

Proyecto CECI-MICITT

Curso Alfabetización Digital de Microsoft



Modulo 04

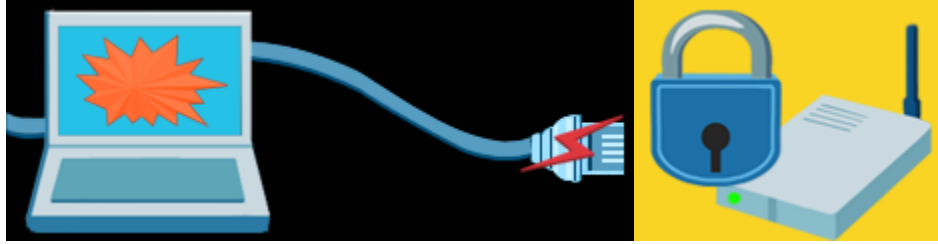
“Seguridad y privacidad de las computadoras”



Facilitador **Carlo Carranza**

Palmares, Alajuela. (2019).

Objetivo: Identificar y dominar el vocabulario de este módulo de tal manera que el estudiante logre dar soluciones efectivas a determinada situación.



Descripción

Este curso te ayudará a identificar las distintas amenazas a las que se enfrentan una computadora y los datos que se almacenan en ella. Aprenderás a proteger tu computadora de estas amenazas mediante algunas medidas preventivas. Por último, en el curso se describen los problemas éticos y legales relacionados con el uso de Internet.

Beneficios

Al igual que cualquier otro dispositivo electrónico, tu computadora puede sufrir daños accidentales o intencionales. Algunos de estos daños pueden ser permanentes. No obstante, es posible evitar que se produzcan determinados daños al hardware, el software y los datos de la computadora si se toman ciertas medidas preventivas.

Créditos

Microsoft Learning quisiera reconocer y agradecer a todos los individuos que han contribuido con el desarrollo de este título. Su esfuerzo en distintas etapas del desarrollo es lo que asegura que tengas una buena experiencia de aprendizaje.



Seguridad y privacidad informáticas

Si usas computadoras con frecuencia, es posible que tengas una gran cantidad de información almacenada en ellas. Es necesario que te asegures de que otras personas no consulten esta información sin tu permiso. También necesitas protegerla de posibles daños. Toda información es susceptible de daños o robo y es importante proteger información como la siguiente:

- Detalles de impuestos
- Cartas personales
- Correspondencia de negocios
- Proyectos
- y más

En esta lección, aprenderás por qué es necesario proteger el hardware, el software y los datos electrónicos de la computadora de daños, extravío y robos. También conocerás los distintos dispositivos y soluciones que puedes usar para proteger los datos de tu computadora.

¿Qué son la seguridad y la privacidad informáticas?

La privacidad y la seguridad informáticas son dos temas importantes hoy en día. La seguridad informática se refiere a la intrusión en cuentas personales. La privacidad se refiere a cómo las empresas manejan la información que les has dado. A medida que crecemos con más tecnología, la percepción social evolucionará. En esta lección, examinaremos diversos aspectos de la seguridad y la privacidad informáticas.

- **Actividad:** Interactúe con la aplicación (Link: https://digital-literacy-courses-es.azurewebsites.net/es/digitalliteracy/courses/2698de/es-xx/content/content00002/4_1_1_computer_security_and_privacy/lesson_4_1_1.html)

Evaluación de conocimiento

¿Cualquier daño potencial a tu computadora se considera una amenaza?

- ☐ Sí
- ☐ No



Evaluación de conocimiento

¿Qué es la privacidad informática?

- ☐ Mantener tus archivos personales y tus datos seguros y en secreto.
- ☐ Mantener la computadora alejada de todos.
- ☐ Conservar la información de otra persona.



Amenazas naturales

La privacidad y la seguridad informáticas pueden verse amenazadas por peligros naturales como terremotos, inundaciones o tormentas eléctricas.

Estas amenazas naturales pueden conducir a incendios, temperaturas extremas e incluso descargas eléctricas a la computadora, que pueden causar daños físicos y pérdida de datos.



Esas son causas naturales:

Incendio

Incendio

El fuego puede ser devastador para una computadora. Más allá del daño directo de las llamas, el calor generado puede derretir los componentes sensibles dentro de la computadora. El humo puede dañar el ventilador de la CPU, lo que también puede causar un sobrecalentamiento. En caso de incendio, siempre ve a un lugar seguro antes de intentar rescatar tu computadora.

Temperaturas extremas

Temperaturas extremas

Generalmente, las computadoras están diseñadas para funcionar dentro de un intervalo de temperaturas moderadas. El frío o el calor excesivos pueden hacer que los componentes

importantes funcionen mal o se rompan. En casos de cambios drásticos de temperatura, es mejor permitir que la computadora vuelva a temperatura ambiente antes de usarla.

Rayos

Rayos

Los rayos son una gran amenaza para tu computadora, incluso si nunca alcanzan realmente tu hardware. A veces, un rayo crea una sobretensión eléctrica (o pico de voltaje) que aumenta la tensión que recibe la computadora a través de la alimentación. Este aumento repentino de la electricidad puede destruir los componentes esenciales de la computadora, incluida la placa base.

Evaluación de conocimiento

¿Pueden las llamas derretir los componentes de una computadora?

- ☐ Sí
- ☐ No



Evaluación de conocimiento

¿Qué componente puede destruir un pico de voltaje?

- ☐ Pantalla
- ☐ Teclado
- ☐ Placa base



Medidas de protección contra las amenazas naturales

Las amenazas naturales pueden causar daños importantes a tu computadora. La siguiente tabla explica las medidas que puedes tomar para proteger los datos y la computadora de estas amenazas naturales.

Realizar una copia de seguridad de los datos



guardar los datos

mayor capacidad de recuperación, mantén una copia de los datos importantes en una ubicación física distinta, como otro edificio u otra ciudad.

Realizar una copia de seguridad de los datos

Realizar copias de seguridad de los datos implica crear varias copias de los datos. Los desastres tales como inundaciones y terremotos pueden ocurrir sin previo aviso. Hacer una copia de seguridad te ayuda, en caso de pérdida de datos, a recuperar tus datos a través de un disco duro externo o un sitio de copias de seguridad en línea como la nube. De esta manera, puedes ver y en línea en cualquier computadora. Para disponer de una

Instalar las computadoras en lugares seguros

Instalar las computadoras en lugares seguros

Instala la computadora en un lugar donde no sea probable que sufra daños por factores naturales. Por ejemplo, evita instalarla en salas que estén expuestas a un exceso de polvo o humedad.

