Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. **Relaciona los siguientes elementos y determina si pertenecen a la seguridad física o a la lógica:**

    a. Uso del procedimiento correcto.
    b. Blindaje contra robos.
    c. Comprobación de la veracidad de una información transmitida.
    d. Creación de usuarios restringidos.
    e. Sistema de protección contra incendios.
    f. Control de acceso a los recintos donde se sitúan los ordenadores.

    b. e. f. Seguridad física
    a. c. d. Seguridad lógica

2. **Los conocimientos o datos que tienen valor para una organización, así como los sistemas de información que engloban a las aplicaciones y servicios, se conocen con el nombre de:**

    a. Activos de la información.
    b. Pasivos de la información.
    c. Híbridos de la información.
    d. Libros de información.

3. **Determina si la siguiente oración es verdadera o falsa: "Las posibles reglas que podemos definir en el *firewall* son de entrada y de salida".**

    ■ **Verdadero**
    ■ Falso

4. **Señala en cuál de los siguientes puntos no se centra la seguridad:**

    a. Confidencialidad
    b. Integridad
    c. No repudio
    d. Autenticación

5. Indica cuál de los siguientes no es un objetivo de seguridad:

a. La infraestructura informática.
b. Los usuarios.
c. Los roles de usuarios.
d. La información.

6. El conjunto de técnicas usadas por los ciberdelincuentes para estafar a los usuarios con el fin de obtener sus datos confidenciales, infectar sus equipos informáticos o usarlos como atacantes para otros equipos con el fin de que dichos ciberdelincuentes no sean descubiertos se denomina:

a. Ingeniería robótica.
b. Ingeniería del *software*.
c. Ingeniería del saber.
d. Ingeniería social.

7. Indica cuál de las siguientes no es considerada una medida de seguridad informática:

a. Seguridad física y lógica.
b. Seguridad activa y pasiva.
c. No cifrado.
d. Seguridad de *hardware, software* y redes.

8. En función de las medidas puestas en marcha para cubrir las necesidades de seguridad real, la seguridad se puede clasificar en:

a. *Hardware* y *software*.
b. De red y de *software*.
c. Activa y pasiva.
d. *Hardware* y red.

9. Se garantiza que solamente los usuarios autorizados son capaces de poder modificar los datos o información cuando sea necesario, y no se produce un fraude por otros usuarios que carecen de autorización; hablamos de:

a. Integridad
b. Confidencialidad

c. Autenticación
d. Disponibilidad

10. ¿Cuál de las siguientes opciones está asociada generalmente a fallos en el *software* de los dispositivos informáticos (tanto a nivel de sistema operativo como a nivel de aplicaciones) que ponen en riesgo la seguridad del dispositivo informático y mucho más si está conectado a una red como internet?

a. Amenaza
b. Vulnerabilidad
c. Virus
d. *Randware*

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. **Determina si la siguiente oración es verdadera o falsa: "La impresora es un componente principal de la arquitectura Von Neumann".**

   - Verdadero
   - **Falso**

2. **Las capas que forman el modelo OSI son:**

   a. Cuatro
   b. Cinco
   c. Seis
   d. Siete

3. **Indica cuál de las siguientes no es una topología de red:**

   a. Conmutada
   b. Bus
   c. Anillo
   d. Punto a punto

4. **La capa más baja de todo el modelo OSI y la encargada de gestionar la topología de red y las conexiones que realiza un sistema informático, es:**

   a. Capa enlace de datos.
   b. Capa física.
   c. Capa de red.
   d. Capa de transporte.

5. **Ordena de menor a mayor (por menor se entiende la capa más cercana al medio físico y por mayor, la más aleja de este) las siguientes capas del modelo OSI:**

   1. Físico
   2. Sesión
   3. Presentación
   4. Aplicación

6. ¿Qué dispositivo informático brinda un servicio para todo aquel dispositivo que quiera consumirlo?

a. Arquitectura cliente/servidor
b. Servidor
c. Cliente
d. Alojador

7. _____ está integrada por dispositivos que son usados por una sola persona. Tiene un rango de alcance de varios metros.

a. WAN
b. CAN
c. PAN
d. ZAN

8. _____ se monta sobre una red física y tiene por objetivos aumentar la seguridad y el rendimiento.

a. LAN
b. WAN
c. VLAN
d. VWAN

9. ¿Cuál de los siguientes medios se caracteriza por estar formado por cables que se encargan de la conducción o guiado de las señales de un punto a otro punto?

a. Medios de transmisión.
b. Medios de transmisión guiados.
c. Medios de transmisión no guiados.
d. Medios de transmisión conmutados.

