Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación Unidad de Aprendizaje 1

1. **Indica si las siguientes afirmaciones son verdaderas o falsas. ¿Cuál es la importancia de la ciberseguridad?**

   a. Proteger la información personal y la privacidad.

      - **Verdadero**
      - Falso

   b. Mantener los dispositivos actualizados.

      - **Verdadero**
      - Falso

   c. Evitar ataques cibernéticos.

      - **Verdadero**
      - Falso

2. **Rellena los siguientes huecos:**

   Los sistemas de **control** de accesos a través de **listas** y **registros** son herramientas para **gestionar** y controlar el acceso a **sistemas** informáticos.

3. **¿Qué implica la seguridad activa en la ciberseguridad?**

   a. Prevenir y detectar amenazas en tiempo real.
   b. Realizar copias de seguridad regularmente.
   c. Implementar contraseñas fuertes.
   d. Restringir el acceso solo a usuarios autorizados.

4. **¿Qué implica la seguridad pasiva en la ciberseguridad?**

   a. Realizar análisis de vulnerabilidades periódicos.
   b. Establecer medidas de respuesta y recuperación después de un incidente.
   c. Mantener los dispositivos actualizados.
   d. Implementar un sistema de detección de intrusiones.

5. ¿Cuál es uno de los principios fundamentales de la ciberseguridad?

a. Mantener contraseñas seguras y únicas.
b. Descargar archivos adjuntos desconocidos.
c. Compartir información personal en redes sociales.
d. Utilizar *software* desactualizado.

6. ¿Cuál es el propósito de los registros en la ciberseguridad?

a. Auditar y rastrear la actividad del sistema.
b. Restringir el acceso a recursos específicos.
c. Proteger la información personal.
d. Mantener los dispositivos actualizados.

7. Rellena los siguientes huecos:

El ***phishing*** es una técnica empleada por la ciberdelincuencia en la que se **suplantan** identidades para **sustraer** información personal válida para ejecutar un **ciberataque.**

8. ¿Qué deben hacer los usuarios para protegerse contra ataques de *phishing?*

a. Hacer clic en enlaces desconocidos.
b. Compartir información personal en correos electrónicos.
c. Descargar archivos adjuntos sospechosos.
d. Tener cautela y no proporcionar información personal a fuentes no confiables.

9. ¿Quién es responsable de la ciberseguridad?

a. Solo los expertos en informática.
b. Únicamente los proveedores de servicios de seguridad.
c. Todos los usuarios de sistemas informáticos.
d. El gobierno y las autoridades de seguridad.

10. ¿Cuál de las siguientes opciones NO es un principio de la ciberseguridad?

a. Mantener los dispositivos actualizados.
b. Implementar contraseñas seguras.
c. Compartir información personal en línea.
d. Realizar copias de seguridad de los datos.

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. Indica si las siguientes afirmaciones son verdaderas o falsas. ¿Cuál de las siguientes opciones NO es una amenaza común en internet?

a. *Phishing*

- Verdadero
- **Falso**

b. *Malware*

- Verdadero
- **Falso**

c. *Spam*

- **Verdadero**
- Falso

2. ¿Cuál es el objetivo principal de la evaluación de riesgos en la gestión de la seguridad en internet?

a. Identificar amenazas comunes.
b. Evaluar la probabilidad de ocurrencia de riesgos.
c. Implementar medidas de seguridad.
d. Cumplir con normativas internacionales.

3. ¿Cuál de las siguientes no es una medida de seguridad recomendada para proteger la información y los sistemas en internet?

a. Uso de contraseñas fuertes y únicas.
b. Instalación de *software* antivirus.
c. Descargar archivos adjuntos de fuentes desconocidas.
d. Implementación de actualizaciones de seguridad.

4. Rellena los siguientes huecos:

El concepto **"impacto"** hace referencia a las **consecuencias** que tendría la **materialización** de un **riesgo** en términos de daño o pérdida.