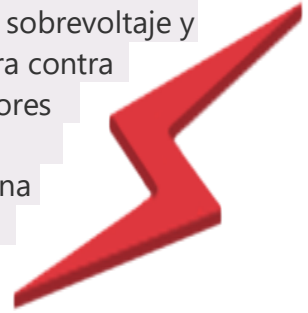


Instalar dispositivos eléctricos de protección

Instalar dispositivos eléctricos de protección

Instala dispositivos, como un Sistema de alimentación ininterrumpida (UPS), que puedan proporcionar una reserva de batería en caso de una interrupción en el suministro eléctrico. Un SAI evita posibles daños al software a causa de un apagado repentino de la

computadora. Un SAI también ofrece características de protección contra sobrevoltaje y de acondicionamiento de la línea, lo que permite proteger la computadora contra sobrevoltaje y picos en la línea eléctrica. También puedes instalar protectores contra sobrevoltaje y acondicionadores de línea independientes. Sin embargo, en caso de un fuerte sobrevoltaje, como el que podría causar una gran tormenta, debes apagar la computadora y desconectarla de la red eléctrica para evitar posibles daños.



Aislar las computadoras del fuego

Aislar las computadoras del fuego

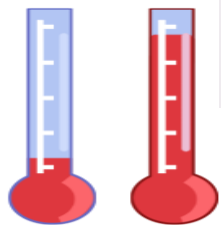
Aísla las computadoras del fuego almacenándolas en ambientes que retarden la propagación del fuego. Además, puedes instalar equipo de protección contra incendios adecuado y adoptar procedimientos de seguridad contra incendios para un rápido control de los daños.



Mantener la temperatura y la humedad adecuadas

Mantener la temperatura y la humedad adecuadas

Debes mantener un nivel de temperatura y humedad óptimo para garantizar el correcto funcionamiento de la computadora. Puedes hacerlo instalando dispositivos tales como aparatos de aire acondicionado o controladores de humedad. Si usas una computadora de escritorio (una computadora diseñada para entrar cómodamente sobre un escritorio de oficina típico), entonces puedes instalar un ventilador que se una al frente o a la parte posterior del gabinete, instalar un kit de refrigeración por agua, etc.



Evaluación de conocimiento

Las computadoras son duraderas y no se dañan fácilmente.

- ☐ Verdadero
- ☐ Falso



Evaluación de conocimiento

El daño físico es una amenaza.

- ☐ Verdadero
- ☐ Falso



Amenazas por acciones humanas

Una fuente humana malintencionada puede ser una amenaza para tu computadora. Un hacker es una persona que intenta obtener acceso de forma ilegal a tu computadora cuando te conectas a Internet. Los hackers suelen ser programadores que pueden obtener acceso no autorizado a otras computadoras. Pueden sabotear tu información personal, tus finanzas, tu computadora, otras computadoras y tus programas. Los hackers también envían información personal a compañías de publicidad. Además de las amenazas malintencionadas provocadas por personas, los errores humanos, como la eliminación accidental de datos y el daño físico, también son una amenaza para tu computadora.



1. Robo

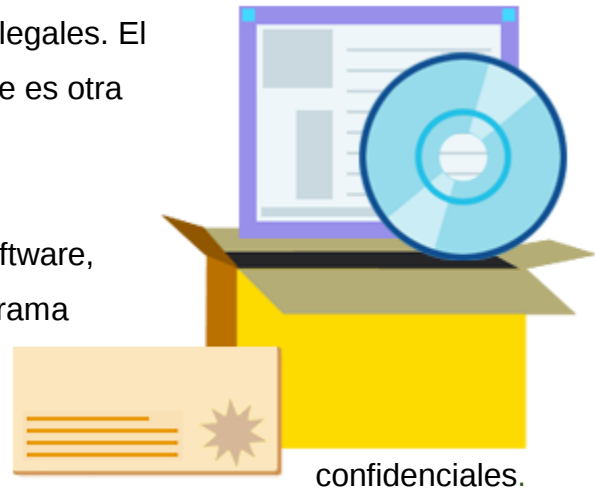
Cualquier persona puede robar tu computadora o sus componentes si tiene acceso a ella. Con la popularidad que han adquirido las computadoras portátiles, el robo físico de computadoras se ha convertido en un hecho muy habitual.

También puedes llegar a convertirte en una víctima del robo virtual cuando tu

computadora se encuentra conectada a Internet.

Un ejemplo de robo virtual es el robo de identidad. El robo de identidad ocurre cuando alguien, generalmente un hacker, te roba tu información personal y la usa sin tu permiso para asumir tu identidad. El hacker usará tu identidad para acceder a tus finanzas o realizar acciones ilegales. El hacker también puede arruinar tu reputación, que es otra razón para evitar el robo de identidad.

Otro ejemplo de robo virtual es la piratería de software, que hace referencia al robo de un diseño o programa informático. También puede hacer referencia a la distribución y el uso no autorizados de un programa informático o de documentos



confidenciales.

2. Virus, gusanos y caballos de Troya

Los virus, los gusanos y los caballos de Troya son programas informáticos que pueden dañar los datos o el software de una computadora o robar la información almacenada en ella. Estos virus pueden llegar a la computadora, sin tu conocimiento, a través de

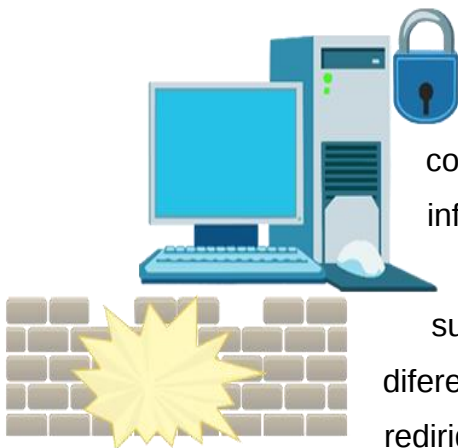
Internet o de dispositivos de almacenamiento, como disquetes y CD-ROM.



Los gusanos son programas malintencionados que se autorreplican y luego penetran en un sistema operativo mediante la propagación de código malintencionado. Los gusanos están diseñados para difundirse por las redes informáticas, enviando copias del código original a otras computadoras. Esto puede causar daño por el consumo

de ancho de banda o posiblemente el borrado de archivos o documentos enviados.

Un caballo de Troya es un tipo de software malintencionado diseñado para proporcionar acceso autorizado a la computadora de un usuario. A diferencia de los gusanos, los caballos de Troya no tienen la capacidad de replicarse. Los caballos de Troya pueden causar graves daños a tu computadora. Los Troyanos pueden instalar virus en una computadora porque está bajo el control del creador del virus. Esto permite robar datos, instalar más malware, registrar las teclas que se presionan y otras acciones ilegales.



3. Spyware

El spyware son programas que se instalan en tu computadora sin tu conocimiento. El spyware recopila información privada del propietario, como sus hábitos de navegación, sus descargas o sus datos personales, como su nombre o su dirección. Existen muchas variedades diferentes de spyware. Algunos programas de spyware pueden redirigirte a un sitio diferente, instalar software adicional que ralentiza la computadora, cambiar la configuración de la computadora, cambiar la página de inicio o servirte un anuncio personal que se conoce como adware.

