Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación Unidad de Aprendizaje 1

1. **La práctica consistente en la defensa de los equipos informáticos se denomina...**

   a. ... antivirus.
   b. ... ataque.
   c. ... ciberseguridad.
   d. ... recuperación.

2. **Cuando nos referimos a la manipulación de datos hablamos de...**

   a. ... aplicaciones y programas.
   b. ... redes informáticas.
   c. ... seguridad en el almacenamiento.
   d. Todas las opciones son correctas.

3. **La concienciación del personal que compone la organización se incluye dentro de...**

   a. ... formación del usuario final.
   b. ... seguridad de la información.
   c. ... seguridad de las aplicaciones.
   d. ... seguridad del almacenamiento.

4. **Las medidas de seguridad para la protección de la red de sistemas contra intrusos...**

   a. ... incluyen exclusivamente las redes cableadas.
   b. ... incluyen exclusivamente las redes inalámbricas.
   c. ... incluyen las conexiones cableadas e inalámbricas.
   d. Todas las opciones son incorrectas.

5. **El análisis de riesgos debe...**

   a. ... cumplir la normativa vigente de prevención de riesgos.
   b. ... incluirse dentro del plan director de seguridad.

c. ... realizarse juntamente con el nombramiento del personal encargado de la seguridad de los equipos.
d. ... realizarse únicamente en empresas tecnológicas.

6. Dentro de un análisis de riesgos no se encuentra...

a. ... la definición del alcance y las amenazas.
b. ... la definición del personal responsable.
c. ... la evaluación del riesgo.
d. ... el tratamiento de los riesgos detectados.

7. Un riesgo cuyo impacto es alto y una probabilidad media de que suceda lo clasificamos como...

a. ... alto.
b. ... bajo.
c. ... medio.
d. ... muy alto.

8. La mayor parte de los ataques que sufren las empresas son mediante...

a. ... correo electrónico.
b. ... *malware.*
c. ... ventanas emergentes.
d. ... virus informáticos.

9. El ataque en el cual el usuario navega por internet envuelto en una gran cantidad de anuncios es...

a. ... *adware.*
b. ... *malware.*
c. ... *spyware.*
d. ... *troyware.*

10. Los ataques consistentes en obtener la información que se transmite entre equipos son ataques...

a. ... activos.
b. ... de interrupción del servicio.
c. ... de repetición.
d. ... pasivos.

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. Los ciberataques se producen sobre...

a. ... empresas.
b. ... organismos oficiales.
c. ... particulares.
d. Todas las opciones son correctas.

2. Un objetivo de la ciberseguridad se enfoca sobre...

a. ... aplicaciones y programas.
b. ... la integridad de los datos.
c. ... redes informáticas.
d. ... seguridad en el almacenamiento.

3. El objetivo que garantiza que los datos no se han modificado es:

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

4. La definición de ciberseguridad se refiere a...

a. ... las empresas y sus infraestructuras.
b. ... las estrategias y las acciones que se implantan.
c. ... los dispositivos y equipos.
d. Todas las opciones son incorrectas.

5. La mayor parte de las empresas tienen una protección en ciberseguridad...

a. ... gratuita en empresas tecnológicas.
b. ... pasiva.
c. ... reactiva.
d. ... subcontratada en empresas de servicios.

6. ¿Cuál de los siguientes elementos debe cuidar las empresas dentro de la ciberseguridad?

a. El personal con acceso al Departamento Informático.
b. La formación del personal, estableciendo cursos regularmente.
c. El personal que pueda acceder directa o indirectamente a los datos.
d. Las opciones b y c son correctas.

7. La ciberseguridad no beneficia a las empresas en cuanto a su...

a. ... contratación de personal.
b. ... fiabilidad.
c. ... productividad.
d. ... reputación.

8. Si se mantienen los equipos con un nivel de seguridad adecuado, se aumenta...

a. ... el tiempo de trabajo.
b. ... la productividad.
c. ... los costes empresariales.
d. ... los riesgos.

9. El ataque más habitual en los dispositivos móviles es el...

a. ... *criptoware.*
b. ... *phishing.*
c. ... antivirus.
d. ... *spyware.*

10. Un error desde el punto de vista de la ciberseguridad es:

a. No conectarse a redes wifi públicas.
b. Realizar transacciones usando los datos del dispositivo.
c. Realizar transacciones usando redes wifi gratuitas.
d. Usar un antivirus gratuito.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. Se considera un sistema seguro cuando se garantiza...

a. ... la confidencialidad.
b. ... la instalación de un antivirus.
c. ... la recuperación.
d. ... la resistencia a un ataque.

