
Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación

Unidad de Aprendizaje 1

1. La seguridad informática NO se encarga de:

- a. Desinfectar equipos informáticos vulnerados.
- b. Eliminar vulnerabilidades en equipos informáticos.
- c. Diseñar un modelo de datos óptimo en una base de datos.**
- d. Detectar vulnerabilidades en equipos informáticos.

2. Determina si la siguiente oración es verdadera o falsa: “Un virus de tipo troyano notifica al usuario de los cambios que va a realizar”.

- Verdadero
- Falso

3. Determina si la siguiente oración es verdadera o falsa: “Los gusanos informáticos se encuentran en la memoria RAM y tienen una baja capacidad de replicación”.

- Verdadero
- Falso

4. Determina si la siguiente oración es verdadera o falsa: “El virus *Recycler* recibe su nombre por una de las primeras señales de alarma que genera”.

- Verdadero
- Falso

5. Indica cuál es el primer paso a seguir en un sistema en el que se ha realizado una instalación limpia de un sistema operativo *Windows*:

- a. Instalar un antivirus desde un almacenamiento externo previamente analizado.**
- b. Conectarlo a la red para poder navegar y descargar programas y actualizaciones.
- c. Instalar todos los programas que pueda necesitar.
- d. Deshabilitar el cortafuegos.

6. Un ejemplo de herramienta gratuita de desinfección es:

- a. *Steam*
- b. *TunnelBear*
- c. *Whireshark*
- d. **Avast**

7. Ordena los pasos a realizar durante la desinfección de un virus tro-
yano:

- a. Instalar un antivirus.
- b. Iniciar el sistema en modo seguro.
- c. Analizar el sistema.
- d. Eliminar el virus.
- e. Reiniciar el sistema.

8. Una de las causas de la aparición de un mensaje de error durante la
instalación de un antivirus es:

- a. El sistema no cuenta con la suficiente memoria RAM.
- b. **Ya hay un antivirus instalado en el sistema.**
- c. La versión del sistema es de 64 bits y la del antivirus de 32 bits.
- d. Instalar el antivirus después de las 12:00 de la noche.

9. Determina si la siguiente oración es verdadera o falsa: “Las bombas
lógicas necesitan que ocurra un acontecimiento concreto, general-
mente relacionado con la fecha, para poder activarse”.

- Verdadero
- Falso

10. Determina si la siguiente oración es verdadera o falsa: “Los *keylog-
gers* almacenan la posición del ratón cuando el usuario realiza un
clic y envían esta información al atacante”.

- Verdadero
- Falso

Ejercicios de autoevaluación

Unidad de Aprendizaje 2

1. Los antivirus...

- a. ... no tienen opciones de configuración.
- b. ... cuentan con una configuración por defecto automáticamente adaptada al equipo.
- c. ... necesitan ser configurados en relación con las necesidades de cada equipo.**
- d. ... se configuran automáticamente de forma periódica.

2. Determina si la siguiente oración es verdadera o falsa: "Los antivirus solo cuentan con protección en tiempo real".

- Verdadero
- Falso

3. Determina si la siguiente oración es verdadera o falsa: "Los antivirus permiten establecer análisis periódicos del sistema".

- Verdadero
- Falso

4. Las bases de datos de los antivirus:

- a. Tienen que ser actualizadas constantemente. Algunas lo hacen de forma automática.**
- b. Los antivirus no tienen bases de datos.
- c. No deben ser actualizadas porque suponen un riesgo para el sistema.
- d. Son inaccesibles para el usuario y por lo tanto no pueden ser actualizadas.

5. Los virus de tipo troyano:

- a. Se instalan sin el consentimiento del usuario.
- b. Necesitan el consentimiento del usuario para ser instalados.**

- c. Son muy virulentos.
- d. Son poco virulentos, pero se instalan sin el consentimiento del usuario.

6. Cuando un equipo es infectado por un virus de tipo troyano...

- a. ... es prácticamente imposible detectarlos, puesto que permanecen a la espera de una acción concreta para activarse, como por ejemplo, en una determinada fecha.
- b. ... suelen aparecer ventanas emergentes con publicidad.**
- c. ... se incrementa drásticamente el consumo de red del equipo.
- d. ... mejora el rendimiento del equipo.