10. Determina si la siguiente oración es verdadera o falsa: "El modo de transmisión simplex se caracteriza por que permite que la información fluya en los dos sentidos, pero no de forma simultánea".

■ Verdadero
■ **Falso**

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. **Entró en vigor en 2016 y es de cumplimiento obligatorio a partir del 25 de mayo de 2018, hablamos de:**

   a. LOPDGDD.
   b. LOPD.
   c. RGPD.
   d. Serie ISO 27004.

2. **La Ley Orgánica 3/2018 se corresponde con:**

   a. RGPD
   b. LOPD
   c. Reglamento General Europe
   d. LOPDGDD

3. **Las siglas DPD se corresponde con:**

   a. Delegado de protección de pérdidas.
   b. Delegado de protección de datos.
   c. Delegado de protección de directivos.
   d. Delegado de protección de *phishing.*

4. **Indica, de los siguientes conceptos, cuál no se corresponde con un principio de la LOPDGDD:**

   a. Datos exactos.
   b. Datos inexactos.
   c. Deber de confidencialidad.
   d. Consentimiento del titular.

5. **Las infracciones que prescriben a los dos años son las infracciones:**

   a. Mínimas
   b. Leves
   c. Graves
   d. Muy graves

Ejercicios de autoevaluación Unidad de Aprendizaje 4

1. **¿Cuál de las siguientes opciones tiene como objetivo principal iniciar y comprobar que el *hardware* del sistema o equipo informático donde se encuentra insertado funciona correctamente y, mediante un gestor de arranque, dar paso a la carga del sistema operativo en el dispositivo o equipo informático?**

    a. Sistema operativo
    b. *Malware*
    c. BIOS
    d. *Windows*

2. **El *software* que nos permite emular un sistema operativo dentro de otro se denomina:**

    a. UEFI
    b. BIOS
    c. Máquina virtual
    d. Sistema operativo

3. **Determina si la siguiente oración es verdadera o falsa: "Si queremos realizar una instalación de *Windows 10,* lo primero es pasar por la tienda *online* de *Windows* para adquirir dicho sistema operativo".**

    - Verdadero
    - **Falso**

4. **El Centro de Seguridad lo podemos localizar en:**

    a. *Windows*
    b. *Ubuntu*
    c. *Android*
    d. IOS

5. Cuando se realiza el proceso de instalación de este sistema operativo, este nos permite escoger el cifrado de disco. Hablamos de:

a. *Windows*
b. *Ubuntu*
c. *Android*
d. IOS

6. El sistema operativo que se caracteriza por tener un gran conjunto de programas que trabajan en serie es:

a. *Windows*
b. *Unix*
c. *Linux*
d. IOS

7. Determina si la siguiente oración es verdadera o falsa: *Android* fue diseñado para implementarse en dispositivos móviles con pantalla táctil, tales como *Smartphones,* tabletas, relojes inteligentes, televisiones...

- **Verdadero**
- Falso

8. El antivirus que nos proporciona *Microsoft* en *Windows* se denomina:

a. *Norton*
b. *Defender*
c. *Avast*
d. Essed Nod32

9. Un *antimalware OpenSource* y totalmente gratuito para *Ubuntu* se corresponde con:

a. *Norton*
b. *Defender*
c. *Avast*
d. *ClamAV*

10. Relaciona los siguientes sistemas operativos con sus tipos:

a. *IOS*
b. *Android*
c. *Mac OS*
d. *Linux/Unix*
e. *Windows*

c. d. e. Sistema operativo
a. b. Sistema operativo móvil

Ejercicios de autoevaluación Unidad de Aprendizaje 5

1. **Indica cuáles de las siguientes opciones corresponde a virus y cuáles gusanos:**

   a. *I Love You*

   - Virus
   - **Gusanos**

   b. *Blaster (Lovesan)*

   - **Virus**
   - Gusanos

   c. *SobigWorm*

   - Virus
   - **Gusanos**

   d. *Code Red*

   - **Virus**
   - Gusanos

2. **Determina si la siguiente oración es verdadera o falsa: "Para que un *software* con código malicioso pueda llevar a cabo sus objetivos (sean cuales sean), es primordial que pase desapercibido para el usuario o usuarios del equipo o dispositivo informático infectado".**

