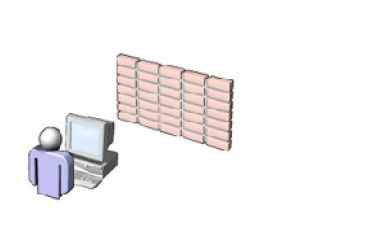
Bloquear la computadora

Cuando deja la computadora encendida y sin supervisión, alguien puede alterar el software y los datos de la computadora. Esto puede evitarse si bloquea temporalmente la computadora mientras no la usa.

Cuando una computadora se bloquea, inmediatamente se oculta el contenido de la pantalla y no se permite que se realice ninguna operación hasta que se desbloquee mediante la combinación correcta de nombre de usuario y contraseña.

(Microsoft Corporation2006 p. 28)

Instalar software protector



Una computadora debe protegerse continuamente de amenazas como los virus y el spyware.

En ocasiones, el daño que un virus puede causar es considerable y puede hacer que pierda datos importantes o que tenga que volver a instalar el sistema operativo y otro tipo de software. Para proteger la computadora de virus y de spyware deberá instalar un software antivirus y anti spyware.

Estos programas de software protectores sirven para detectar y eliminar los virus y spyware que hay en la computadora, así como para evitar que ésta vuelva a infectarse.

Es conveniente instalar un firewall, que filtra el contenido que llega a la computadora. Con un firewall la computadora también estará protegida frente a los piratas informáticos, ya que restringe el acceso de otros usuarios en línea.

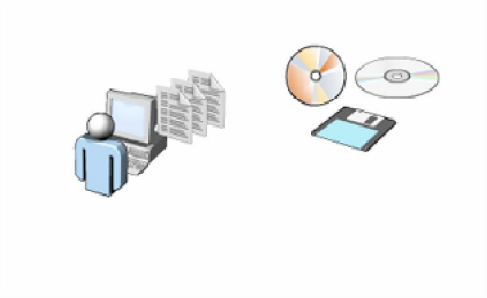
(Microsoft Corporation2006 p. 29)

Cifrar los datos

Se llama cifrado a la conversión de los datos a un formato ilegible para protegerlos del acceso no autorizado. Un usuario autorizado puede volver a convertir los datos cifrados a un formato legible y que se pueda usar. Esto se conoce como descifrado.

(Microsoft Corporation2006 p. 29)

Realizar una copia de seguridad de los datos

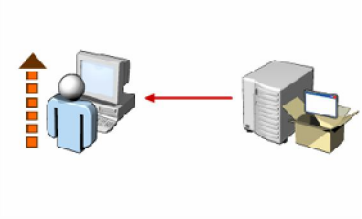


También podrá impedir que los archivos se pierdan o sufran daños, si hace copias de los archivos importantes y los almacena en un medio de almacenamiento distinto, como un CD, un DVD o un disquete.

Este proceso se denomina copia de seguridad de datos. Las copias de seguridad deben conservarse en ubicaciones seguras, con el fin de poder usar estos datos en caso de que los originales se pierdan o dañen.

(Microsoft Corporation2006 p. 30)

Mantener la computadora actualizada



A medida que surgen nuevas amenazas, las compañías de software crean periódicamente actualizaciones que se pueden instalar en la computadora.

Estas actualizaciones complementan el software o el sistema operativo ya instalado en la computadora para disminuir la vulnerabilidad frente a las amenazas de seguridad.

Asegúrese de actualizar el software antivirus con regularidad para que pueda detectar la presencia de nuevos virus.

(Microsoft Corporation2006 p. 30)

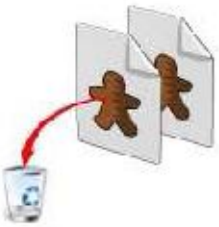
Protección de las transacciones en línea y en red

La conexión de una computadora a Internet supone su entrada en un mundo de información y entretenimiento. No obstante, también hace que su computadora sea vulnerable a las distintas amenazas en línea. Por ejemplo, los virus podrían pasar más fácilmente de una computadora infectada a la suya. Es posible reducir los riesgos de estas amenazas en línea combinando varias recomendaciones, como la creación de contraseñas seguras, el cifrado de datos y el uso de un software antivirus.