7. Respecto a los troyanos:

- a. No cuentan con una apariencia única y la capacidad de algunos de ellos para aparentar ser *software* legítimo puede poner en duda a usuarios expertos.**
- b. Existen varios subtipos de troyanos y su capacidad para aparentar ser *software* legítimo es prácticamente nula, por lo que es muy fácil detectarlos.
- c. No existen subtipos dentro de los virus troyanos. Todos realizan las mismas funciones y tienen apariencias muy similares.
- d. Existen dos subtipos de virus troyanos, los que cuentan con la capacidad para replicarse y los que no.

8. Asocia los siguientes términos con seguridad física o seguridad lógica:

- a. Antivirus
- b. Vigilancia de equipos
- c. Instalaciones acondicionadas
- d. *Backups*

a. d. Seguridad lógica

b. c. Seguridad física

9. Respecto a la virulencia del virus Sasser:

- a. Es un troyano que afectó a millones de equipos en 2004.
- b. Es un gusano que tuvo poco impacto, puesto que apenas logró infectar equipos.
- c. Logró infectar a millones de equipos y aumentó su rendimiento en un 50 %.
- d. Logró infectar a compañías importantes causando grandes pérdidas.**

10. El virus Sasser...

- a. ... es un gusano que aprovecha una vulnerabilidad de seguridad en los accesos de memoria RAM de los sistemas *Windows XP* y *Windows 2000*.
- b. ... es un gusano que aprovecha una vulnerabilidad de seguridad en los puertos de los sistemas *Windows XP* y *Windows 2000*.**
- c. ... tuvo poco alcance, infectando apenas 200 equipos antes de ser neutralizado.
- d. ... afecta a los dispositivos móviles haciendo que la duración de la batería se incremente en un 100 %.

Ejercicios de autoevaluación

Unidad de Aprendizaje 3

1. Un cortafuegos...

- a. ... es único en el sistema, es decir, no puede haber más de uno.
- b. ... puede ser implementado por *software* y/o *hardware* y debe ser complementado con otras herramientas.**
- c. ... sustituye a los antivirus.
- d. ... solo pueden implementarse por *software* y puede haber más de uno en el sistema.

2. Determina si la siguiente oración es verdadera o falsa: "Un cortafuegos constituye un sistema de seguridad completo".

- Verdadero
- Falso

3. Determina si la siguiente oración es verdadera o falsa: "Los puertos solo pueden ser físicos y están limitados a 1024".

- Verdadero
- Falso

4. Los cortafuegos NO están limitados por:

- a. Errores humanos.
- b. Ataques internos originados por virus.
- c. Tráfico que circula fuera de su alcance.
- d. Tráfico que circula dentro de su alcance.**

5. Determina si la siguiente oración es verdadera o falsa: "ZoneAlarm no es configurable y su instalación es bastante complicada".

- Verdadero
- Falso

6. Determina si la siguiente oración es verdadera o falsa: "Para poder instalar *ZoneAlarm* o cualquier otro cortafuegos es necesario desinstalar todos los que se encuentren instalados en el sistema".

- Verdadero
- Falso

7. Determina si la siguiente oración es verdadera o falsa: "Es posible configurar completamente el cortafuegos de un sistema exclusivamente mediante la consola de comandos".

- Verdadero
- Falso

8. USG, el cortafuegos USB:

- a. Es no comercial y no se encuentra a la venta.
- b. Es *open source* y es posible construir uno propio.**
- c. Es *open source* pero no es posible construir uno propio.
- d. No es *open source* y hay escasas unidades a la venta.

9. Determina si la siguiente oración es verdadera o falsa: "Un USG es unidireccional, es decir, solo detecta USB infectados cuando se conectan a un equipo".

- Verdadero
- Falso

10. Determina si la siguiente oración es verdadera o falsa: "Un IDS constituye un sistema de seguridad completo y por lo tanto no requiere antivirus ni cortafuegos adicionales".

- Verdadero
- Falso

Ejercicios de autoevaluación

Unidad de Aprendizaje 4

1. Los módulos espía:

- a. Se propagan a otros equipos.
- b. No se propagan a otros equipos.**
- c. Analizan el sistema en busca de virus.
- d. Eliminan la publicidad durante la navegación web.

2. Determina si la siguiente oración es verdadera o falsa: “Todos los programas espía afectan exclusivamente al navegador”.

- Verdadero
- Falso

3. Indica con “Exclusivo” o “No exclusivo” los siguientes tipos de espía en función de si afectan o no exclusivamente a los navegadores web:

- a. *Tibs Dialer*
- b. *Gator*
- c. *n-CASE*
- d. *Perfect Keylogger*
- e. *Purity Scan*

- a. d.** No exclusivo
b. c. e. Exclusivo

4. Determina si la siguiente oración es verdadera o falsa: “Las cookies están anticuadas y actualmente en desuso”.

- Verdadero
- Falso

5. Determina si la siguiente oración es verdadera o falsa: "Las *cookies* son la mejor opción respecto a utilidad y fiabilidad para almacenar información referente a la navegación".