5. ¿Cuál es el objetivo principal de la Norma ISO 27001?

a. Establecer pautas para la gestión de la seguridad en internet.
b. Proteger los datos personales de los usuarios en línea.
c. Regular el uso de criptomonedas en transacciones comerciales.
d. Promover el uso responsable de las redes sociales.

6. ¿Qué requieren los riesgos cibernéticos con una alta probabilidad y un impacto significativo?

a. Utilizar un estándar de seguridad.
b. Evitar intervenir de forma inmediata.
c. Implementación de medidas de mitigación básicas.
d. Una atención inmediata e implementación de medidas de mitigación.

7. ¿Cuál es una de las ventajas de utilizar la autenticación de dos factores (2FA)?

a. Proporciona anonimato en las transacciones en línea.
b. Permite rastrear y capturar a los delincuentes cibernéticos.
c. Agrega una capa adicional de seguridad al requerir un código de verificación único.
d. Reduce la necesidad de realizar copias de seguridad regulares.

8. ¿Cuál es uno de los principales beneficios de seguir las directrices de seguridad de la Norma ISO 27001?

a. Aumento de la velocidad de conexión a internet.
b. Cumplimiento de las regulaciones gubernamentales.
c. Obtención de descuentos en la compra de criptomonedas.
d. Mejora de la protección de la información y los sistemas en línea.

9. ¿Qué tipo de información confidencial podría obtener un atacante a través de un ataque de *phishing?*

a. Nombres de usuarios y contraseñas
b. Historial de navegación en internet

c. Números de tarjetas de crédito de los clientes
d. Ubicación geográfica del dispositivo

10. Rellena los siguientes huecos:

Una medida de **seguridad** efectiva para **proteger** un sitio web de posibles ataques de fuerza **bruta** es el implementar un sistema de **autenticación** de dos factores.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

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

a. En la actual era digital, internet se ha convertido en una herramienta esencial en la vida de las personas facilitando el acceso a una amplia gama de información y servicios. Sin embargo, junto con los beneficios que ofrece, también surgen riesgos y desafíos relacionados con la seguridad y la veracidad de la información *online*.

- **Verdadero**
- Falso

b. Es transcendental la implementación de estrategias formativas y el suministro de recursos accesibles que busquen empoderar a las personas usuarias en el uso seguro de internet.

- **Verdadero**
- Falso

c. En un mundo digital saturado de datos y contenidos, es esencial que las personas usuarias adquieran las habilidades necesarias para discernir entre información confiable y engañosa.

- **Verdadero**
- Falso

2. ¿Cuál de los siguientes es un peligro común en internet relacionado con la ciberseguridad?

a. *Phishing*
b. Información
c. Consumo de internet
d. Todas las opciones son incorrectas.

3. ¿Qué medida preventiva ayuda a protegerse contra el *malware* en línea?

a. Compartir información personal en redes sociales.
b. Mantener el *software* actualizado.

c. Hacer clic en cualquier enlace.
d. Usar contraseñas débiles.

4. Rellena los siguientes huecos:

La capacidad de **evaluar** y analizar de forma **crítica** la información *online* es fundamental para garantizar un uso seguro y **responsable** de internet. En un mundo digital saturado de **datos** y contenidos, es esencial que las personas usuarias adquieran las habilidades necesarias para **discernir** entre información confiable y **engañosa.**

5. ¿Cuál es una forma efectiva de evitar caer en un ataque de *phishing?*

a. No compartir información personal en línea.
b. Validar la autenticidad de correos electrónicos y enlaces antes de hacer clic.
c. Usar la misma contraseña para todas las cuentas.
d. Abrir archivos adjuntos de correos electrónicos desconocidos.

6. ¿Qué significa evaluar críticamente la información *online?*

a. Creer en todo lo que se lee en internet.
b. Analizar y cuestionar la información antes de aceptarla como verdadera.
c. Compartir sin verificar la información en las redes sociales.
d. Ignorar por completo la información en línea.

