Nombre: _____ **Fecha:** _____ **Puntuación:** _____

Protección de datos y almacenamiento empresarial Guía de seguridad

Enmascaramiento de datos, tokenización, cifrado en reposo frente a en tránsito, copias de seguridad sin conexión

RESUMEN DE APRENDIZAJE: PROTECCIÓN DE DATOS

PROTEGIDO
CIFRADO DE DATOS
Estándar AES de 256 bits

CONFORME
ESTÁNDARES GLOBALES
Marcos del RGPD (GDPR) y la CCPA

CONFIANZA CERO
POLÍTICA DE ACCESO
Autenticación multifactor

¡Hola! Este paquete de actividades te guía por las normas y los controles de protección de datos. Explorarás el cifrado de disco completo, los controles de acceso seguro, las copias de seguridad en hardware, la postura de seguridad en la nube y las técnicas de enmascaramiento de datos.

PUNTOS DE CONTROL DE LA HOJA DE TRABAJO

- [ ] **Partes 1-4: Domina la ciberseguridad y la prevención de amenazas.**
- [ ] **Partes 5-7: Resuelve crucigramas y sopas de letras.**
- [ ] **Partes 8-9: Resuelve casos prácticos y el reto de cifrado.**
- [ ] **Parte 10: Repasa las páginas de preguntas frecuentes básicas y avanzadas.**
- [ ] **Parte 11: Explora 10 datos reales interesantes.**
- [ ] **Extra: reto Piensa rápido.**

Abre la guía de ciberseguridad de VPN.com

URL: https://www.vpn.com/es/ciberseguridad/proteccion-de-datos/

Tu hoja de ruta de aprendizaje sobre estrategia de protección de datos

- Distingue entre las técnicas de enmascaramiento de datos y tokenización.
- Implantar el cifrado en reposo de las unidades de almacenamiento y el cifrado en tránsito mediante TLS.
- Diseña sistemas de copia de seguridad sin conexión y aislados de la red para protegerte del ransomware.

INSTRUCCIONES DE LA GUÍA DE PROTECCIÓN DE DATOS

Responde a las preguntas de opción múltiple y de verdadero/falso, completa las frases con huecos usando el banco de palabras, relaciona las definiciones y resuelve el crucigrama y la sopa de letras. Aplica tus conocimientos a la protección de datos. Termina con la actividad extra Piensa rápido.

PROTECCIÓN DE DATOS Y SEGURIDAD DEL ALMACENAMIENTO EMPRESARIAL (INTRODUCCIÓN)

La protección de datos salvaguarda los activos de datos corporativos mediante enmascaramiento, tokenización, cifrado de bases de datos en reposo y protocolos de tránsito seguros. Diseñar copias de seguridad aisladas de la red ayuda a garantizar que las bases de datos clave puedan restaurarse en caso de una intrusión activa.

LEE ATENTAMENTE CADA PUNTO DE CONTROL Y SELECCIONA O ESCRIBE LA RESPUESTA CORRECTA.

Punto de control 1: Reto de opción múltiple

1. ¿Cuál es la finalidad principal del enmascaramiento de datos?

- A. Sustituir los identificadores sensibles por caracteres ficticios pero realistas para proteger la privacidad
- B. Comprimir archivos grandes de bases de datos para ahorrar espacio de almacenamiento físico en el servidor
- C. Eliminar los correos de contacto de clientes antiguos de los sistemas de copia de seguridad de archivo
- D. Ocultar la dirección IP pública del servidor de la base de datos frente a los escaneos de internet

2. ¿Qué mecanismo cifra los archivos almacenados en el disco duro de un servidor de bases de datos?

- A. Cifrado de disco completo en reposo
- B. Protocolos de negociación de sesión TLS en tránsito
- C. Reglas de reenvío de servidores de nombres de DNS dinámico
- D. Autenticación multifactor con llaves de hardware

3. ¿Qué opción representa los datos en tránsito?

- A. Paquetes de datos que circulan por routers y conmutadores de red
- B. Registros de transacciones de la base de datos almacenados en una unidad de copia de seguridad en frío
- C. Archivos de usuario archivados guardados en una bóveda aislada en la nube
- D. Archivos de configuración estáticos del sistema en el almacenamiento de un ordenador local

4. ¿Por qué es fundamental una copia de seguridad periódica sin conexión para protegerse del ransomware?