- Verdadero
- Falso

6. Determina si la siguiente oración es verdadera o falsa: "Las *cookies* pueden almacenar las credenciales de usuario de un sitio web".

- Verdadero
- Falso

7. Una *cookie* NO puede ser:

- a. Robada.
- b. Cruzada con otra *cookie*.
- c. Aceptada, bloqueada o eliminada.
- d. Única para todos los sitios web.**

8. El programa *Malwarebytes*:

- a. Es un programa antiespía compatible con otras herramientas de seguridad.**
- b. Es uno de los programas espía más peligrosos en la actualidad.
- c. Es un programa antiespía incompatible con otras herramientas de seguridad.
- d. Constituye un sistema de protección completo.

9. El programa *SpywareBlaster*:

- a. Permite proteger varios aspectos y navegadores web del sistema y seleccionar únicamente las funciones deseadas.**
- b. Constituye un sistema de protección completo.
- c. Es uno de los mejores cortafuegos del mercado, además de ser gratuito.
- d. Permite proteger únicamente navegadores web del sistema y seleccionar las funciones deseadas.

10. Podemos afirmar que *Evidence Eliminator*:

- a. Es un antiespía muy eficaz y sus campañas de *marketing* son muy recomendadas.
- b. Consigue eliminar datos del equipo de forma permanente incluso cuando estos no pueden ser eliminados de forma convencional.**
- c. Cuenta con una gran reputación, aunque no es muy eficaz contra programas espía.
- d. Es un programa espía que intenta convencer al usuario de que es un programa legítimo.

Ejercicios de autoevaluación

Unidad de Aprendizaje 5

1. La ficha Aplicación de *Malwarebytes* contiene la configuración de:

- a. Actualizaciones de aplicaciones, notificaciones, servidores proxy, acceso de usuarios y actualizaciones de aplicaciones beta.
- b. Protección en tiempo real, opciones de análisis, protección contra amenazas potenciales, actualizaciones, opciones de inicio y cuarentena automática.
- c. Actualizaciones de aplicaciones, notificaciones, opciones de análisis, protección contra amenazas potenciales.
- d. Protección en tiempo real, opciones de análisis, acceso de usuarios y actualizaciones de aplicaciones beta.

2. La ficha Protección de *Malwarebytes* contiene la configuración de:

- a. Actualizaciones de aplicaciones, notificaciones, servidores proxy, acceso de usuarios y actualizaciones de aplicaciones beta.
- b. Protección en tiempo real, opciones de análisis, protección contra amenazas potenciales, actualizaciones, opciones de inicio y cuarentena automática.
- c. Actualizaciones de aplicaciones, notificaciones, opciones de análisis, protección contra amenazas potenciales.
- d. Protección en tiempo real, opciones de análisis, acceso de usuarios y actualizaciones de aplicaciones beta.

3. Determina si la siguiente oración es verdadera o falsa: “La ficha Programación de análisis de *Malwarebytes* permite establecer varias rutinas de análisis. Cada rutina viene definida por el tipo (el cual puede ser normal, rápido o personalizado), la fecha y hora de inicio y la periodicidad con la que se va a realizar”.

- Verdadero
- Falso

4. Determina si la siguiente oración es verdadera o falsa: “La ficha Exclusiones de *Malwarebytes* consta de una base de datos en la que se muestra al usuario un registro de los virus existentes en la red y que son cotejados con los archivos del sistema en busca de software malicioso”.

- Verdadero
- Falso

5. Los análisis programados en *Malwarebytes*:

- a. Solo pueden ser completos.
- b. Solo pueden ser rápidos.
- c. Pueden ser rápidos o completos, pero solo puede estar programado uno de estos tipos de forma simultánea.
- d. Pueden ser rápidos, completos o personalizados y pueden estar programados de forma simultánea.**

6. Respecto a los programas antiespía:

- a. *Malwarebytes Antimalware* es el más potente y por lo tanto la mejor opción.
- b. Apenas existen dos o tres en la red y son prácticamente inútiles.
- c. Existe una gran variedad de ellos en la red y *Malwarebytes Antimalware* es de los más potentes.**
- d. No es recomendado instalarlos puesto que suelen contener software espía.