7. ¿Cuál de las siguientes acciones ayuda a evaluar la credibilidad de una fuente en línea?

a. No verificar la información en diferentes fuentes.
b. Compartir la información sin cuestionar su veracidad.
c. Revisar la reputación y credibilidad de la fuente.
d. No prestar atención a los errores gramaticales o de ortografía.

8. ¿Por qué es importante considerar el contexto al evaluar información en línea?

a. El contexto no tiene relevancia en la evaluación de la información.
b. El contexto proporciona información adicional para evaluar la veracidad de la información.
c. El contexto no afecta la comprensión de la información.
d. El contexto solo es importante en situaciones *offline*.

9. ¿Cuál es un indicador de que una fuente de información en línea puede no ser confiable?

a. Citación de fuentes reconocidas y estudios.
b. Coherencia y consistencia en la información presentada.
c. Ausencia de errores gramaticales o de ortografía.
d. Uso excesivo de lenguaje técnico sin explicación clara.

10. ¿Por qué es importante cuestionar la información en línea antes de aceptarla como verdadera?

a. La información en línea siempre es confiable y precisa.
b. La información en línea puede contener errores y ser engañosa.
c. No es necesario cuestionar la información en línea.
d. Cuestionar la información puede llevar mucho tiempo y esfuerzo.

Ejercicios de autoevaluación Unidad de Aprendizaje 4

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

a. En el actual paradigma digital, donde la información se ha convertido en uno de los activos más valiosos, la protección de datos personales no tiene por qué ser crucial para salvaguardar la privacidad y los derechos de las personas.

- Verdadero
- **Falso**

b. En España, al igual que en muchos otros países, se han establecido normativas y regulaciones específicas para garantizar la protección de datos y regular su uso adecuado.

- **Verdadero**
- Falso

2. Rellena los siguientes huecos:

La **ciberseguridad** hace referencia a la **protección** de los sistemas **informáticos,** redes y datos frente a **amenazas** cibernéticas, como ataques de ***hackers*** no éticos, *malware* y robo de **información.** La gestión **efectiva** de la ciberseguridad implica no solo la implementación de medidas técnicas y tecnológicas, sino también la comprensión de los aspectos **legales,** regulatorios y éticos relacionados con la protección de **datos.**

3. ¿Qué es la LOPDGDD?

a. Una normativa fuera del marco europeo
b. Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
c. El Reglamento General de Protección de Datos (RGPD) de la Unión Europea
d. Todas las opciones son incorrectas.

4. ¿Qué objetivo común comparten la LOPDGDD y el RGPD?

a. Proteger los derechos fundamentales de los individuos en relación con el tratamiento de sus datos personales, aunque no establecen mecanismos para garantizar la transparencia, la seguridad y la privacidad.
b. Proteger los derechos fundamentales de los individuos en relación con el tratamiento de sus datos personales y establecer mecanismos para garantizar la transparencia, la seguridad y la privacidad.
c. Exclusivamente establecer mecanismos para garantizar la transparencia, la seguridad y la privacidad.
d. Exclusivamente proteger los derechos fundamentales de los individuos en relación con el tratamiento de sus datos personales.

5. ¿Cuál de los siguientes enunciados no es acorde a la LOPDGDD?

a. Establece los conceptos clave en relación con los datos personales y los divide en diferentes categorías, como datos especialmente protegidos (religión, orientación sexual, origen étnico, etc.) y datos de menores.
b. Enfatiza la importancia del consentimiento del titular de los datos como base legal para el tratamiento de los mismos.
c. Otorga a los individuos una serie de derechos, como el derecho de acceso, rectificación, supresión, oposición y portabilidad de sus datos personales.
d. Impone una serie de obligaciones a las organizaciones que tratan datos personales, como implementar medidas de seguridad adecuadas, notificar las brechas de seguridad, designar un Delegado de Protección de Datos (DPD) en todos los casos y llevar registros de las actividades de tratamiento.