- A. Proporciona una copia limpia y sin conexión para restaurar los archivos sin pagar un rescate
- B. Impide que los hackers escaneen las configuraciones de puertos abiertos
- C. Aumenta la velocidad del ancho de banda de transmisión de la red local
- D. Automatiza los registros de aceptación del consentimiento de cookies en los navegadores

5. ¿Qué hace la tokenización de datos?

- A. Sustituye los números de tarjeta sensibles por tokens aleatorios no sensibles
- B. Enruta el tráfico web a través de varios nodos onion seguros
- C. Analiza los directorios del sistema en busca de malware basado en firmas
- D. Audita la duración de las sesiones de inicio de sesión del administrador de la base de datos

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. El enmascaramiento de datos modifica de forma permanente los registros de las bases de datos en los entornos de producción.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. Las copias de seguridad externas deben estar aisladas de la red corporativa principal para evitar la propagación del ransomware.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. Los certificados SSL/TLS protegen las bases de datos cifrando los datos almacenados en reposo en soportes físicos.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. El acceso a la red de confianza cero (ZTNA) verifica la identidad de cada usuario antes de concederle acceso a la base de datos.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. La tokenización basada en bóveda guarda los valores originales de las tarjetas en una bóveda de tokens central y segura.

- ○ Verdadero
- ○ Falso

Punto de control 3: Inserción de términos clave

Lee cada una de las frases siguientes y rellena el espacio en blanco con el término correcto del banco de palabras.

1. Sustituir los nombres de las personas por marcadores realistas se denomina _____ de datos.

2. Cifrar los bloques de almacenamiento físico protege los datos de la base de datos _____ .

3. Los protocolos TLS cifran los paquetes de datos activos que están en _____ .

4. Los permisos basados en roles limitan qué usuarios pueden obtener _____ a la base de datos.

5. Restaurar archivos corporativos limpios tras una brecha requiere un _____ seguro sin conexión.

6. Auditar las configuraciones en la nube permite evaluar la _____ de seguridad de una organización.

BANCO DE PALABRAS DE VOCABULARIO

ACCESO CIFRADO EN REPOSO ENMASCARADO MINIMIZACIÓN POSTURA RESPALDO TRÁNSITO

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

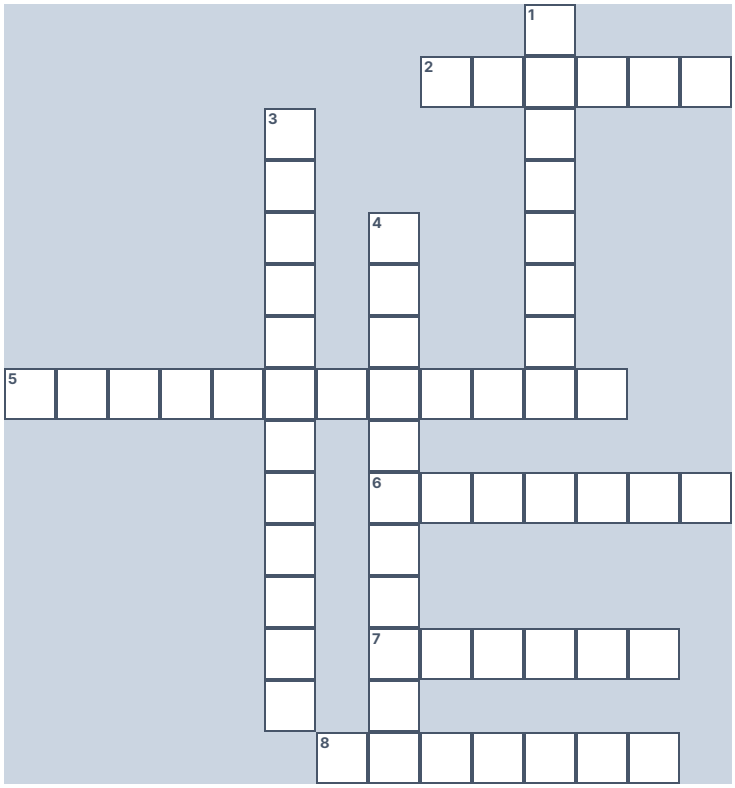
RELACIÓN DE DEFINICIONES

Relaciona cada término de vocabulario de la izquierda con su definición correcta de la derecha escribiendo la letra correspondiente (A-H) en la casilla rellenable.