En la siguiente tabla se describen las distintas medidas que puede tomar para proteger las transacciones en línea y en red.

Medida	Descripción	
Usar contraseñas seguras	Una contraseña segura es una contraseña compleja que no se puede averiguar fácilmente. La contraseña debe contener una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, como el símbolo de *Y comercial* y el *signo de número*, y no puede contener palabras ni nombres completos. Una contraseña segura es su principal defensa ante las amenazas de seguridad y privacidad. Las contraseñas seguras deben crearse para: • El acceso local a computadoras independientes • El acceso a redes • El acceso a sitios Web que tienen información confidencial, como detalles personales o financieros • El acceso a cualquier dato importante • Los datos personales almacenados en su computadora	

Proteger la computadora de piratas informáticos y spyware	Mientras navega por Internet, es posible que un programa de software instalado en su computadora esté transmitiendo su información personal a un pirata informático en otro país. Estos programas son ejemplos de spyware. Por lo general, se instalan en su computadora sin que lo sepa y transfieren datos confidenciales en secreto desde su computadora a los piratas informáticos. En algunas ocasiones, las empresas instalan spyware en las computadoras usadas por los empleados para realizar un seguimiento de sus actividades informáticas. Puede instalar en su computadora programas de software como Microsoft Defender para evitar que el spyware se instale en ella de forma inadvertida. También debe instalar un software antivirus y un firewall en la computadora para protegerla de virus y piratas informáticos.	
Borrar el historial y la memoria caché regularmente	Los sitios y las páginas Web que visita mientras navega por Internet se guardan en el *historial* del explorador. También se almacenan algunos archivos en la memoria temporal de su computadora. Esta memoria temporal se conoce como *memoria caché*. Los archivos almacenados en esta memoria registran información de las páginas Web que se visitan. No obstante, algunos de estos archivos temporales de Internet pueden contener	

	información personal, como su nombre de usuario y contraseña, a la que podrían tener acceso los piratas informáticos. Para evitar que estos piratas tengan acceso a su información personal, elimine el contenido del historial del explorador y la memoria caché con cierta regularidad.	
Eliminar cookies regularmente	Al visitar un sitio Web, puede que su nombre aparezca en él. Esto es posible gracias al uso de *cookies*, que son pequeños archivos creados en su computadora por los sitios Web visitados previamente para identificar y realizar un seguimiento de sus preferencias. Su finalidad es ofrecer una experiencia más personal al visitar un sitio Web. No obstante, las cookies también pueden suponer una amenaza para la privacidad de la computadora, ya que contienen información personal. Por ejemplo, las cookies podrían contener los detalles de la tarjeta de crédito que usó al realizar compras en línea. Por estos motivos, se recomienda eliminar las cookies regularmente para evitar un mal uso de su información personal.	
Evitar compartir información personal	Algunos sitios Web requieren que se rellenen formularios donde se solicita información personal, como el nombre, el sexo y la edad. En los sitios de comercio electrónico, incluso podría tener que compartir los detalles de su cuenta bancaria o el número de su tarjeta de	

	crédito. No obstante, no olvide que los piratas informáticos pueden tener acceso a esta información y hacer un mal uso de ella. Algunas compañías podrían usar también esta información para enviarle mensajes de correo electrónico comerciales no deseados. Por ello, antes de compartir cualquier información personal en un sitio Web, asegúrese de que se trata de un sitio seguro y de que es estrictamente necesario proporcionar la información.	
Asegurarse de que las transacciones en línea se realizan en sitios seguros	Al realizar compras en línea, normalmente debe proporcionar información confidencial, como el número de su cuenta bancaria o los detalles de su tarjeta de crédito. Por lo tanto, es muy importante asegurarse de que sólo se realizan transacciones en línea en sitios Web seguros. Un sitio Web es seguro si su nombre tiene el prefijo *https*. Este prefijo indica que el sitio Web implementa el protocolo *Capa de sockets seguros (SSL)*. SSL es un protocolo de seguridad de Internet que garantiza una comunicación de datos segura mediante el cifrado de la información transmitida. El protocolo SSL certifica que el sitio Web es genuino y garantiza que no se hará un mal uso de los datos proporcionados en él. Cuando se obtiene acceso a un sitio Web seguro, la mayoría de los exploradores Web muestran un mensaje para confirmar que se	

