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

Análisis de malware y mitigación de amenazas Guía

Troyanos, ransomware, spyware, rootkits, entornos aislados de virtualización (sandboxes), contención

RESUMEN DE APRENDIZAJE: ANÁLISIS DE MALWARE

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 el análisis y la prevención del malware. Explorarás el spyware, los troyanos, las cargas útiles de ransomware, las herramientas de ingeniería inversa, el comportamiento de los rootkits y las estrategias de contención.

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/malware/

Tu hoja de ruta de aprendizaje sobre mitigación de malware

- Distingue entre los tipos de malware troyano, gusano y rootkit.
- Implantar la ejecución virtualizada en entornos aislados (sandbox) para el análisis de código.
- Diseña planes de contención y saneamiento para cargas útiles de ransomware activas.

INSTRUCCIONES DE LA GUÍA DE ANÁLISIS DE MALWARE

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 mitigación del malware. Termina con la actividad extra Piensa rápido.

ANÁLISIS DE MALWARE Y CONTENCIÓN DE AMENAZAS (INTRODUCCIÓN)

El código malicioso, como troyanos, gusanos y ransomware, supone amenazas de alto impacto para los equipos y servidores. Los equipos de seguridad analizan el malware dentro de entornos aislados (sandbox) virtuales y aplican controles rápidos de aislamiento de red para contener la propagación de la carga útil.

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 característica que define a un troyano?

- A. Se hace pasar por software legítimo para engañar a los usuarios y que lo ejecuten
- B. Se replica automáticamente a través de las líneas de la red local
- C. Infecta archivos dentro de entornos aislados (sandbox) virtuales
- D. Intercepta el tráfico del proveedor de servicios de internet

2. ¿Qué tipo de malware cifra archivos y exige un pago?

- A. Ransomware
- B. Spyware
- C. Rootkit
- D. Adware

3. ¿Qué opción representa el spyware?

- A. Malware diseñado para supervisar en secreto las pulsaciones de teclado y la actividad del navegador del usuario
- B. Código de programa que se ejecuta dentro de un contenedor virtual aislado
- C. Actualizaciones antimalware descargadas de registros de bases de datos
- D. Ajuste automático del brillo de la pantalla

4. ¿Por qué los desarrolladores de malware usan rootkits?

- A. Ocultar procesos activos y archivos maliciosos al sistema operativo
- B. Aumentar la velocidad de procesamiento de la CPU en los dispositivos finales
- C. Para hacer copias de seguridad de los archivos de la base de datos en almacenes seguros en la nube
- D. Para mejorar la duración de la batería de los portátiles

5. ¿Qué significa el sandboxing en el análisis de malware?

- A. Ejecutar archivos sospechosos en una cámara virtual aislada para observar su comportamiento de forma segura
- B. Comparar los hashes de los archivos con bases de datos de amenazas conocidas
- C. Restaurar copias de seguridad de la base de datos después de una intrusión
- D. Desconectar los routers de la red local de las líneas públicas

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Los gusanos informáticos necesitan la interacción de un usuario humano para propagarse por las redes locales.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. El adware siempre es inofensivo y no rastrea el comportamiento del usuario ni el historial del navegador.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. Restaurar copias de seguridad limpias y sin conexión permite a las víctimas recuperar los archivos cifrados sin pagar el rescate.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. El antivirus basado en firmas detiene de forma fiable el malware de día cero antes de que exista ninguna firma para él.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. El malware sin archivos ejecuta scripts maliciosos en la memoria del sistema y evita escribir archivos en el disco.

- ○ 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. Un malware disfrazado de programa útil y seguro es un _____ .

