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

Software antivirus y protección de Guía de protección

Detección por firmas, heurística, supervisión del comportamiento, sandboxing, actualizaciones

RESUMEN DE APRENDIZAJE: SOFTWARE ANTIVIRUS

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 software antivirus y la protección de puntos finales. Explorarás las bases de datos de firmas, los escáneres heurísticos, la supervisión del comportamiento, los archivos virtuales en sandbox y la mitigación de falsos positivos.

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/antivirus/

Tu hoja de ruta de aprendizaje sobre estrategia antivirus

- Distingue entre la detección de malware basada en firmas y la basada en heurística.
- Comprende los protocolos de supervisión del comportamiento y de aislamiento en entornos sandbox.
- Evalúa el impacto del análisis en tiempo real en el rendimiento del sistema y en los equipos.
- Mitigar las clasificaciones de falsos positivos mediante la verificación de certificados digitales.
- Gestionar la distribución diaria de actualizaciones de definiciones en los equipos corporativos.

INSTRUCCIONES DE LA GUÍA DE ANTIVIRUS

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 seguridad antivirus de los dispositivos finales. Termina con la actividad extra Piensa rápido.

PROTECCIÓN ANTIVIRUS Y ANÁLISIS POR FIRMAS (INTRODUCCIÓN)

El software antivirus protege los dispositivos finales identificando, poniendo en cuarentena y eliminando el malware. Los sistemas modernos combinan bases de datos de firmas (que comparan hashes de amenazas conocidas) con heurística (que analiza la estructura de los archivos) y supervisión del comportamiento para detectar exploits de día cero.

LEE ATENTAMENTE CADA PUNTO DE CONTROL Y SELECCIONA O ESCRIBE LA

Punto de control 1: Reto de opción múltiple

1. ¿Qué limitación tiene la detección basada en firmas?

- A. No puede identificar malware desconocido o modificado
- B. Genera altas tasas de falsos positivos
- C. Requiere una gran potencia de procesamiento de la CPU
- D. Solo funciona cuando hay conexión a internet

2. ¿Cómo detectan los escáneres heurísticos las nuevas variantes de malware?

- A. Identificando patrones y estructuras de código sospechosos
- B. Comparando los hashes de los archivos con una base de datos de amenazas
- C. Eliminando automáticamente todos los ejecutables sin firmar
- D. Subiendo todos los archivos a una carpeta pública en la nube

3. ¿Cuál es la finalidad de la ejecución en sandbox de un antivirus?

- A. Aislar y analizar archivos en una cámara virtual segura
- B. Acelerar la transferencia de la copia de seguridad del sistema de archivos local
- C. Instalar los parches de seguridad del sistema operativo local
- D. Comprimir archivos de documentos grandes para ahorrar espacio

4. ¿Qué método de detección señala comportamientos de amenaza en tiempo real?

- A. Análisis de comportamiento que supervisa las acciones del software
- B. Inspección de registros históricos realizada durante la noche
- C. Intervención manual del usuario para informar de aplicaciones lentas
- D. Revisiones manuales semanales de los programas instalados

5. ¿Por qué son fundamentales las actualizaciones periódicas de definiciones para los escáneres?

- A. Alimentar la base de datos de los motores de firmas con identificadores de amenazas
- B. Aumentar la velocidad de reloj de la CPU durante las operaciones
- C. Para modificar los tiempos de caché globales de los servidores de nombres DNS
- D. Para autorizar los ajustes de cookies del navegador web

Punto de control 2: Reto de verdadero o falso

6 Pregunta vf 6

6. La detección por firmas compara los hashes criptográficos de los archivos con listas de bases de datos.

- ◯ Verdadero
- ◯ Falso

7 Pregunta vf 7

7. Los escáneres heurísticos pueden generar alertas de falsos positivos con archivos seguros.

- ◯ Verdadero
- ◯ Falso

8 Pregunta vf 8

8. Un sandbox permite que el malware acceda sin límites a los archivos de la red.

- ◯ Verdadero
- ◯ Falso

9 Pregunta vf 9

9. El análisis del comportamiento bloquea los archivos cuando muestran acciones maliciosas.

- ◯ Verdadero
- ◯ Falso

10 Pregunta vf 10

10. El software antivirus estándar detiene por completo todos los ataques de día cero.

- ◯ 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 escáner tradicional se basa en la coincidencia de _____ para identificar malware conocido.