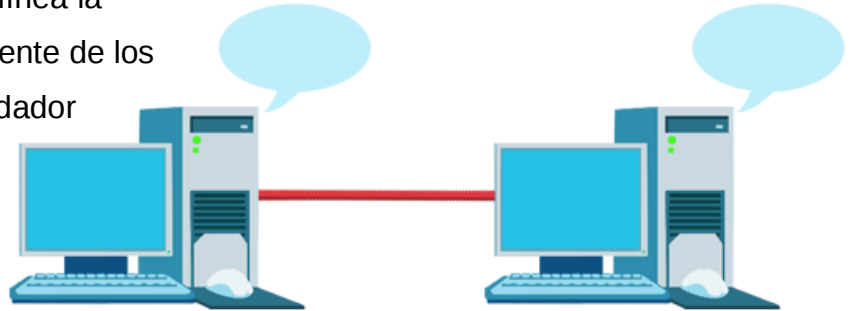
4. Fraudes en Internet

Cuando usas Internet, puedes toparse con ofertas atractivas a través de mensajes de correo electrónico o conversaciones en salones de chat. Pueden parecer reales al principio, pero suelen ser falsas. Pueden hacer daño, porque pueden robar tu información personal y robarte dinero.

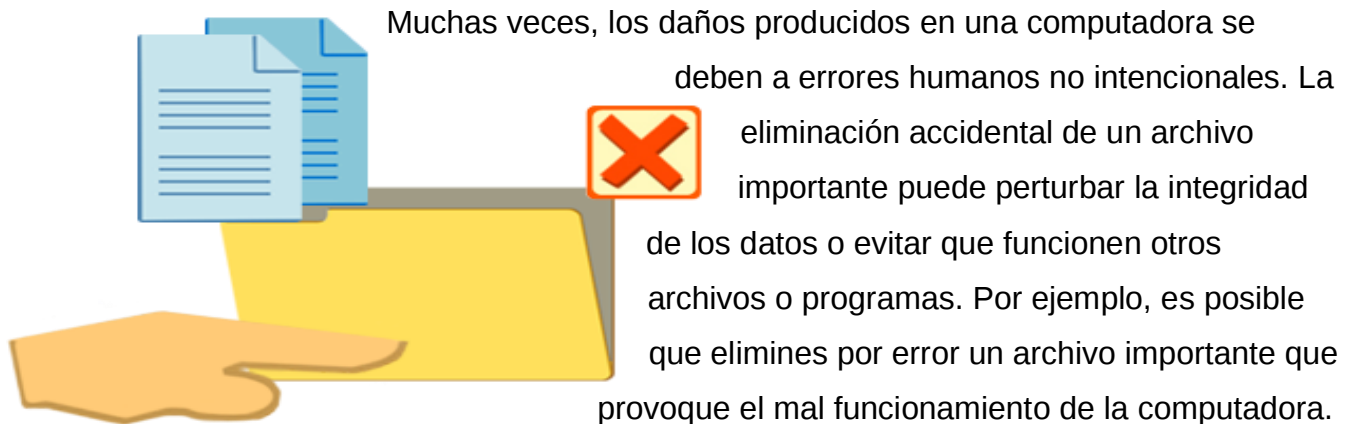


5. Depredadores en línea

Los depredadores en línea son personas que atraen a cualquier persona que esté en línea para mantener relaciones inapropiadas y poco éticas. Es común que, para atacar a una víctima, un depredador en línea la manipule para que no sea consciente de los peligros. Normalmente, un depredador en línea puede encontrarse en salones de mensajería instantánea, salones de chat y sitios de redes sociales.



6. Eliminación accidental de los datos



Muchas veces, los daños producidos en una computadora se deben a errores humanos no intencionales. La eliminación accidental de un archivo importante puede perturbar la integridad de los datos o evitar que funcionen otros archivos o programas. Por ejemplo, es posible que elimines por error un archivo importante que provoque el mal funcionamiento de la computadora.

7. Daños accidentales al hardware

Los componentes de la computadora son extremadamente delicados, lo cual los hace propensos a dañarse si uno no es cuidadoso. Por ejemplo, si dejas caer accidentalmente una computadora portátil, los componentes de hardware, como la

placa base o la lectora de CD-ROM, podrían dañarse. En consecuencia, perderías los datos almacenados en la computadora. Además, tu computadora se puede ver afectada por el daño físico a los datos debido a derrames de comidas y bebidas en dispositivos de almacenamiento o periféricos.



Evaluación de conocimiento

¿Qué es un hacker?

- ☐ Una persona que intenta acceder ilegalmente a tu computadora
- ☐ Un arma que puede dañar tu computadora
- ☐ Un programa para proteger tus programas



Evaluación de conocimiento

El robo de identidad es un ejemplo de robo virtual.

- ☐ Verdadero
- ☐ Falso



Medidas de protección contra las amenazas por acciones humanas

Puedes tomar algunas medidas simples para minimizar los riesgos asociados con las amenazas humanas malintencionadas y los errores humanos.

Almacenar datos de manera segura

Almacenar datos de manera segura

Para minimizar la posibilidad de robo o alteración de los datos, mantén tus datos en lugares seguros y protegidos a los que las personas tengan acceso limitado. Un lugar seguro y protegido podría ser tu oficina privada en casa o un lugar en el que la gente no tenga fácil acceso a tus archivos. Si sientes que no tienes un lugar seguro para almacenar los datos, establece una buena contraseña para tu cuenta. Asegúrate de que tu contraseña no sea simple, como el nombre de tu mascota o tu fecha de cumpleaños. Tu contraseña debe tener más de ocho caracteres, debe contener números y caracteres especiales y debe tener letras en mayúsculas y en minúsculas.



Cifrar los datos

Cifrar los datos



Para evitar que los archivos y documentos perdidos, robados o hackeados se puedan ver, puedes cifrar los datos usando las características BitLocker o BitLocker To Go disponibles en Windows 8. BitLocker es compatible con Windows 7, Vista Enterprise y Vista Ultimate o Windows Server 2008 y R2. BitLocker no cifrará los discos duros de Windows XP, Windows 2000 ni Windows 2003. BitLocker es una función que protege los

archivos de la computadora para que no puedan leerse. Si tu información se pierde, la roban, la hackean o la fuerzan, tus archivos estarán cifrados, lo que significa que el contenido puede ser leído sólo por alguien que tiene la clave de cifrado correcta para descifrarlo. BitLocker no permite a nadie tener acceso a tu disco duro interno e incluso se puede aplicar a unidades de disco duros externas como las unidades de bus serie universal (USB). BitLocker ayuda a proteger contra los ataques en línea y sin conexión. Aunque no es probable, un ataque sin conexión podría provenir de un usuario malintencionado que tome el disco duro de tu computadora y lo conecte a otra computadora para poder extraer tus datos.