2. Las cargas maliciosas que bloquean sistemas de bases de datos a cambio de dinero son _____ .

3. Los keyloggers que graban contraseñas en secreto son un tipo de _____ .

4. Para ocultarse en lo más profundo del núcleo del sistema operativo se necesita un _____ .

5. Para analizar archivos sospechosos en una cámara segura y separada se usa un _____ virtual.

6. Para detener la propagación de malware activo se necesita una _____ inmediata de la red.

BANCO DE PALABRAS DE VOCABULARIO

CONTENCIÓN | ENTORNO AISLADO | GUSANO | PROGRAMA ESPÍA | RANSOMWARE | ROOTKIT | SIN ARCHIVOS | TROYANO

Escribe aquí tus respuestas:

1. | **2.**

3. | **4.**

5. | **6.**

Punto de control 4: Relación de conceptos de seguridad

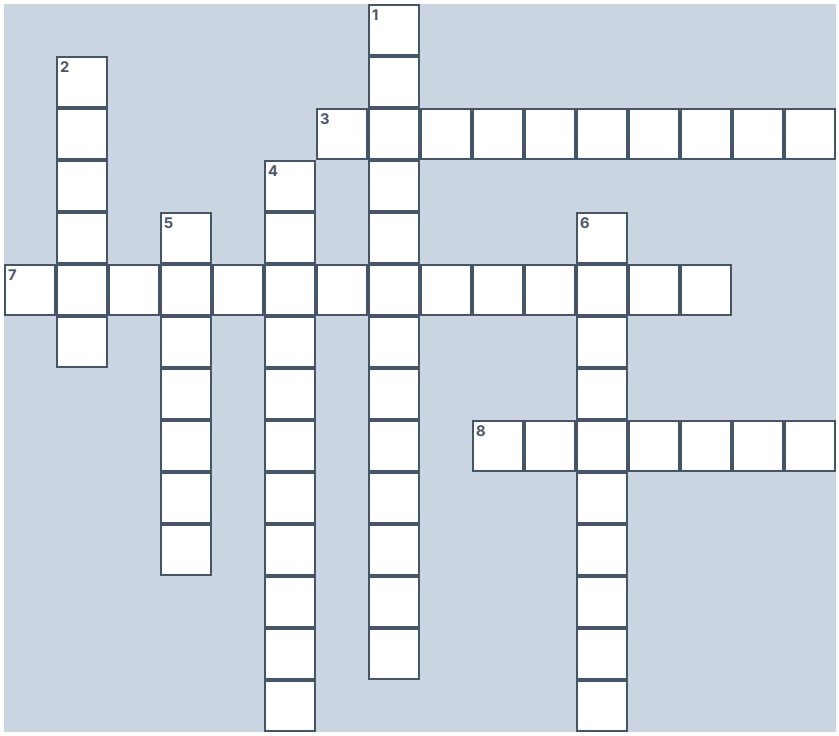
RELACIÓN DE DEFINICIONES

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. TROYANO	A	Programa diseñado para supervisar y registrar en secreto la actividad y las entradas del usuario.
☐	2. RANSOMWARE	B	Malware que se ejecuta directamente en la RAM para evitar que lo detecten los escáneres de disco.
☐	3. SPYWARE	C	Aislar los equipos infectados para evitar la propagación de cargas maliciosas.
☐	4. ROOTKIT	D	Software malicioso disfrazado de programa de utilidad benigno o útil.
☐	5. SANDBOX	E	Malware que se replica a sí mismo y se propaga por las redes sin intervención humana.
☐	6. CONTENCIÓN	F	Malware que cifra el almacenamiento del sistema y exige un pago a cambio de entregar la clave.
☐	7. GUSANO	G	Entorno virtual aislado que se utiliza para analizar archivos maliciosos de forma segura.
☐	8. SIN ARCHIVOS	H	Malware sigiloso que se oculta en lo más profundo del kernel del sistema para mantener el control administrativo.