7. Determina si la siguiente oración es verdadera o falsa: “Los navegadores no cuentan con medidas de seguridad ni es posible instalarles ninguna extensión o herramienta de protección”.

- Verdadero
- Falso

8. El proceso para eliminar *software* espía:

- a. Consta de 8 pasos y el primero de ellos es instalar un programa antiespía.**
- b. Consta de 8 pasos y el primero es hacer una copia de seguridad.

- c. Es muy sencillo, basta con formatear el equipo.
- d. Consiste en analizar el sistema y eliminar las amenazas encontradas.

9. Las compañías antivirus...

- a. ... están bastante relajadas, puesto que con la seguridad de hoy día no hace falta mejorar los programas antivirus.
- b. ... están saturadas de usuarios descontentos con sus servicios.
- c. ... están saturadas de virus de todo tipo, puesto que es relativamente sencillo para cualquier tipo de usuario crearlos.**
- d. ... están saturadas de *spam*.

10. Respecto a la seguridad en los sistemas operativos de *Apple* y *Microsoft*:

- a. *Apple* es mucho más seguro y fiable que *Microsoft*.
- b. *Microsoft* es mucho más seguro y fiable que *Apple*.
- c. Tanto *Apple* como *Microsoft* son tremendamente inseguros y no cuentan con medidas de seguridad.
- d. Tanto *Apple* como *Microsoft* cuentan con medidas de protección ajustadas a sus características y ofrecen seguridad al usuario.**

Ejercicios de autoevaluación

Unidad de Aprendizaje 6

1. *Windows Update* es una aplicación...

- a. ... preinstalada, que se encarga de buscar, descargar e instalar actualizaciones en el sistema.
- b. ... que es necesario descargar desde la tienda de *Microsoft* y sirve para analizar el sistema en busca de programas espía.
- c. ... que es necesario descargar desde la tienda de *Microsoft* y sirve para buscar, descargar e instalar de forma manual actualizaciones en el sistema.
- d. ... preinstalada, que se encarga de buscar, descargar e instalar de forma manual actualizaciones en el sistema.

2. Determina si la siguiente oración es verdadera o falsa: “El botón *Buscar actualizaciones de Windows Update* no tiene ninguna función, puesto que estas se buscan de forma automática”.

- Verdadero
- Falso

3. Determina si la siguiente oración es verdadera o falsa: “*Windows Update* no permite ver un registro de las actualizaciones que han sido instaladas en el sistema”.

- Verdadero
- Falso

4. Respecto a la configuración de *Windows Update*:

- a. No permite cambiar las horas de actividad.
- b. Permite cambiar la hora de inicio de actividad, pero no la de fin.
- c. Permite cambiar la hora de fin de actividad, pero no la de inicio.
- d. **Permite cambiar la hora de inicio y fin de actividad.**

5. Respecto a los programas espía en *Windows 10*:

- a. No es necesario mantener el sistema operativo y *Windows Defender* actualizados, puesto que no son capaces de eliminar virus de tipo espía. Es mejor instalar un programa antiespía.
- b. Es necesario mantener el sistema operativo y *Windows Defender* actualizados, puesto que son los únicos que pueden eliminar los programas espía que logren instalarse.
- c. Es necesario mantener el sistema operativo y *Windows Defender* actualizados y no instalar ningún programa antiespía, puesto que son incompatibles con *Windows Defender*.
- d. Es necesario mantener el sistema operativo y *Windows Defender* actualizados, puesto que son la primera barrera de defensa contra amenazas. Adicionalmente, hay que instalar un programa antiespía que actúe contra espías que logren acceder al sistema.**

6. *Microsoft Edge*:

- a. Es un navegador completo que no requiere de extensiones.
- b. Es un navegador completo al que no se le pueden instalar extensiones.
- c. Es un navegador que cuenta con un amplio catálogo de extensiones que lo complementan.**
- d. Es el navegador más usado en la actualidad.

7. Determina si la siguiente oración es verdadera o falsa: "*Microsoft Edge* permite configurar y desinstalar las extensiones instaladas en él".

- Verdadero
- Falso

8. Las extensiones *Ghostery* y *AdGuard AdBlocker*:

- a. Son exclusivas de *Google Chrome* y *Mozilla Firefox*.
- b. También están disponibles para *Microsoft Edge*.**
- c. Son extensiones espía.
- d. Solo *Ghostery* está disponible para *Microsoft Edge*.

