Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

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

a. Un activo de información puede ser tanto un dato como una persona o un sistema que lo gestiona.

- **Verdadero**
- Falso

b. Una amenaza por sí sola siempre genera un incidente de seguridad.

- Verdadero
- **Falso**

2. ¿Qué es un activo de información?

a. Un *software* antivirus
b. Cualquier recurso que contiene, procesa o gestiona información relevante
c. Un tipo de amenaza informática
d. Un sistema de copia de seguridad

3. ¿Cuál de los siguientes es un ejemplo de activo humano?

a. Un servidor en la nube
b. Una base de datos
c. Un técnico que gestiona sistemas
d. Un sistema de almacenamiento

4. ¿Qué se entiende por amenaza en seguridad de la información?

a. Una herramienta de protección
b. Una debilidad del sistema
c. Un evento que puede causar daño a la información
d. Un procedimiento interno

5. ¿Cuál de las siguientes situaciones representa una amenaza humana accidental?

a. Un ataque informático planificado
b. Un empleado que elimina archivos por error
c. Un *malware* instalado intencionadamente
d. Un robo de datos organizado

6. ¿Qué es una vulnerabilidad?

a. Un tipo de ataque
b. Una medida de protección
c. Una debilidad que puede ser explotada
d. Un sistema de seguridad

7. ¿Cuál de las siguientes opciones es una vulnerabilidad habitual en empresas?

a. Uso de cifrado de datos
b. Contraseñas robustas
c. Sistemas sin actualizar
d. Formación en seguridad

8. ¿Cuándo se produce un riesgo en seguridad de la información?

a. Cuando existe un activo
b. Cuando hay una amenaza únicamente
c. Cuando una amenaza aprovecha una vulnerabilidad sobre un activo
d. Cuando se instala un antivirus

9. ¿Cuál es la primera fase del análisis de riesgos?

a. Evaluación del impacto
b. Identificación de activos
c. Aplicación de medidas
d. Eliminación de amenazas

10. ¿Qué tipo de riesgo se produce cuando no existen normas claras en la empresa?

a. Riesgo tecnológico
b. Riesgo humano
c. Riesgo organizativo
d. Riesgo ambiental

Ejercicios de autoevaluación
Unidad de Aprendizaje 2

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

a. La Norma ISO 27001 es un estándar internacional orientado a la gestión de la seguridad de la información.

- **Verdadero**
- Falso

b. Un Sistema de Gestión de Seguridad de la Información consiste únicamente en aplicar herramientas tecnológicas de protección.

- Verdadero
- **Falso**

c. La certificación ISO 27001 se obtiene sin necesidad de auditoría externa.

- Verdadero
- **Falso**

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

a. Proteger únicamente los sistemas informáticos
b. Gestionar la seguridad de la información de forma organizada
c. Evitar cualquier tipo de ciberataque
d. Eliminar todos los riesgos de seguridad

3. ¿Qué es un Sistema de Gestión de Seguridad de la Información (SGSI)?

a. Un *software* de protección de datos
b. Un conjunto de herramientas tecnológicas
c. Un conjunto de políticas, procesos y controles para proteger la información
d. Un sistema de copias de seguridad

4. ¿Cuál de los siguientes NO es un principio de la seguridad de la información?

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

5. ¿Qué garantiza la confidencialidad?

a. Que la información esté siempre disponible
b. Que la información no se pierda
c. Que solo accedan personas autorizadas
d. Que los datos sean correctos

6. ¿Qué fase del ciclo PDCA implica aplicar medidas de seguridad?

a. Planificar
b. Hacer
c. Verificar
d. Actuar

7. ¿Qué se revisa en la fase de "Check" del SGSI?

a. La política de seguridad
b. Los recursos económicos
c. El funcionamiento del sistema y sus resultados
d. Los contratos de la empresa

8. ¿Cuál es el ámbito de aplicación de un SGSI?

a. Las herramientas de seguridad utilizadas
b. Los límites y el alcance del sistema de seguridad
c. El presupuesto de la empresa
d. El número de empleados

9. ¿Qué elemento es necesario para obtener la certificación ISO 27001?

a. Tener antivirus instalado
b. Contar con un departamento de informática
c. Superar una auditoría realizada por una entidad certificadora
d. Utilizar *software* específico

10. ¿Qué aporta la certificación ISO 27001 a una empresa?

a. Reduce los costes automáticamente
b. Elimina todos los riesgos
c. Mejora la confianza y la gestión de la seguridad
d. Sustituye a las leyes de protección de datos

Ejercicios de autoevaluación Unidad de Aprendizaje 3

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

a. Una política de seguridad define únicamente medidas técnicas como antivirus o cifrado.

- Verdadero
- **Falso**

b. Las políticas de seguridad ayudan a orientar el comportamiento de las personas dentro de la organización.