6. ¿Cuál es uno de los aspectos clave del alcance del Reglamento General de Protección de Datos (RGPD) de la Unión Europea?

a. Aplica solo a organizaciones ubicadas dentro de la Unión Europea.
b. Aplica solo a organizaciones que procesan datos personales de ciudadanos europeos.

c. Aplica extraterritorialmente a todas las organizaciones que procesan datos personales de individuos residentes en la Unión Europea, independientemente de su ubicación geográfica.
d. Aplica solo a organizaciones que procesan datos personales en el ámbito de la salud.

7. ¿Cuál de los siguientes principios rectores es establecido por el RGPD?

a. Principio de transparencia
b. Principio de retención de datos
c. Principio de responsabilidad proactiva
d. Principio de anonimización

8. ¿Cuáles son las posibles sanciones y multas establecidas por el RGPD en caso de incumplimiento?

a. Multas que ascienden al 1 % de la facturación anual global de una organización.
b. Multas que ascienden al 4 % de la facturación anual global de una organización o 20 millones de €, según el importe que resulte mayor.
c. Multas que ascienden al 10 % de la facturación anual global de una organización.
d. No se establecen sanciones o multas por incumplimiento.

9. ¿Qué implica el principio ético de respetar la confidencialidad de la información en el manejo de datos personales?

a. Compartir la información con terceros no autorizados.
b. Implementar medidas de seguridad adecuadas y asegurarse de que no se divulgue a terceros no autorizados.
c. Utilizar la información para fines no autorizados.
d. No tomar medidas de seguridad para proteger la privacidad de los individuos.

10. ¿Qué implica el principio ético de garantizar la privacidad de los individuos en el tratamiento de datos personales?

a. Recopilar la máxima cantidad de datos posible.
b. No obtener el consentimiento informado de los individuos antes de recopilar sus datos.
c. No implementar medidas de seguridad adecuadas para proteger los datos personales.
d. Limitar la recopilación de datos al mínimo necesario y permitir que los individuos ejerzan sus derechos de privacidad.

Ejercicios de autoevaluación Unidad de Aprendizaje 5

1. Indica si las siguientes oraciones son verdaderas o falsas.

a. Un *ransomware* es un tipo de ciberdelito empleado por la ciberdelincuencia que bloquea archivos y sistemas usando un código malicioso.

- **Verdadero**
- Falso

b. La técnica comúnmente utilizada para propagar el *ransomware* es mediante las actualizaciones automáticas de sistemas operativos.

- Verdadero
- **Falso**

2. Rellena los siguientes huecos:

Un **ciberdelito** se refiere a cualquier actividad **delictiva** que se lleva a cabo en el ciberespacio o mediante el **uso** de tecnologías de la **información** y la comunicación. Estos delitos implican el uso **ilegal** o no autorizado de sistemas **informáticos, redes** y dispositivos **electrónicos** para cometer actos ilegales, causar daño u obtener beneficios **ilícitos.**

3. ¿Qué es la ingeniería social?

a. Una técnica de encriptación de datos.
b. Un tipo de ataque cibernético.
c. El estudio de la interacción humana en línea.
d. Una táctica de manipulación y engaño para obtener información confidencial.

4. ¿Cuál es el objetivo del *ransomware?*

a. Acceder a sistemas informáticos de manera legítima.
b. Proporcionar seguridad adicional a los archivos.
c. Bloquear el acceso a archivos o sistemas y exigir un rescate.
d. Difundir información falsa en línea.

5. ¿Cuál de las siguientes opciones es una medida de seguridad proactiva contra el *ransomware*?

a. Mantener actualizado el *software* de seguridad.
b. Compartir contraseñas con personas de confianza.
c. Abrir correos electrónicos de remitentes desconocidos sin precaución.
d. Descargar archivos adjuntos de fuentes no verificadas.

6. ¿Cuál es la técnica más común utilizada para propagar el *ransomware* a través de correos electrónicos?

a. Suplantación de identidad.
b. Encriptación de archivos.
c. Uso de archivos adjuntos maliciosos.
d. Utilización de enlaces fraudulentos.