☐	1. CIFRADO	A	Crear copias externas seguras de los datos para restaurarlos en caso de fallos del sistema.
☐	2. COPIA DE SEGURIDAD	B	Transformar el texto plano en texto cifrado ilegible para que los datos interceptados sigan siendo privados.
☐	3. MINIMIZACIÓN DE DATOS	C	El estado de seguridad general y la preparación defensiva de la nube de una organización.
☐	4. ACCESO	D	Cumplir normas como el RGPD (GDPR) o la CCPA en la gestión de la información privada de los usuarios.
☐	5. ESTADO DE SEGURIDAD	E	Incidente de seguridad en el que se accede a datos protegidos o se divulgan sin autorización.
☐	6. BRECHA	F	Restringir los permisos de lectura y escritura de la base de datos a roles de usuario autenticados.
☐	7. CUMPLIMIENTO NORMATIVO	G	Sustituir caracteres sensibles en los campos de la base de datos para proteger las identidades personales.
☐	8. ENMASCARAMIENTO	H	Limitar la recopilación de datos personales al mínimo imprescindible para las operaciones.

Punto de control 5: Crucigrama

Resuelve el crucigrama escribiendo letras en las casillas blancas activas. Los números corresponden a las pistas de abajo.



HORIZONTALES

2. Incidente de seguridad en el que se accede a datos protegidos o se divulgan sin autorización (6)

5. Limitar la recogida de datos personales al mínimo imprescindible para las operaciones (12)

6. Transformar texto plano en texto cifrado ilegible para que los datos interceptados sigan siendo privados (7)

7. Restricción de los permisos de lectura y escritura de la base de datos a roles de usuario autenticados (6)

8. Estado de seguridad global y preparación defensiva de la nube de una organización (7)

VERTICALES

1. Creación de copias seguras de los datos fuera de las instalaciones para restaurarlos en caso de fallos del sistema (8)

3. Respetar normas como el RGPD (GDPR) o la CCPA al gestionar la información privada de los usuarios (12)

4. Sustitución de caracteres sensibles en los campos de la base de datos para proteger la identidad de las personas (11)

Punto de control 5, alternativa: Pistas accesibles del crucigrama

Los usuarios de lectores de pantalla y de teclado pueden escribir las respuestas del crucigrama directamente en los campos de texto de abajo.

HORIZONTALES

2 horizontal: Incidente de seguridad en el que se accede a datos protegidos o se divulgan sin autorización (6 letras):

5 horizontal: Limitar la recogida de datos personales al mínimo imprescindible para las operaciones (12 letras):

6 horizontal: Transformar texto plano en texto cifrado ilegible para que los datos interceptados sigan siendo privados (7 letras):

7 horizontal: Restricción de los permisos de lectura y escritura de la base de datos a roles de usuario autenticados (6 letras):

8 horizontal: Estado de seguridad global y preparación defensiva de la nube de una organización (7 letras):

VERTICALES

1 vertical: Creación de copias seguras de los datos fuera de las instalaciones para restaurarlos en caso de fallos del sistema (8 letras):

3 vertical: Respetar normas como el RGPD (GDPR) o la CCPA al gestionar la información privada de los usuarios (12 letras):

4 vertical: Sustitución de caracteres sensibles en los campos de la base de datos para proteger la identidad de las personas (11 letras):

Punto de control 6: Sopa de letras

Encuentra los 8 términos clave del vocabulario ocultos en la cuadrícula de abajo. Las palabras pueden estar en horizontal, en vertical o en diagonal.

O M O P X P Ñ C C T S S E L J
T B S A B C O I X L P K Y L X
N T E K E Q N F K D O I N N L
E Q C P H N N R Q R S S T T G
I C C S P Ñ I A R B T V D E S
M Z A U C Z V D G K U H Z N D
I N E Q X P C O R U R B A M Z
L Ñ D L A E Ñ E E B A F H A I
P D R Q M E I R S R Z S F S Q
M V F A A Q O N P E P T X C Q
U M I N I M I Z A C I O N A K
C R T R D N Y B L H G R X R W
J A R Z Y Y L G D A I N Q A K
M M T O H P Q H O Z A O V D G
U C Y R Y B H M Z G K Ñ P O Ñ

LISTA DE PALABRAS DE VOCABULARIO

CIFRADO RESPALDO MINIMIZACION ACCESO POSTURA BRECHA
CUMPLIMIENTO ENMASCARADO

Punto de control 6, alternativa: Relación de vocabulario accesible

Relaciona cada uno de los 8 términos de vocabulario de la sopa de letras con su definición correcta escribiendo la letra (A-H) en el espacio en blanco.