Instalar programas antivirus y anti spyware

Instalar programas antivirus y anti spyware

Cuando usas Internet, puedes toparte con un virus o con spyware. Los virus y el spyware pueden hacer gran daño a tu computadora. Es importante descargar un programa antivirus y antispyware que pueda prevenir y eliminar los virus. Los programas antivirus y antispyware presentes en la memoria de la computadora pueden alertarte e impedir que ingresen virus. Debes actualizar regularmente estos programas porque actualizan su base de datos con información sobre nuevos virus y spyware, que mejoran la protección de la computadora. La mayoría de los programas ofrece una función de

actualización automática que instala automáticamente la versión actualizada del programa.

Porque muchos virus, spyware y caballos de Troya provienen de fuentes de correo electrónico y software de correo electrónico. Windows Live Mail te permite bloquear los mensajes de correo electrónico no deseado, filtrar los mensajes con virus, caballos de Troya o spyware y escanear los archivos adjuntos.

En Windows 8, hay una función llamada Windows Defender, que es un programa gratuito que ayuda a proteger la computadora contra las ventanas emergentes, la lentitud y las amenazas de seguridad causadas por virus, spyware y otro software malintencionado. Windows Defender se ejecuta en segundo plano. Puede advertirte si hay algún programa o actividad sospechosos, aunque también puedes ejecutar tu propio análisis. Otra característica integrada es Windows SmartScreen, que es una nueva característica de seguridad de Windows 8 y Windows RT (sistema operativo de Windows 8 diseñado para tablet PC y dispositivos móviles). Windows SmartScreen te ayuda a protegerte de malware nuevo que el software antimalware aún no detecta. SmartScreen cuenta con protección antiphishing, protección para administradores de descargas, reputación de aplicaciones y protección antimalware.



Instalar un firewall

Instalar un firewall

Otro paso efectivo para protegerte contra las amenazas malintencionadas es instalar un firewall. Un sistema de firewall evita el acceso no autorizado del tráfico de red a una red privada. Un sistema de firewall forma una barrera entre sitios web confiables y no confiables y protege contra amenazas como los hackers y los gusanos. Puedes configurar la administración de tu firewall de dos maneras diferentes: política de denegación predeterminada y política de aceptación predeterminada. Una política de denegación predeterminada sólo permite los servicios de red enumerados. Una política de aceptación predeterminada

enumerados y permite con el el acceso todos los aplicación



bloquea los servicios de red todos los demás. Windows 8 viene Firewall de Windows, que bloquea no deseado a tu computadora.

Un programa de firewall no te protege de virus, así que es necesario instalar una antivirus o antimalware. Windows

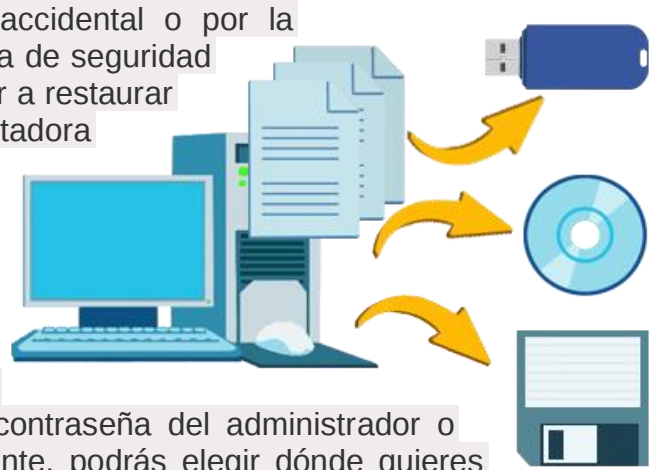
Defender puede ayudar a proteger tu computadora de los virus contra los que el firewall no protege.



Realizar una copia de seguridad de los datos

Realizar una copia de seguridad de los datos

Puedes perder tus datos por un borrado accidental o por la destrucción de datos. Puedes hacer una copia de seguridad de los datos digitales importantes para ayudar a restaurar elementos perdidos o eliminados. Tu computadora de Windows viene con un sistema de copias de seguridad. Puedes localizar la opción de copia de seguridad de datos haciendo clic en el botón Inicio, luego en Panel de control, luego en Sistema y seguridad y por último en Copia de seguridad y restauración. Haz clic en Crear una copia de seguridad ahora. Si no eres un administrador, quizás necesites la contraseña del administrador o confirmación. Si sigues los pasos del Asistente, podrás elegir dónde quieres guardar la copia de seguridad de la información y qué quieres respaldar. Si haz hecho una copia de seguridad de tu información antes, puedes esperar hasta la siguiente copia de seguridad de mantenimiento programada o proseguir a hacer una copia de seguridad de tu información. Es bueno hacer copias de seguridad de tu información regularmente porque puedes tener nuevos programas o archivos que no se encuentran entre tu información antigua. Es mejor que hagas copias de seguridad en varios lugares, como un disco duro externo o un CD. De esta manera, siempre tendrás una copia de seguridad en caso de robo o de daño físico o digital.



Mantener la computadora en un lugar seguro

Mantener la computadora en un lugar seguro

Coloca la computadora en una zona que esté a temperatura ambiente, no tenga polvo ni vibraciones y esté fuera del alcance de posibles golpes.

La mesa o el estante donde está la computadora deben ser firmes y estables para evitar que la computadora se caiga, incluso si alguien la golpea.



Se recomienda que la temperatura ambiente esté comprendida entre 65° y 70° F (18° y 21° C) para una confiabilidad óptima del sistema. Si la temperatura es demasiado baja, pueden existir niveles de humedad demasiado altos que pueden causar condensación de agua que resulte en la corrosión del hardware y la falla de un componente. Cuando la habitación está demasiado caliente, el nivel de humedad puede bajar demasiado. Si la humedad es demasiado baja, se pueden producir descargas electrostáticas que afectan a los componentes sensibles. Las habitaciones calientes también pueden causar recalentamiento, que puede reducir considerablemente la vida útil de los componentes electrónicos. Debes mantener tu espacio informático a cierta humedad relativa. La

humedad relativa es la cantidad de humedad en el aire a una temperatura determinada en relación con la cantidad máxima de humedad que puede haber a la misma temperatura.

Para mantener la computadora a una temperatura segura, puedes instalar un ventilador en la computadora. Ciertos ventiladores enfrían la computadora mediante sistemas de circulación de líquido.

Evaluación de conocimiento

¿Qué es hacer una copia de seguridad de datos?