2. Examinar los patrones de código de los archivos se denomina _____ .

3. Las herramientas antivirus aíslan los archivos sospechosos en un entorno _____ .

4. La supervisión en tiempo real vigila el _____ de los programas en busca de actividades sospechosas.

5. Los escáneres descargan a diario _____ de la base de datos para reconocer nuevas amenazas.

6. Los programas seguros marcados como malware generan alertas de _____ .

BANCO DE PALABRAS DE VOCABULARIO

ACTUALIZACIONES AISLAMIENTO ANÁLISIS HEURÍSTICO ANTIVIRUS
COMPORTAMIENTO FALSO POSITIVO FIRMAS SANDBOX

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

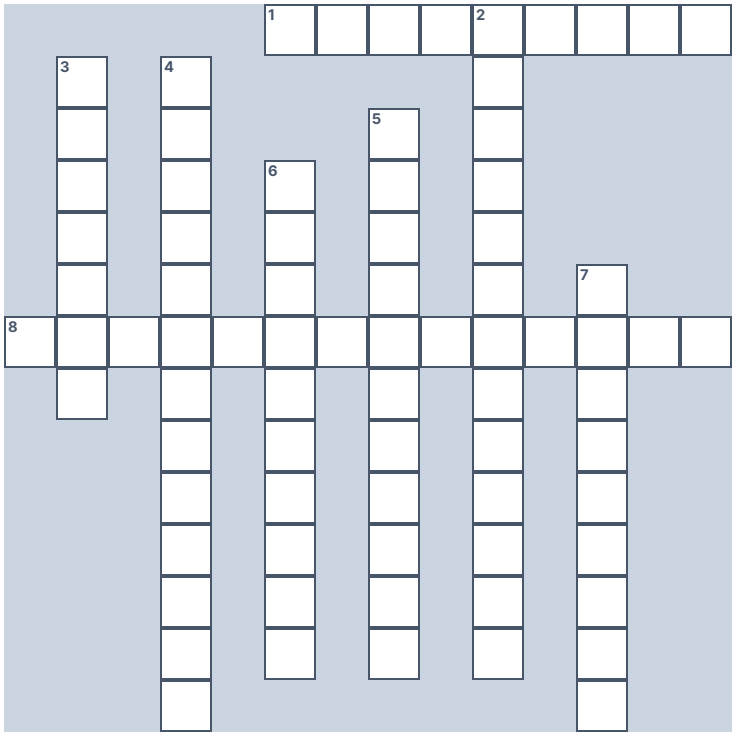
RELACIÓN DE DEFINICIONES

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. Firma hash	A	Aislar los archivos sospechosos para evitar que el sistema local quede expuesto.
☐	2. Heurística de código	B	Suite de software que analiza los dispositivos y los protege frente a exploits.
☐	3. Entorno aislado (sandbox) de archivos	C	Supervisar las acciones del software en ejecución en busca de patrones de funcionamiento maliciosos.
☐	4. Análisis de comportamiento	D	Huella única en una base de datos criptográfica que se usa para identificar amenazas conocidas.
☐	5. Actualizaciones diarias	E	Entorno de prueba virtual seguro que ejecuta código no fiable de forma segura.
☐	6. Falso positivo	F	Descargas periódicas de definiciones que alimentan la base de datos de amenazas.
☐	7. Aislamiento de amenazas	G	Análisis basado en reglas que marca los archivos con estructuras de código sospechosas.
☐	8. Herramienta antivirus	H	Alerta de seguridad que clasifica erróneamente software seguro como malware.

Punto de control 5: Crucigrama

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



HORIZONTALES

1. Huella criptográfica única en la base de datos que se usa para identificar amenazas conocidas (9)

8. Supervisión de las acciones del software en ejecución en busca de patrones de funcionamiento malicioso (14)

VERTICALES

2. Descarga periódica de definiciones que alimenta la base de datos de amenazas (13)

3. Entorno de prueba virtual y seguro que ejecuta código no fiable sin riesgo (7)

4. Alerta de seguridad que clasifica por error un software seguro como malware (13)

5. Confinamiento de archivos sospechosos para evitar que el sistema local quede expuesto (11)

6. Análisis basado en reglas que marca archivos con estructuras de código sospechosas (10)

7. Paquete de software que analiza y protege los dispositivos finales frente a exploits (9)

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. PISTAS HORIZONTALES PISTAS VERTICALES

HORIZONTALES

1 horizontal: Huella criptográfica única en la base de datos que se usa para identificar amenazas conocidas (9 letras):