   - **Verdadero**
   - Falso

3. **Señala cuál de los siguientes elementos no se clasifica dentro del *malware* oculto:**

   a. Puertas traseras
   b. *Drive-by download*
   c. *Rootkits*
   d. *Dialers*

4. Indica cuál de los siguientes elementos no se corresponde con *malware* para obtener beneficios:

a. Puertas traseras.
b. *Spyware.*
c. *Keyloggers.*
d. *Dialers.*

5. Determina cuál de los siguientes hábitos no se corresponde con un hábito seguro:

a. Aprender a detectar sitios web y correos *phishing.* Se recomienda la comprobación de los enlaces web, no abrir los correos sospechosos y, sobre todo, no facilitar información sensible por este medio.
b. No descargar ni ejecutar adjuntos que no tengamos claro su procedencia, su origen o la persona que nos los envía. Además, debe ponerse especial atención si se abre un correo de la carpeta spam.
c. Usar contraseñas robustas y, a ser posible, diferentes en cada uno de los servicios que usemos en internet. Lo más probable es que si nos capturan una contraseña, dicha contraseña la prueben en todos los servicios de internet contratados.
d. No usar el doble factor de autenticación para obtener una capa más de seguridad.

6. La técnica que consiste en buscar archivos de papel que haya arrojados en las papeleras, contenedores de información, CD, DVD..., se corresponde con:

a. *Dumpster diving*
b. *Drive-by download*
c. *Rootkits*
d. *Dialers*

7. El ataque a equipos o dispositivos informáticos en red que hace que uno o más servicios sean inaccesibles se denomina:

a. *Malware* infeccioso
b. *Malware* oculto
c. Ataques distribuidos
d. Ataques centralizados

8. Indica cuál de los siguientes no es un ataque relacionado con DDoS:

a. Ataque pitufo
b. *SYN Flood*
c. *UPD Flood*
d. *Ping Flood*

9. La técnica que consiste en poner delante de nuestro servidor otro servidor para que reciba y filtre los ataques se conoce con el nombre de:

a. Bloquear IP
b. Aplicar filtros
c. Balanceo de carga
d. CDN

10. Determina si la siguiente oración es verdadera o falsa: "Siempre que sea posible, debemos actualizar a la última versión el sistema operativo que tiene nuestro dispositivo o equipo informático. La mayoría de los sistemas operativos no cuentan con un mecanismo de actualizaciones automático, simplemente bastaría con comprobar que está activado o configurado correctamente".

- Verdadero
- **Falso**

Ejercicios de autoevaluación Unidad de Aprendizaje 6

1. **Determina si la siguiente oración es verdadera o falsa: "Tan importante es vigilar la seguridad de los dispositivos informáticos como las instalaciones en las que se encuentran instalados".**

   - **Verdadero**
   - Falso

2. **¿Cuál de las siguientes opciones no se considera un tipo de desastre?**

   a. Inundaciones.
   b. Tormentas.
   c. Terremotos.
   d. Plaga de ratas.

3. **Indica cuál de las siguientes fases no está presente en la elaboración de un plan de contingencia:**

   a. Identificación de riesgos.
   b. Identificación de soluciones.
   c. Monitoreo.
   d. Resolución de desastres.

4. **Determina si la siguiente oración es verdadera o falsa: "El plan de recuperación es un proceso de recuperación mediante el cual alcanzamos objetivos tales como datos, *hardware* y *software* crítico cuando se produce un desastre o riesgo y con la garantía de que el comercio electrónico puede seguir operando con normalidad como si no hubiera ocurrido desastre alguno".**

   - **Verdadero**
   - Falso

5. **Indica cuál de los siguientes conceptos no está presente en un plan de recuperación:**

   a. Testeo de riesgos.
   b. Planificación.

c. Identificación de riesgos.
d. Identificación de soluciones.

