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

Ataques de ransomware y empresas Recuperación

Ejecución de la carga útil, cifrado criptográfico de archivos, copias de seguridad sin conexión, procedimientos de contención y recuperación ante desastres.

RESUMEN DE APRENDIZAJE: ATAQUES DE RANSOMWARE

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 los ataques de ransomware y la recuperación empresarial. Explorarás la ejecución de cargas útiles, el cifrado de archivos, las copias de seguridad sin conexión, la contención de amenazas, los pagos con criptomonedas y los planes de recuperación ante desastres.

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/ataque-ransomware/

Tu hoja de ruta de aprendizaje sobre recuperación ante ransomware

- Distingue entre cargas útiles de troyanos, ransomware y spyware.
- Analiza archivos maliciosos dentro de entornos aislados (sandbox) seguros.
- Formular procedimientos rápidos de aislamiento y contención de la red.

INSTRUCCIONES DE LA GUÍA SOBRE ATAQUES DE RANSOMWARE

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 recuperación tras un ransomware. Termina con la actividad extra Piensa rápido.

ATAQUES DE RANSOMWARE Y RECUPERACIÓN ANTE DESASTRES (INTRODUCCIÓN)

Las cargas de ransomware bloquean criptográficamente el almacenamiento del sistema y exigen pagos en criptomonedas a cambio de las claves de descifrado. Mitigar esta amenaza implica reglas de aislamiento de red, análisis de malware en entornos aislados (sandbox) y copias de seguridad en frío sólidas y aisladas (air-gapped).

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

Punto de control 1: Reto de opción múltiple

1. ¿Cuál es el mecanismo principal de un ataque de ransomware?

- A. Cifrado criptográfico de los archivos del usuario para denegar el acceso al sistema
- B. Inyectar comandos SQL maliciosos en los campos de formularios
- C. Interceptar (sniffing) paquetes de red en una conexión wifi pública
- D. Falsificar las cabeceras del correo electrónico para eludir la validación SPF

2. ¿Qué es una copia de seguridad sin conexión (en frío)?

- A. Una copia de almacenamiento desconectada de la red para protegerla de la propagación del malware
- B. Una copia de seguridad almacenada en el disco duro del servidor web principal
- C. Una caché temporal de los registros del registro del sistema
- D. Una herramienta administrativa para restablecer las contraseñas de los usuarios

3. ¿Cómo deben aislar los equipos de seguridad los sistemas infectados durante un ataque de ransomware?

- A. Desconectar los cables de red y desactivar las interfaces inalámbricas de inmediato
- B. Actualizar la base de datos de firmas del antivirus
- C. Apagar el servidor DNS principal
- D. Cambiar el nombre de las extensiones de los archivos comprometidos

4. ¿Por qué los organismos de seguridad desaconsejan pagar las exigencias del ransomware?

- A. Pagar anima a los atacantes y no garantiza que entreguen la clave de descifrado
- B. Anula automáticamente todas las pólizas de seguro corporativas
- C. Avisa automáticamente a todos los clientes por correo electrónico
- D. Daña los archivos de copia de seguridad del sistema restantes

5. ¿Qué es un plan de recuperación ante desastres (DRP)?

- A. Un proceso estructurado para restablecer las operaciones y los datos tras un compromiso del sistema
- B. Una configuración de cortafuegos que asigna los puertos de red entrantes
- C. Un esquema de base de datos que enumera los privilegios administrativos de los usuarios
- D. Un protocolo de autenticación del correo electrónico que rechaza los dominios suplantados

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Las cargas de ransomware pueden propagarse fácilmente a las copias de seguridad en línea conectadas a la red.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. Pagar el rescate en criptomonedas garantiza que los archivos se descifrarán correctamente.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. Desconectar de la red los sistemas infectados ayuda a evitar que el ransomware se propague a los sistemas contiguos.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. El ransomware nunca usa criptografía simétrica para cifrar el almacenamiento del sistema.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. Probar periódicamente los procedimientos de restauración de datos es una parte fundamental de la recuperación ante desastres.