7. ¿Cuál es el objetivo principal de la ingeniería social en relación con el *ransomware*?

a. Proteger la información personal.
b. Obtener acceso no autorizado a sistemas informáticos.
c. Proporcionar medidas de seguridad adicionales.
d. Manipular a las personas para revelar información confidencial.

8. ¿Cuál es una de las consecuencias comunes del *ransomware* para las víctimas?

a. Actualización automática de sistemas operativos.
b. Pérdida de datos importantes.
c. Incremento de la velocidad de conexión a internet.
d. Mayor protección contra ataques cibernéticos.

9. ¿Por qué es importante comprender el funcionamiento y las técnicas de propagación del *ransomware*?

a. Para evitar actualizaciones automáticas del sistema.
b. Para mejorar la velocidad de conexión a internet.
c. Para prevenir y mitigar ataques de *ransomware*.
d. Para compartir información personal con terceros.

10. ¿Cuál es el objetivo principal de los ciberdelincuentes detrás del ciberdelito con *ransomware*?

a. Proteger la información confidencial.
b. Ayudar a las víctimas a recuperar sus datos.
c. Obtener beneficios económicos a través del rescate.
d. Promover la seguridad cibernética en la sociedad.

Ejercicios de autoevaluación Unidad de Aprendizaje 6

1. Indica si las siguientes oraciones son verdaderas o falsas.

a. La ciberseguridad personal es una necesidad cada vez más apremiante, ya que los delincuentes cibernéticos buscan constantemente aprovechar las vulnerabilidades para acceder a nuestra información personal, financiera y confidencial.

- **Verdadero**
- Falso

b. A medida que aumenta nuestra interacción con el mundo digital a través de los dispositivos móviles, los intrusos y delincuentes cibernéticos encuentran mayores dificultades para acceder a la información personal y realizar actividades maliciosas.

- Verdadero
- **Falso**

2. ¿Cuál de las siguientes medidas está recomendada para protegerse del ingreso de intrusos en dispositivos móviles?

a. Actualizar regularmente el *software* y las contraseñas.
b. Compartir información personal en redes sociales.
c. Descargar aplicaciones de fuentes no confiables.
d. Utilizar contraseñas débiles.

3. ¿Qué es una red privada virtual (VPN)?

a. Una red inalámbrica segura para uso público.
b. Un programa antivirus para dispositivos móviles.
c. Un método para cifrar y proteger la conexión a internet.
d. Una técnica de *phishing* para robar contraseñas.

4. ¿Cuál es uno de los riesgos asociados con el uso de redes wifi públicas no seguras?

a. Mayor velocidad de conexión.
b. Acceso seguro a información confidencial.
c. Interceptación de datos por parte de intrusos.
d. Reducción de la exposición a ciberataques.

5. ¿Por qué es importante limitar la concesión de permisos a las aplicaciones instaladas en dispositivos móviles?

a. Para mejorar la velocidad de las aplicaciones.
b. Para ahorrar espacio en el dispositivo.
c. Para evitar que las aplicaciones accedan a información confidencial innecesaria.
d. Para facilitar la instalación de nuevas aplicaciones.

6. ¿Qué medida es recomendada al utilizar redes wifi públicas?

a. Realizar transacciones financieras sin precaución.
b. Desactivar las actualizaciones automáticas del dispositivo.
c. Utilizar una red privada virtual (VPN).
d. Compartir contraseñas con amigos cercanos.

7. ¿Qué es el *sniffing* de red en el contexto de la ciberseguridad?

a. Una técnica para proteger los datos de los usuarios en redes wifi.
b. Un tipo de ataque que intercepta y analiza el tráfico de red.
c. Una forma de garantizar la velocidad de conexión en redes públicas.
d. Un proceso de actualización del *software* de seguridad.

8. ¿Cuál es una buena práctica para proteger la información personal en línea?

a. Compartir contraseñas con familiares cercanos.
b. Configurar opciones de privacidad adecuadas en redes sociales.

c. Descargar aplicaciones de cualquier fuente sin verificar su confiabilidad.
d. Utilizar contraseñas cortas y fáciles de recordar.