TÉRMINOS DE VOCABULARIO

- **A. CIFRADO**
- **B. RESPALDO**
- **C. MINIMIZACION**
- **D. ACCESO**
- **E. POSTURA**
- **F. BRECHA**
- **G. CUMPLIMIENTO**
- **H. ENMASCARADO**

DEFINICIONES Y CAMPOS DE RELACIÓN

1. Incidente de seguridad en el que se accede a datos protegidos o se divulgan sin autorización.
2. Sustitución de caracteres sensibles en los campos de la base de datos para proteger la identidad de las personas.
3. Restricción de los permisos de lectura y escritura de la base de datos a roles de usuario autenticados.
4. Estado de seguridad global y preparación defensiva de la nube de una organización.
5. Respetar normas como el RGPD (GDPR) o la CCPA al gestionar la información privada de los usuarios.
6. Limitar la recogida de datos personales al mínimo imprescindible para las operaciones.
7. Transformar texto plano en texto cifrado ilegible para que los datos interceptados sigan siendo privados.
8. Creación de copias seguras de los datos fuera de las instalaciones para restaurarlos en caso de fallos del sistema.

Punto de control 7: Reto de palabras desordenadas

Ordena las letras de abajo para descubrir conceptos y términos clave de ciberseguridad. Escribe tus respuestas en los campos proporcionados.

1. RDCAOFI
2. NIMIMIONACZI
3. TPUASRO
4. TILMMOINECUP
5. ALEOPRDS
6. SEACOC
7. HBCAER
8. AAOCMESNDRA

Actividad extra: Piensa rápido

3 RESPUESTAS POR CATEGORÍA. GANA QUIEN COMPLETE PRIMERO LA LISTA.

1	Cosas de las que haces copia de seguridad			
2	Palabras relacionadas con la ciberseguridad			
3	Personas autorizadas a ver datos sensibles			
4	Formas de borrar datos de forma segura			
5	Lugares donde se almacenan los datos			
6	Cosas que deberían estar cifradas			
7	Datos que un hospital debe proteger			
8	Tipos de copia de seguridad			
9	Información que nunca deberías compartir			
10	Señales de alerta en un correo electrónico			
11	Hábitos seguros que puedes empezar hoy			
12	Personas a las que puedes pedir ayuda informática			
13	Dispositivos que pueden ser hackeados			
14	Formas de proteger los datos			
15	Cosas que pueden destruir datos			

Punto de control 8: Casos prácticos de ciberseguridad

Aplica los conceptos que has aprendido para resolver los escenarios reales que aparecen a continuación.

CASO PRÁCTICO 1: MEJORA DEL CIFRADO EN REPOSO DE LA BASE DE DATOS EMPRESARIAL



Escenario: Un comercio en línea almacena bases de datos de transacciones en el almacenamiento en la nube sin cifrado de disco completo. Una auditoría de cumplimiento reciente lo señaló como un riesgo grave para la seguridad de los datos según la CCPA. Diseña una arquitectura de recuperación.

Pregunta de debate: Analiza los riesgos de cumplimiento de la CCPA y propón una estrategia de cifrado en reposo.

CASO PRÁCTICO 2: CONTENCIÓN DEL RANSOMWARE Y RESTAURACIÓN DE DATOS



Escenario: Un ataque de ransomware activo está cifrando las unidades de red de una red local corporativa. El administrador ha detectado la infección a tiempo. Planifica los pasos de contención y recuperación.

Pregunta de debate: Detalla las medidas de contención inmediatas y planifica un proceso de restauración seguro.

Punto de control 9: Descifrar el código

Un profesional de la ciberseguridad protege los activos de la red frente a los actores de amenazas en línea. Usa la clave de letras y números de abajo para descifrar el mensaje escribiendo las letras correspondientes en los espacios en blanco.