- ○ 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. Para impedir el acceso a los archivos locales se usa el _____ criptográfico.

2. El código malicioso activo que se ejecuta en un sistema es la _____ .

3. Las copias de almacenamiento desconectadas y externas constituyen una _____ segura.

4. Para impedir que el malware se propague se necesita el _____ de red de los equipos.

5. El pago en criptomonedas que exigen los ciberdelincuentes es el _____ .

6. Restaurar los archivos de datos operativos forma parte de la _____ ante desastres.

BANCO DE PALABRAS DE VOCABULARIO

AISLAMIENTO CARGA ÚTIL CIFRADO COPIA EN FRÍO DESASTRE
RECUPERACIÓN RESCATE TROYANO

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

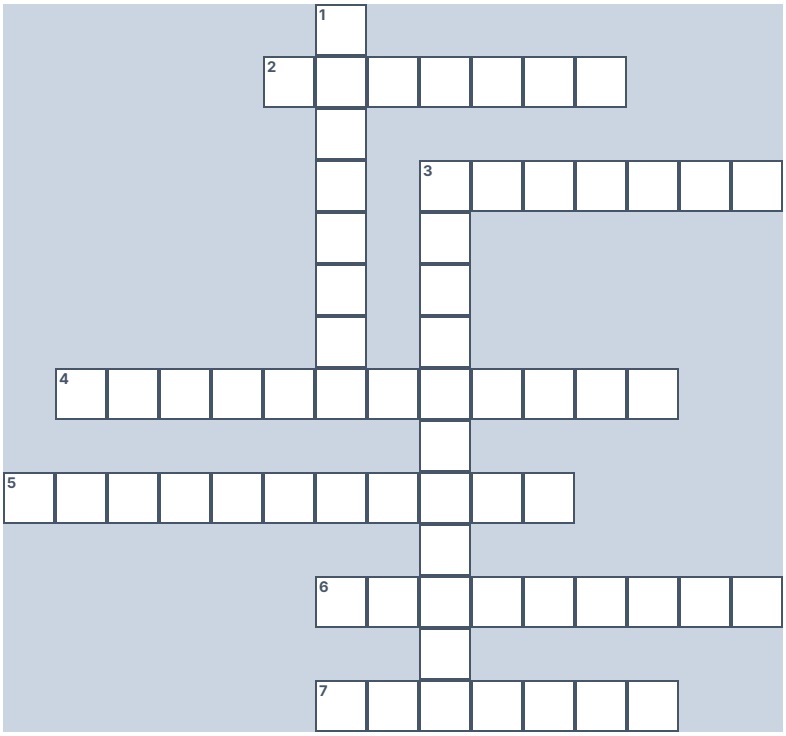
RELACIÓN DE DEFINICIONES

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	Desconectar los sistemas de red infectados.
☐	2. CARGA ÚTIL	B	Archivo malicioso disfrazado de limpio.
☐	3. COPIA DE SEGURIDAD EN FRÍO	C	Bloquear archivos criptográficamente.
☐	4. AISLAMIENTO	D	Incidente de interrupción grave del sistema.
☐	5. RESCATE	E	Ejecutar software malicioso.
☐	6. RECUPERACIÓN	F	Copia desconectada sin conexión.
☐	7. DESASTRE	G	Restaurar la base de datos desde una copia de seguridad.
☐	8. TROYANO	H	Solicitud de pago de una clave criptográfica.

