Ejercicios de repaso y autoevaluación

1. Indique qué normativa ISO se corresponde con las siguientes definiciones:

iso 27002

a. Estándar para la seguridad de la información (también se considera una guía de buenas prácticas) en la que se incluyen los distintos objetivos de control y controles recomendados para mantener un nivel de seguridad de la información óptimo.

iso 27000

b. Manual de buenas prácticas que incluye fundamentalmente el vocabulario que se va a utilizar en las normas incluidas en toda la serie para una mayor comprensión de las mismas.

iso /iec 27001

c. Manual de buenas prácticas en el que se incluyen los requisitos necesarios de los sistemas de gestión de seguridad de la información.

2. ¿Cuál de las siguientes secciones no forma parte de la norma ISO/IEC 27002?

a. Política de seguridad.
b. Gestión de archivos.
c. Seguridad física y del entorno.
d. Política de privacidad.

3. Relacione las siguientes definiciones con los conceptos que se describen a continuación:

a. Evento o serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.
b. Cualquier sistema, servicio o infraestructura de procesamiento de la información.
c. Preservación de la confidencialidad, integración y disponibilidad de la información. También puede involucrar otras propiedades como la autenticidad, responsabilidad, no repudiación y confiabilidad.

c __ Seguridad de la información.
a __ Incidente de la seguridad de la información.
b __ Medios de procesamiento de la información.

4. ¿Qué diferencias fundamentales hay entre análisis del riesgo, evaluación del riesgo y tratamiento del riesgo? Descríbalas.

Análisis de riesgo: Se enfoca en identificar y comprender los riesgos.

Evaluación de riesgo: Es la valoración y comparación de los riesgos identificados

Tratamiento de riesgo: Se centra en la respuesta a los riesgos evaluados.

En resumen, el análisis identifica, la evaluación prioriza y el tratamiento actúa.

5. Complete la siguiente fase:

El objetivo del apartado de gestión de activo seguridad de la norma ISO/27002 es conseguir y mantener una protección adecuada de los activos de la organización (la información es considerada un activo principal de esta). Para ello, es necesario realizar un control de todos los activos de la organización.

intangible

inventario

6. El ciclo de vida del servicio está compuesto por una serie de fases. ¿Cuántas fases son y qué nombre tienen? Menciónelas por orden.

Etapa 1: Creación de datos Etapa 2: Almacenamiento y organización Etapa 3: Procesamiento y análisis

Etapa 4: Distribución y acceso Etapa 5: Retención y copia de seguridad

Etapa 6: Archivado y gestión de datos históricos Etapa 7: Eliminación segura

Estrategia, Diseño, transicion, operacion y mejora continua del servicio

7. Indique a qué fase del ciclo de vida del servicio corresponde la siguiente definición: "Fase en la que se define el servicio que se va a prestar, la tipología de clientes a la que se va a destinar y en qué mercados se va a prestar".

Estrategia

8. De la nueva LOPDGDD, ¿qué significan las siglas "GDD"?

a. Garantía de Derechos Digitales.
b. Gestión Datos Directos.
c. Garantía de Derechos de Datos.
d. Todas las opciones son incorrectas.

9. Según la LOPDGDD, ¿quién es el responsable del tratamiento?

El responsable del tratamiento de datos es la persona física, jurídica, autoridad pública, servicio u otro organismo que determina los fines y medios del tratamiento de datos personales

10. Encuentre en la siguiente sopa de letras los derechos de las personas sobre sus datos personales reconocidos en la LOPDGDD.

R	E	C	T	I	F	I	C	A	C	I	O	N
A	B	C	E	Z	I	O	L	C	Z	A	N	I
A	C	O	S	R	L	J	P	C	O	N	A	L
S	E	T	O	S	I	E	Y	E	S	R	T	A
U	S	A	C	I	M	I	A	S	O	N	A	R
P	O	P	O	S	I	C	I	O	N	A	R	T
R	U	E	R	A	T	I	C	O	L	A	E	M
E	P	O	R	T	A	B	I	L	I	D	A	D
S	A	L	U	R	C	O	R	E	A	S	T	E
I	C	A	S	C	I	O	N	A	R	E	A	R
O	H	C	U	L	O	R	Y	E	R	T	O	S
N	I	M	R	A	N	A	M	A	R	E	R	O

11. Indique cuál de las opciones tiene un dato incorrecto (selección múltiple).

a. Los soportes y documentos que contengan datos personales no deben estar identificados e inventariados.
b. Conservar los datos de acceso registrados durante, por lo menos, 10 años.
c. Registrar al menos algún procedimiento realizado de recuperación de datos en el registro de incidencias.
d. Cada 2 años, el responsable del fichero debe verificar la correcta definición, funcionamiento y aplicación de los procedimientos de copias de seguridad y de recuperación de datos.

12. ¿Cuáles de las siguientes funciones son responsabilidad de la Agencia Española de Protección de Datos (AEPD)?

a. Controlar a los agentes implicados en el tratamiento de los datos.
b. Asesorar a otras instituciones y organismos sobre las medidas legislativas y administrativas.
c. Velar por la publicidad de los datos.
d. Ejercer la potestad sancionadora.

13. Complete la siguiente tabla de infracciones y sanciones que aplica la AEPD:

Tipo de infracción	Sanción	Prescripción
Leve	hasta 40.000 €	1 año
Grave	hasta 300.000 €	2 Años
Muy grave	desde 300.001 €	3 Años

14. En la norma ISO/IEC 27002 hay un capítulo dedicado a las medidas de seguridad física y del entorno, divididas estas en dos partes: medidas para áreas seguras y medidas para la seguridad de los equipos. De las siguientes medidas, indique si corresponden a áreas seguras o a la seguridad de los equipos:

a. Controles físicos de entrada. Areas
b. Seguridad del cableado. Equipos
c. Servicios públicos de soporte. Equipos
d. Protección contra amenazas externas e internas. Areas

15. Complete la siguiente frase sobre las medidas de seguridad física del mantenimiento de los equipos:

integridad

Los equipos deben mantenerse correctamente para asegurar su continua disponibilidad e ~~integración~~ _____. Por ejemplo, solo el personal de mantenimiento autorizado _____ debe realizar las reparaciones y dar servicio al equipo.