9. Además de *Microsoft Edge*:

- a. No existe ningún otro navegador web.
- b. Existen una amplia variedad de navegadores web, como *Google Chrome* o *Mozilla Firefox*.**
- c. Existen una amplia variedad de navegadores web, como *WhireShark* y *TunnelBear*.
- d. Existe otro navegador web exclusivo de *Windows*, *Safari*.

10. Entre las características de *Google Chrome* destaca:

- a. Su consumo reducido de recursos.
- b. La integración de los servicios de *Google* de forma nativa.
- c. Su alta compatibilidad con las aplicaciones web existentes.
- d. Todas las opciones son correctas.**

Ejercicios de autoevaluación

Unidad de Aprendizaje 7

1. Los aspectos de seguridad en los navegadores web a tener en cuenta son:

- a. Gran variedad de temas personalizables.
- b. Compatibilidad con los servicios y aplicaciones de *Google*.
- c. Que sea intuitivo y poco intrusivo durante la navegación.
- d. **Que prevenga el acceso a sitios web maliciosos, cuente con *antiphishing* y *sandboxing*.**

2. Determina si la siguiente oración es verdadera o falsa: "Los certificados digitales solo tienen validez dentro de España y exclusivamente en sitios web de administración pública".

- Verdadero
- Falso

3. Los certificados digitales de tipo persona física...

- a. ... no son gratuitos y requieren seguir una compleja serie de pasos.
- b. ... no son gratuitos, pero son fáciles de obtener.
- c. **... son gratuitos y pueden obtenerse directamente si contamos con un DNI electrónico.**
- d. ... son gratuitos, pero es obligatorio ir a una oficina de acreditación para confirmar nuestra identidad en todos los casos.

4. Para firmar un mensaje de correo electrónico...

- a. **... es necesario contar con un archivo de firma electrónica, una tarjeta criptográfica, un *token* USB o un DNI electrónico.**
- b. ... los mensajes de correo electrónico no pueden ser firmados.
- c. ... solo se puede hacer con una tarjeta criptográfica.
- d. Todas las opciones son correctas.

5. Las tarjetas criptográficas y los *tokens* USB:

- a. Pueden almacenar certificados digitales y firmas electrónicas, pero son bastante caros.
- b. Pueden almacenar certificados digitales y firmas electrónicas y son económicamente asequibles.**
- c. Solo pueden almacenar certificados digitales.
- d. Solo pueden almacenar firmas electrónicas.

6. Un ataque de denegación de servicio:

- a. Consiste en que un conjunto de servidores se ponga de acuerdo para negar el servicio a los usuarios en modo de protesta.
- b. Consiste en crear muchas cuentas de usuario en el servidor víctima para que no se puedan crear más.
- c. Consiste en saturar la red o los recursos del servidor y que no pueda atender a usuarios legítimos.**
- d. Era un tipo de ataque muy popular en los años 90 pero ha quedado obsoleto en la actualidad.

7. Determina si la siguiente oración es verdadera o falsa: “Un ataque de tipo *Smurf* se considera como un ataque de tipo inundación ICMP amplificado”:

- Verdadero
- Falso

8. Dentro de los ataques de denegación de servicio podemos encontrar:

- a. Inundación TCP, *Smurf* e inundación UDP.
- b. *SACKPanic*, *WhireShark* y *Smurf*.
- c. Inundación SYN, *Smurf* y *Worm*.**
- d. Inundación SYN, inundación ICMP e inundación UDP.

9. Determina si la siguiente oración es verdadera o falsa: “En la actualidad, todos los DNI españoles son DNI electrónicos”:

- Verdadero
- Falso

10. El DNI electrónico:

- a. Almacena información del usuario, así como certificados digitales y firmas electrónicas.**
- b. Almacena información del usuario exclusivamente y se puede acceder a esta información mediante un *smartphone* con NFC.
- c. Almacena la firma electrónica del usuario y no se puede acceder a ella mediante un *smartphone* con NFC.
- d. Puede ser digitalizado en 3D.

Ejercicios de autoevaluación

Unidad de Aprendizaje 8

1. Respecto a los certificados de seguridad en correo electrónico:

- a. SSL no cuenta con vulnerabilidades conocidas.
- b. SSL surgió como una mejora de TLS.
- c. TLS es una actualización de SSL, aunque cuenta con vulnerabilidades en la actualidad.
- d. TLS surgió como una mejora de SSL, el cual es vulnerable actualmente.**

2. Determina si la siguiente oración es verdadera o falsa: “Gmail es el único proveedor de servicios web de correo electrónico que cuenta con certificados SSL”.

- Verdadero
- Falso

3. Respecto a los proveedores de servicios web de correo electrónico seguro:

- a. *Gmail* implementa una red VPN de forma nativa.
- b. *ProtonMail* cuenta con cifrado de extremo a extremo de código abierto.
- c. Cuentan con versión gratuita y ofrecen servicios de cifrado de alta confianza.**
- d. *Tutanota* cuenta con modo confidencial y permite establecer el tiempo de vida de los mensajes enviados.

4. Determina si la siguiente oración es verdadera o falsa: “Microsoft Outlook permite enlazar distintas cuentas de la mayoría de proveedores de servicios web de correo electrónico”:

- Verdadero
- Falso

5. Las cuentas de correo anónimas:

- a. Se usan únicamente para cometer fraudes.
- b. Son complementarias a las cuentas de correo principales.**
- c. A nivel personal, no tienen ninguna utilidad.
- d. A nivel empresarial, no tienen ninguna utilidad.

6. Las cuentas de correo temporales:

- a. Se usan únicamente para cometer fraudes.
- b. Permiten enviar correos en entornos potencialmente inseguros.**
- c. Permiten adjuntar archivos para posteriormente ser enviados.
- d. Son recomendadas en entornos seguros.

7. Determina si la siguiente oración es verdadera o falsa: "Gmail permite la creación de cuentas sin necesidad de introducir datos personales":

- Verdadero
- Falso

8. AnonEmail:

- a. Permite adjuntar archivos en sus mensajes.
- b. Envía los mensajes de forma instantánea.
- c. Permite acceder a la bandeja de entrada y leer las respuestas de los usuarios a los que envías mensajes.
- d. Envía los mensajes en rango de 12 horas de forma aleatoria.**

9. Hushmail es un proveedor de servicios web de correo electrónico que:

- a. Cuenta con certificado PGP, que significa *pretty good privacy*.**
- b. Cuenta con certificado PGP, que significa *pretty good point*.
- c. No permite a sus usuarios subir claves públicas para cifrar los mensajes que envían.
- d. Solo permite usar encriptación en su versión de pago.

10. Cuando se quiere enviar un correo de forma anónima:

- a. Basta con usar un proveedor de servicios web de correo electrónico seguro en cualquier caso.
- b. Es necesario distinguir la seguridad del entorno en el que nos encontramos y si es necesario el uso de redes VPN.**
- c. No es necesario utilizar redes VPN, puesto que es imposible rastrear la dirección IP desde donde se envían los mensajes.
- d. Solo es posible utilizar cuentas de correo temporales.

Ejercicios de autoevaluación

Unidad de Aprendizaje 9

1. Respecto a la seguridad en las redes P2P:

- a. Son las redes más seguras y rápidas.
- b. Son altamente inseguras puesto que sus usuarios son totalmente visibles por el resto de usuarios.
- c. Pueden ser potencialmente inseguras si no contamos con las medidas de protección y la cautela necesaria.**
- d. Las redes P2P, al igual que el resto de redes, son inseguras y además no es posible prevenir posibles accesos malintencionados a través de ellas.

2. Determina si la siguiente oración es verdadera o falsa: *“PeerBlock solo bloquea accesos malintencionados de redes P2P”*.

- Verdadero
- Falso

3. Las compañías proveedoras de internet:

- a. Realizan la facturación exclusivamente en papel.
- b. Cuentan con sistemas de facturación que nunca cometen errores.
- c. Cuentan con servicios web y telefónicos de atención al cliente para consultar posibles errores de facturación (entre otras cosas).**
- d. Solo permiten consultar posibles errores de facturación en sus oficinas de atención al cliente.

4. Determina si la siguiente oración es verdadera o falsa: *“Los correos electrónicos enviados por compañías pueden solicitar información personal como respuesta a sus mensajes”*.

- Verdadero
- Falso

5. Los ataques de tipo *dialer*:

- a. Fueron muy famosos en la década de los 90, pero no se producen en la actualidad.
- b. Aunque se realizaban con mayor frecuencia en la década de los 90, en la actualidad siguen produciéndose en menor medida.**
- c. Consisten en llamar a números al azar de la agenda de contactos de la víctima.
- d. *Dialer* no es un tipo de ataque.

6. *CheckDialer*...

- a. ... es un subtipo de ataque de tipo dialer.
- b. ... comprueba que el número de teléfono al que se va a llamar es válido.
- c. ... es un programa exclusivo de los sistemas basados en Unix.
- d. ... es un programa que bloquea las llamadas a números especiales anotados en su lista negra.**

7. Determina si la siguiente oración es verdadera o falsa: "Los servidores proxy ofrecen menor tiempo de latencia cuanto más cerca estén de nuestra ubicación real".