CLAVE DE CIFRADO DE LETRAS A NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9

J=10 K=11 L=12 M=13 N=14 Ñ=15 O=16 P=17 Q=18

R=19 S=20 T=21 U=22 V=23 W=24 X=25 Y=26 Z=27

17 19 16 21 5 7 5 21 22 20 4 1 21 16 20

17 19 9 23 1 4 16 20 3 16 14

3 16 14 21 19 16 12 5 20 20 5 7 22 19 16 20

Mensaje descifrado:

CONSEJO: CADA NÚMERO REPRESENTA LA POSICIÓN DE ESA LETRA EN EL ALFABETO (P. EJ., 1 = A, 2 = B, 27 = Z).

Punto de control 10: Preguntas frecuentes básicas sobre ciberseguridad (Parte A)

Repasa preguntas y respuestas habituales sobre la mitigación de amenazas en línea.

Q1: ¿Qué es la protección de datos?

Es el proceso de proteger los datos personales y empresariales frente al acceso no autorizado, la pérdida o la corrupción mediante controles técnicos.

Q2: ¿Por qué es importante el cifrado de disco completo?

Protege los bloques de datos almacenados en las unidades físicas, lo que impide que nadie lea los datos si roba físicamente el disco duro.

Q3: ¿Cuál es la diferencia entre el cifrado en reposo y en tránsito?

El cifrado en reposo protege los archivos almacenados en los discos, mientras que el cifrado en tránsito protege los paquetes de red activos que pasan por los routers.

Q4: ¿Qué es el enmascaramiento de datos?

Sustituye los datos sensibles (como los números de tarjetas de crédito) por datos ficticios pero realistas para hacer pruebas sin exponer registros reales.

Q5: ¿Por qué es importante la copia de seguridad sin conexión?

Mantiene una copia limpia de tus archivos aislada de la red, lo que ayuda a proteger tus copias de seguridad para que el ransomware no las cifre.

Punto de control 10: Preguntas frecuentes básicas sobre ciberseguridad (Parte B)

Repasa preguntas y respuestas habituales sobre la mitigación de amenazas en línea.

Q6: ¿Qué es una bóveda de tokenización de datos?

Una base de datos segura y aislada que asigna tokens aleatorios a sus valores sensibles originales (como los números principales de las tarjetas de crédito).

Q7: ¿Qué significa el acceso de confianza cero a las bases de datos?

Significa verificar la identidad y el estado del dispositivo de cada usuario en cada inicio de sesión, en lugar de confiar en cualquiera que esté dentro de la red.

Q8: ¿Cómo protege TLS los datos en tránsito?

TLS cifra el contenido de la sesión TCP, lo que impide que actores maliciosos en redes públicas intercepten o modifiquen los paquetes en tránsito.

Q9: ¿Qué es la auditoría de accesos a bases de datos?

El registro continuo de las consultas a la base de datos y de los inicios de sesión para detectar patrones de acceso no autorizado o anomalías de seguridad.

Q10: ¿Qué es una auditoría del estado de seguridad en la nube?

Un proceso que analiza la configuración de la nube para detectar puertos abiertos, reglas de acceso mal configuradas y carencias en el cumplimiento de seguridad.

Punto de control 10: Preguntas frecuentes avanzadas sobre seguridad (Parte C)

Explora aspectos técnicos avanzados de los marcos de seguridad, el análisis de malware y el cumplimiento normativo de los datos.

Q1: ¿Cómo funciona el cifrado de sobre?

Cifra los datos con una clave de datos y después cifra esa clave de datos con una clave maestra, lo que simplifica el almacenamiento y la rotación de claves.

Q2: ¿Qué es el cifrado homomórfico?

Un método de cifrado avanzado que permite realizar operaciones directamente sobre datos cifrados sin descifrarlos antes.

Q3: ¿Por qué se utiliza el cifrado a nivel de columna en las bases de datos?

Cifra individualmente columnas sensibles concretas (como los SSN), lo que las protege incluso si los administradores obtienen acceso general de lectura a la tabla.

Q4: ¿Qué es la prevención de pérdida de datos (DLP)?

Software que supervisa los puntos de salida de la red para detectar y bloquear transferencias salientes no autorizadas de archivos confidenciales.

Q5: ¿Cómo protegen contra el ransomware las copias de seguridad de escritura única y lectura múltiple (WORM)?