6. ¿En qué fase se realiza un estudio de aquello que la empresa tiene implantado y de cómo pueden afectar los riesgos más importantes?

a. Testeo de riesgos.
b. Planificación.
c. Identificación de riesgos.
d. Identificación de soluciones.

7. Si se usa un cable Ethernet, se recomienda...

a. ... tirarlo en línea recta al dispositivo para consumir menos cable.
b. ... entubarlo o integrarlo en la estructura del edificio.
c. ... acercarlo a conducciones de alta potencia.
d. ... acercarlo a conducciones o canalizaciones de agua.

8. Si en la empresa hay cámaras de seguridad, se tendrá en cuenta la privacidad del personal y además se deberá...

a. ... poner en su conocimiento la existencia de dichas cámaras, su localización y la función de vigilancia que realizan.
b. ... poner en su conocimiento la existencia de dichas cámaras.
c. ... poner en su conocimiento la existencia de dichas cámaras y su localización.
d. ... poner en su conocimiento la existencia de dichas cámaras y las grabaciones para el visionado de los usuarios que son grabados.

9. La importancia de un plan de recuperación ante desastres es directamente proporcional a la complejidad, importancia, costes del servicio y...

a. ... riesgo.
b. ... amenazas.
c. ... seguridad.
d. ... información.

10. La segunda fase de identificación de riesgos se caracteriza por:

a. Maximizar lo máximo posible el riesgo.
b. Minimizar lo mínimo posible el riesgo.
c. Minimizar lo máximo posible el riesgo.
d. Maximizar lo mínimo posible el riesgo.

Ejercicios de autoevaluación Unidad de Aprendizaje 7

1. **Determina si la siguiente oración es verdadera o falsa: "SIM tendrá como objetivo la recolección de todos los eventos de una red usando para ello a los agentes (a modo de introducción se puede decir que un agente es un pequeño programa *software* desarrollado o escrito específicamente para un determinado equipamiento de nuestra red)".**

   - **Verdadero**
   - Falso

2. **El *software* que toma el control de acceso en una determinada red informática para proteger sus recursos y contestar frente a ataques y abusos en la misma se denomina:**

   a. *OSSIM*
   b. *IPS*
   c. *SPI*
   d. *PSSIM*

3. **Controla y observa las MAC que existen en una red, manteniéndolas en un archivo con su correspondiente IP asociada; además, en este archivo también se almacena la última conexión de la MAC/IP a la red y se generan notificaciones en caso de que haya cambios. Nos referimos a:**

   a. *Arpwatch*
   b. *P0f*
   c. *Pads*
   d. *OpenVas*

4. **Indica cuál de las siguientes herramientas se usan para la detección de vulnerabilidades:**

   a. *KeyLoggers*
   b. *Nessus*
   c. *Arpwatch*
   d. *P0f*

5. Señala cuál de las siguientes afirmaciones no se puede realizar con la herramienta *Ntop:*

a. Ordenar el tráfico de una red en función de determinados protocolos.
b. Mostrar el tráfico de una red en función de determinados criterios.
c. Mostrar las estadísticas del tráfico de una red.
d. Identificar activamente el sistema operativo.

6. ¿Cuál de las siguientes opciones tiene como objetivo realizar *forward* de los datos almacenados por nfcapd hacia otros *host* de la red?

a. nfcapd
b. nfdump
c. nfreplay
d. nfclean

7. ¿Cuál de las siguientes opciones es un proceso que se ejecuta en cada *host* que se monitorea y su misión es escanear el sistema de ficheros y enviar los datos al *host* o consola de administración?

a. Agente de escaneo.
b. Consola de red.
c. Consola de administración.
d. Aplicación de administración CLI.

