Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. **Señala la medida que no se considera de seguridad:**

    a. Instalar *software legal.*
    b. Usar criptografía.
    c. Ser cuidadosos con la ingeniería social.
    d. No usar sistema de cortafuegos.

2. **Determina si la siguiente oración es verdadera o falsa: "La seguridad informática se fundamenta en tres pilares básicos".**

    - Verdadero
    - **Falso**

3. **Indica cuál de los siguientes no es un pilar básico en la seguridad informática:**

    a. Autentificación
    b. Disponibilidad
    c. Negociación
    d. Integridad

4. **¿Cuál de los siguientes enunciados no puede clasificarse dentro de las medidas de seguridad informática?**

    a. Crear contraseñas complejas y grandes.
    b. Ser cuidadosos con la ingeniería social.
    c. Usar criptografía.
    d. Enviar la documentación sin cifrar.

5. **Determina si la siguiente oración es verdadera o falsa: "Las medidas de seguridad informática se pueden clasificar desde tres puntos de vista".**

    - **Verdadero**
    - Falso

6. Señala cuál de los siguientes no es considerado como un ataque:

a. *Adware*
b. Virus
c. Antivirus
d. *Malware*

7. La capacidad de garantizar que los datos o información no han sido modificados desde su creación sin una autorización correspondiente, se denomina...

a. ... confidencialidad.
b. ... integridad.
c. ... compatibilidad.
d. ... no repudio.

8. El no repudio puede darse en...

a. ... origen.
b. ... destino.
c. ... origen y destino.
d. Todas las opciones son incorrectas.

9. "Se trata de garantizar que la persona que recibe el mensaje, datos o información, no pueda decir que no recibió dicho mensaje". Hablamos de:

a. Disponibilidad.
b. Confidencialidad.
c. Repudio en origen.
d. No repudio en destino.

10. Indica al menos 3 tipos de ataques de entre los siguientes conceptos:

a. Confidencialidad.
b. Virus.
c. Gusanos.
d. Integridad.
e. *Adware.*
f. DDoS.
g. No repudio.

Ejercicios de autoevaluación
Unidad de Aprendizaje 2

1. La ciberseguridad...

a. ... se usa para proteger la información o datos.
b. ... se usa solamente para prevenir ataques.
c. ... normalmente como usuarios no debemos tener en cuenta la ciberseguridad, únicamente las empresas lo contemplan.
d. ... solo nos defiende de virus.

2. "Conocimientos o datos que tienen valor para una organización así como los sistemas de información que engloban a las aplicaciones y servicios", hablamos de:

a. Ciberseguridad.
b. Activos.
c. Activos de información.
d. Seguridad activa.

3. Determina si la siguiente oración es verdadera o falsa: "A mayor nivel de ciberseguridad menor será el riesgo a sufrir".

- **Verdadero**
- Falso

4. Indica cuál de los siguientes no se considera un tipo de ataque:

a. *Sniffers.*
b. *Crackers.*
c. *Lammers.*
d. *Crammers.*

5. Indica cuál de los siguientes no se corresponde con un tipo de ataque:

a. Modificación.
b. Intercepción.
c. Fabricación.
d. Realización.

6. Indica cuál de las siguientes no se considera una amenaza:

a. *Spoofing.*
b. *Sniffing.*
c. *Hacking.*
d. *Malware.*

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

a. *Hardware.*
b. *Software.*
c. Redes.
d. Copias de seguridad.

8. Determina si la siguiente oración es verdadera o falsa: "En función del recurso al que hay que proteger o darle seguridad, esta puede ser activa o pasiva".

- Verdadero
- **Falso**

9. La seguridad física se engloba conjuntamente con:

a. Activa.
b. Pasiva.
c. Física.
d. Lógica.

10. "Protección de activos de información a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información interconectados" es una definición de:

a. ISO 38:2014.
b. ISO 27001.
c. ISO 76001.
d. ISACA.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. **Determina si la siguiente oración es verdadera o falsa: "Un *software* maligno tiene como objetivo principal bloquear un determinado equipo informático para causar un cierto tipo de daño, sin el consentimiento del propietario o dueño del equipo informático".**

   - **Verdadero**
   - Falso

2. **Indica cuál de los siguientes no se considera *malware:***

   a. *Bug*
   b. *Bug Bunny*
   c. *Crakers*
   d. *Ramsonware*

3. **APT se corresponde con:**

   a. Alta profundización técnica
   b. Análisis profundo técnico
   c. Amenazas persistentes y avanzadas
   d. *Amateur Programming Trainning*

4. **Un ATP consta de...**

   a. ... una parte.
   b. ... dos partes.
   c. ... tres partes.
   d. ... cuatro partes.