- Verdadero
- Falso

8. Los usuarios de las redes P2P:

- a. Prefieren la velocidad al anonimato.
- b. Prefieren el uso de métodos que garanticen su anonimato en esa red a expensas de perder parte de la velocidad de transferencia que proporcionan.**
- c. Usan métodos de encriptación que aumentan la velocidad de transferencia de sus archivos.
- d. Mantienen pública su información para que cualquier usuario pueda solicitar sus archivos.

9. Las redes P2P, según su topología, pueden ser:

- a. Centralizadas, híbridas o puras.**
- b. Mundiales, de rango medio o locales.
- c. Las redes P2P no pueden clasificarse según su topología.
- d. Centralizadas o descentralizadas.

10. Las redes P2P centralizadas:

- a. Permiten enlazar los nodos a servidores HUB que a su vez se enlazan con otros servidores HUB.
- b. Son aquellas en las que sus usuarios son al mismo tiempo cliente y servidor y todos están interconectados.
- c. Presentan problemas de escalabilidad y saturación de recursos cuando el número de usuarios es elevado.**
- d. Todas las opciones son incorrectas.

Ejercicios de autoevaluación

Unidad de Aprendizaje 10

1. Microsoft Baseline Security Analyzer es:

- a. Un programa diseñado para dispositivos móviles.
- b. Un programa que se encarga de detectar programas en un equipo.
- c. Un programa que comprueba si las actualizaciones instaladas en el sistema concuerdan con las últimas versiones disponibles.**
- d. Una aplicación antivirus especial para sistemas *Windows*.

2. Las herramientas como *Microsoft Baseline Security Analyzer* surgieron debido a:

- a. La escasa concienciación de los usuarios sobre la importancia de mantener el sistema actualizado y la limitada accesibilidad a internet.**
- b. La necesidad de *Microsoft* de desarrollar herramientas que no resultaran útiles a los usuarios.
- c. El incremento de virus de tipo troyano en la década de los 90.
- d. El alto nivel de concienciación de los usuarios sobre la importancia de mantener el sistema actualizado y el fácil acceso a internet.

3. Determina si la siguiente oración es verdadera o falsa: “La última versión desarrollada por *Microsoft Baseline Security Analyzer* es la 2.3, aunque la más reciente que puede ser descargada es la 2.1.1”.

- Verdadero
- Falso

4. Determina si la siguiente oración es verdadera o falsa: “Uno de los peligros potenciales de internet es la descarga de archivos procedentes de instituciones oficiales”:

- Verdadero
- Falso

5. A la hora de descargar archivos desde páginas web personales:

- a. Se recomienda descargar aquellos que no ofrezcan garantías de ser lo que prometen y ejecutarlos una vez descargados.
- b. Es muy importante analizar debidamente dichos archivos, sobre todo si no cuentan con algún tipo de informe procedente de una herramienta de análisis *online* que los respalde.**
- c. Son sometidos a exhaustivos análisis antes de poder publicarse, por lo que son seguros.
- d. No es necesario tomar ninguna serie de precauciones, puesto que son archivos procedentes de otros usuarios y por lo tanto es prácticamente imposible que contengan virus.

6. *MetaDefender* y *VirusTotal*:

- a. Son herramientas que analizan por completo un equipo en busca de programas maliciosos.
- b. Permiten analizar URL y programas pesados en busca de virus.
- c. Analizan archivos potencialmente peligrosos con un único antivirus, pero este siempre es el más fiable del mercado.
- d. Analizan URL, IP y archivos con una serie de programas antivirus en busca de programas maliciosos.**

7. Determina si la siguiente oración es verdadera o falsa: “*MetaDefender* permite subir archivos de un peso máximo de 140 MB, mientras que *VirusTotal* soporta archivos de hasta 256 MB”.

- Verdadero
- Falso

8. *Panda Cloud Cleaner*:

- a. Es una herramienta online que permite analizar URL, IP y archivos de forma similar a *MetaDefender* o *VirusTotal*.
- b. Es una aplicación que analiza el sistema en busca de virus con la particularidad de que los archivos son analizados en la nube.**
- c. Es una alternativa a los antivirus, puesto que realiza las mismas funciones.
- d. Es un servicio que permite almacenar archivos en la nube los cuales son analizados automáticamente al ser almacenados.