Punto de control 5: Crucigrama

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



HORIZONTALES

3. Restricción de los equipos infectados para evitar que se propaguen las cargas de la amenaza. (10)

7. Entorno virtual separado que se usa para analizar archivos maliciosos de forma segura (sandbox). (14)

8. Software malicioso disfrazado de programa inofensivo o útil. (7)

VERTICALES

1. Programa diseñado para vigilar y registrar en secreto la actividad y las pulsaciones del usuario. (13)

2. Malware que se replica a sí mismo y se propaga por las redes sin intervención humana. (6)

4. Malware que se ejecuta directamente en la RAM para evitar que lo detecten los escáneres de disco. (11)

5. Malware sigiloso que se oculta en lo más profundo del núcleo del sistema para mantener el control administrativo. (7)

6. Malware que cifra el almacenamiento del sistema y exige un pago a cambio de la clave. (10)

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

3 horizontal: Restricción de los equipos infectados para evitar que se propaguen las cargas de la amenaza. (10 letras):

7 horizontal: Entorno virtual separado que se usa para analizar archivos maliciosos de forma segura (sandbox). (14 letras):

8 horizontal: Software malicioso disfrazado de programa inofensivo o útil. (7 letras):

VERTICALES

1 vertical: Programa diseñado para vigilar y registrar en secreto la actividad y las pulsaciones del usuario. (13 letras):

2 vertical: Malware que se replica a sí mismo y se propaga por las redes sin intervención humana. (6 letras):

4 vertical: Malware que se ejecuta directamente en la RAM para evitar que lo detecten los escáneres de disco. (11 letras):

5 vertical: Malware sigiloso que se oculta en lo más profundo del núcleo del sistema para mantener el control administrativo. (7 letras):

6 vertical: Malware que cifra el almacenamiento del sistema y exige un pago a cambio de la clave. (10 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.

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

LISTA DE PALABRAS DE VOCABULARIO

TROYANO RANSOMWARE PROGRAMAESPIA ROOTKIT ENTORNOAISLADO
CONTENCION GUSANO SINARCHIVOS

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. TROYANO**
- **B. RANSOMWARE**
- **C. PROGRAMAESPIA**
- **D. ROOTKIT**
- **E. ENTORNOAISLADO**
- **F. CONTENCION**
- **G. GUSANO**
- **H. SINARCHIVOS**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Malware sigiloso que se oculta en lo más profundo del núcleo del sistema para mantener el control administrativo.

_____ 2. Restricción de los equipos infectados para evitar que se propaguen las cargas de la amenaza.

_____ 3. Malware que se ejecuta directamente en la RAM para evitar que lo detecten los escáneres de disco.

_____ 4. Malware que se replica a sí mismo y se propaga por las redes sin intervención humana.

_____ 5. Malware que cifra el almacenamiento del sistema y exige un pago a cambio de la clave.

_____ 6. Programa diseñado para vigilar y registrar en secreto la actividad y las pulsaciones del usuario.

_____ 7. Software malicioso disfrazado de programa inofensivo o útil.

_____ 8. Entorno virtual separado que se usa para analizar archivos maliciosos de forma segura (sandbox).

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. YNTAOOR
2. IRRAOPPMAE SAG
3. EINDAOSLTO RNAO
4. OASNGU
5. AMEASWORR N
6. IOKRTTO
7. OTCCNIONEN
8. VHSCNSRIOIA

Actividad extra: Piensa rápido

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

1	Lugares donde descargar apps seguras			
2	Dispositivos que pueden ser hackeados			
3	Cosas de las que haces copia de seguridad			
4	Señales de alerta en un correo electrónico			
5	Señales de que un teléfono tiene malware			
6	Tipos de malware que conoces			
7	Tipos de archivo con los que hay que tener cuidado			
8	Formas en que el malware llega a un PC			
9	Hábitos seguros que puedes empezar hoy			
10	Palabras relacionadas con la ciberseguridad			
11	Cosas que hacer tras una filtración de datos			
12	Razones para actualizar el software			
13	Animales o personajes con nombres parecidos a los del malware			
14	Cosas que puede robar el malware			
15	Cosas que hacer si has hecho clic en el enlace equivocado			

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. Establece políticas de contención.

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

CASO PRÁCTICO 2: INYECCIÓN EN MEMORIA DE MALWARE SIN ARCHIVOS



Escenario: Una analista detecta patrones de scripts sospechosos que se ejecutan directamente en la RAM volátil del sistema mediante herramientas administrativas estándar, pero no hay archivos maliciosos en el disco.

Pregunta de debate: Explica la estrategia de análisis de memoria y especifica herramientas para bloquear la ejecución sin archivos.