8 horizontal: Supervisión de las acciones del software en ejecución en busca de patrones de funcionamiento malicioso (14 letras):

VERTICALES

2 vertical: Descarga periódica de definiciones que alimenta la base de datos de amenazas (13 letras):

3 vertical: Entorno de prueba virtual y seguro que ejecuta código no fiable sin riesgo (7 letras):

4 vertical: Alerta de seguridad que clasifica por error un software seguro como malware (13 letras):

5 vertical: Confinamiento de archivos sospechosos para evitar que el sistema local quede expuesto (11 letras):

6 vertical: Análisis basado en reglas que marca archivos con estructuras de código sospechosas (10 letras):

7 vertical: Paquete de software que analiza y protege los dispositivos finales frente a exploits (9 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.

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

LISTA DE PALABRAS DE VOCABULARIO

FIRMAHASH HEURISTICA SANDBOX COMPORTAMIENTO ACTUALIZACION
FALSOPOSITIVO AISLAMIENTO ANTIVIRUS

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. FIRMAHASH**
- **B. HEURISTICA**
- **C. SANDBOX**
- **D. COMPORTAMIENTO**
- **E. ACTUALIZACION**
- **F. FALSOPOSITIVO**
- **G. AISLAMIENTO**
- **H. ANTIVIRUS**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Supervisión de las acciones del software en ejecución en busca de patrones de funcionamiento malicioso.

_____ 2. Paquete de software que analiza y protege los dispositivos finales frente a exploits.

_____ 3. Descarga periódica de definiciones que alimenta la base de datos de amenazas.

_____ 4. Análisis basado en reglas que marca archivos con estructuras de código sospechosas.

_____ 5. Confinamiento de archivos sospechosos para evitar que el sistema local quede expuesto.

_____ 6. Huella criptográfica única en la base de datos que se usa para identificar amenazas conocidas.

_____ 7. Entorno de prueba virtual y seguro que ejecuta código no fiable sin riesgo.

_____ 8. Alerta de seguridad que clasifica por error un software seguro como malware.

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. HAMIFASHR
2. SNXOBDA
3. CAZCAONTIA LIU
4. ITOMSANEAIL
5. ISAERTIHCU
6. RTEOMNATIC OMOP
7. TISPFAIOOVL OS
8. SVUAINIRT

Actividad extra: Piensa rápido

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

1	Razones para actualizar el software			
2	Personas a las que puedes pedir ayuda informática			
3	Cosas que hacer cuando el antivirus encuentra algo			
4	Señales de un virus informático			
5	Cosas que se ponen en cuarentena			
6	Lugares donde se esconden los virus			
7	Información que nunca deberías compartir			
8	Tipos de software malicioso			
9	Herramientas de seguridad que conoces			
10	Cosas que analiza un antivirus			
11	Cosas de las que haces copia de seguridad			
12	Dispositivos que pueden ser hackeados			
13	Programas antivirus que conoces			
14	Razones de las falsas alarmas			
15	Hábitos seguros que puedes empezar hoy			

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: ANÁLISIS POR FIRMAS FRENTE A ANÁLISIS HEURÍSTICO



Escenario: Un empleado descarga una utilidad personalizada creada internamente por otro equipo. El escáner de firmas la da por buena, pero el escáner heurístico la marca como sospechosa.

Pregunta de debate: Explica por qué ha ocurrido esto y cómo verificar si el archivo es seguro.

CASO PRÁCTICO 2: GESTIÓN DE FALSOS POSITIVOS



Escenario: Un desarrollador de software compila su aplicación. El antivirus del sistema marca el nuevo ejecutable como malware y lo pone en cuarentena.

Pregunta de debate: Describe los riesgos de incluirlo en una lista blanca y explica la forma correcta de resolverlo.

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		13	1	12	24	1	19	5		14	22	5	23	16

3	16	14		1	14	1	12	9	20	9	20

8	5	22	19	9	20	21	9	3	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: ¿Cómo identifica el software antivirus el malware?

Identifica el malware mediante la comparación de firmas con bases de datos, el análisis heurístico de la estructura del código y la supervisión del comportamiento en tiempo real.

Q2: ¿Qué es la detección basada en firmas?

Es un método de análisis que compara los hashes criptográficos de los archivos con listas de bases de datos de amenazas de malware conocidas.

Q3: ¿Qué es un escáner heurístico?

La heurística analiza la estructura de un archivo y sus instrucciones de código, y marca patrones sospechosos comunes en variantes de malware.

Q4: ¿Qué significa que un archivo esté en cuarentena?

El antivirus mueve el archivo a una carpeta segura y aislada (cuarentena) y bloquea su ejecución para proteger el sistema operativo.

Q5: ¿Qué es un falso positivo de un antivirus?

Es un error en el que los algoritmos de análisis marcan incorrectamente como malware un software legítimo y seguro.

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

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

Q6: ¿Cómo protege la supervisión del comportamiento los sistemas?

Supervisa el software en ejecución en tiempo real y bloquea los procesos que intentan hacer cambios sospechosos, como inyectar código.

Q7: ¿Por qué son importantes las pruebas en entornos aislados (sandbox)?

El sandboxing ejecuta archivos no fiables en una máquina virtual aislada y observa sus acciones de forma segura sin exponer el sistema.

Q8: ¿Con qué frecuencia deben actualizarse las definiciones del antivirus?

Los analizadores deben actualizar sus definiciones a diario o cada hora para reconocer las nuevas variantes de malware descubiertas.

Q9: ¿Cuál es la diferencia entre un antivirus y un EDR?

El antivirus se centra en el análisis de archivos, mientras que la detección y respuesta en dispositivos finales (EDR) ofrece seguimiento y contención de amenazas en toda la red.

Q10: ¿Puedo usar dos programas antivirus a la vez?

No. Ejecutar dos escáneres activos provoca conflictos en el sistema, reduce el rendimiento y puede hacer que se bloqueen mutuamente.

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 minimizan las reglas heurísticas la evasión de amenazas?

La heurística analiza patrones generales de amenazas en lugar de firmas específicas, lo que permite detectar variantes modificadas de familias de malware conocidas.

Q2: ¿Qué es un virus polimórfico?

Es un malware que cambia la estructura de sus archivos y su rutina de descifrado en cada ejecución, lo que hace ineficaces los análisis por firmas.

Q3: ¿Cómo detectan los entornos aislados (sandboxes) la evasión de máquinas virtuales?

Los entornos aislados (sandbox) modernos simulan clics del ratón y tiempo de actividad del sistema, lo que engaña al malware diseñado para ocultarse cuando se ejecuta en máquinas virtuales.

Q4: ¿Qué formatos de descarga tienen las actualizaciones de firmas?

Las actualizaciones suelen ser archivos ligeros de diferencias binarias incrementales, lo que minimiza el consumo de ancho de banda de la red del cliente.

Q5: ¿Cómo gestionan los agentes de endpoint los análisis locales?

Los agentes realizan comprobaciones ligeras en segundo plano y delegan las búsquedas profundas de hashes criptográficos en bases de datos de amenazas en la nube.

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 es el análisis de detección de rootkits?

Analiza las tablas de memoria a nivel del kernel, evitando las API del sistema operativo que los rootkits interceptan para ocultar sus hilos activos.

Q7: ¿Cómo bloquea el ransomware el análisis del comportamiento?

Detecta los bucles automatizados de cifrado masivo de archivos y finaliza el proceso del host antes de que se bloqueen las bases de datos del sistema.

Q8: ¿Qué es la verificación de certificados de firma de código?

Los analizadores comprueban las firmas digitales del código frente a autoridades de certificación raíz de confianza, validando la identidad del desarrollador del software.

Q9: ¿Cómo afectan los empaquetadores (packers) a los motores de análisis?

Los empaquetadores comprimen o cifran las cargas útiles del malware. Los escáneres deben desempaquetar el archivo en memoria antes de comparar firmas.

Q10: ¿Cómo automatizan el aislamiento las herramientas EDR?

Los agentes EDR ponen en cuarentena los equipos comprometidos a nivel de red, bloqueando el movimiento lateral y permitiendo a la vez el acceso de los analistas.

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

Las bases de datos de firmas almacenan hashes de malware conocido, por lo que los archivos totalmente nuevos o modificados pasan desapercibidos hasta que se actualizan las definiciones.

2. PERSPECTIVA SOBRE SEGURIDAD

Los motores heurísticos pueden detectar algunas variantes nuevas de malware antes de que existan firmas, a costa de más falsos positivos.

3. PERSPECTIVA SOBRE SEGURIDAD

Las alertas de falsos positivos hacen que los equipos de TI pierdan tiempo verificando y restaurando archivos puestos en cuarentena por error.

4. PERSPECTIVA SOBRE SEGURIDAD

El malware polimórfico cambia su código con cada copia, por lo que los defensores combinan las firmas con comprobaciones heurísticas y de comportamiento.

6. PERSPECTIVA SOBRE SEGURIDAD

Los autores de malware escriben código personalizado diseñado para detectar entornos aislados (sandbox) y retrasar la ejecución para burlar los temporizadores.

5. PERSPECTIVA SOBRE SEGURIDAD

Los motores antivirus en la nube comparan los hashes de los archivos sospechosos con grandes bases de datos de amenazas en línea casi en tiempo real.

7. PERSPECTIVA SOBRE SEGURIDAD

Los fabricantes envían periódicamente actualizaciones de definiciones a los endpoints para que los escáneres puedan reconocer las amenazas confirmadas recientemente.

8. PERSPECTIVA SOBRE SEGURIDAD

Los monitores de comportamiento contra el ransomware vigilan llamadas concretas a la API Win32 asociadas con el cifrado de archivos y la eliminación de instantáneas (shadow copies).

9. PERSPECTIVA SOBRE SEGURIDAD

Las firmas de código válidas pueden reducir el riesgo de falsos positivos, pero los archivos firmados también se analizan, ya que el malware también puede estar firmado.

10. PERSPECTIVA SOBRE SEGURIDAD

Los rootkits modifican las estructuras del kernel del sistema, por lo que hacen falta analizadores especializados en el arranque para detectarlos y eliminarlos.

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

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
https://csrc.nist.gov/pubs/sp/800/83/r1/final

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

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

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

Clave de respuestas: Punto de control 1 – Opción múltiple

1 Pregunta 1 FIRMAS **Respuesta correcta: A**

NOTA PARA DOCENTES

El análisis por firmas se basa en hashes conocidos de una base de datos, por lo que no detecta malware desconocido o modificado. Cita: OWASP Secure Configuration.

2 Pregunta 2 HEURÍSTICA **Respuesta correcta: A**

NOTA PARA DOCENTES

La heurística analiza la estructura y las instrucciones del código para identificar características sospechosas de nuevas variantes de amenazas. Cita: Center for Internet Security (CIS).

3 Pregunta 3 AISLAMIENTO EN SANDBOX **Respuesta correcta: A**

NOTA PARA DOCENTES

Un sandbox ejecuta los archivos sospechosos en una máquina virtual aislada para observar su comportamiento de ejecución de forma segura. Cita: NIST Digital Identity.

4 Pregunta 4 CONDUCTUAL **Respuesta correcta: A**

NOTA PARA DOCENTES

El análisis del comportamiento supervisa en tiempo real los programas en ejecución para bloquear cambios no autorizados en el sistema. Cita: Center for Internet Security (CIS).

5 Pregunta 5 ACTUALIZACIONES **Respuesta correcta: A**

NOTA PARA DOCENTES

Los analizadores descargan actualizaciones incrementales diarias de las definiciones para mantenerse al día con el panorama de amenazas. Cita: OWASP Secure Configuration.

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

6 **Pregunta 6** FIRMAS **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Las herramientas basadas en firmas calculan hashes criptográficos y los comparan con una base de datos de hashes de amenazas conocidas. Cita: OWASP Secure Configuration.

7 **Pregunta 7** HEURÍSTICA **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los motores heurísticos aplican esquemas basados en reglas que pueden marcar como sospechosos archivos legítimos y seguros. Cita: Center for Internet Security (CIS).

8 **Pregunta 8** AISLAMIENTO EN SANDBOX **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Un sandbox ejecuta el código en un contenedor virtual y bloquea estrictamente el acceso a los recursos compartidos de la red. Cita: NIST Digital Identity.

9 **Pregunta 9** CONDUCTUAL **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La supervisión en tiempo real marca los procesos en ejecución que intentan escrituras ilegítimas o bloquear archivos. Cita: Center for Internet Security (CIS).

10 **Pregunta 10** **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Ningún antivirus detiene todos los ataques de día cero; las amenazas desconocidas pueden eludir las firmas y la heurística.

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. Firma hash	G 2. Heurística de código	E 3. Entorno aislado (sandbox) de archivos	C 4. Análisis de comportamiento
F 5. Actualizaciones diarias	H 6. Falso positivo	A 7. Aislamiento de amenazas	B 8. Herramienta antivirus

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 FIRMAS	2 ANÁLISIS HEURÍSTICO	3 SANDBOX	4 COMPORTAMIENTO
5 ACTUALIZACIONES	6 FALSO POSITIVO		

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

1 D – COMPORTAMIENTO	2 H – ANTIVIRUS	3 E – ACTUALIZACION	4 B – HEURISTICA
5 G – AISLAMIENTO	6 A – FIRMAHASH	7 C – SANDBOX	8 F – FALSOPOSITIVO

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar Firma hash, Heurística de código y Entorno aislado (sandbox) de archivos 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.

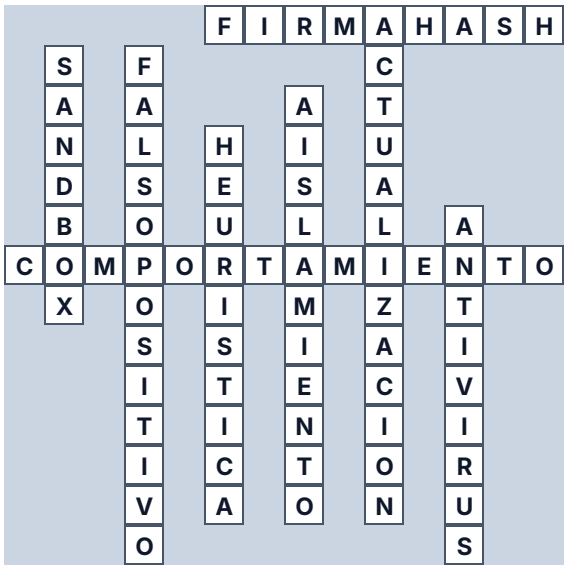
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



HORIZONTALES

1 horizontal: FIRMAHASH Huella criptográfica única en la base de datos que se usa para identificar amenazas conocidas (9 letras)

8 horizontal: COMPORTAMIENTO Supervisión de las acciones del software en ejecución en busca de patrones de funcionamiento malicioso (14 letras)

VERTICALES

2 vertical: ACTUALIZACION Descarga periódica de definiciones que alimenta la base de datos de amenazas (13 letras)

3 vertical: SANDBOX Entorno de prueba virtual y seguro que ejecuta código no fiable sin riesgo (7 letras)

4 vertical: FALSOPOSITIVO Alerta de seguridad que clasifica por error un software seguro como malware (13 letras)

5 vertical: AISLAMIENTO Confinamiento de archivos sospechosos para evitar que el sistema local quede expuesto (11 letras)

6 vertical: HEURISTICA Análisis basado en reglas que marca archivos con estructuras de código sospechosas (10 letras)

7 vertical: ANTIVIRUS Paquete de software que analiza y protege los dispositivos finales frente a exploits (9 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. HAMIFASHR — **FIRMAHASH**
2. SNXOBDA — **SANDBOX**
3. CAZCAONTIALIU — **ACTUALIZACION**
4. ITOMSANEAIL — **AISLAMIENTO**
5. ISAERTIHCU — **HEURISTICA**
6. RTEOMNATICOMOP — **COMPORTAMIENTO**
7. TISPFAIOOVLOS — **FALSOPOSITIVO**
8. SVUAINIRT — **ANTIVIRUS**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"DETECTA MALWARE NUEVO CON ANALISIS HEURISTICO"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Análisis por firmas frente a análisis heurístico

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un empleado descarga una utilidad personalizada creada internamente por otro equipo. El analizador de firmas la da por buena, pero el analizador heurístico la marca como sospechosa.
- Estrategia y solución recomendadas: Por qué ocurrió: el análisis por firmas comprueba los hash de los archivos; como es personalizado, no está en la base de datos de amenazas. La heurística analiza la estructura y marcó acciones sospechosas (p. ej., escrituras en el registro). Verificación: ejecutar el archivo en un entorno aislado (sandbox) para observar sus acciones, comprobar las firmas digitales y enviar el hash a portales de inteligencia de amenazas.

B Caso práctico 2: Gestión de falsos positivos

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: una desarrolladora de software compila su aplicación. El antivirus del sistema marca el nuevo ejecutable como malware y lo pone en cuarentena.
- Estrategia y solución recomendadas: Riesgos de la lista de permitidos: saltarse los analizadores puede permitir que se ejecute código realmente infectado. Vía de resolución: enviar el archivo al fabricante del antivirus para su análisis, firmar digitalmente el código mediante autoridades de certificación y configurar temporalmente excepciones para carpetas concretas en lugar de desactivar el antivirus.