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. Exigencia de pago a cambio de la clave criptográfica. (7)

3. Bloqueo criptográfico de archivos. (7)

4. Restauración de la base de datos a partir de una copia de seguridad. (12)

5. Desconexión de los sistemas de red infectados. (11)

6. Ejecución de software malicioso. (9)

7. Archivo malicioso disfrazado de archivo limpio. (7)

VERTICALES

1. Incidente que causa una interrupción grave del sistema. (8)

3. Copia desconectada y fuera de línea. (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: Exigencia de pago a cambio de la clave criptográfica. (7 letras):

3 horizontal: Bloqueo criptográfico de archivos. (7 letras):

4 horizontal: Restauración de la base de datos a partir de una copia de seguridad. (12 letras):

5 horizontal: Desconexión de los sistemas de red infectados. (11 letras):

6 horizontal: Ejecución de software malicioso. (9 letras):

7 horizontal: Archivo malicioso disfrazado de archivo limpio. (7 letras):

VERTICALES

1 vertical: Incidente que causa una interrupción grave del sistema. (8 letras):

3 vertical: Copia desconectada y fuera de línea. (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.

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

LISTA DE PALABRAS DE VOCABULARIO

CIFRADO CARGAUTIL COPIAENFRIO AISLAMIENTO RESCATE RECUPERACION DESASTRE TROYANO

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. CARGAUTIL**
- **C. COPIAENFRIO**
- **D. AISLAMIENTO**
- **E. RESCATE**
- **F. RECUPERACION**
- **G. DESASTRE**
- **H. TROYANO**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Copia desconectada y fuera de línea.

_____ 2. Archivo malicioso disfrazado de archivo limpio.

_____ 3. Bloqueo criptográfico de archivos.

_____ 4. Exigencia de pago a cambio de la clave criptográfica.

_____ 5. Desconexión de los sistemas de red infectados.

_____ 6. Incidente que causa una interrupción grave del sistema.

_____ 7. Ejecución de software malicioso.

_____ 8. Restauración de la base de datos a partir de una copia de seguridad.

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. **AOOCIEPRFNI** _____
3. **CRAESTE** _____
4. **ARETSDES** _____
5. **TAALUGCIR** _____
6. **AOMETNAIISL** _____
7. **ACPRERNIOCEU** _____
8. **RYOTNAO** _____

Actividad extra: Piensa rápido

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

1	Información que nunca deberías compartir			
2	Dispositivos que pueden ser hackeados			
3	Razones para no pagar un rescate			
4	Hábitos seguros que puedes empezar hoy			
5	Herramientas de seguridad que conoces			
6	Formas de proteger tus cuentas			
7	Señales de que un ordenador está infectado			
8	Lugares donde guardar una copia de seguridad			
9	Archivos que nunca querrías perder			
10	Formas en que se propaga el ransomware			
11	Cosas que hacer en la primera hora de un ataque			
12	Personas a las que contactar durante un ataque			
13	Cosas que el ransomware puede bloquear			
14	Palabras relacionadas con la ciberseguridad			
15	Organizaciones que suelen ser objetivo de ataques			

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: CONTENCIÓN DE LA CARGA DE RANSOMWARE EN UNA EMPRESA



Escenario: La red de área local de una empresa ha sido vulnerada por un ransomware activo. Los servidores de archivos clave han empezado a mostrar extensiones de archivo .locked.

Pregunta de debate: Detalla los pasos de contención y describe el protocolo de recuperación de datos.

CASO PRÁCTICO 2: EVALUAR ARQUITECTURAS DE COPIAS DE SEGURIDAD SIN CONEXIÓN



Escenario: Una empresa quiere diseñar una estrategia de copias de seguridad que reduzca el riesgo de que las copias se vean comprometidas, incluso si el ransomware secuestra por completo la red local principal.

Pregunta de debate: diseña un sistema seguro de almacén de copias de seguridad sin conexión.

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

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

4	5	20	4	5		22	14	1		3	16	17	9	1		5	14

6	19	9	16

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 el ransomware?

El ransomware es un software malicioso diseñado para bloquear el acceso a sistemas informáticos o archivos hasta que se pague un rescate.

Q2: ¿Cómo se propaga el ransomware?

Mediante archivos adjuntos de phishing por correo electrónico, vulnerabilidades de software sin parchear y sistemas de acceso remoto comprometidos. [1]

Q3: ¿Por qué se solicita el pago en criptomonedas?

