Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. Indica si las siguientes afirmaciones son verdaderas o falsas:

a. En el teletrabajo deben adoptarse las políticas de seguridad de las empresas.

- **Verdadero**
- Falso

b. El teletrabajo no está considerado una modalidad laboral.

- Verdadero
- **Falso**

c. El teletrabajo requiere de tecnología y telecomunicaciones.

- **Verdadero**
- Falso

2. ¿Cuál de los siguientes elementos puede considerarse activo de información?

a. Datos.
b. Soportes de información.
c. Equipos informáticos.
d. Todas las opciones son correctas.

3. ¿Qué principio de la seguridad de la información garantiza el acceso a la información cuando se requiere?

a. Disponibilidad
b. Integridad
c. Autenticidad
d. Confidencialidad

4. ¿Qué principio de la seguridad de la información garantiza que la información intercambiada entre extremos viaje exacta y completa?

a. Trazabilidad
b. Confidencialidad
c. Autenticidad
d. Integridad

5. ¿A qué hace referencia el concepto de confidencialidad?

a. A aquello que garantiza el análisis de seguridad de los procesos y mecanismos que han facilitado el acceso a la información de cara a detectar y resolver un incidente de seguridad.
b. A aquello que garantiza que la información almacenada o en comunicación no pueda ser accesible por usuarios no autorizados.
c. A aquello que garantiza el control y acceso a la información a usuarios exclusivamente autorizados.
d. Todas las opciones son correctas.

6. ¿En qué año comenzó a regularse legislativamente el teletrabajo?

a. 2018
b. 2019
c. 2020
d. 2021

7. ¿Con qué nombre se reconoce en el ámbito de la ciberseguridad la condición para que un daño pueda materializarse?

a. Amenaza
b. Riesgo
c. Vulnerabilidad
d. Ciberdelito

8. ¿De qué se vale una amenaza para intimidar y comprometer un equipo informático?

a. De un riesgo.
b. De una vulnerabilidad.

c. De un cibercriminal.
d. De una política de seguridad.

9. ¿Qué nombre recibe el tipo de información más comprometida para una empresa?

a. Información restringida.
b. Información interna.
c. Información pública.
d. Información administrativa.

10. ¿Cómo puede infectarse con un *malware* un dispositivo móvil?

a. Con la descarga de algún archivo malicioso.
b. Con el uso inadecuado del correo electrónico.
c. Con el acceso a sitios web no confiables.
d. Todas las opciones son correctas.

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. Indica si las siguientes afirmaciones son verdaderas o falsas:

a. Acceder remotamente a recursos corporativos por medio del teletrabajo añade nuevas oportunidades a los cibercriminales para violar la seguridad de una organización.

- **Verdadero**
- Falso

b. Los dispositivos que son utilizados en el ejercicio del teletrabajo se ven afectados en su seguridad principalmente por el temido *malware*.

- **Verdadero**
- Falso

c. Un *malware* es una herramienta clave para llevar a cabo un ciberataque.

- **Verdadero**
- Falso

2. ¿Qué nombre recibe el virus informático que infecta un equipo a través de un programa con apariencia legítima?

a. Gusano
b. Troyano
c. *Ransomware*
d. RAT

3. ¿Qué tipo de *malware* permite tomar el control total del sistema de información de una víctima?

a. Virus
b. *Exploit*
c. RAT
d. *Cryptojacking*

4. ¿Qué nombre recibe el conjunto de equipos y dispositivos zombis infectados por un *malware?*

a. *Red Adware*
b. *Exploits*
c. *Red Botnet*
d. *Dark web*

5. ¿Qué particularidad caracteriza a los gusanos informáticos?

a. Convierten los equipos infectados en equipos zombis.
b. Contagian a los equipos de forma rápida y automática.
c. Tienen la capacidad de crear *backdoors*.
d. Todas las opciones son correctas.

6. ¿Qué tipo de *software* debe ser prioritario actualizar?

a. *Software* de acceso remoto.
b. *Software* antivirus.
c. *Software* cortafuegos.
d. Todas las opciones son correctas.

7. ¿Qué nombre reciben los dispositivos antihurto que impiden el robo físico de terminales?

a. Credenciales.
b. Contraseñas.
c. Cerraduras de cable.
d. Cerraduras en nube.

8. ¿Para qué sistema operativo es útil la herramienta *AntiBotnet CONAN mobile?*

a. *Linux*
b. *Android*
c. *Windows*
d. *Mac OS*

9. ¿Qué nombre recibe la combinación de artilugios en forma de *hardware* y *software* que proporciona el acceso remoto a una red de equipos y dispositivos llamados clientes?

a. Acceso remoto.
b. Sistema remoto.
c. Dispositivo remoto.
d. Servidor remoto.

10. ¿Con qué iniciales se reconoce a la solución de gestión de dispositivos móviles?

a. MCM
b. UEM
c. MDM
d. MAM