	obtuvo acceso a un sitio Web seguro. El icono de candado cerrado de la parte inferior derecha de la pantalla del explorador también ayuda a identificar un sitio Web seguro. Además, se puede comprobar el certificado de seguridad de un sitio Web antes de realizar una transacción en línea en dicho sitio.	
Configurar los componentes de seguridad.	• **Firewall**: debe habilitar el firewall antes de conectarse a Internet. El firewall ayuda a evitar que cualquier contenido malintencionado, como virus y gusanos, tenga acceso a su computadora. También evita que los piratas informáticos obtengan acceso a ella. • **Actualizaciones automáticas (del sistema operativo y de los programas instalados)** • **Antivirus**	

(Microsoft Corporation2006 pp. 31-34).

Es posible que reciba mensajes de correo electrónico irrelevantes o que no desee, procedentes de remitentes desconocidos. Estos mensajes reciben el nombre de correo no deseado.

No responder al correo no deseado

Se recomienda no responder a los remitentes de tales mensajes, ya que el correo electrónico no deseado a menudo es de carácter malintencionado y puede incluir contenido dañino para la computadora. Los programas de correo electrónico, como Microsoft Outlook, incluyen una carpeta de correo electrónico no deseado en la que es posible almacenar todo el correo sospechoso.

Seguridad del correo electrónico y la mensajería instantánea

El correo electrónico y la mensajería instantánea (MI) se usan de forma generalizada en la comunicación personal y empresarial. Sin embargo, los piratas informáticos, depredadores en línea e individuos que crean gusanos y virus, usan el correo electrónico y la mensajería instantánea con fines malintencionados. Por ejemplo, estas personas pueden enviar archivos adjuntos de correo electrónico con software malintencionado. También pueden usar el correo electrónico para solicitar información confidencial o para atraerle hacia ofertas falsas. Por lo tanto, es importante que tome ciertas medidas para garantizar la seguridad del correo electrónico y la mensajería instantánea.

Para garantizar la seguridad del correo electrónico, evite abrir los mensajes con archivos adjuntos, no responda al correo no deseado, no responda al correo comercial no solicitado y protéjase de la suplantación de identidad. Para garantizar la seguridad de la mensajería instantánea, charle sólo con personas que conozca y no abra archivos adjuntos que reciba a través de mensajería instantánea.

1. No abrir archivos adjuntos recibidos a través de mensajería instantánea

La mensajería instantánea es una forma muy habitual de recibir datos adjuntos malintencionados. Por lo tanto, debe evitar abrir cualquier archivo adjunto que reciba en un mensaje instantáneo, a menos que esté absolutamente seguro de su origen. Un archivo adjunto de mensajería instantánea podría contener un virus o spyware que pueden dañar la computadora (Microsoft Corporation2006 pp. 38).

2. Protegerse de la suplantación de identidad

La suplantación de identidad es una actividad habitual que sirve para obtener información personal de los usuarios de computadoras con el fin de usarla posteriormente con fines malintencionados. Por ejemplo, alguien le envía mensajes de correo electrónico fingiendo que proceden de un banco o de una organización de

confianza y le pide información confidencial como el número de la tarjeta de crédito o la contraseña.

Esta información se venderá o se usará para causarle pérdidas económicas. Por lo tanto, debe comprobar la autenticidad de estos mensajes de correo electrónico antes de responder con cualquier tipo de información personal.

3. Charlar sólo con personas conocidas

Debe restringir las conversaciones por chat únicamente a aquellas personas que conozca. Si se comunica con personas nuevas o desconocidas, resultará más vulnerable ante amenazas como los depredadores o los fraudes en línea (Microsoft Corporation2006 p. 37).

4. Protección de la privacidad

Con la creciente popularidad de las computadoras e Internet, su privacidad puede verse comprometida de varias formas. Todos los miembros de su familia deben evitar las amenazas que afectan a la privacidad. Puede tomar estas sencillas medidas para proteger a toda la familia de la invasión de la privacidad:

4.1 Proteja su identidad

Evite compartir información personal con cualquier persona, a menos que la conozca. Ésta es la regla de oro de la protección de la privacidad. Cuando intercambie mensajes de correo electrónico o charle a través de la mensajería instantánea, asegúrese de no revelar detalles personales acerca de su persona u otras personas que conozca. Use también contraseñas seguras para tener acceso a su computadora y conexiones de correo electrónico.