Las criptomonedas como Bitcoin ofrecen un anonimato relativo, lo que dificulta que las fuerzas de seguridad rastreen los fondos.

Q4: ¿Bloquea el antivirus el ransomware?

Sí, pero los antivirus basados en firmas pueden fallar ante cargas útiles de ransomware de día cero recién creadas.

Q5: ¿Qué es una copia de seguridad aislada (air-gapped)?

Una copia de seguridad que no tiene ninguna conexión física ni lógica con la red principal, lo que la protege de la propagación.

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 la doble extorsión?

Cuando los atacantes no solo cifran los archivos, sino que también roban datos confidenciales para amenazar con filtrarlos públicamente si no se paga.

Q7: ¿Qué es un descifrador?

Una utilidad de software que contiene la clave criptográfica necesaria para devolver los archivos bloqueados a texto plano.

Q8: ¿Cómo se detecta el ransomware a tiempo?

Supervisando los sistemas de archivos en busca de actividad repentina y masiva de modificación y cambio de nombre de archivos.

Q9: ¿Qué papel desempeña el seguro?

Un ciberseguro puede ayudar a cubrir los costes de recuperación, pero las condiciones de cobertura y las normas sobre el pago de rescates varían según la póliza.

Q10: ¿Debo reiniciar un sistema infectado?

No, reiniciar puede destruir las pruebas de la memoria volátil; en su lugar, aísla el equipo de la red. [1]

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 usa el ransomware el cifrado asimétrico?

Utiliza una clave pública incrustada en el malware para cifrar los archivos, de modo que se necesita la clave privada del atacante para descifrarlos.

Q2: ¿Por qué también se utiliza el cifrado simétrico?

El cifrado simétrico (como AES) es rápido y puede bloquear bases de datos enormes en minutos, mientras que las claves asimétricas protegen la clave AES.

Q3: ¿Qué es la segmentación lógica?

Dividir las redes en zonas aisladas para impedir que el malware se propague lateralmente desde los equipos de trabajo hasta los servidores principales.

Q4: ¿Qué es el almacenamiento WORM?

Soportes de escritura única y lectura múltiple (WORM), que impiden que las cargas útiles de ransomware editen, sobrescriban o eliminen los datos de las copias de seguridad.

Q5: ¿Qué son las instantáneas (shadow copies)?

Instantáneas de copia de seguridad locales creadas por Windows; el ransomware suele eliminarlas primero mediante herramientas administrativas.

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: ¿Cómo facilita el robo de credenciales el ransomware?

Los atacantes compran credenciales de administrador filtradas para iniciar sesión a través de escritorios remotos y ejecutar manualmente ransomware en toda la red.

Q7: ¿Qué son las pruebas de restauración en simulacro?

Restaurar periódicamente las bases de datos de copia de seguridad en entornos de prueba aislados para comprobar que la velocidad de restauración y la integridad de los datos cumplen los objetivos de recuperación ante desastres.

Q8: ¿Cómo frena el ransomware la detección en endpoints (EDR)?

Analizando el comportamiento de los procesos (p. ej., un cifrado rápido) y suspendiendo rápidamente la aplicación maliciosa.

Q9: ¿Qué es un modelo de ransomware como servicio (RaaS)?

Un modelo de franquicia en el que los desarrolladores de malware alquilan generadores de ransomware a afiliados a cambio de un porcentaje de los pagos.

Q10: ¿Cómo desencadena un RDP sin parches un ataque de ransomware?

Las pasarelas del protocolo de escritorio remoto expuestas y sin parches permiten a los atacantes forzar los inicios de sesión por fuerza bruta y lanzar malware manualmente.

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

Los actores de ransomware suelen usar herramientas como vssadmin.exe para eliminar las instantáneas (shadow copies) de Windows e impedir las restauraciones locales. [1]

2. PERSPECTIVA SOBRE SEGURIDAD

Las claves simétricas AES-256 suelen usarse para cifrar el contenido de los archivos, que después se bloquea con claves públicas RSA.