9. Microsoft Safety Scanner se encarga de:

- a. Analizar el sistema en tiempo real.
- b. Complementar los programas antivirus ofreciendo una base de datos actualizada.
- c. Analizar el sistema cuando es ejecutado en busca de archivos maliciosos.**
- d. Realizar el trabajo de los programas antivirus y antiespía en tiempo real.

10. Las actualizaciones de seguridad:

- a. No están exentas de fallos y pueden suponer nuevos fallos de seguridad en el sistema que no existían previamente.**
- b. Implican que el sistema es completamente seguro hasta que sea necesario volver a instalar otra actualización.
- c. No son importantes siempre y cuando contemos con un amplio catálogo de herramientas de seguridad.
- d. Solo aplican correcciones en la interfaz del sistema operativo e incrementan la estabilidad del sistema frente a errores *hardware*.

Ejercicios de autoevaluación

Unidad de Aprendizaje 11

1. Las copias de seguridad deben realizarse:

- a. Diariamente, tanto las copias completas como las parciales.
- b. Cada mes, independientemente del tipo de copia de seguridad.
- c. De forma periódica, siendo más frecuentes las copias completas y menos frecuentes las copias incrementales.
- d. De forma periódica, siendo menos frecuentes las copias completas y más frecuentes las copias incrementales.**

2. Una contraseña robusta es aquella que:

- a. Cuenta como mínimo con 8 caracteres y contiene mayúsculas, minúsculas, dígitos y caracteres especiales.**
- b. Cuenta como máximo con 8 caracteres y contiene mayúsculas, minúsculas, dígitos y caracteres especiales.
- c. Está formada por palabras comunes y fáciles de recordar.
- d. Contiene únicamente letras en mayúscula.

3. Determina si la siguiente oración es verdadera o falsa: "Los programas de control remoto se utilizan exclusivamente con fines maliciosos".

- Verdadero
- Falso**

4. Determina si la siguiente oración es verdadera o falsa: "Telegram es uno de los proveedores de servicios de mensajería instantánea más seguros".

- Verdadero**
- Falso

5. Respecto a la privacidad en internet:

- a. Es relativamente sencillo permanecer en el anonimato en internet.
- b. Las compañías siempre preguntan de forma clara y explícita a sus usuarios que su información privada va a ser recolectada.
- c. Es relativamente difícil permanecer en el anonimato en internet y hay que ser cuidadosos al aceptar los términos de uso de programas.**
- d. Los términos de uso de un programa siempre marcan en negrita las cláusulas de privacidad y estas se encuentran al principio de dichos términos.

6. Los boletines electrónicos:

- a. Son utilizados exclusivamente por instituciones públicas para informar a los ciudadanos.
- b. Son utilizados exclusivamente por empresas para informar a sus clientes.
- c. Pueden pertenecer a diversos ámbitos y son utilizados por todo tipo de organizaciones, empresas, instituciones, etc.**
- d. Son exclusivos del ámbito informático y en ellos se encuentran actualizaciones de seguridad.

7. Determina si la siguiente oración es verdadera o falsa: “A la hora de comprar por internet se recomienda comprar en sitios web que solo permitan el pago mediante transferencia bancaria”.

- Verdadero
- Falso

8. Las compras por internet:

- a. Se encuentran en un estado inicial de desarrollo y requieren que el usuario sea cuidadoso a la hora de elegir dónde comprar.**
- b. Se encuentran en un avanzado estado de desarrollo y es prácticamente imposible encontrar sitios web fraudulentos de venta.
- c. No cuentan con políticas de garantía ni devoluciones.
- d. No son seguras si uno de los métodos disponibles para realizar el pago es *PayPal*.

9. Respecto a los sistemas operativos *Linux*:

- a. Son recomendados para usuarios avanzados.**
- b. Son recomendados para usuarios novatos.
- c. Son de pago y suelen estar preinstalados en los equipos comerciales.
- d. Cuentan con una única distribución que satisface las necesidades de la mayoría de usuarios.

10. La seguridad de las redes wifi:

- a. Es de las más robustas, por lo que no es necesario tomar medidas de protección adicionales.
- b. Está configurada por defecto, por lo que no se recomienda cambiar nada.
- c. Viene dada por los proveedores de servicios de internet, los cuales usan claves de seguridad únicas y difíciles de descifrar para cada equipo de conexión.
- d. Se encuentra expuesta constantemente a todo tipo de usuarios, por lo que es vital cambiar las contraseñas de acceso a la red y de inicio de sesión por defecto.**