Las copias de seguridad WORM impiden que los archivos se eliminen o modifiquen durante un periodo determinado, lo que evita que el ransomware cifre las copias de seguridad existentes.

Punto de control 10: Preguntas frecuentes avanzadas sobre seguridad (Parte D)

Explora aspectos técnicos avanzados de los marcos de seguridad, el análisis de malware y el cumplimiento normativo de los datos.

Q6: ¿Qué riesgo tiene reutilizar claves?

Reutilizar la misma clave criptográfica en distintas bases de datos significa que comprometer una sola clave expone todas las bases de datos.

Q7: ¿Cómo mejora la tokenización de bases de datos el cumplimiento de la CCPA?

Los tokens seudonimizan los registros en los sistemas que no son de producción y limitan la exposición en caso de filtración, pero los datos tokenizados pueden seguir siendo información personal.

Q8: ¿Por qué es fundamental la clasificación de datos?

Clasifica los archivos por nivel de sensibilidad, lo que ayuda a las organizaciones a aplicar el cifrado y los controles de acceso más estrictos a los datos de alto riesgo.

Q9: ¿Qué papel desempeña la rotación de claves?

Actualizar periódicamente las claves de cifrado limita la cantidad de datos históricos expuestos si una sola clave llega a descifrarse.

Q10: ¿Cómo protegen los enclaves seguros las consultas a la base de datos en memoria?

Los enclaves seguros aíslan las operaciones de consulta en bloques de memoria protegidos por la CPU, lo que impide que los administradores del host vean texto sin cifrar en la RAM.

Parte 11: 10 datos reales sobre ciberseguridad y su aplicación

Repasa datos reales sobre filtraciones de seguridad, mecanismos de defensa y normas de cumplimiento.

1. PERSPECTIVA SOBRE SEGURIDAD

El RGPD (GDPR) entró en vigor en mayo de 2018 y cambió la forma en que los sitios de todo el mundo gestionan el consentimiento de cookies y los registros de datos personales.

2. PERSPECTIVA SOBRE SEGURIDAD

Una multa por infringir el RGPD (GDPR) puede alcanzar los 20 millones de euros o el 4 % de la facturación mundial, lo que supone una exposición legal considerable. [4]

3. PERSPECTIVA SOBRE SEGURIDAD

La CCPA entró en vigor en enero de 2020 y estableció derechos pioneros de privacidad digital para los consumidores en Estados Unidos.

4. PERSPECTIVA SOBRE SEGURIDAD

La minimización de datos reduce el espacio de almacenamiento de las bases de datos, recortando los costes de operación de los servidores y reduciendo la magnitud del impacto de las filtraciones.

5. PERSPECTIVA SOBRE SEGURIDAD

El borrado criptográfico resuelve el problema de eliminar datos de las copias de seguridad, ya que destruye las claves en lugar de editar los archivos históricos de las cintas de copia de seguridad.

6. PERSPECTIVA SOBRE SEGURIDAD

La mayoría de los países del mundo han promulgado ya leyes de protección de datos personales para proteger los derechos de privacidad de los consumidores.

7. PERSPECTIVA SOBRE SEGURIDAD

Los formularios de consentimiento con casillas premarcadas están expresamente prohibidos según las definiciones de la normativa europea de privacidad de datos.

8. PERSPECTIVA SOBRE SEGURIDAD

El RGPD (GDPR) exige notificar las violaciones de datos personales a la autoridad de control en un plazo de 72 horas desde que se tenga conocimiento de ellas, cuando sea posible. [3]

9. PERSPECTIVA SOBRE SEGURIDAD

Aplicar hash a las contraseñas con algoritmos lentos como bcrypt o Argon2 dificulta mucho más el descifrado sin conexión de los hashes robados. [6]

10. PERSPECTIVA SOBRE SEGURIDAD

Los datos en reposo son los archivos de bases de datos guardados, mientras que los datos en tránsito son los paquetes que se desplazan activamente por los routers de la red.

Referencias técnicas y fuentes

La guía de estudio y los pasatiempos interactivos se han elaborado a partir de los estándares internacionales del NIST, de OWASP y de cumplimiento en materia de privacidad de datos.