- ☐ Mover los datos a una caja de seguridad
- ☐ Asegurar la computadora
- ☐ Almacenar datos para restaurarlos en caso de que se pierdan

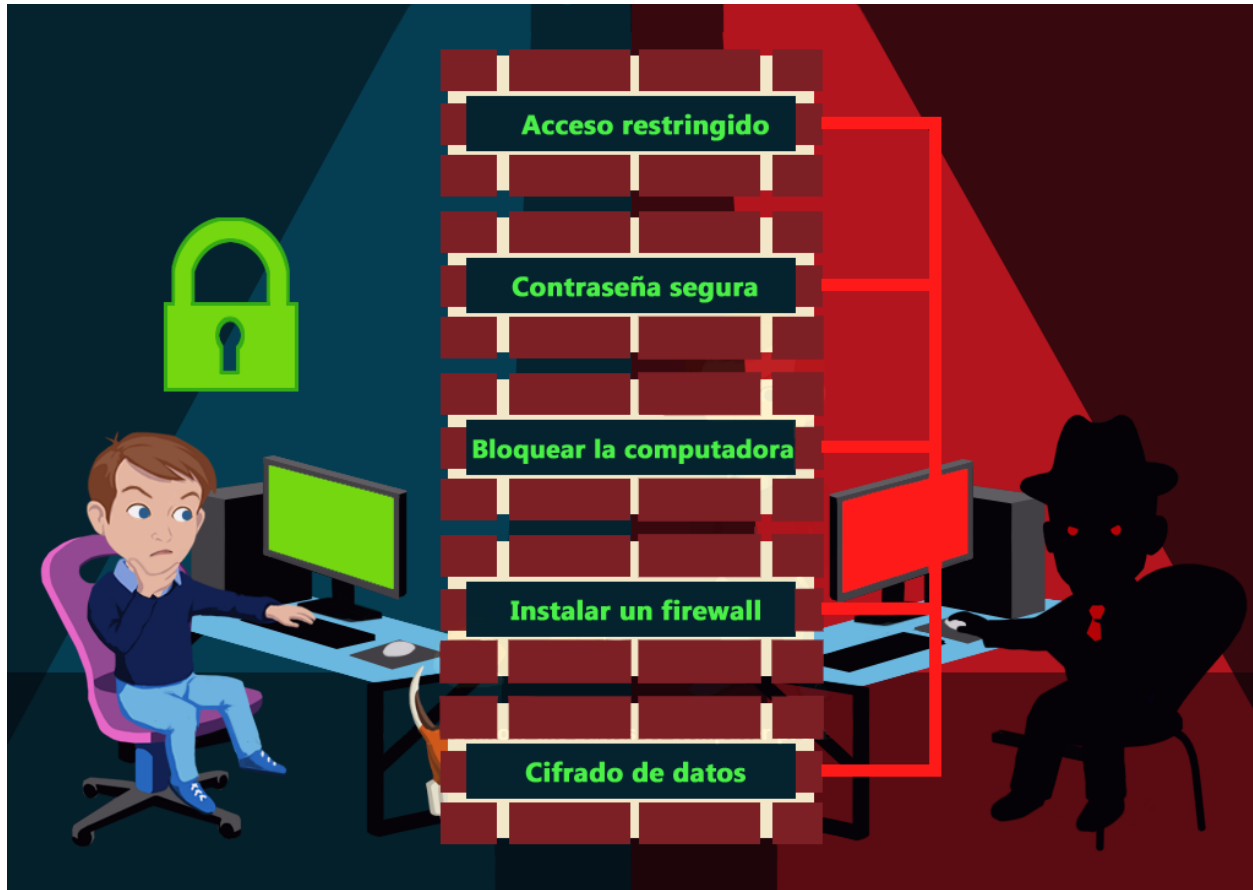


Evaluación de conocimiento

Un firewall es una forma efectiva de protección contra las amenazas.

- ☐ Verdadero
- ☐ Falso





Protección de la computadora

Para tener acceso a la caja de seguridad del banco, necesitas proporcionar tu identificación. Esta identificación sirve para garantizar que nadie más pueda tener acceso a tus pertenencias. De igual modo, es posible implementar distintas medidas de seguridad para minimizar las amenazas a las que se enfrenta tu computadora y los datos que contiene.

Esta lección es una introducción a algunas recomendaciones comunes que te ayudarán a proteger el sistema operativo, el software y los datos de tu computadora.

Pautas para proteger la computadora

Debes proteger tu computadora para asegurar los datos y los archivos que contiene y para proteger tu identidad. La simulación de esta página te presentará dos maneras de proteger tu computadora.

- **Actividad:** Ver video

Evaluación de conocimiento

Crear cuentas puede mantener los datos a salvo de otros.

☐ Verdadero

☐ Falso



Evaluación de conocimiento

Debes mantener tu contraseña en secreto.

☐ Verdadero

☐ Falso



Prácticas recomendadas para las transacciones en línea y de red seguras

Tener tu computadora conectada a Internet te da acceso a todo tipo de actividades y servicios. Pero también presenta riesgos. Pueden acceder personas no autorizadas a tu computadora o puedes descargar archivos y programas que pueden dañar tu computadora. Lee el texto de la derecha para aprender algunas formas de proteger tu computadora.

Contraseña segura

Una contraseña segura es aquella que es suficientemente compleja para que no pueda adivinarse ni descubrirse accidentalmente. Una contraseña segura combina diferentes elementos de contraseñas, tales como letras en mayúsculas y minúsculas, números y

caracteres de teclado únicos tales como "!", "#", u otros símbolos. Las mejores contraseñas no son palabras completas y no podrían ser adivinadas por alguien que te conoce ni por un desconocido.

Una contraseña segura es especialmente crucial para proteger tus datos en los sitios web, pero también se usa para limitar el acceso a redes, sitios con información personal o confidencial e incluso para proteger los datos en tu propia computadora.

Protección contra spyware y hackers

Los programas de spyware pueden entrar desde Internet sin que lo sepas y transmitir información personal sobre ti a un hacker. Este ataque ilegal a tu computadora podría venir de cualquier parte en el mundo, independientemente de donde estés. Los hackers intentan poner spyware en tu computadora para poder robar tus datos confidenciales.

Debes usar toda la protección que puedas conseguir, incluyendo las herramientas antispyware integradas de Windows y apoyo de seguridad en línea de tu proveedor de servicios Internet (ISP). A menudo, este apoyo será en forma de recomendaciones de software antispyware, protección de firewall, análisis del correo electrónico y protección contra el spam.

Borrar periódicamente el historial de navegación

Para tu conveniencia, los sitios web que visitas en Internet durante la navegación se guardan y pueden encontrarse fácilmente en el historial de tu navegador. La computadora usa memoria temporal llamada memoria caché para guardar tu historial de navegación en Internet. A menudo, algunos de estos datos almacenados temporalmente contienen información personal que has proporcionado a un sitio, como información de tu tarjeta de crédito proporcionada para comprar un artículo. Los hackers pueden intentar recuperar esta información, pero puedes limitar este riesgo si eliminas regularmente el historial de navegación y la memoria caché.