8. Determina cuál de las siguientes herramientas se usa para auditorías:

a. *KeyLoggers*
b. *Snare*
c. *OSSEC*
d. *Nessus*

9. ¿Cuál de las siguientes opciones se corresponde con un demonio y que tiene como fin la ejecución de comandos, leer o escribir archivos en el sistema de ficheros del equipo/*host* o servicio?

a. *OSSIM-Server.*
b. *OSSIM-Framework.*

c. *OSSIM-Agent.*
d. *OSSIM-WorkStation.*

10. Determina si la siguiente oración es verdadera o falsa: "El *software OSSIM* no puede ser instalado en máquinas virtuales".

- Verdadero
- **Falso**

Ejercicios de autoevaluación Unidad de Aprendizaje 8

1. Indica en qué tipo de ataque se clasifica un ataque LAND:

a. Gusano
b. Virus
c. Ataque DoS
d. Ataque de secuencia TCP

2. ¿Cuál de las siguientes opciones es un ataque que basa su funcionamiento en el envío de un paquete ICMP que se caracteriza por tener un tamaño de más de 65.536 *bytes*?

a. *Ping* de la muerte
b. Virus
c. Ataque DoS
d. Ataque de secuencia TCP

3. El envenenamiento de caché DNS se clasifica dentro de:

a. *Ping* de la muerte
b. ARP *Spoofing*
c. Ataque DoS
d. Ataque de secuencia TCP

4. Señala cuál de las siguientes técnicas no pertenece a un ataque de ingeniería social:

a. Ofertas falsas
b. Controlar enlaces
c. Filtros de *spam*
d. Rapidez

5. ¿Cuál de las siguientes opciones es un *software* o programa cuyo objetivo es registrar las pulsaciones de un usuario en el teclado con el fin de su envío *a posteriori*?

a. Gusano
b. ICMP *Tunneling*

c. *KeyLoggers*
d. Ataque de secuencia TCP

6. ¿Cuál de las siguientes opciones es un programa o aplicación *software* que tiene la capacidad de copiarse e infectar los equipos o dispositivos informáticos?

a. Gusano
b. Virus
c. *KeyLoggers*
d. Ataque de secuencia TCP

7. La recreación de situaciones reales de seguridad informática mediante la simulación de juegos y con el fin de que el usuario aprenda conceptos y formas de protegerse, informáticamente hablando, se denomina:

a. *CrackGames*
b. *HackGames*
c. *ProGames*
d. *WarGames*

8. ¿Cuál de los siguientes comandos permite obtener la definición del literal buscado?

a. define:termino
b. filetype:extension
c. site:URL
d. related:URL

9. Si lo que queremos es obtener páginas web similares a una determinada URL, debemos usar el comando en *Google:*

a. define:termino
b. filetype:extension
c. site:URL
d. related:URL

10. Si queremos realizar una búsqueda filtrando por el título de la página, debemos usar el comando:

a. define:termino
b. filetype:extension
c. intitle:termino
d. related:URL

Ejercicios de autoevaluación Unidad de Aprendizaje 9

1. **Determina si la siguiente oración es verdadera o falsa: "Por tanto, una vez que se instala un dispositivo *router* en una red, el siguiente paso que deberíamos dar sería la configuración del mismo en cuanto a materia de seguridad se refiere".**

   - **Verdadero**
   - Falso

2. **Indica cuál de los siguientes conceptos no está asociado con la configuración mínima de seguridad:**

   a. Modificar las credenciales de acceso al *router.*
   b. Asignar una contraseña de acceso a la red.
   c. Facilitar la contraseña de acceso a la red.
   d. Configurar el tipo de cifrado de la red.

3. **Señala cuál de los siguientes conceptos no se relaciona con una configuración avanzada de seguridad:**

   a. Configuración del *firewall.*
   b. Acceso al *router* por http.
   c. Acceso al *router* por https.
   d. Ocultar el SSID de la red.

4. **Determina cuál de los siguientes no es un mecanismo de seguridad relacionado con el wifi:**

   a. RC4
   b. WEP
   c. WEB
   d. WPA

5. Determina si la siguiente oración es verdadera o falsa: "La familia 802.11 consta de una serie de técnicas basadas en la modulación dúplex usadas en el aire que emplean el mismo protocolo básico".

- Verdadero
- **Falso**

6. Tiene la función de hacer de puente (conecta dos redes con niveles de enlace parecidos o distintos) y realiza las conversiones de tramas oportunas al respecto. Hablamos de:

a. Punto de acceso.
b. Estaciones.
c. Medio.
d. Sistema de distribución.