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Clave de respuestas: Punto de control 1 – Opción múltiple

1 Pregunta 1

Respuesta correcta: A

NOTA PARA DOCENTES

¿Cuál es la finalidad principal del enmascaramiento de datos? → Sustituir los identificadores sensibles por caracteres ficticios pero realistas para proteger la privacidad

2 Pregunta 2

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué mecanismo cifra los archivos almacenados en el disco duro de un servidor de bases de datos? → Cifrado de disco completo en reposo

3 Pregunta 3

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué opción representa los datos en tránsito? → Paquetes de datos que circulan por routers y conmutadores de red

4 Pregunta 4

Respuesta correcta: A

NOTA PARA DOCENTES

¿Por qué es fundamental una copia de seguridad periódica sin conexión para protegerse del ransomware? → Proporciona una copia limpia y sin conexión para restaurar los archivos sin pagar un rescate

5 Pregunta 5

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué hace la tokenización de datos? → Sustituye los números de tarjeta sensibles por tokens aleatorios no sensibles

Clave de respuestas: Punto de control 2 – Verdadero o falso

6 Pregunta 6

Respuesta correcta: Falso

NOTA PARA DOCENTES

El enmascaramiento modifica las copias de prueba u oculta valores en el momento de la consulta; los registros de producción no cambian.

7 Pregunta 7

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Las copias de seguridad externas deben estar aisladas de la red corporativa principal para evitar la propagación del ransomware.

8 Pregunta 8

Respuesta correcta: Falso

NOTA PARA DOCENTES

Los certificados TLS protegen los datos en tránsito; los datos en reposo necesitan cifrado de disco, de archivos o de base de datos.

9 Pregunta 9

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

El acceso a la red de confianza cero (ZTNA) verifica la identidad de cada usuario antes de concederle acceso a la base de datos.

10 Pregunta 10

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

La tokenización basada en bóveda guarda los valores originales en una bóveda de tokens segura que asocia cada token con sus datos.

Claves de vocabulario y rúbrica de calificación

Rúbrica de calificación para docentes: concede 1 punto por cada relación correcta (8 puntos en total) y por cada término de contexto (6 puntos en total).

PUNTO DE CONTROL 4: SOLUCIÓN DE LA RELACIÓN DE CONCEPTOS

B 1. CIFRADO	A 2. COPIA DE SEGURIDAD	H 3. MINIMIZACIÓN DE DATOS	F 4. ACCESO
C 5. ESTADO DE SEGURIDAD	E 6. BRECHA	D 7. CUMPLIMIENTO NORMATIVO	G 8. ENMASCARAMIENTO

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 ENMASCARADO	2 EN REPOSO	3 TRÁNSITO	4 ACCESO
5 RESPALDO	6 POSTURA		

PUNTO DE CONTROL 6, ALTERNATIVA: SOLUCIÓN DE LA RELACIÓN DE PALABRAS

1 F – BRECHA	2 H – ENMASCARADO	3 D – ACCESO	4 E – POSTURA
5 G – CUMPLIMIENTO	6 C – MINIMIZACION	7 A – CIFRADO	8 B – RESPALDO

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar CIFRADO, COPIA DE SEGURIDAD y MINIMIZACIÓN DE DATOS con sus propias palabras y dar un ejemplo de cada uno.

Casos prácticos:
Pide a los estudiantes que justifiquen sus recomendaciones con datos de la hoja de trabajo y no con suposiciones.

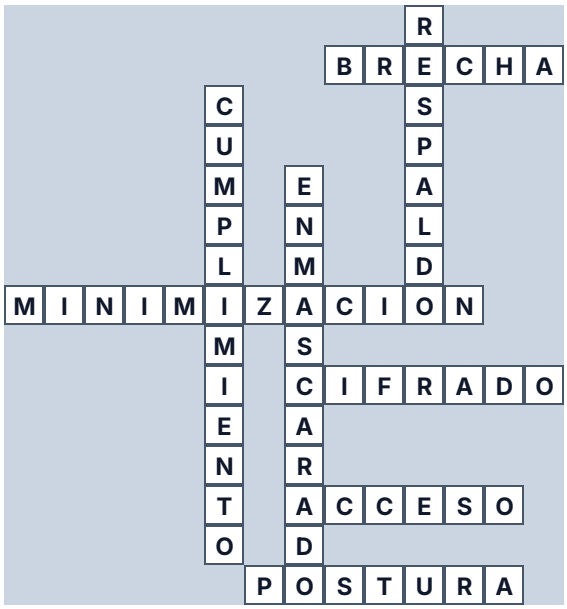
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