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

4	5	21	5	3	21	1		1	13	5	14	1	27	1	20		3	16	14
							13	16	14	9	21	16	19	5	20		4	5	
						3	16	13	17	16	19	21	1	13	9	5	14	21	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 malware?

Software malicioso diseñado por actores de amenazas para dañar, secuestrar o robar datos de dispositivos y redes.

Q2: ¿Qué diferencia hay entre un virus y un gusano?

Un virus necesita una acción humana (como abrir un archivo) para propagarse, mientras que un gusano se propaga automáticamente por las redes.

Q3: ¿Cómo infecta un troyano un ordenador?

Engaña a los usuarios haciéndose pasar por un programa inofensivo o seguro y oculta en su interior su carga útil maliciosa.

Q4: ¿Qué es el ransomware?

Un tipo de malware que cifra los archivos del sistema atacado y exige un pago a cambio de la clave de descifrado. [1]

Q5: ¿Qué es el spyware?

Software malicioso que registra en secreto las pulsaciones de teclas, las contraseñas y los hábitos de navegación del usuario para enviarlos a los atacantes.

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 significa el aislamiento en entornos controlados (sandboxing)?

Ejecutar archivos sospechosos en un entorno virtual seguro y aislado para observar su comportamiento sin riesgo para los sistemas de producción.

Q7: ¿Qué es el malware sin archivos?

Malware que se ejecuta directamente en la memoria del sistema (RAM) mediante utilidades legítimas y evita escribir archivos en el disco para burlar los escáneres básicos.

Q8: ¿Cómo protege un rootkit al malware?

Oculta procesos y archivos maliciosos, a menudo subvirtiendo el kernel del sistema operativo, de modo que los antivirus pueden no detectarlos.

Q9: ¿Qué es la supervisión dinámica del comportamiento?

Análisis antivirus que supervisa los procesos activos en tiempo real para bloquear acciones típicas del malware, como el cifrado masivo de archivos.

Q10: ¿Por qué es urgente la contención durante la respuesta a incidentes?

Aislar los endpoints comprometidos evita que las cargas útiles de malware activas se propaguen a otros dispositivos de la red.

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 eluden los desarrolladores de malware los escáneres antivirus basados en firmas?

Usan el polimorfismo: cambian el hash y la estructura del código del archivo en cada infección, mientras el comportamiento malicioso sigue siendo el mismo.

Q2: ¿Qué riesgo suponen las herramientas de doble uso en las campañas de malware?

Los atacantes usan herramientas administrativas legítimas (como PowerShell o Sysinternals) para camuflarse en el tráfico normal de la red, lo que dificulta su detección.

Q3: ¿Cómo ejecuta el vaciado de procesos (process hollowing) cargas maliciosas?

Inicia un proceso legítimo del sistema en estado suspendido, sustituye su código en memoria por malware y reanuda la ejecución.

Q4: ¿Qué papel desempeña un servidor de mando y control (C2)?

Un servidor remoto gestionado por hackers para enviar instrucciones y cargas maliciosas al malware que se ejecuta en máquinas comprometidas.

Q5: ¿Por qué es difícil detectar el registro de pulsaciones de teclas (keylogging)?

Los keyloggers básicos consumen pocos recursos de CPU y ocultan sus procesos dentro de utilidades legítimas del espacio de usuario.

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 retrasa la ofuscación del código el análisis del malware?

Cifra o reorganiza el código fuente, haciéndolo ilegible para las herramientas de análisis y los escáneres de seguridad.

Q7: ¿Cuál es la función de un bootkit?

Un rootkit que infecta el proceso de arranque (el MBR, el sector de arranque o el firmware UEFI), de modo que se ejecuta antes de que se cargue el sistema operativo.

Q8: ¿Cómo identifica el análisis heurístico las amenazas de día cero?

Busca patrones de código y comandos administrativos sospechosos en lugar de buscar un hash coincidente en una base de datos.

Q9: ¿Qué amenaza supone el secuestro de DLL?