3. PERSPECTIVA SOBRE SEGURIDAD

Recuperarse de un ataque de ransomware que ha tenido éxito puede llevar semanas, por eso importan las copias de seguridad sin conexión probadas.

4. PERSPECTIVA SOBRE SEGURIDAD

El FBI no apoya el pago de rescates y advierte que pagar no garantiza que recuperes ningún dato. [2]

5. PERSPECTIVA SOBRE SEGURIDAD

Los planes de recuperación ante desastres (DRP) deben definir un objetivo de tiempo de recuperación (RTO) y un objetivo de punto de recuperación (RPO).

6. PERSPECTIVA SOBRE SEGURIDAD

El FBI recomienda copias de seguridad cifradas e inmutables, es decir, que no se puedan modificar ni eliminar. [3]

7. PERSPECTIVA SOBRE SEGURIDAD

Los desarrolladores de ransomware utilizan técnicas avanzadas de ofuscación para eludir los antivirus tradicionales basados en firmas.

8. PERSPECTIVA SOBRE SEGURIDAD

La segmentación de la red restringe el movimiento lateral, lo que ayuda a impedir que el ransomware se propague más allá del primer equipo infectado. [3]

9. PERSPECTIVA SOBRE SEGURIDAD

Los servicios remotos expuestos y mal protegidos, como el protocolo de escritorio remoto (RDP), son un punto de entrada habitual del ransomware. [1]

10. PERSPECTIVA SOBRE SEGURIDAD

La CISA aconseja guardar las copias de seguridad cifradas sin conexión, ya que muchas variantes de ransomware buscan y eliminan las copias de seguridad a las que pueden acceder. [1]

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] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Clave de respuestas: Punto de control 1 – Opción múltiple

1 Pregunta 1

Respuesta correcta: A

NOTA PARA DOCENTES

¿Cuál es el mecanismo principal de un ataque de ransomware? → Cifrado criptográfico de los archivos del usuario para denegar el acceso al sistema

2 Pregunta 2

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué es una copia de seguridad sin conexión (en frío)? → Una copia de almacenamiento desconectada de la red para protegerla de la propagación del malware

3 Pregunta 3

Respuesta correcta: A

NOTA PARA DOCENTES

¿Cómo deben aislar los equipos de seguridad los sistemas infectados durante un ataque de ransomware? → Desconectar los cables de red y desactivar las interfaces inalámbricas de inmediato

4 Pregunta 4

Respuesta correcta: A

NOTA PARA DOCENTES

¿Por qué los organismos de seguridad desaconsejan pagar las exigencias del ransomware? → Pagar anima a los atacantes y no garantiza que entreguen la clave de descifrado

5 Pregunta 5

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué es un plan de recuperación ante desastres (DRP)? → Un proceso estructurado para restablecer las operaciones y los datos tras un compromiso del sistema

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

6 **Pregunta 6** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Las cargas de ransomware pueden propagarse fácilmente a las copias de seguridad en línea conectadas a la red.

7 **Pregunta 7** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Falso: el FBI advierte de que pagar no garantiza que recuperes ningún dato. [2]

8 **Pregunta 8** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Verdadero: CISA aconseja desconectar los equipos infectados o dejar la red sin conexión para contener la propagación.

9 **Pregunta 9** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Falso: el ransomware suele cifrar los archivos con cifrados simétricos rápidos como AES.

10 **Pregunta 10** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Probar periódicamente los procedimientos de restauración de datos es una parte fundamental de la recuperación ante desastres.