Las cookies son otro tipo de archivo que se crea para facilitar la navegación y las compras por Internet. Se usan para guardar preferencias e información que se requiere con frecuencia en los sitios que visitas a menudo. Permiten recordar cosas como tu nombre y tu contraseña y ofrecen una experiencia más personal y menos problemática.

Las cookies también pueden convertirse en una amenaza a la privacidad de tu computadora porque, una vez más, los hackers pueden robar esta información personal. Al igual que con el historial del navegador, es una buena costumbre eliminar regularmente las cookies.

Evitar compartir información personal

Antes de dar cualquier información personal a un sitio web, asegúrate de que se trata de una empresa de renombre y que la información solicitada sea adecuada para los servicios que se ofrecen. Hacer compras en línea a menudo requiere información de tu tarjeta de crédito y te hace vulnerable a los hackers y los fraudes. Para minimizar tus riesgos, asegúrate de que todo comercio por Internet sea en un sitio web seguro y lee cuidadosamente cómo se compartirá tu información con otros. La mejor práctica consiste en evitar dar información personal en Internet a menos que sepas exactamente qué está dando y qué harán con esa información.

Hacer transacciones en línea solo en sitios seguros

En algún momento, usarás Internet para hacer una compra. Esto requerirá que compartas tu número de tarjeta de crédito u otros datos personales. Cuando estés listo para hacer una transacción, es crucial que te asegures de que el sitio web sea un sitio web seguro. Para identificar un sitio web seguro, observa que el nombre del sitio tenga el prefijo https. Este prefijo te dice el sitio web implementa el protocolo Capa de sockets seguros (SSL), usa comunicaciones cifradas y certifica que el sitio web es el que dice ser.

Asegúrate de verificar siempre el certificado de seguridad de toda página web antes de ofrecer tu información personal o realizar una transacción en línea.

Deshabilitar el contenido activo

El contenido activo son pequeños programas que se instalan en tu computadora para mejorar tu experiencia de navegación en Internet. A menudo proporcionan barras de herramientas o video para hacer que interactuar con Internet sea más fácil y más atrapante. En algunos casos, sin embargo, algunas personas malintencionadas usan estos programas atacar tu computadora y robar información sin tu conocimiento. Puedes deshabilitar el contenido activo en tu computadora a través de la configuración del navegador.

- **ARCHIVOS ADJUNTOS EN CORREO ELECTRONICO- Actividad:** Ver video
 - **SPAM Y CORREO BASURA- Actividad:** Ver video
 - **PISHING- Actividad:** Ver video
 - **COMUNICACIÓN EN LIBEA- Actividad:** Ver video
- **ARCHIVOS ADJUNTOS EN MENSAJES INSTANTANEOS- Actividad:** Ver video

Evaluación de conocimiento

La suplantación de identidad (phishing) es una actividad habitual que se usa para obtener información personal de los usuarios de computadoras con fines malintencionados.

☐ Verdadero

☐ Falso



Evaluación de conocimiento

Un mensaje instantáneo pueden tener archivos adjuntos que tengan propósitos malintencionados.

☐ Verdadero

☐ Falso





Protección de la familia contra las amenazas de seguridad

Las computadoras no se usan únicamente en los colegios, las escuelas y las oficinas, sino que también se usan habitualmente en los hogares. Todos los miembros de la familia pueden encontrarle alguna utilidad a la computadora. Debido al uso cada vez mayor de las computadoras en el hogar y en el trabajo, es importante que todos comprendan las distintas amenazas asociadas con el uso de las computadoras e Internet. Cada miembro de la familia puede usar la computadora para diversos fines, tales como:

- Llevar la contabilidad doméstica
- Escribir correo electrónico
- Navegar en Internet
- Jugar
- Escuchar música
- y más

En esta lección, conocerás las distintas medidas que pueden ayudarte a proteger tu computadora de estas amenazas.

Medidas para proteger la privacidad

Proteger tu computadora va desde evitar que software malintencionado infecte tu computadora hasta ocultar información privada en los sitios web. El software antivirus, los filtros de correo electrónico y la configuración de privacidad son métodos para proteger tu privacidad. En esta lección, jugaremos un juego para mostrarte qué software usar para proteger tu privacidad.



• Actividad: Ver video

Evaluación de conocimiento

Los correos electrónicos de spam se pueden detener con...

- ☐ Software antivirus
- ☐ Config. de privacidad
- ☐ Filtros de correo



Evaluación de conocimiento

Los virus troyanos se puede detener con...

- ☐ Software antivirus
- ☐ Config. de privacidad
- ☐ Filtros de correo



Depredadores en línea

Los depredadores en línea apuntan a los niños y a los ancianos para conducirlos hacia relaciones inadecuadas. En esta lección, aprenderás algunas estrategias para reducir el riesgo de ser víctima de ellos.



• Actividad: Ver video

Evaluación de conocimiento

Los depredadores en línea apuntan a...

- ☐ los niños

☐ los ancianos

☐ Todas las anteriores



Evaluación de conocimiento

Los padres deben hablar con sus hijos sobre los depredadores en línea

☐ Verdadero

☐ Falso



Pautas para la protección contra los depredadores en línea

No te conviertas en víctima de los depredadores en línea ni permitas que los miembros de tu familia lo hagan. Usa las siguientes pautas para evitar que los depredadores en línea les hagan daño a ti y a tu familia.



Identificar el comportamiento de un depredador

Los depredadores en línea pueden mostrar ciertos comportamientos que deberían parecer extraños para el observador cuidadoso. Por ejemplo, tienen en mente la meta de conocerte tan bien y tan pronto como sea posible. A menudo, esto resulta en que son demasiado amistosos o familiares temprano en la relación. Están impacientes por el avance natural de una relación normal en línea y forzarán un afecto no merecido, frustrándose rápidamente incluso con un rechazo leve. Si un contacto en línea quiere conocer a un menor de edad en el mundo real en algún momento, debería ser una señal de advertencia.

Tener cuidado de las ofertas hechas por extraños

Los depredadores en línea a menudo ganan confianza y la ponen a prueba ofreciendo regalos u ofertas tentadoras de bondad. Siempre está atento a los regalos ofrecidos a menores de edad. Incluso los adultos deben ser cuidadosos con las ofertas que parecen no merecidas o inadecuadas. Incluso si el regalo es genuino, las intenciones detrás del regalo pueden no serlo.

Educar a los amigos sobre la seguridad en línea

Hay muchas medidas que puedes tomar para crear una mayor seguridad en línea para tus amigos y familiares. Indica a tus seres queridos que nunca usen su nombre real en un salón de chat. Además, nunca deben divulgar ninguna información personal sobre ellos mismos, incluidas la edad y toda información de contacto, como el lugar donde viven o incluso el número de teléfono.

Por encima de todo, nunca reveles, bajo ninguna circunstancia ninguno de tus nombres de usuario ni tus contraseñas a nadie, desconocido o no.

Supervisar a los niños en Internet

Los padres o tutores deben mantener siempre un ojo en lo que sus hijos hacen en Internet. Ellos deben estar protegidos de posibles depredadores en línea y de sitios web inadecuados. Siempre es recomendable que un padre o tutor esté presente cuando un niño visita sitios en línea.

Saber qué sitios visitan los niños

Es importante saber qué sitios ha visitado tu hijo. Si no puedes estar allí en persona siempre para controlar la actividad en línea de tus hijos, es una buena idea rastrear qué sitios han visitado a través del historial de navegación. También hay software especial puedes comprar para supervisar los hábitos informáticos y los historiales web de tus hijos.

Bloquear el acceso a sitios web no adecuados

Asegúrate de bloquear todo sitio web que te parezca inadecuado para tu hijo, incluidos los sitios con contenido para adultos, los tableros de mensajes donde los menores de edad interactúan sin saberlo con adultos y todo otro sitio que no desees que tu hijo visite.

Controlar el historial de chat

También hay programas que los padres pueden comprar para rastrear y controlar las actividades de un niño en un salón de chat. Estos programas pueden detectar instantáneamente temas comunes en los salones de chat, como imágenes o lenguaje inadecuados y llamar su atención sobre ellos.

Evaluación de conocimiento

Hay programas que monitorizan o rastrean las actividades en un salón de chat.

- ☐ Verdadero
- ☐ Falso



Evaluación de conocimiento

Es posible bloquear sitios web.

- ☐ Verdadero
- ☐ Falso





Seguridad y actualización de la computadora

Cuando conectas la computadora a Internet, el resto del mundo puede obtener acceso al software y los datos que contiene. La conexión a Internet aumenta la amenaza de virus, spyware y hackers. Sin embargo, puedes minimizar estas amenazas de seguridad si configuras las opciones de seguridad de la computadora y mantienes el software de seguridad actualizado.

En esta lección, aprenderás la importancia de proteger una computadora y cómo maximizar la seguridad de la misma mediante la configuración de las opciones de seguridad del sistema operativo. Esta lección también describe cómo configurar la computadora para que actualice automáticamente su software de seguridad.

Protección de la computadora

Cuando estás en Internet, las mayores amenazas de seguridad para tu computadora proceden de los hackers y los virus. A menudo, puedes reducir enormemente amenazas como éstas con solo asegurarte de que la configuración de seguridad informática sea correcta y que tu software de seguridad esté actualizado.

Windows 8 puede ayudarte a mantener tu computadora segura y libre de virus porque te alerta de cuestiones de seguridad y mantenimiento y ofrece protección antivirus, un firewall de red y copias de seguridad del sistema. Cada una de estas configuraciones de seguridad se puede ajustar de acuerdo con tus necesidades de seguridad.

Se puede acceder a los siguientes elementos a través de Windows 8 para ayudar a proteger la computadora:

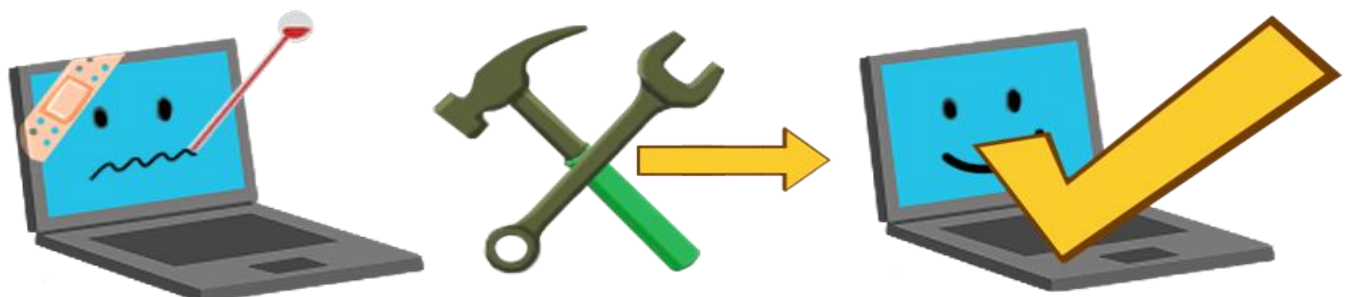
Configuración del firewall para restringir el acceso no autorizado a tu computadora mientras estás en línea.

Configuración para permitir que la computadora descargue e instale automáticamente las actualizaciones de seguridad para ofrecer protección contra los virus más recientes.

Ajustes de privacidad y seguridad que puedes establecer en los sitios de Internet individuales que visitas.

Configuración de protección contra malware para detectar y eliminar software peligroso que podría dañar tu computadora.

Herramientas de mantenimiento que pueden realizar tareas tales como solucionar problemas de Windows y obtener las actualizaciones más recientes.



Evaluación de conocimiento

Los mayores riesgos de seguridad para la computadora son:

- a. Los hackers**
- b. Los amigos**

c. Los virus

d. El daño físico

- ☐ Las opciones a y d
- ☐ Las opciones a y c
- ☐ Las opciones b y c
- ☐ Todas las anteriores



Evaluación de conocimiento

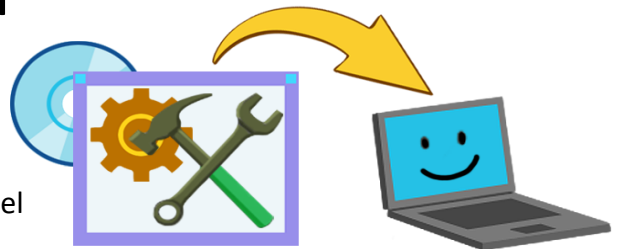
Windows 8 puede mantener tu computadora protegida y libre de virus.

- ☐ Verdadero
- ☐ Falso



Actualización de la computadora

Asegurarse de que la computadora tenga las actualizaciones de sistema y de seguridad más recientes no solo mantendrá la computadora segura, sino que también ayudará con la velocidad y el rendimiento.



- **Actividad: Ver video**

Evaluación de conocimiento

Una computadora nueva puede quedar desactualizada.

- ☐ Verdadero
- ☐ Falso



Evaluación de conocimiento

Las actualizaciones de Windows 8 se deben hacer manualmente.

- ☐ Verdadero
- ☐ Falso



Ética informática

La búsqueda en Internet suele ser la forma más rápida y sencilla de recopilar información en cualquier momento. Por ejemplo, puedes usar Internet para buscar información para los deberes del colegio, o bien ideas para incluir en una presentación de trabajo. También se pueden descargar canciones y películas desde distintos sitios web. En la mayoría de los sitios, la descarga de información es gratuita, pero estas

descargas gratuitas pueden no serlo realmente. La información de un sitio web es propiedad legal del autor que la creó o del sitio web que la publicó. Por lo tanto, puede que necesites el permiso del autor o del propietario del sitio web para usar su contenido. Debes conocer los derechos o permisos que tienes respecto del contenido disponible en un sitio web antes de descargarlo. Eso incluye las descargas de los siguientes elementos:

- Canciones
- Películas
- Software
- y más

En esta lección se describe el significado de la propiedad intelectual en el campo de la informática y cómo un uso no autorizado de ella puede suponer una infracción de las leyes de derechos de autor. Asimismo, esta lección describe los distintos problemas legales asociados con el intercambio de información.

