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

Fundamentos de ciberseguridad y prevención de amenazas Prevención

Amenazas de ciberseguridad, cortafuegos de red, autenticación multifactor, marcos de seguridad

RESUMEN DE APRENDIZAJE: FUNDAMENTOS DE CIBERSEGURIDAD

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 principios fundamentales de la ciberseguridad y la prevención de amenazas en línea. Explorarás las amenazas de malware, la autenticación multifactor, los cortafuegos de red y los marcos de respuesta a incidentes.

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/

Tu hoja de ruta de aprendizaje sobre fundamentos de ciberseguridad

- Identificar los vectores habituales de malware, phishing e intrusión en redes corporativas.
- Implantar controles de ciberseguridad estándar, como MFA, cortafuegos y protección de los endpoints.
- Evalúa los procedimientos de respuesta ante incidentes para mitigar el impacto de las filtraciones de datos.
- Analiza los factores de riesgo de la organización y la alineación de la seguridad según las directrices del NIST.
- Configura prácticas de higiene de seguridad para mitigar el relleno automatizado de credenciales.

INSTRUCCIONES DE LA GUÍA DE CIBERSEGURIDAD

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 prevención de amenazas. Termina con la actividad extra Piensa rápido.

FUNDAMENTOS DE CIBERSEGURIDAD Y PREVENCIÓN DE AMENAZAS (INTRODUCCIÓN)

La ciberseguridad protege las redes, los sistemas y los datos frente a ataques digitales no autorizados. Desarrollar hábitos de seguridad sólidos, configurar cortafuegos, exigir la autenticación multifactor y formar al personal para reconocer amenazas son componentes esenciales de la defensa de la red corporativa.

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 objetivo principal de un ataque de phishing?

- A. Robar credenciales y datos sensibles de los usuarios
- B. Mejorar la visibilidad del sitio web en los motores de búsqueda
- C. Aumentar la capacidad del ancho de banda de la red
- D. Gestionar la replicación de los centros de datos de respaldo

2. ¿Qué mecanismo ofrece la protección más sólida para las cuentas?

- A. Autenticación multifactor con llaves de hardware
- B. Contraseñas complejas actualizadas cada treinta días
- C. Limitar el inicio de sesión de la cuenta al horario laboral
- D. Ocultar el nombre de usuario de la cuenta en los directorios públicos

3. ¿Qué define la carga útil de una infección de ransomware?

- A. Cifrar los archivos del sistema y exigir un pago
- B. Registrar silenciosamente las pulsaciones de teclas y enviarlas a servidores remotos
- C. Inyectar publicidad no autorizada en los navegadores
- D. Usar los recursos de la CPU local para minar criptomonedas

4. ¿Cómo afecta un exploit de día cero a las defensas de seguridad?

- A. Ataca vulnerabilidades desconocidas y sin parchear
- B. Desactiva automáticamente el cortafuegos corporativo
- C. Obliga al sistema a hacer un reinicio forzado
- D. No requiere ningún presupuesto para solucionarlo

5. ¿Qué marco rige los controles de seguridad corporativos?

- A. Directrices del Marco de Ciberseguridad del NIST
- B. Especificaciones del esquema de documentos HTML5 del W3C
- C. Manuales de instalación de controladores de impresora
- D. Definiciones de protocolos de enrutamiento del IETF

Punto de control 2: Reto de verdadero o falso

6 Pregunta vf 6

6. Los ataques de phishing solo se dirigen a cuentas de correo electrónico personales.

- ◯ Verdadero
- ◯ Falso

7 Pregunta vf 7

7. La autenticación multifactor ayuda a bloquear los ataques de relleno de credenciales.

- ◯ Verdadero
- ◯ Falso

8 Pregunta vf 8

8. Los cortafuegos inspeccionan el tráfico de red para bloquear el acceso no autorizado a los puertos.

- ◯ Verdadero
- ◯ Falso

9 Pregunta vf 9

9. Corregir los exploits de día cero requiere actualizaciones estándar de las definiciones del antivirus.

- ◯ Verdadero
- ◯ Falso

10 Pregunta vf 10

10. Un honeypot es un servidor señuelo que se usa para atraer a los ciberdelincuentes.

- ◯ 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. Los administradores de red instalan un _____ para filtrar el tráfico entrante.