4.2 Realice copias de seguridad de su computadora y datos importantes con regularidad

Es aconsejable realizar copias de seguridad de todo tipo de datos importantes y confidenciales almacenados en la computadora. Estos datos podrían ser documentos, bases de datos o información de contacto. Puede

usar varios medios de almacenamiento, como un disco compacto u otra unidad de disco duro, para realizar las copias de seguridad. Si realiza copias de seguridad de los datos contenidos en la computadora con regularidad, podrá recuperarlos en el caso de que los originales se pierdan o se dañen. También es aconsejable almacenar los datos de las copias de seguridad en un lugar seguro y restringir el acceso a ellos mediante contraseñas y cifrado.

4.3 Compruebe la seguridad de su sistema con regularidad

Compruebe el nivel de seguridad de su sistema con regularidad. Los sistemas operativos modernos tienen características integradas que permiten realizar un seguimiento de la capacidad de la computadora para protegerse de las distintas amenazas de seguridad y privacidad.

4.4 Ejecute detecciones de virus a diario

Cada día, cuando tiene acceso a Internet, existe la posibilidad de que su computadora se infecte con un virus. Por lo tanto, es importante que ejecute una detección de virus en la computadora todos los días. También debe mantener el software antivirus de la computadora actualizado para protegerla de nuevos virus.

4.5 Use un programa anti spyware

Los programas spyware pueden obtener acceso a su computadora en secreto y transmitir información personal sobre el usuario o su familia. Use un software anti spyware que controle estos programas malintencionados y mantenga el software actualizado.

4.6 Realice las transacciones en línea en sitios seguros con proveedores acreditados

Al realizar una transacción en línea, debe proporcionar en el sitio Web cierta información personal, como los detalles de su tarjeta de crédito o su cuenta bancaria. Si esta información se revelara a otras personas, podría usarse para realizar un fraude económico. Por lo tanto, es muy importante realizar las transacciones en línea sólo en sitios Web seguros.

4.7 Comunique cualquier abuso al ISP

La mayoría de los ISP (Proveedor de servicios de Internet) acreditados, cuentan con términos y condiciones que no permiten a sus usuarios realizar ninguna práctica ilegal o poco ética. Debe comunicar al ISP si alguien intentó invadir su privacidad en línea, enviándole correo no deseado, o piratear su computadora. De este modo, el ISP podrá tomar medidas contra estas personas.

4.8 Filtre los mensajes de correo electrónico procedentes de remitentes desconocidos o anónimos

Es posible que reciba mensajes de correo electrónico de personas que no conoce. Estos mensajes, conocidos como correo no deseado, pueden ser muchas veces portadores de virus o spyware. Los piratas informáticos que intentan recuperar su información personal pueden también enviarle correo no deseado. Por lo tanto, es importante que tenga cuidado con este tipo de mensajes. Los programas de software de correo electrónico permiten crear filtros que le permitan bloquear el correo no deseado. También debe asegurarse de que nunca responde a correo no deseado, ya que puede hacer que aumenten los mensajes no deseados y comparta por error información personal.

Referencias.

Colaboradores de Wikipedia (2010a). Actualización o Parche. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Parche_%28inform%C3%A1tica%29

Colaboradores de Wikipedia (2010b).Adware. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Adware

Colaboradores de Wikipedia (2010c).Antivirus. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Antivirus

Colaboradores de Wikipedia (2010d).Backup. En Wikipedia la enciclopedia libre. Extraido el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Backup

Colaboradores de Wikipedia (2010e).Firewall. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

Colaboradores de Wikipedia (2010f). Malware. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Malware

Colaboradores de Wikipedia (2010g).Seguridad informática. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Colaboradores de Wikipedia (2010h).Spam. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Spam

Colaboradores de Wikipedia (2010i).Spyware. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Spyware

Colaboradores de Wikipedia (2010j). Troyano (informática). En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Troyano_%28inform%C3%A1tica%29

Colaboradores de Wikipedia (2010k). Virus informático. En Wikipedia la enciclopedia libre. Extraído el 30 de marzo de 2010 de http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico