Co-funded by the
Erasmus+ Programme
of the European Union

Contenido Unidad

[Protección de hardware y software]

Proyecto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nombre del autor: EDIT VALUE®
Última fecha de procesamiento: 02.09.2020

Co-funded by the
Erasmus+ Programme
of the European Union

Protección de hardware y software

Introducción

El hardware y el software están interconectados: sin software, el hardware de un ordenador no tendría ninguna función.

La digitalización está transformando nuestra economía en todo el mundo. Ya sea en el trabajo o en la vida privada, siempre hay algunos problemas relacionados con el hardware y el software que nos afectan a todos. Además, el hardware y el software deben actualizarse, mejorarse o reemplazarse regularmente debido a la existencia de riesgos graves para las organizaciones y también para la sociedad en general.

En esta unidad de contenido, aprenderás sobre los ataques más comunes relacionados con el hardware y el software y qué puedes hacer para protegerte.

¿Sabes que la mayoría de los problemas son de software? Por ejemplo, el software del ordenador puede fallar por múltiples razones ya que las infecciones de virus y/o malware en tu ordenador son muy comunes, las personas a menudo descargan o hacen clic en enlaces que tienen como objetivo causar algún daño a tu ordenador. Hay muchas maneras de rectificar problemas de software, como desinstalar y reinstalar, actualizar, usar un software antivirus actualizado y revisar el sitio web del fabricante en busca de parches. Pero puedes hacer más como verás en esta unidad de contenido.

Relevancia práctica: esto es para lo que necesitarás el conocimiento y las habilidades

Después de trabajar en esta unidad de contenido, conocerás los tipos más comunes de ataques contra hardware y software y también qué hacer en términos de consejos y recomendaciones que puedes aplicar regularmente para tener una protección de hardware y software mejor y más segura.

1. Construye conocimiento - Hardware y software y los ataques más comunes

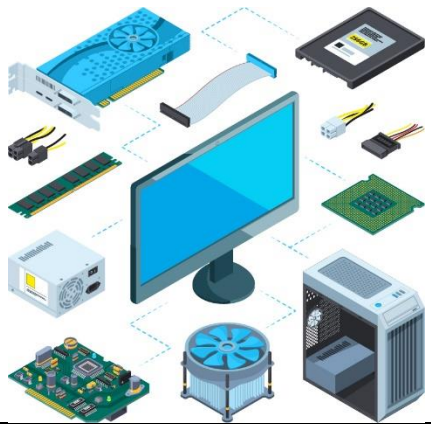
La digitalización está transformando nuestras economías a nivel mundial. A pesar de la cantidad de beneficios que surgen con este fenómeno, también hay amenazas avanzadas para la seguridad digital

que afectan la seguridad y la privacidad en nuestros hogares, automóviles, negocios o incluso redes. Esto se debe a que constantemente usamos dispositivos digitales en la vida cotidiana, una tendencia que aumenta constantemente.
Por lo tanto, el hardware y el software de estos dispositivos deben actualizarse, mejorarse o reemplazarse con frecuencia debido a la existencia de graves riesgos y amenazas para la sociedad en general.

Pero empecemos desde cero: ¿a qué nos referimos exactamente cuando hablamos de hardware y software? En la siguiente tabla encontrarás una definición detallada sobre hardware y software.

Definición
El **hardware** es cualquier componente físico utilizado en o con tu dispositivo, mientras que el software es lo que tiene dentro del disco duro, teléfono inteligente y/o tableta de tu ordenador. El hardware es la parte de tu ordenador o teléfono inteligente, mientras que el software recopila y procesa datos en el disco duro. Algunos ejemplos de componentes de hardware son: procesador del ordenador (CPU), disco duro, placa principal, monitor del ordenador, impresora o ratón. El **software** es la parte lógica de tu ordenador o teléfono inteligente; no puede ser tocado ya que es inmaterial. Aún así, todos los software utilizan al menos un componente de hardware para operar. Puedes imaginar el software como un conjunto de instrucciones que le dicen a un dispositivo exactamente qué hacer. Pueden ser programas o datos. Por ejemplo, un videojuego o Microsoft Outlook.

Para aclararlo, verás las principales diferencias entre hardware y software en la siguiente tabla:

	Hardware	Software
		
Función	El hardware es una parte física de un dispositivo físico que es responsable del procesamiento de datos/información El hardware no puede funcionar sin ningún software	El software es un conjunto de instrucciones que le dice al ordenador exactamente qué hacer. El software es responsable de hacer que el hardware funcione
Características	El hardware es un dispositivo electrónico físico que podemos ver y tocar.	Podemos ver y también usar el software, pero no podemos tocarlo.

	El hardware no puede verse afectado por virus informáticos.	El software se ve afectado por virus informáticos.
Ciclo de vida	Pueden dañarse físicamente.	Puede volverse obsoleto.
Inicialización	Funcionan tan pronto como se instala el software.	Necesita ser instalado en el hardware para trabajar.
Mantenimiento	Las piezas se pueden transferir de un lugar a otro.	Se pueden reinstalar y transferir.
Ejemplos	Ratón, CPU, monitor, impresora, disco duro, etc.	Microsoft Word, Firefox, Skype, Adobe Reader, etc.

Como podemos ver en la tabla anterior, el hardware y el software están interconectados y sin software el hardware de un ordenador no tendría ninguna función.

La protección de hardware y software se ha convertido en un tema candente para todos, especialmente hoy en día. ¿Pero por qué es ese el caso? A continuación puedes ver tres propósitos principales de protección de hardware y software.

Protección de hardware	Protección de software
1. El hardware del orednador puede ser muy frágil (por ejemplo, el calor, el agua, el uso inadecuado, los accidentes físicos causados por personas son las mayores amenazas para la seguridad física de un ordenador)	1. Las actualizaciones periódicas del software tienen muchas ventajas, como evitar errores informáticos, debilidad en los programas de software o sistemas operativos.
2. El hardware debe estar adecuadamente limpio para protegerlo del calor excesivo.	2. Las actualizaciones de software ayudan a lidiar con fallos/vulnerabilidades de seguridad.
3. Algunos incidentes como un robo o el agua en tu hardware pueden causar pérdida/robo de datos, información, dañar tu sistema y archivos de datos.	3. El software ayuda a proteger tus datos/información valiosa de fuentes externas de malware.

Por lo tanto, la seguridad del hardware y el software juega un papel importante para garantizar la confianza, la integridad y la autenticidad. Veamos ahora algunos ejemplos que aclaran por qué la protección del hardware y el software es crucial.

Ejemplo
¿Sabías que en 2011 Sony Pictures sufrió un ataque de un grupo de hacktivistas que lanzó alrededor de 1 millón de cuentas de usuario, incluidos datos personales (contraseñas, correos electrónicos, domicilios, fechas de nacimiento, etc.) que rompieron la política de privacidad de su servicio? En 2017, el gigante HBO fue atacado y el pirata informático lanzó el guión de un episodio de una serie de televisión muy popular (Game of Thrones) que no se había transmitido y también obtuvo acceso a documentos financieros, lista de contactos del elenco y el equipo y otros datos confidenciales. información. Este tipo de incidentes se pueden evitar si tienes una protección sólida de software y hardware.

Co-funded by the
Erasmus+ Programme
of the European Union

1. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_01_01

Situación: ¿Cuál es el significado de hardware y software?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- El software es una parte del ordenador que se puede tocar.
- El hardware puede verse afectado por virus informáticos.
- El software es responsable de hacer que el hardware funcione.
- El hardware y el software solo funcionan si están juntos.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_01_02

Situación: Con respecto a la protección de hardware y software, selecciona las oraciones correctas.
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Los ataques más comunes al hardware son causados principalmente por fuentes externas.
- La protección del software debe hacerse con regularidad.
- Los ataques de software son los más comunes, por lo tanto, debes buscar múltiples protecciones de software.
- El software debe estar protegido por algún antivirus.

2. Construye conocimiento - Mejor protección de hardware

Ahora que sabes qué es el hardware y el software y por qué deberías protegerlo, en los próximos dos capítulos conocerás los ataques típicos contra el hardware y el software y las medidas para evitar ambos.

En las siguientes páginas, estarás en contacto con los ataques más comunes al hardware y, para ayudarte a protegerlo, te daremos algunos consejos y recomendaciones para evitar problemas con el mismo.

Pero, antes que nada, necesitas saber qué es la protección de hardware y cuáles son los ataques más comunes al hardware.

La **protección del hardware** está relacionada con la protección de los dispositivos físicos que debe realizar una persona.

¿Pero cuáles son los ataques más comunes al hardware?

Co-funded by the Erasmus+ Programme of the European Union

Hay tres ataques que ocurren con mayor frecuencia. Los dos problemas más comunes están en la tabla:

HARDWARE	
Accidentes físicos	Modificaciones
Los accidentes físicos, como la caída de agua en un componente físico o el uso inadecuado, pueden ser causados por personas. Este tipo de problemas de hardware pueden comprometer la seguridad física del ordenador.	Modificación de hardware, software o cualquier otra cosa para realizar una función que originalmente no fue concebida o prevista por el diseñador original/futuro propietario del hardware.

Por ejemplo, **las principales consecuencias de los ataques comunes al hardware** son:

Modificaciones 	Las **modificaciones maliciosas de hardware** de los expertos representan una grave amenaza. Por lo tanto, es importante conocer la fuente original donde compras los componentes de hardware. Por ejemplo, los componentes críticos de la infraestructura, como los microprocesadores, pueden estar dentro de tu ordenador para controlarlo.
Accidentes físicos 	El **hardware puede ser muy frágil y también muy valioso**. El calor, la humedad, la vibración, las temperaturas extremas, el polvo, el agua y los accidentes físicos a los componentes físicos son en realidad las mayores amenazas para la seguridad del hardware de tu ordenador. Por lo tanto, debes mantener todo tu hardware limpio, lejos de fuentes de calor excesivas y debes mantener los líquidos lejos de los ordenadores, teléfonos inteligentes y tabletas.

Después de saber qué puede sucederle a tu hardware, debes tener curiosidad acerca de los consejos y recomendaciones que puedes usar para mantenerlo seguro.

Por favor, sigue algunos pasos de la siguiente lista para proteger tu hardware:

1. Las modificaciones de hardware son ilegales a menos que esté de acuerdo con ese tipo de alteraciones. Por ejemplo, si lo deseas, puedes hacer algunas modificaciones en tu ordenador para mejorar algo (velocidad, capacidad, etc.). Debes **evitar comprar componentes de hardware de fuentes/países poco fiables** como plataformas en línea que aún son desconocidas para el público en general, incluso si el precio es muy bajo y atractivo porque, por lo general, el hardware que proviene de fuentes no confiables puede representar una amenaza para la seguridad ;
2. También hay **sistemas especiales de rastreo** que pueden usarse para localizar tu dispositivo si, por ejemplo, es robado o perdido;
3. Para cuidar bien tu hardware, siempre debes i**nstalar y usar software de seguridad actualizado**. Este consejo será más detallado después de hablar sobre la protección del software;
4. **Evita colocar tu hardware en superficies altas y lejos de fuentes de calor, agua, circuitos eléctricos;**
5. **Limpie su hardware muy suavemente** con un paño seco o una herramienta especial, como un cepillo de mango largo y cerdas suaves y toallitas que puede comprar en tiendas específicas donde venden artículos de hardware. Sigue este consejo como regla de mantenimiento y con la frecuencia que sea necesaria.

2. Aplica conocimiento

Ejercicio ELECCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_02_01

Situación: ¿Cuál es el significado de la protección de hardware?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- La protección del hardware solo depende de las personas.
- La protección de hardware es lo que una persona puede hacer para proteger los componentes físicos.
- La protección del hardware no puede ser realizada solo por una persona.
- La protección de hardware solo está relacionada con la implementación de acciones/medidas físicas.

Ejercicio ELECCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_02_02

Situación: ¿Qué puede suceder en el caso de un ataque de hardware?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- El ataque más común al hardware solo está relacionado con modificaciones físicas no autorizadas.
- Los accidentes físicos ocurren con mayor frecuencia porque las personas a veces tienen comportamientos/acciones irresponsables.
- Los ataques al hardware pueden comprometer la información personal y la seguridad física del propietario del hardware.
- Los ataques de hardware están relacionados con incidentes físicos y modificación de hardware.

Ejercicio ELECCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_02_03

Situación: ¿Qué recomendaciones se pueden implementar con respecto a la protección de hardware?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Mantén tu hardware limpio y alejado de fuentes de calor y agua.
- La protección del hardware debe complementarse con la protección del software.
- Debes evitar comprar componentes de hardware de fuentes/países poco fiables debido a posibles alteraciones no deseadas.
- Las personas pueden usar sistemas especiales de rastreo y dispositivos de autodestrucción si es necesario.

3. Construye conocimiento – Mejor protección de software

Ahora es el momento de saber más sobre la protección del software, pues hay muchos ataques que pueden ocurrir. Hoy en día, todos usamos varios tipos de software y, a veces, ni siquiera nos damos cuenta.

Ahora que sabes qué es la protección de hardware, debes conocer también la definición de protección de software.

La **protección de software** es una arquitectura y metodología de seguridad de red informática que combina dispositivos de seguridad y protección defensiva de fuentes (externas e internas). La protección del software requiere una combinación de técnicas relacionadas con diferentes programas y es ahora un aspecto crítico no solo para las empresas sino también para las personas.

Pero, ¿cuáles son los ataques más comunes al software?

A pesar de que hay muchos ataques al software, en la tabla puedes encontrar los más comunes.

SOFTWARE

Troyano	Malware	Virus	Suplantación de identidad
Programa de ordenador que obtiene acceso a una al mismo o al sistema y que está camuflado en forma de software regular para causar daños a los procesos del sistema, datos del disco duro, etc.	Puede incluir spyware, ransomware, virus y gusanos. El malware generalmente ocurre debido a clics peligrosos o archivos adjuntos de correo electrónico que luego instalan software poco fiable	Programa de ordenador diseñado para infectar otros programas del mismo, destruyendo datos esenciales del sistema y haciendo que las redes no funcionen	Práctica de enviar comunicaciones fraudulentas que parecen provenir de una fuente de confianza, generalmente a través de correo electrónico. El objetivo es robar información/datos de alguien (como tarjeta de crédito, información de inicio de sesión, etc.)
Secuestro de datos	**Gusanos**	**Spyware**	**Cryptojacking**
Bloquea el acceso a los componentes clave de tu red	Programa informático de malware que se replica para propagarse a otros ordenadores	Software que permite a un usuario obtener información sobre las actividades informáticas de otro	Uso no autorizado del ordenador de otra persona para extraer criptomonedas. Estos ataques se realizan mediante un enlace malicioso en un correo electrónico, infectando un sitio web o mediante publicidad en línea

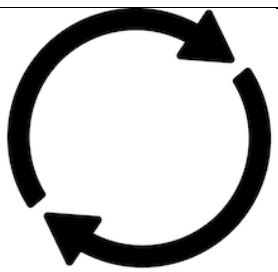
Por ejemplo, las **tres consecuencias principales de los ataques comunes al software** son:

Bugs	Una fuente común de defectos de seguridad de software. Algunos errores representan vulnerabilidades de seguridad que pueden dar lugar a una fuga de información o acceso no autorizado.
Autenticación interrumpida y falta de protección de datos	A veces, las funciones relacionadas con la autenticación son incorrectas y por eso pueden surgir algunos problemas de seguridad. Esta situación puede llevar a que personas no autorizadas accedan a las cuentas de los usuarios para asumir su identidad. En este caso, las personas pueden perder información corporativa

	crucial y la información personal robada puede usarse para perjudicarte a ti y/o tus clientes.
Interrumpir las actividades comerciales	Un ataque al software puede llevar a tu empresa a la bancarrota. Además, la confianza de los clientes puede verse afectada si saben que has sido víctima de un ataque.

Después de ver los ataques más comunes al software hoy en día, necesitas saber qué puedes hacer para prevenir este tipo de incidentes. Y, después de ver algunos de los ataques más comunes, seguramente aceptarás que la protección del software es un tema clave.

Encuentre **algunos consejos** sobre lo que puede hacer para protegerse con respecto a los ataques más comunes al software:

	Mantén tu información personal segura mediante el uso de múltiples contraseñas y copias de seguridad frecuentes. También puedes encriptar información. Crea varias copias de seguridad de todos tus datos importantes y asegúrate de que no estén todos almacenados en el mismo lugar/fuente. Mantén siempre los firewalls. Para ello, debes verificar la configuración de tu hardware y debes tener habilitado tu firewall predeterminado junto con un software antivirus de buena reputación.
	Instala actualizaciones con frecuencia y mantén siempre actualizado tu software. Instala un filtro/software de phishing en su aplicación de correo electrónico y también en tu navegador web. Estos filtros no excluirán todos

	los mensajes de phishing, pero reducirán la cantidad de intentos de phishing. Mantén actualizado tu sistema operativo y software de seguridad. Ejecuta análisis programados regularmente con tu software antivirus y asegúrate de que tu software antivirus y antispyware sean compatibles.
	Nunca abras un archivo adjunto de correo electrónico ni ejecutes un programa cuando no estés 100% seguro de si es una fuente segura. Verifica las credenciales SSL del sitio web y nunca uses información personal/confidencial en sitios web que no tengan un certificado SSL válido instalado. Para ver las credenciales SSL del sitio web, haz clic en el candado cerrado en un viento del navegador "Haz clic en la marca de confianza". Evita usar redes públicas. Implementa un filtro de sitio web para bloquear sitios web maliciosos. Un filtro de sitio web puede ayudarte a controlar los sitios web mediante la creación de una lista permitida o lista bloqueada. Mira en este sitio web cómo puedes hacerlo: www.currentware.com/web-filter.

Como podemos ver, la prevención es la clave para evitar problemas de software y ser proactivo, en otras palabras, tomar algunas medidas para protegerse siempre es la mejor opción.

Para finalizar, es importante tener en cuenta que los ataques evolucionan cada día y, por eso, debes mantenerte actualizado sobre los últimos ataques y medidas de protección. El objetivo principal es mantenerse al día con el malware que existe, se trata de garantizar tu seguridad.

3. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_03_01

Situación: ¿Cuál es el significado de la protección de software?
Tarea: Elige la(s) opcion(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- La protección de software requiere una combinación de múltiples técnicas y métodos.
- La protección del software es principalmente reactiva.
- La seguridad del hardware y el software debe ser una prioridad, pero la protección del software debe hacerse con mayor frecuencia.
- La protección del software es más importante porque las personas usan más software a diario.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_03_02

Situación: ¿Qué puede suceder en el caso de un ataque de software?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Una consecuencia común de un ataque de software es la fuga de información.
- Otra consecuencia común de un ataque de software es el acceso no autorizado.
- Es muy común tener pérdidas financieras en el caso de un ataque de software.
- La autenticación interrumpida y la falta de protección a menudo ocurren al mismo tiempo.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Protección de hardware y software_03_03

Situación: ¿Qué recomendaciones se pueden implementar con respecto a la protección del software?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Las personas deben implementar varios métodos para proteger el software y realizar pruebas de rendimiento con la mayor frecuencia posible.
- Tener firewalls actualizados, antivirus, filtros de phishing son ejemplos de protección de software.
- Debido a que los ataques se vuelven más complejos, el uso de los métodos de protección debe actualizarse.
- Debido a que los ataques de software están evolucionando, las medidas de protección de software también deben actualizarse.

Co-funded by the
Erasmus+ Programme
of the European Union

Fuentes

Diana, J. (n.d.). *Hardware e Sorfware.* https://www.todamateria.com.br/hardware-e-software/

Hossain, F. R. (July 4 2018). *Importance of Security in Software Development.* Retrieved from https://medium.com/brainstation23/importance-of-security-in-software-development-f92669838a90

Images:

https://www.google.com/search?q=trust+symbol&tbm=isch&ved=2ahUKEwjBmqGzoPoAhVFEhoKHfAFDCIQ2cCegQIABAA&oq=trust+symbol&gs_l=img.3..0j0i7i30l9.3932.4753..5400...0.0..0.144.230.1j1.....0....1..gwswizimg.....0i10i19j0i7i30i19.OAgckFFNM7Q&ei=2xVhXoHBLcWkaPCLsJAC&bih=625&biw=1366&rlz=1C1GCEU_pt-PT#imgrc=mN-kWUAz8wqOvM

www.shutterstock.com/search/stop+symbol

www.shutterstock.com/pt/search/update+icon

medium.com/@kluce305/rivetz-platform-cyber-security-with-blockchain-technology-1518d691cfa0

https://www.google.com/search?q=hardware+symbol&tbm=isch&ved=2ahUKEwj1orXBzoPoAhUXwIKHYd_A2IQ2cCegQIABAA&oq=hardware+symbol&gs_l=img.3..0i19l2j0i7i30i19j0i7i5i30i19j0i5i30i19l3j0i8i30i19l2j0i7i30i19.114272.115896..116061...3.0..0.123.1099.6j5.....0....1..gwswizimg.....0i7i30.z7Zef8YKloU&ei=4hVhXvWpFpeAlwSH_42QBg&bih=625&biw=1366&rlz=1C1GCEU_pt-PT#imgrc=uvu4JDot9OTNFM

Afianza conocimiento

La protección de hardware y software son aspectos esenciales de la seguridad, siendo responsable de preservar los activos de software valiosos debido a actividades maliciosas en el software.

Aunque el hardware y el software están interconectados, y sin el software, el hardware de una computadora no funcionaría, y viceversa, el hardware y el software son dos cosas diferentes: el hardware es cualquier componente físico utilizado en o con su dispositivo, mientras que el software es la parte lógica. de su computadora u otro dispositivo. Algunos ejemplos de hardware son la placa principal, el monitor de la computadora, la impresora o un mouse, y algunos ejemplos de software son un videojuego o un programa, como Microsoft Office.

Aunque es imposible evitar la posibilidad de tener un incidente de hardware o software, existen múltiples medidas / herramientas que puede seguir para prevenirlo de la mejor manera posible. El hardware está expuesto a errores humanos, dañándose sin el cuidado adecuado, como limpiezas periódicas y protección física contra los elementos (agua, calor, frío, etc.). El software es

exponencialmente más sensible a las amenazas externas: puede verse afectado por ciberataques como caballos de Troya, virus, ataques de phishing, spywares, malwares, entre muchos otros. Por lo tanto, es fundamental que tome medidas para minimizar el riesgo de amenazas cibernéticas. Por ejemplo, debe utilizar varias contraseñas seguras y copias de seguridad frecuentes, mantener los firewalls de software y un antivirus actualizado, así como implementar un filtro de sitios web para bloquear sitios web maliciosos.

Como vemos, la prevención es la clave para evitar problemas de software, de ahí que la solución sea proactiva. En otras palabras, ¡la mejor opción es siempre tomar algunas medidas para protegerse de las amenazas de ciberseguridad!

Para concluir, es importante tener en cuenta que los ataques están en constante evolución y, por eso, es necesario estar al día sobre los últimos comportamientos de seguridad y medidas de protección.

Las respuestas correctas están marcadas en negrita

Situación: ¿Cuál es el significado de hardware y software?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- El software es una parte del ordenador que se puede tocar.
- El hardware puede verse afectado por virus informáticos.
- **El software es responsable de hacer que el hardware funcione.**
- **El hardware y el software solo funcionan si están juntos.**

Situación: Con respecto a la protección de hardware y software, selecciona las oraciones correctas.
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Los ataques más comunes al hardware son causados principalmente por fuentes externas.
- **La protección del software debe hacerse con regularidad.**
- **Los ataques de software son los más comunes, por lo tanto, debes buscar múltiples protecciones de software.**
- **El software debe estar protegido por algún antivirus.**

Situación: ¿Cuál es el significado de la protección de hardware?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **La protección del hardware solo depende de las personas.**
- **La protección de hardware es lo que una persona puede hacer para proteger los componentes físicos.**
- La protección del hardware no puede ser realizada solo por una persona.
- La protección de hardware solo está relacionada con la implementación de acciones/medidas físicas.

Co-funded by the
Erasmus+ Programme
of the European Union

Situación: ¿Qué puede suceder en el caso de un ataque de hardware?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- El ataque más común al hardware solo está relacionado con modificaciones físicas no autorizadas.
- Los accidentes físicos ocurren con mayor frecuencia porque las personas a veces tienen comportamientos/acciones irresponsables.
- Los ataques al hardware pueden comprometer la información personal y la seguridad física del propietario del hardware.
- Los ataques de hardware están relacionados con incidentes físicos y modificación de hardware.

Situación: ¿Qué recomendaciones se pueden implementar con respecto a la protección de hardware?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Mantén tu hardware limpio y alejado de fuentes de calor y agua.
- La protección del hardware debe complementarse con la protección del software.
- Debes evitar comprar componentes de hardware de fuentes/países poco fiables debido a posibles alteraciones no deseadas.
- Las personas pueden usar sistemas especiales de rastreo y dispositivos de autodestrucción si lo desean.

Situación: ¿Cuál es el significado de la protección de software?
Tarea: Elige la(s) opcion(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- La protección de software requiere una combinación de múltiples técnicas y métodos.
- La protección del software es principalmente reactiva.
- La seguridad del hardware y el software debe ser una prioridad, pero la protección del software debe hacerse con mayor frecuencia.
- La protección del software es más importante porque las personas usan más software a diario.

Situación: ¿Qué puede suceder en el caso de un ataque de software?
Tarea: Elige la(s) opcion(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Una consecuencia común de un ataque de software es la fuga de información.
- Otra consecuencia común de un ataque de software es el acceso no autorizado.
- Es muy común tener pérdidas financieras en el caso de un ataque de software.
- La autenticación interrumpida y la falta de protección a menudo ocurren al mismo tiempo.

Situación: ¿Qué recomendaciones se pueden implementar con respecto a la protección del software?
Tarea: Elige la(s) opción(es) correcta(s) siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Las personas deben implementar varios métodos para proteger el software y realizar pruebas de rendimiento con la mayor frecuencia posible.

Co-funded by the
Erasmus+ Programme
of the European Union

- Tener firewalls actualizados, antivirus, filtros de phishing son ejemplos de protección de software.
- Debido a que los ataques se vuelven más complejos, el uso de los métodos de protección debe actualizarse.
- Debido a que los ataques de software están evolucionando, las medidas de protección de software también deben actualizarse.