O	M	O	P	X	P	Ñ	C	C	T	S	S	E	L	J
T	B	S	A	B	C	O	I	X	L	P	K	Y	L	X
N	T	E	K	E	Q	N	F	K	D	O	I	N	N	L
E	Q	C	P	H	N	N	R	Q	R	S	S	T	T	G
I	C	C	S	P	Ñ	I	A	R	B	T	V	D	E	S
M	Z	A	U	C	Z	V	D	G	K	U	H	Z	N	D
I	N	E	Q	X	P	C	O	R	U	R	B	A	M	Z
L	Ñ	D	L	A	E	Ñ	E	E	B	A	F	H	A	I
P	D	R	Q	M	E	I	R	S	R	Z	S	F	S	Q
M	V	F	A	A	Q	O	N	P	E	P	T	X	C	Q
U	M	I	N	I	M	I	Z	A	C	I	O	N	A	K
C	R	T	R	D	N	Y	B	L	H	G	R	X	R	W
J	A	R	Z	Y	Y	L	G	D	A	I	N	Q	A	K
M	M	T	O	H	P	Q	H	O	Z	A	O	V	D	G
U	C	Y	R	Y	B	H	M	Z	G	K	Ñ	P	O	Ñ

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

2 horizontal: BRECHA Incidente de seguridad en el que se accede a datos protegidos o se divulgan sin autorización (6 letras)

5 horizontal: MINIMIZACION Limitar la recogida de datos personales al mínimo imprescindible para las operaciones (12 letras)

6 horizontal: CIFRADO Transformar texto plano en texto cifrado ilegible para que los datos interceptados sigan siendo privados (7 letras)

7 horizontal: ACCESO Restricción de los permisos de lectura y escritura de la base de datos a roles de usuario autenticados (6 letras)

8 horizontal: POSTURA Estado de seguridad global y preparación defensiva de la nube de una organización (7 letras)

VERTICALES

1 vertical: RESPALDO Creación de copias seguras de los datos fuera de las instalaciones para restaurarlos en caso de fallos del sistema (8 letras)

3 vertical: CUMPLIMIENTO Respetar normas como el RGPD (GDPR) o la CCPA al gestionar la información privada de los usuarios (12 letras)

4 vertical: ENMASCARADO Sustitución de caracteres sensibles en los campos de la base de datos para proteger la identidad de las personas (11 letras)

Clave de soluciones de palabras desordenadas y del cifrado

Clave de calificación de la actividad de ordenar letras del vocabulario y del Reto del código secreto.

CLAVE DE LAS PALABRAS DESORDENADAS

1. RDCAOFI — **CIFRADO**
2. NIMIMIONACZI — **MINIMIZACION**
3. TPUASRO — **POSTURA**
4. TILMMOINECUP — **CUMPLIMIENTO**
5. ALEOPRDS — **RESPALDO**
6. SEACOC — **ACCESO**
7. HBCAER — **BRECHA**
8. AAOCMESNDRA — **ENMASCARADO**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"PROTEGE TUS DATOS PRIVADOS CON CONTROLES SEGUROS"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Mejora del cifrado en reposo de la base de datos empresarial

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Un comercio online almacena bases de datos de transacciones en almacenamiento en la nube sin cifrado de disco completo. Una auditoría de cumplimiento reciente lo señaló como un riesgo grave de seguridad de datos según la CCPA. Diseña una arquitectura de recuperación.
- Estrategia y solución recomendadas: implementar cifrado de disco completo AES-256 en reposo en todos los sistemas de archivos. Usar un servicio de gestión de claves (KMS) centralizado con rotación automática y aplicar políticas IAM estrictas para controlar el acceso al descifrado.

B Caso práctico 2: Contención del ransomware y restauración de datos

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un ataque de ransomware activo está cifrando las unidades de red de la red local de una empresa. El administrador ha detectado la infección a tiempo. Planifica los pasos de contención y recuperación.
- Estrategia y solución recomendadas: aislar de inmediato el segmento comprometido. Formatear los equipos afectados y restaurar desde la última copia de seguridad sin conexión de escritura única y lectura múltiple (WORM). Verificar la integridad de la copia antes de volver a conectar los sistemas.