2. Un atacante usa un _____ de día cero para eludir los parches del sistema.

3. Los atacantes envían correos falsificados para llevar a cabo campañas de _____ contra los empleados.

4. El ransomware es una forma destructiva de _____ que bloquea los datos del usuario.

5. Establecer una buena _____ de contraseñas reduce el riesgo de robo de credenciales.

6. Para proteger las comunicaciones sensibles, los usuarios aplican protocolos de _____ .

BANCO DE PALABRAS DE VOCABULARIO

CIFRADO CORTAFUEGOS EXPLOIT HIGIENE MALWARE MULTIFACTOR PHISHING RANSOMWARE

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

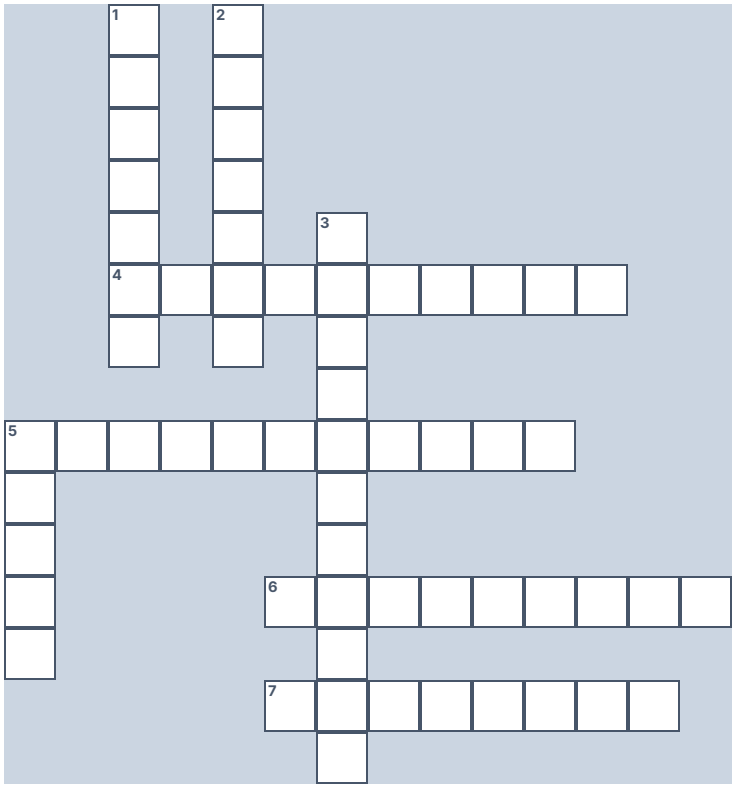
RELACIÓN DE DEFINICIONES

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. Amenaza de ransomware	A	Directrices estructuradas, como las del NIST, que se usan para gestionar los riesgos cibernéticos.
☐	2. Autenticación multifactor	B	Plan estructurado para gestionar y mitigar las brechas de seguridad.
☐	3. Exploit de día cero	C	Barrera de red que filtra el tráfico según reglas de seguridad.
☐	4. Honeypot señuelo	D	Malware que cifra los datos y exige un pago económico para descifrarlos.
☐	5. Cortafuegos contra intrusiones	E	Explotación de una vulnerabilidad antes de que el fabricante publique un parche.
☐	6. Respuesta a incidentes	F	Buenas prácticas para gestionar credenciales y claves de autenticación.
☐	7. Higiene de contraseñas	G	Validación de seguridad que exige dos o más factores de autenticación.
☐	8. Marco de seguridad	H	Sistema señuelo creado para atraer y analizar a actores maliciosos.