2. La homogeneidad en el uso de los sistemas operativos es...

a. ... un problema porque se puede explotar la misma vulnerabilidad en todos los equipos a la vez.
b. ... una dificultad al personalizar los equipos.
c. ... una ventaja para mantener las redes informáticas.
d. ... una ventaja que dificulta la explotación de una vulnerabilidad.

3. El riesgo que permite el acceso indebido a los sistemas informáticos es...

a. ... de almacenamiento.
b. ... de conexión.
c. ... de *hardware.*
d. ... de *software.*

4. Los caminos elegidos para atacar un equipo se denominan...

a. ... ataques.
b. ... vectores de ataque.
c. ... vulnerabilidades.
d. Todas las opciones son incorrectas.

5. Un consejo para tratar de reducir el impacto de un ciberataque es:

a. Implantar un sistema de acceso informático a la empresa.
b. Implantar una aplicación que guarde las contraseñas de todos los empleados.

c. Implantar una política de contraseñas robustas.
d. Permitir el acceso a la red corporativa desde cualquier red pública.

6. Los ataques que más han aumentado debido al teletrabajo son...

a. ... ataques de fuerza bruta.
b. ... ataques por dispositivos extraíbles.
c. ... correos electrónicos maliciosos.
d. ... explotación de vulnerabilidades.

7. Una etapa que no se encuentra entre las que conforman un ciberataque es:

a. Distribución.
b. Evaluación.
c. Instalación.
d. Reconocimiento.

8. La última etapa de la gestión de los incidentes de ciberseguridad es:

a. Contención
b. Mitigación
c. Posincidente
d. Recuperación

9. Una buena estrategia para realizar copias de seguridad de la información es la que se denomina...

a. ... 3-2-1.
b. ... 2-3-1.
c. ... 1-3-2.
d. ... 1-2-3.

10. El elemento que protege a los equipos contra los ciberataques en primera línea es:

a. El antivirus.
b. El *firewall.*
c. El *malware.*
d. La contraseña del usuario.

Ejercicios de autoevaluación Unidad de Aprendizaje 4

1. Las bases de datos se organizan mediante...

a. ... tablas, filas y columnas.
b. ... tablas, filas, columnas y celdas.
c. ... filas y celdas.
d. ... sistemas alfabéticos o aleatorios.

2. La herramienta que permite detectar amenazas y comportamientos inadecuados es...

a. ... el aprendizaje automático.
b. ... la ciberseguridad.
c. ... la inteligencia artificial.
d. ... los sistemas de *malware*.

3. Entre los ataques que más sufren las empresas se encuentran...

a. ... brechas de seguridad.
b. ... noticias falsas.
c. ... ataques a la cadena de suministro.
d. Todas las opciones son correctas.

4. Los *crackers* informáticos especializados en telefonía se denominan...

a. ... *ciberpunks*.
b. ... *phreakers*.
c. ... criptográficos.
d. ... *lammers*.

5. La acreditación que certifica las capacidades de identificación y evaluación de los riesgos de una organización es:

a. CISM – *(Certified Information Security Manager)*
b. CEH – *(Certified Ethical Hacker)*
c. CRISC – *(Certified in Risk and Information Security Control)*
d. CISSP – *(Certified Information Systems Security Professional)*

6. La ley europea que establece los requisitos y estándares que deben cumplir los productos con componentes digitales es:

a. Ley de Ciberresilencia.
b. Ley de Protección de Datos Digitales.
c. Ley de Sistemas Tecnológicos.
d. Ley de Protección contra la Explotación de Vulnerabilidades.

7. La computación cuántica utiliza como unidad de medida...

a. ... el bit cuántico.
b. ... el qubit.
c. ... el quera.
d. ... el byte cuántico.

8. Una ventaja en el uso de las redes autoadaptables es que...

a. ... solo analizan los datos que emiten los dispositivos.
b. ... realizan una protección reactiva.
c. ... realizan una protección proactiva.
d. ... solo analizan los datos que reciben los dispositivos.

9. El sistema de análisis basado en el comportamiento del usuario se denomina...

a. ... UEBA – análisis de amenazas internas.
b. ... CASB – gestor de seguridad para el acceso *cloud.*
c. ... *shadow IT.*
d. ... inteligencia artificial.

10. Entre los distintos factores de autenticación multifactor se encuentra...

a. ... el de control.
b. ... el de conocimiento.
c. ... el de personalización.
d. ... el de integración.