Forzar a una aplicación legítima a cargar una biblioteca de vínculos dinámicos (DLL) maliciosa colocándola en la ruta del directorio de la aplicación.

Q10: ¿Cómo usan la virtualización los procesos automatizados de análisis de malware?

Ejecutan archivos sospechosos en varias máquinas virtuales con distintos sistemas operativos y generan automáticamente registros de comportamiento y archivos PCAP de red.

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 troyanos siguen siendo un método de infección habitual porque ocultan código malicioso dentro de programas que parecen inofensivos.

2. PERSPECTIVA SOBRE SEGURIDAD

El IC3 del FBI recibió más de 3600 denuncias de ransomware en 2025, con pérdidas declaradas superiores a 32 millones de dólares. [3]

3. PERSPECTIVA SOBRE SEGURIDAD

Los gusanos pueden propagarse rápidamente por las redes aprovechando vulnerabilidades de protocolos sin parchear, como EternalBlue en SMB.

4. PERSPECTIVA SOBRE SEGURIDAD

El malware sin archivos es difícil de detectar porque se ejecuta en memoria mediante herramientas legítimas y deja pocos rastros en el disco.

5. PERSPECTIVA SOBRE SEGURIDAD

Los sandboxes de análisis suelen volver a una instantánea limpia después de cada ejecución, de modo que cada prueba empieza desde un estado conocido.

6. PERSPECTIVA SOBRE SEGURIDAD

Los rootkits pueden modificar las llamadas al sistema del kernel y devolver resultados de diagnóstico falsos a los analizadores antimalware.

7. PERSPECTIVA SOBRE SEGURIDAD

La ofuscación de código usa herramientas de empaquetado para comprimir y ocultar la verdadera estructura binaria de la carga útil del malware.

8. PERSPECTIVA SOBRE SEGURIDAD

El malware polimórfico cambia su código, y con ello el hash del archivo, en cada nueva copia para eludir las comprobaciones de firmas.

9. PERSPECTIVA SOBRE SEGURIDAD

El secuestro de DLL aprovecha las configuraciones del orden de búsqueda en sistemas operativos habituales como Windows.

10. PERSPECTIVA SOBRE SEGURIDAD

Los proveedores de seguridad detectan cada día una enorme cantidad de nuevas muestras de malware, por lo que las firmas necesitan actualizarse constantemente.

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. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

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

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/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 la característica que define a un troyano? → Se hace pasar por software legítimo para engañar a los usuarios y que lo ejecuten

2 Pregunta 2

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué tipo de malware cifra archivos y exige un pago? → Ransomware [1]

3 Pregunta 3

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué opción representa el spyware? → Malware diseñado para supervisar en secreto las pulsaciones de teclado y la actividad del navegador del usuario

4 Pregunta 4

Respuesta correcta: A

NOTA PARA DOCENTES

¿Por qué los desarrolladores de malware usan rootkits? → Ocultar procesos activos y archivos maliciosos al sistema operativo

5 Pregunta 5

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué significa el sandboxing en el análisis de malware? → Ejecutar archivos sospechosos en una cámara virtual aislada para observar su comportamiento de forma segura

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

6 Pregunta 6

Respuesta correcta: Falso

NOTA PARA DOCENTES

Falso: los gusanos se replican y se propagan por las redes sin ninguna acción del usuario.

7 Pregunta 7

Respuesta correcta: Falso

NOTA PARA DOCENTES

Falso: el adware no siempre es inofensivo; gran parte de él rastrea la navegación para dirigir anuncios.

8 Pregunta 8

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Verdadero: las copias de seguridad limpias y sin conexión restauran los archivos cifrados sin pagar, aunque los datos robados aún pueden filtrarse.

9 Pregunta 9

Respuesta correcta: Falso

NOTA PARA DOCENTES

Falso: los escáneres de firmas necesitan una muestra conocida, por lo que el malware de día cero totalmente nuevo puede pasar desapercibido.

10 Pregunta 10

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

El malware sin archivos ejecuta scripts maliciosos en la memoria del sistema y evita escribir archivos en el disco.