Punto de control 5: Crucigrama

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



HORIZONTALES

4. Malware que cifra los datos y exige un pago económico para descifrarlos (10)

5. Validación de seguridad que exige dos o más factores de autenticación (11)

6. Plan estructurado para gestionar y mitigar las brechas de seguridad (9)

7. Sistema señuelo creado para atraer y analizar a los actores maliciosos (8)

VERTICALES

1. Explotación de una vulnerabilidad antes de que el fabricante publique un parche (7)

2. Buenas prácticas para gestionar credenciales y claves de autenticación (7)

3. Barrera de red que filtra el tráfico según reglas de seguridad (11)

5. Directrices estructuradas, como las del NIST, que se usan para gestionar los riesgos cibernéticos (5)

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

4 horizontal: Malware que cifra los datos y exige un pago económico para descifrarlos (10 letras):

5 horizontal: Validación de seguridad que exige dos o más factores de autenticación (11 letras):

6 horizontal: Plan estructurado para gestionar y mitigar las brechas de seguridad (9 letras):

7 horizontal: Sistema señuelo creado para atraer y analizar a los actores maliciosos (8 letras):

VERTICALES

1 vertical: Explotación de una vulnerabilidad antes de que el fabricante publique un parche (7 letras):

2 vertical: Buenas prácticas para gestionar credenciales y claves de autenticación (7 letras):

3 vertical: Barrera de red que filtra el tráfico según reglas de seguridad (11 letras):

5 vertical: Directrices estructuradas, como las del NIST, que se usan para gestionar los riesgos cibernéticos (5 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.

M A R C O C O H X L K Y L X T

K E Q N K D I O N N D L Q P H

E E N N Q R S N T T I G C S P

R N Ñ I R B V E D S A Z U C Z

A E V G K M H Y Z D C N E R Q

W I X P C U U P B A E Z Ñ E D

M G L A E L Ñ O E F R H I S D

O I R Q M T E T I R O Z S P F

S H Q V F I A A Q O N P T U X

N Q K R T F R D N Y B G R E X

A C O R T A F U E G O S W S J

R A R Z Y C Y L G I N Q K T M

M T O H P T Q H Z A O V G A U

C Y R Y B O H M Z G K Ñ P Ñ W

C M Z Y G R Y O W U L U P B Ñ

LISTA DE PALABRAS DE VOCABULARIO

RANSOMWARE MULTIFACTOR DIACERO HONEYPOT CORTAFUEGOS
RESPUESTA HIGIENE MARCO

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. RANSOMWARE**
- **B. MULTIFACTOR**
- **C. DIACERO**
- **D. HONEYPOT**
- **E. CORTAFUEGOS**
- **F. RESPUESTA**
- **G. HIGIENE**
- **H. MARCO**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Barrera de red que filtra el tráfico según reglas de seguridad.

_____ 2. Plan estructurado para gestionar y mitigar las brechas de seguridad.

_____ 3. Malware que cifra los datos y exige un pago económico para descifrarlos.

_____ 4. Validación de seguridad que exige dos o más factores de autenticación.

_____ 5. Buenas prácticas para gestionar credenciales y claves de autenticación.

_____ 6. Directrices estructuradas, como las del NIST, que se usan para gestionar los riesgos cibernéticos.

_____ 7. Explotación de una vulnerabilidad antes de que el fabricante publique un parche.

_____ 8. Sistema señuelo creado para atraer y analizar a los actores maliciosos.

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. RWMOARAESN
2. DAORECI
3. CUFEROOSAGT
4. EIEINHG
5. TUCALRIFMOT
6. OTEPHYON
7. ERTASPEUS
8. OMRCA

Actividad extra: Piensa rápido

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

1	Profesiones de la ciberseguridad			
2	Razones para actualizar el software			
3	Cosas que puede bloquear un cortafuegos			
4	Señales de alerta en un correo electrónico			
5	Cosas de las que haces copia de seguridad			
6	Tipos de ciberataque conocidos			
7	Cosas que puede atraer un honeypot			
8	Información que nunca deberías compartir			
9	Señales de que un ordenador está infectado			
10	Películas o series sobre hackers			
11	Capas de seguridad que puedes crear			
12	Cosas que practicar en un simulacro de seguridad			
13	Herramientas de seguridad que conoces			
14	Personas a las que puedes pedir ayuda informática			
15	Palabras que empiezan por 'ciber'			

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: ESTRATEGIA DE RECUPERACIÓN FRENTE AL RANSOMWARE



Escenario: Una red corporativa está infectada con ransomware, que bloquea bases de datos críticas. Los atacantes exigen un pago de $100,000 en criptomonedas. La empresa tiene copias de seguridad sin conexión de hace 24 horas.