5. **La tercera parte de un ATP se corresponde con:**

   a. Propagación
   b. Extensión
   c. Estudio de la víctima
   d. Infección

6. Los accesos no autorizados se corresponden con:

a. *Social media marketing*
b. *Email marketing*
c. Ingeniería social
d. Ingeniería *datamining*

7. Determina si la siguiente oración es verdadera o falsa: "Las redes sociales no son un buen escenario para la propagación de malware".

- Verdadero
- **Falso**

8. "Son *software* robotizados cuya apariencia es totalmente normal pero que tienen el fin de ir creando cuentas de correo electrónico en los distintos servidores que las ofrecen de forma gratuita para después desde estas cuentas atacarnos", nos referimos a:

a. Bomba *fork*
b. *Bots*
c. *Bug*
d. Ladilla virtual

9. "Se trata de un software que puede autocopiarse y cuyo fin es la dañar nuestro sistema informático a base de engaños", hablamos de:

a. *Ramsomware*
b. *Crackers*
c. Caballo de Troya
d. *Exploit*

10. "*Software* maligno que busca las claves de acceso y cuentas de correo electrónico para usarlas posteriormente para su propio interés", nos referimos a:

a. Parásito informático
b. *Pharming*
c. *Worms*
d. *Leapfrog*

Ejercicios de autoevaluación
Unidad de Aprendizaje 4

1. **Determina si la siguiente oración es verdadera o falsa: "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. **El dispositivo que adquirimos y que conectamos a internet es:**

   a. *Firewall*
   b. *Proxy*
   c. *Router*
   d. *Smartphone*

3. **El *router* se conecta a internet por el puerto...**

   a. ... LAN.
   b. ... FAN.
   c. ... PAN.
   d. ... WAN.

4. **Para la configuración de los parámetros de seguridad nos conectamos...**

   a. ... externamente al *router* por medio de internet.
   b. ... internamente al *router* por medio de internet.
   c. ... a través de clave con el *router.*
   d. ... por wifi.

5. **Indica cuál suele ser la dirección de acceso a un *router:***

   a. 192.178.X.X
   b. 192.168.X.X
   c. 192.158.X.X
   d. 192.148.X.X

6. **Indica cuál de las siguientes opciones no se corresponde con una configuración mínima:**

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

7. **Indica cuál de las siguientes no se corresponde con la configuración avanzada:**

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

8. **El nombre de la red se conoce por la nomenclatura...**

    a. ... SSID.
    b. ... SIID.
    c. ... DISS.
    d. ... SISD.

9. **Determina si la siguiente oración es verdadera o falsa: "Una red es segura cuando no requiere de contraseña ni de cifrado".**

    - Verdadero
    - **Falso**

10. **Determina si la siguiente oración es verdadera o falsa: "Las redes se cifran para evitar que las terceras personas que acceden a la misma puedan descifrar la información que viaja por ella".**

    - **Verdadero**
    - Falso

Ejercicios de autoevaluación
Unidad de Aprendizaje 5

1. Indica cuál de las siguientes no es una medida de protección:

a. *Spam*
b. Copias de seguridad
c. Protección wifi
d. Limitar acceso a datos

2. Indica cuál de las siguientes no es una medida de protección:

a. Portátiles y *smartphones*
b. Políticas de seguridad
c. *Firewall*
d. *Phishing*

3. Determina si la siguiente oración es verdadera o falsa: "Un control de acceso se usa para impedir el acceso no autorizado al sistema operativo por parte de terceros a los que no les corresponde su uso".

- **Verdadero**
- Falso

4. Indica cuál de las siguientes opciones no se corresponde con control de acceso:

a. Restricciones horarias de conexión cuando no sea necesario.
b. Programar un *software* antivirus y *antimalware.*
c. Registro de privilegios especiales del sistema.
d. Registro de los intentos de autentificación correctos y fallidos en el sistema.

5. Indica cuál de los siguientes no es un permiso:

a. Leer y analizar
b. Colaboración
c. Modificación
d. Edición

6. **Determina si la siguiente oración es verdadera o falsa: "La autentificación es el proceso mediante el cual se confirma que algo o alguien es quien dice ser".**

   - **Verdadero**
   - Falso

7. **Indica cuál de los siguientes no se corresponde con un tipo de acceso:**

   a. Control total
   b. Cambiar
   c. Modificar
   d. Leer

8. **Indica la opción incorrecta:**

   a. Para compartir una impresora no necesitamos el driver correspondiente.
   b. Accedemos a la carpeta impresoras para compartir una impresora.
   c. Es necesario localizar la pestaña de "Compartir".
   d. Es necesario seleccionar "Compartir esta impresora".

9. **Indica cuál de los siguientes elementos no nos protege frente a código malicioso.**

   a. Antivirus
   b. *Antimalware*
   c. *Firewall*
   d. Antivirus *online*

10. **El antivirus es...**

    a. ... parte del sistema operativo.
    b. ... parte del *hardware del ordenador.*
    c. ... *software* específico.
    d. ... un *firmware.*