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

D 1. TROYANO	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDBOX	C 6. CONTENCIÓN	E 7. GUSANO	B 8. SIN ARCHIVOS

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 TROYANO	2 RANSOMWARE	3 PROGRAMA ESPÍA	4 ROOTKIT
5 ENTORNO AISLADO	6 CONTENCIÓN		

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

1 D – ROOTKIT	2 F – CONTENCION	3 H – SINARCHIVOS	4 G – GUSANO
5 B – RANSOMWARE	6 C – PROGRAMAESPIA	7 A – TROYANO	8 E – ENTORNOAISLADO

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar TROYANO, RANSOMWARE y SPYWARE 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.

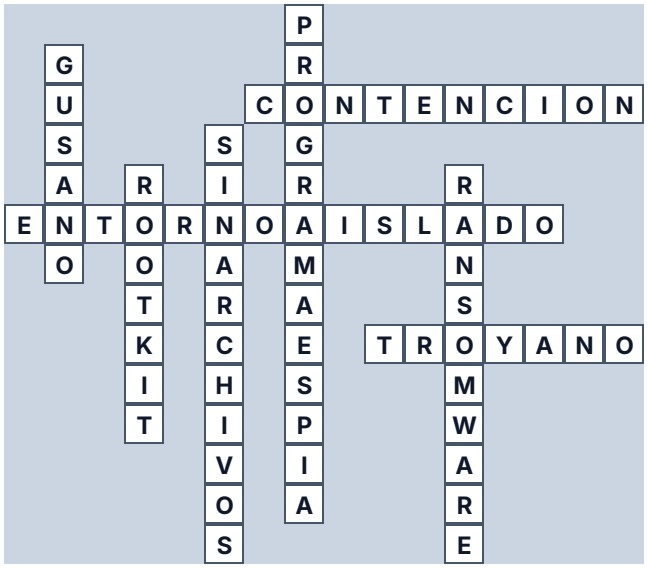
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

3 horizontal: CONTENCION Restricción de los equipos infectados para evitar que se propaguen las cargas de la amenaza. (10 letras)

7 horizontal: ENTORNOAISLADO Entorno virtual separado que se usa para analizar archivos maliciosos de forma segura (sandbox). (14 letras)

8 horizontal: TROYANO Software malicioso disfrazado de programa inofensivo o útil. (7 letras)

VERTICALES

1 vertical: PROGRAMAESPIA Programa diseñado para vigilar y registrar en secreto la actividad y las pulsaciones del usuario. (13 letras)

2 vertical: GUSANO Malware que se replica a sí mismo y se propaga por las redes sin intervención humana. (6 letras)

4 vertical: SINARCHIVOS Malware que se ejecuta directamente en la RAM para evitar que lo detecten los escáneres de disco. (11 letras)

5 vertical: ROOTKIT Malware sigiloso que se oculta en lo más profundo del núcleo del sistema para mantener el control administrativo. (7 letras)

6 vertical: RANSOMWARE Malware que cifra el almacenamiento del sistema y exige un pago a cambio de la clave. (10 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. Y N T A O O R — **TROYANO**
2. I R R A O P P M A E S A G — **PROGRAMAESPIA**
3. E I N D A O S L T O R N A O — **ENTORNOAISLADO**
4. O A S N G U — **GUSANO**
5. A M E A S W O R R N — **RANSOMWARE**
6. I O K R T T O — **ROOTKIT**
7. O T C C N I O N E N — **CONTENCION**
8. V H S C N S R I O I A — **SINARCHIVOS**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"DETECTA AMENAZAS CON MONITORES DE COMPORTAMIENTO"

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. Establece políticas de contención.
- 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: Inyección en memoria de malware sin archivos

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un analista detecta patrones de scripts sospechosos que se ejecutan directamente en la RAM volátil del sistema mediante herramientas administrativas estándar, pero no hay archivos maliciosos en el disco.
- Estrategia y solución recomendadas: aislar primero los equipos afectados y capturar una imagen de la memoria. Revisar los registros de PowerShell y WMI, bloquear los scripts no aprobados con AppLocker y después reiniciar para eliminar la carga maliciosa.