Pregunta de debate: analiza los riesgos de pagar y evalúa la estrategia de recuperación.

CASO PRÁCTICO 2: DEFENSAS CONTRA EL RELLENO DE CREDENCIALES



Escenario: Un servicio en línea sufre un ataque de relleno de credenciales, en el que los hackers prueban millones de pares de usuario y contraseña robados de otros sitios.

Pregunta de debate: Detalla el mecanismo de este ataque y describe dos sistemas de defensa.

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 9 20 21 5 13 1

3 16 14 1 22 21 5 14 21 9 3 1 3 9 16 14

13 22 12 21 9 6 1 3 21 16 19

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: ¿Cuál es el objetivo principal de la ciberseguridad?

El objetivo principal es proteger las redes, los dispositivos y los datos frente a accesos no autorizados, ataques y daños accidentales.

Q2: ¿En qué se diferencia el phishing del spear phishing?

El phishing es una campaña de correo masiva dirigida a usuarios aleatorios, mientras que el spear phishing se dirige a personas concretas usando datos personalizados.

Q3: ¿Qué es un cortafuegos de red?

Un cortafuegos es un sistema de seguridad de red que supervisa y filtra el tráfico entrante y saliente según unas reglas de seguridad predefinidas.

Q4: ¿Por qué es necesaria la autenticación multifactor (MFA)?

La MFA añade una capa de defensa fundamental que impide el acceso aunque los atacantes roben o descifren las credenciales de la contraseña principal.

Q5: ¿Qué define a un virus informático?

Un virus es un malware que se replica a sí mismo, se adjunta a archivos limpios y se propaga por los sistemas una vez ejecutado.

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 bloquea el ransomware los datos locales?

El ransomware utiliza algoritmos criptográficos para cifrar los archivos del usuario y hacerlos ilegibles hasta que se aplica una clave de descifrado.

Q7: ¿Qué es una vulnerabilidad de día cero?

Un zero-day (día cero) es una vulnerabilidad de seguridad de un software que el fabricante desconoce, lo que no deja tiempo para desarrollar un parche antes de que se explote.

Q8: ¿Qué papel desempeña el marco del NIST?

El marco del NIST ofrece directrices y estándares voluntarios para ayudar a las organizaciones a gestionar y reducir los riesgos de ciberseguridad.

Q9: ¿Qué es un plan de respuesta a incidentes de seguridad?

Es un conjunto documentado de procedimientos para detectar y contener las brechas de seguridad y los compromisos de la red, y recuperarse de ellos.

Q10: ¿Cómo explota la ingeniería social a los usuarios?

La ingeniería social usa la manipulación psicológica para engañar a los empleados y que revelen contraseñas o descarguen archivos maliciosos.

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 satura un ataque DDoS los servidores web?

Un ataque DDoS coordina millones de dispositivos comprometidos de una botnet para inundar un servidor de tráfico y agotar su ancho de banda y su capacidad de CPU.

Q2: ¿Qué diferencia hay entre el cifrado simétrico y el asimétrico?

El cifrado simétrico usa una única clave para cifrar y descifrar, mientras que el cifrado asimétrico usa un par de claves pública y privada.

Q3: ¿Cómo ejecutan los hackers los ataques de inyección SQL?

Los atacantes introducen comandos SQL maliciosos en los campos de formularios y engañan a la base de datos del servidor para que revele registros de usuarios sin autorización.

Q4: ¿Qué es el movimiento lateral en las intrusiones de red?

Es la técnica en la que los atacantes aprovechan un acceso inicial a un servidor para comprometer otros sistemas interconectados de la red interna.

Q5: ¿Cómo redirige el tráfico web la suplantación de DNS (DNS spoofing)?

La suplantación de DNS altera los registros de caché de los servidores de nombres y dirige a usuarios legítimos a sitios web maliciosos de aspecto similar en lugar de a los dominios de destino.

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 un token de seguridad físico?

Es un dispositivo físico (como una YubiKey) que genera pruebas de autenticación criptográficas y ofrece la máxima defensa contra el phishing remoto.

Q7: ¿Cómo usan los equipos de seguridad los honeypots señuelo?

Los equipos despliegan servidores señuelo fuera de producción para detectar intrusiones de forma temprana y analizar los patrones de ataque de actores no autorizados.

Q8: ¿Qué es el principio de mínimo privilegio?

Es el estándar de seguridad que restringe los derechos de acceso de los usuarios al mínimo absolutamente necesario para desempeñar sus funciones.

Q9: ¿Cómo explota las conexiones un ataque de intermediario (Man-in-the-Middle)?

Un atacante intercepta y altera las comunicaciones entre dos dispositivos en redes sin cifrar y roba tokens de sesión y credenciales.

Q10: ¿Qué son los indicadores de compromiso (IOC)?

Los IOC son pistas forenses, como modificaciones inusuales del registro o tráfico IP sospechoso, que muestran que un sistema ha sido vulnerado.

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 atacantes escanean constantemente internet en busca de servidores vulnerables y envían correos de phishing a las bandejas de entrada de los empleados.

2. PERSPECTIVA SOBRE SEGURIDAD

El error humano, como hacer clic en enlaces de phishing, es un factor habitual en las violaciones de datos, por eso la formación es importante.

3. PERSPECTIVA SOBRE SEGURIDAD

Los costes de una filtración de datos incluyen multas legales, pérdida de clientes, investigación y reparación, y pueden alcanzar millones de dólares.

4. PERSPECTIVA SOBRE SEGURIDAD

La MFA resistente al phishing, como las llaves de seguridad físicas, es el tipo de MFA más sólido y el estándar que recomienda encarecidamente CISA. [2]

5. PERSPECTIVA SOBRE SEGURIDAD

El ransomware sigue siendo una amenaza importante para las redes empresariales, y la CISA insta a tener copias de seguridad cifradas y sin conexión como defensa clave. [4]

6. PERSPECTIVA SOBRE SEGURIDAD

El NIST Cybersecurity Framework 2.0 (2024) tiene seis funciones básicas: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. [1]

7. PERSPECTIVA SOBRE SEGURIDAD

Los bots de relleno de credenciales prueban a gran escala pares de usuario y contraseña filtrados en los portales de inicio de sesión de bancos y comercios electrónicos.

8. PERSPECTIVA SOBRE SEGURIDAD

Existen mercados de exploits de día cero en todo el mundo, donde las vulnerabilidades de gravedad alta pueden venderse por grandes sumas antes de ser corregidas.

9. PERSPECTIVA SOBRE SEGURIDAD

Un sistema señuelo honeypot notifica las alertas de intrusión de inmediato, ya que los usuarios legítimos no tienen ningún motivo para acceder a él.

10. PERSPECTIVA SOBRE SEGURIDAD

Transport Layer Security (TLS) cifra las sesiones del navegador, lo que impide la captura de paquetes (sniffing) en redes wifi públicas.

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

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

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

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

[6] 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

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Clave de respuestas: Punto de control 1 – Opción múltiple

1 **Ataques de phishing** PHISHING — **Respuesta correcta: A**

NOTA PARA DOCENTES

Las campañas de phishing intentan robar credenciales y datos confidenciales de los usuarios mediante correos electrónicos suplantados. Cita: OWASP Secure Configuration.

2 **Protección de la cuenta** CLAVE MFA — **Respuesta correcta: A**

NOTA PARA DOCENTES

La autenticación multifactor (MFA) con tokens de hardware proporciona la defensa más sólida para el acceso a las cuentas. Cita: NIST Digital Identity.