¿Qué es la propiedad intelectual?



- **Actividad:** Simulación

Evaluación de conocimiento

Una biblioteca es la manera más rápida y fácil de acceder a información, productos y servicios.

- ☐ Verdadero
- ☐ Falso



Evaluación de conocimiento

Está bien distribuir material sin permiso.

- ☐ Verdadero
- ☐ Falso



La infracción del copyright y su prevención



• Actividad: Ver video

Evaluación de conocimiento
¿Qué es una infracción de los derechos de autor?
☐ Copiar los derechos de un elemento
☐ Usar la propiedad intelectual de otro sin su permiso
☐ Tomar una foto de tu colección de fotos



Evaluación de conocimiento
Descargar tu propio poema es piratería.
☐ Verdadero
☐ Falso



Problemas legales del intercambio de información

Si usas Internet con frecuencia, existe la posibilidad de que te veas implicado en actividades ilegales o poco éticas, como los juegos de azar o las difamaciones. Debes tener cuidado con este tipo de actividades y ser consciente de ellas. Además, no olvides que estos problemas pueden variar de un país a otro, e incluso entre las distintas zonas de un mismo país.



Difamación de la reputación de una persona

Cuando te comuniques con otras personas a través del correo electrónico, el chat o los foros públicos en línea, asegúrate de no realizar ninguna afirmación en la que puedas difamar a alguien. La difamación consiste en realizar afirmaciones falsas sobre una persona que puedan afectar negativamente su reputación. Por ejemplo, imaginemos que escribes un mensaje en un foro en línea donde afirmas falsamente que tu vecino, que es una persona famosa, tiene algunas propiedades ilegales. Este hecho puede considerarse una difamación, ya que expresa una información falsa que puede afectar la credibilidad de tu vecino.

Las calumnias y las injurias son dos formas de difamación. Las calumnias son difamaciones escritas publicadas, mientras que las injurias son difamaciones verbales. El sistema legal de casi todos los países considera tanto las calumnias como las injurias delitos punibles por la ley. Puedes enfrentarte a sanciones civiles o penales, según el sistema legal de tu país. La pena puede abarcar desde una sanción económica hasta castigos más severos, como el encarcelamiento. En ocasiones, la gravedad de la infracción depende de la situación. Por ejemplo, en algunos países, un insulto al Presidente se considera un acto delictivo. Sin embargo, en otros países, los funcionarios públicos tienen menos protección que cualquier

ciudadano normal. Por lo tanto, ten en cuenta las leyes locales antes de realizar cualquier afirmación difamatoria.

Nota: una afirmación falsa puede considerarse difamatoria aunque no sea despectiva. En ocasiones, incluso las afirmaciones verdaderas pueden considerarse difamatorias si dañan la reputación de una persona.



Visitas a sitios web inapropiados

Algunos sitios web ofrecen servicios que involucran actividades prohibidas por el sistema legal de tu estado o país. Es posible acceder a ellos a través de Internet, ya que allí no existen límites ni controles. Por ejemplo, puedes tener acceso a un sitio de juegos de azar, incluso si la ley de tu país los prohíbe. Sin embargo, acceder a estos sitios podría causarte problemas legales.

También debes tener en cuenta que el sistema legal es diferente según el estado y el país. Por ejemplo, los productos que puedes comprar o vender legalmente en un país pueden suponer una compra o venta ilegal en otro. Por lo tanto, aunque un sitio web no te prohíba

comprar un artículo que es ilegal en tu país, puede que seas acusado de algún delito por ello.

Evaluación de conocimiento

La difamación consiste en hacer declaraciones falsas acerca de alguien que puedan afectarlo negativamente.

- ☐ Verdadero
- ☐ Falso



Evaluación de conocimiento

Los sitios web pueden ofrecer servicios que sean ilegales en tu estado o país.

- ☐ Verdadero
- ☐ Falso



Próximos pasos en el aprendizaje

Gracias por tomar este curso gratuito de aprendizaje electrónico. Este contenido sobre el sistema Microsoft Office 2013 se desarrolló con la orientación de los equipos de desarrollo de productos de Microsoft Office para ponerte al día rápidamente con las nuevas características y funciones de los últimos productos.

Microsoft Learning



02

Recursos adicionales



Microsoft Learning

Consulta el sitio web de **Microsoft Learning** para conocer otros productos de aprendizaje gratuitos, que incluyen evaluaciones, cursos de aprendizaje electrónico y libros electrónicos. Hay cursos disponibles para usuarios domésticos y de oficina, profesionales informáticos y desarrolladores.



Recursos adicionales

El sitio web en línea de Microsoft Office tiene recursos de aprendizaje adicionales para el sistema Microsoft Office 2013, así como plantillas, ayudas para el trabajo, ofertas especiales y vínculos a una comunidad de usuarios de Office que puedes usar para extender tu productividad.

- **Centro de actividades de Windows**

- Windows BitLocker
- Windows BitLocker To Go
- Conozca Windows Defender
- Protección en línea
- Windows y Office original

II Avance de Evaluación:

Este es el segundo avance de evaluación de la nota final del curso, siga cuidadosamente todas las indicaciones brindadas.

****Este trabajo tiene un valor del 20% de la nota final del curso.
50 puntos***

Indicaciones: Siga las instrucciones dadas en cada paso a desarrollar, el valor es dado en puntos entre paréntesis y cursiva.

1. **Realice los recuadros de Evaluación (cuadros verdes), seleccione la opción correcta y entregarlos en la fecha establecida. (10 puntos)**
2. En el procesador de textos de **Microsoft Office (Word)** y en una página de extensión como mínimo, va a realizar una reflexión personal sobre el tema de este módulo, donde se hable sobre que es la seguridad informática, los peligros y precauciones que podemos tomar como usuarios de estas plataformas virtuales. Escriba su nombre al final del documento. (20 puntos)
3. El texto debe venir en **tamaño 12**, tipo de **letra Arial**, el texto debe venir con su alineación **Justificado** (recuerde dejar un reglón entre párrafos). (10 puntos)
4. Guarde su documento en formato de Word, de la siguiente manera:
Avance2Grupo-NombreCompletoSinEspacios.
Ejemplo: Avance2G8-LuisquitaDelCarrascoConch. (5 puntos)
5. Envíe su trabajo en la fecha establecida a la dirección de correo dada a continuación UNICAMENTE: (5 puntos)

digitalliteracycourse.tsa@gmail.com