7. Indica cuál de los siguientes no es un servicio básico de seguridad proporcionado por el estándar 802.11:

a. Autenticación
b. Confidencialidad
c. Integridad
d. Identificación

8. Se corresponde con un mecanismo creado con el fin de facilitar la conexión de dispositivos a nuestra red wifi. Hablamos de:

a. APS
b. PWS
c. WPS
d. PSW

9. Respecto a WEP, WPA implementa...

a. ... un protocolo de control de clave temporal.
b. ... un protocolo de cifrado de clave temporal.
c. ... un protocolo de integridad de clave temporal.
d. ... un protocolo de eliminación de clave temporal.

10. Ordena los siguientes puntos:

1. La estación cliente envía una petición de autenticación al punto de acceso.
2. El punto de acceso envía de vuelta un reto en texto claro.
3. El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada y volver a enviarlo al punto de acceso en otra petición de autenticación.
4. El punto de acceso descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del valor de esta comparación, el punto de acceso envía una confirmación o una denegación. Después de la autentificación y la asociación, WEP se usa para cifrar los paquetes de datos.

Ejercicios de autoevaluación Unidad de Aprendizaje 10

1. Los troyanos no tienen la capacidad de...

a. ... geolocalización.
b. ... reproducción.
c. ... propagación.
d. ... réplica.

2. ¿Cuál de las siguientes opciones se corresponde con un código, método o programa que directamente realiza una acción contra el sistema operativo o un programa que contenga vulnerabilidades?

a. Gusano
b. Virus
c. Vulnerabilidad
d. *Exploit*

3. Determina si la siguiente oración es verdadera o falsa: "Si un programa que tengamos instalado en nuestro dispositivo informático conlleva un error de programación y, por tanto, una vulnerabilidad, el sistema operativo en su totalidad también es vulnerable".

- **Verdadero**
- Falso

4. Clasifica correctamente los siguientes programas en función de los siguientes parámetros: copias de seguridad, antivirus o gestión de tareas.

a. ***SyncBack***
b. ***Genie Timeline***
c. ***IObit Malware Fighter***
d. ***Panda Free Antivirus***
e. ***System Status Monitor Pro***
f. ***Process Explorer***

Copias de seguridad

- *SyncBack*
- *Genie Timeline*

Antivirus

- *Panda Free Antivirus*
- *IObit Malware Fighter*

Gestión de tareas

- *System Status Monitor Pro*
- *Process Explorer*

5. **Clasifica correctamente los siguientes programas en función de los siguientes parámetros: privacidad y navegación segura, mantenimiento y limpieza, análisis del tráfico de red.**

a. ***Obrot Proxy***
b. ***Blur***
c. ***Clean Master***
d. ***Network Inspector***
e. ***Phone Clean***
f. ***Ip Scanner***

Privacidad y navegación segura

- *Blur*
- *Obrot Proxy*

Mantenimiento y limpieza

- *Phone Clean*
- *Clean Master*

Análisis del tráfico de red

- *Network Inspector*
- *Ip Scanner*

6. Determina si la siguiente oración es verdadera o falsa: "En la actualidad en internet se pueden localizar herramientas de pago únicamente relacionadas con la seguridad informática".

- Verdadero
- **Falso**

7. La herramienta *NoScript* se clasifica dentro de:

a. Antivirus.
b. Privacidad y navegación segura.
c. Antirrobo.
d. *Cleaners.*

8. La herramienta *NetGuard* se corresponde con:

a. Cortafuegos.
b. Análisis *online* y *cleaners.*
c. Mantenimiento y limpieza.
d. Antirrobo.

9. ¿Cuál de las siguientes opciones se corresponde con un fallo en un programa o sistema operativo que compromete la seguridad del sistema?

a. Gusano
b. Virus
c. Vulnerabilidad
d. *Exploit*

10. ¿Cuál de las siguientes opciones se refiere a un *software* o aplicación que se caracteriza por que puede replicarse a sí mismo?

a. Gusano
b. Virus
c. Vulnerabilidad
d. *Exploit*