- **Verdadero**
- Falso

2. ¿Cuál es la función principal de una política de seguridad de la información?

a. Proteger únicamente los sistemas informáticos.
b. Establecer normas, responsabilidades y directrices para proteger la información.
c. Sustituir las herramientas de seguridad.
d. Reducir los costes operativos.

3. ¿Cuál de los siguientes elementos forma parte de una política de seguridad?

a. Instalación de antivirus.
b. Objetivos de seguridad.
c. Copias de seguridad automáticas.
d. Uso de *firewall*.

4. ¿Qué protege una política de seguridad de la información?

a. Solo la tecnología.
b. Tecnología, personas y procesos.
c. Únicamente los datos digitales.
d. Solo los sistemas informáticos.

5. ¿Qué significa que una política sea holística?

a. Que solo protege los sistemas informáticos.
b. Que cubre todos los ámbitos de la organización.
c. Que se aplica solo en situaciones de crisis.
d. Que se centra únicamente en las personas.

6. ¿Cuál es la diferencia entre política y medida de seguridad?

a. No existe diferencia.
b. La política define el marco y las medidas lo aplican.
c. Las medidas definen objetivos y la política los ejecuta.
d. La política es técnica y las medidas son organizativas.

7. ¿Cuál de las siguientes características define una política eficaz?

a. Compleja y difícil de aplicar.
b. Copiada de otras empresas.
c. Adaptada a la realidad de la organización.
d. Centrada únicamente en la tecnología.

8. ¿Qué elemento permite comprobar si una política se está cumpliendo?

a. Las normas básicas.
b. Los objetivos de seguridad.
c. Los sistemas de control y seguimiento.
d. Las responsabilidades del personal.

9. ¿Qué ocurre si una empresa aplica medidas sin una política de seguridad?

a. Mejora automáticamente su seguridad.
b. La seguridad será desorganizada.
c. No afecta a la seguridad.
d. Se eliminan todos los riesgos.

10. ¿Qué implica que cada medida tenga un responsable asignado?

a. Que no es necesario supervisarla.
b. Que se garantiza su correcta aplicación y seguimiento.
c. Que solo la dirección debe aplicarla.
d. Que deja de ser una medida técnica.

Ejercicios de autoevaluación
Unidad de Aprendizaje 4

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

a. Los datos personales solo incluyen información como el nombre o el DNI.

- Verdadero
- **Falso**

b. El RGPD es una norma de aplicación directa en todos los países de la Unión Europea.

- **Verdadero**
- Falso

c. La protección de datos depende únicamente de las herramientas tecnológicas utilizadas por la empresa.

- Verdadero
- **Falso**

2. ¿Cuál de las siguientes situaciones implica tratamiento de datos personales?

a. Guardar documentos sin identificar.
b. Registrar direcciones IP de usuarios en una web.
c. Instalar un programa sin conexión.
d. Utilizar equipos sin acceso a internet.

3. ¿Qué elemento permite demostrar que una empresa cumple con el principio de responsabilidad proactiva?

a. Tener antivirus instalado.
b. Documentar los tratamientos de datos y aplicar controles.
c. Reducir el número de empleados.
d. Usar únicamente contraseñas.

4. ¿Cuál de los siguientes casos representa un uso indebido de datos?

a. Almacenar datos cifrados.
b. Solicitar consentimiento informado.
c. Utilizar datos de clientes para fines distintos a los autorizados.
d. Actualizar información del usuario.

5. ¿Qué característica tienen los datos especialmente protegidos?

a. Son datos públicos.
b. No requieren medidas de seguridad.
c. Solo se usan en *marketing*.
d. Requieren un nivel de protección más elevado.

6. ¿Qué ocurre si una empresa no responde a una solicitud de derechos de un usuario?

a. No tiene consecuencias.
b. Solo afecta internamente.
c. Puede enfrentarse a sanciones y pérdida de confianza.
d. Se elimina automáticamente la solicitud.

7. ¿Qué herramienta permite identificar qué datos se tratan y con qué finalidad en una empresa?

a. Antivirus.
b. *Firewall*.
c. Copia de seguridad.
d. Registro de Actividades de Tratamiento.

8. ¿Cuál es una medida organizativa para proteger los datos personales?

a. Instalar *software*.
b. Usar cifrado.
c. Formar a los empleados en protección de datos.
d. Cambiar dispositivos.

9. ¿Qué aspecto es clave para limitar el acceso a la información dentro de una organización?

a. Compartir todos los datos.
b. Eliminar registros antiguos.
c. Usar redes sociales.
d. Asignar permisos según funciones y responsabilidades.

10. ¿Qué papel desempeña la Agencia Española de Protección de Datos (AEPD)?

a. Gestionar redes informáticas.
b. Crear *software* de seguridad.
c. Controlar el acceso a internet.
d. Supervisar y garantizar el cumplimiento de la normativa de protección de datos.