9. ¿Cuál es una medida recomendada para protegerse contra la ciberdelincuencia en dispositivos móviles?

a. No realizar actualizaciones del sistema operativo.
b. Compartir información personal en correos electrónicos no seguros.
c. Utilizar *software* antivirus y *antimalware* actualizado.
d. Descargar aplicaciones de sitios webs desconocidos.

10. ¿Por qué es importante cambiar regularmente las contraseñas de nuestras cuentas digitales?

a. Para olvidarlas y dificultar el acceso a nuestras cuentas.
b. Para reducir la velocidad de inicio de sesión.
c. Para evitar el uso de contraseñas obvias o fáciles de adivinar.
d. Para facilitar el acceso de intrusos a nuestras cuentas.

Ejercicios de autoevaluación Unidad de Aprendizaje 7

1. Indica si las siguientes oraciones son verdaderas o falsas.

a. En el campo de la ciberseguridad, el conocimiento y entendimiento de las interconexiones y dependencias entre los diferentes elementos de los sistemas y redes digitales es fundamental para garantizar su protección lo suficientemente efectiva.

- **Verdadero**
- Falso

b. La teoría de nodos y lazos, también conocida como teoría de redes, es un enfoque conceptual y analítico que se utiliza para estudiar las relaciones y conexiones entre diferentes elementos en un sistema o una red.

- **Verdadero**
- Falso

2. ¿Qué representa un nodo en la teoría de nodos y lazos?

a. Un ataque cibernético
b. Un elemento individual en un sistema o red
c. Un protocolo de seguridad
d. Un programa antivirus

3. ¿Qué representa un lazo en la teoría de nodos y lazos?

a. Un enlace físico en una red
b. Un tipo de *malware*
c. Un sistema de cifrado
d. Una contraseña segura

4. ¿Cuál es uno de los objetivos principales de la teoría de nodos y lazos en ciberseguridad?

a. Comprender la estructura de las páginas web.
b. Identificar patrones de tráfico sospechoso en internet.

c. Analizar las dependencias y las interconexiones en sistemas y redes.
d. Detectar virus en archivos adjuntos de correo electrónico.

5. ¿Por qué es importante comprender las interconexiones y dependencias en ciberseguridad?

a. Para diseñar aplicaciones móviles seguras.
b. Para identificar a los piratas informáticos.
c. Para mitigar amenazas cibernéticas y proteger los sistemas.
d. Para rastrear la ubicación física de los servidores.

6. ¿Qué implica la propagación de amenazas a través de los lazos en la teoría de nodos y lazos?

a. La transmisión de *malware* a través de dispositivos móviles.
b. El acceso no autorizado a servidores.
c. La creación de nuevas conexiones de red.
d. La afectación de nodos adicionales en una red.

7. ¿Cómo puede contribuir la teoría de nodos y lazos a la detección de amenazas cibernéticas?

a. Ayudando a identificar vulnerabilidades en sistemas operativos.
b. Proporcionando soluciones de *firewall* más avanzadas.
c. Permitiendo el análisis de patrones de comportamiento anómalo.
d. Facilitando el acceso a bases de datos de *malware* conocidos.

8. ¿Qué significa la resiliencia en el contexto de la ciberseguridad?

a. La capacidad de recuperación después de un ataque cibernético.
b. La velocidad de la conexión a internet.
c. El grado de seguridad de una contraseña.
d. La ubicación geográfica de los servidores.

9. ¿Qué se puede lograr mediante la visualización de redes en ciberseguridad?

a. La detección de *phishing* en correos electrónicos.
b. La identificación de enlaces fraudulentos en páginas web.
c. La comprensión de las interconexiones y dependencias en un sistema.
d. El bloqueo de anuncios emergentes en el navegador.

10. Rellena los siguientes huecos:

La reducción del riesgo de propagación de **amenazas** es uno de los beneficios de la **segmentación** de red en ciberseguridad. Al mismo tiempo, es posible decir que para prevenir la **propagación** de *malware* es importante mantener los nodos **actualizados** como **medida** de ciberseguridad.