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

C 1. CIFRADO	E 2. CARGA ÚTIL	F 3. COPIA DE SEGURIDAD EN FRÍO	A 4. AISLAMIENTO
H 5. RESCATE	G 6. RECUPERACIÓN	D 7. DESASTRE	B 8. TROYANO

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 CIFRADO	2 CARGA ÚTIL	3 COPIA EN FRÍO	4 AISLAMIENTO
5 RESCATE	6 RECUPERACIÓN		

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

1 C – COPIAENFRIO	2 H – TROYANO	3 A – CIFRADO	4 E – RESCATE
5 D – AISLAMIENTO	6 G – DESASTRE	7 B – CARGAUTIL	8 F – RECUPERACION

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar CIFRADO, CARGA ÚTIL y COPIA DE SEGURIDAD EN FRÍO 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.

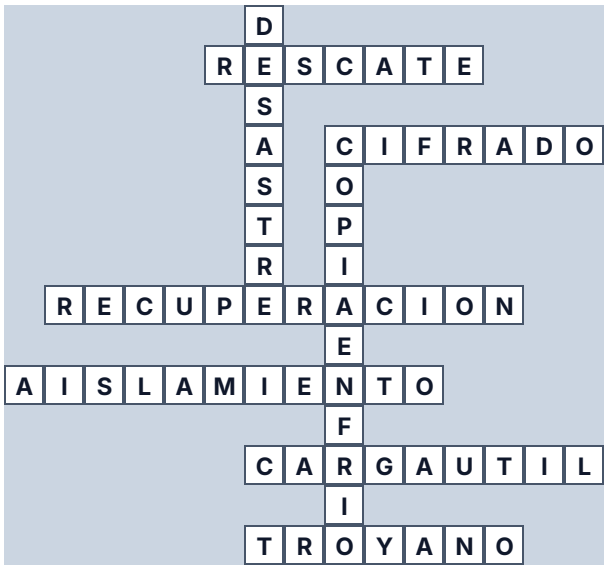
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

2 horizontal: RESCATE Exigencia de pago a cambio de la clave criptográfica. (7 letras)

3 horizontal: CIFRADO Bloqueo criptográfico de archivos. (7 letras)

4 horizontal: RECUPERACION Restauración de la base de datos a partir de una copia de seguridad. (12 letras)

5 horizontal: AISLAMIENTO Desconexión de los sistemas de red infectados. (11 letras)

6 horizontal: CARGAUTIL Ejecución de software malicioso. (9 letras)

7 horizontal: TROYANO Archivo malicioso disfrazado de archivo limpio. (7 letras)

VERTICALES

1 vertical: DESASTRE Incidente que causa una interrupción grave del sistema. (8 letras)

3 vertical: COPIAENFRIO Copia desconectada y fuera de línea. (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	5.	TAALUGCIR	CARGAUTIL
2.	AOOCIEPRFNI	COPIAENFRIO	6.	AOMETNAIISL	AISLAMIENTO
3.	CRAESTE	RESCATE	7.	ACPRERNIOCEU	RECUPERACION
4.	ARETSDES	DESASTRE	8.	RYOTNAO	TROYANO

CLAVE DEL RETO DEL CÓDIGO SECRETO

"RESTAURA TUS DATOS DESDE UNA COPIA EN FRIO"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Contención de la carga de ransomware en una empresa

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un ransomware activo ha penetrado en la red local de una empresa. Los servidores de archivos clave han empezado a mostrar archivos con la extensión .locked.
- Estrategia y solución recomendadas: desconectar todos los servidores afectados de la red de área local. Cerrar las sesiones administrativas activas. Restaurar los archivos no comprometidos desde un sistema de copias de seguridad sin conexión, seguro y bloqueado contra escritura.

B Caso práctico 2: Evaluar arquitecturas de copias de seguridad sin conexión

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Una empresa quiere diseñar una estrategia de copias de seguridad que reduzca el riesgo de que estas se vean comprometidas aunque el ransomware secuestre por completo la red local principal.
- Estrategia y solución recomendadas: implementar almacenamiento de escritura única y lectura múltiple (WORM). Crear un aislamiento lógico (air gap) desconectando el sistema de copias de seguridad de todas las redes y aplicar una rotación diaria de soportes físicos.