3 **Amenaza de ransomware** RANSOMWARE — **Respuesta correcta: A**

NOTA PARA DOCENTES

El ransomware cifra sistemas y datos críticos y exige un pago en criptomonedas a cambio de las claves de descifrado. Cita: Center for Internet Security (CIS).

4 **Vulnerabilidad de día cero** DÍA CERO — **Respuesta correcta: A**

NOTA PARA DOCENTES

Las amenazas de día cero explotan fallos de seguridad desconocidos y sin parchear antes de que el fabricante publique un parche. Cita: OWASP Secure Configuration.

5 **Marcos de seguridad** MARCOS — **Respuesta correcta: A**

NOTA PARA DOCENTES

Marcos como el del NIST ofrecen directrices estructuradas para ayudar a las organizaciones a gestionar y reducir los riesgos cibernéticos. Cita: NIST Digital Identity.

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

6 **Phishing dirigido** PHISHING — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Los ataques de phishing se dirigen tanto a redes corporativas como a cuentas personales para ampliar sus vectores de explotación. Cita: OWASP Secure Configuration.

7 **Pregunta 7** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La MFA exige un segundo factor, por lo que una contraseña robada por sí sola no suele bastar para iniciar sesión.

8 **Cortafuegos de tráfico** CORTAFUEGOS — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los cortafuegos inspeccionan y bloquean el tráfico en puertos de red específicos para filtrar las conexiones no autorizadas. Cita: Center for Internet Security (CIS).

9 **Respuesta ante ataques de día cero** DÍA CERO — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Corregir las vulnerabilidades de día cero requiere parches de código y filtrado con WAF, ya que todavía no existen firmas. Cita: OWASP Secure Configuration.

10 **Honeypots señuelo** HONEYPOT — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los honeypots son servidores señuelo que utilizan los equipos de seguridad para atraer y estudiar a los actores maliciosos y alertar sobre ellos. Cita: Center for Internet Security (CIS).

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. Amenaza de ransomware	G 2. Autenticación multifactor	E 3. Exploit de día cero	H 4. Honeypot señuelo
C 5. Cortafuegos contra intrusiones	B 6. Respuesta a incidentes	F 7. Higiene de contraseñas	A 8. Marco de seguridad

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 CORTAFUEGOS	2 EXPLOIT	3 PHISHING	4 MALWARE
5 HIGIENE	6 CIFRADO		

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

1 E – CORTAFUEGOS	2 F – RESPUESTA	3 A – RANSOMWARE	4 B – MULTIFACTOR
5 G – HIGIENE	6 H – MARCO	7 C – DIACERO	8 D – HONEYPOT

NOTAS DE DEBATE PARA DOCENTES

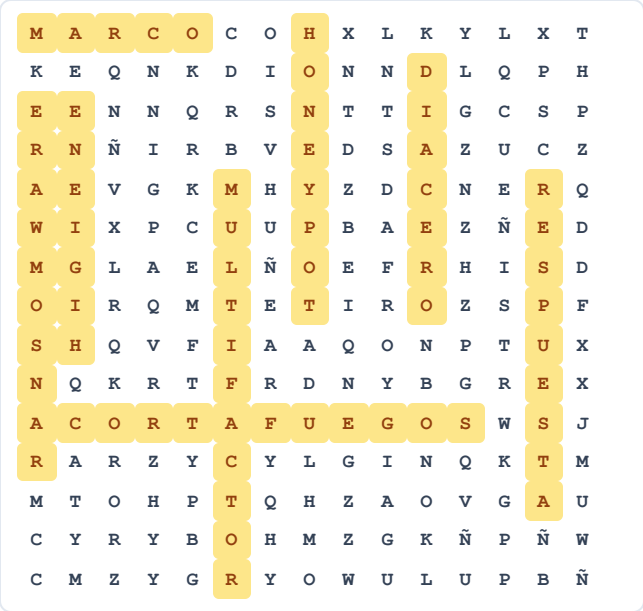
Términos clave:
Comprueba que los estudiantes saben explicar Amenaza de ransomware, Autenticación multifactor y Exploit de día cero con sus propias palabras y dar un ejemplo de cada uno.

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

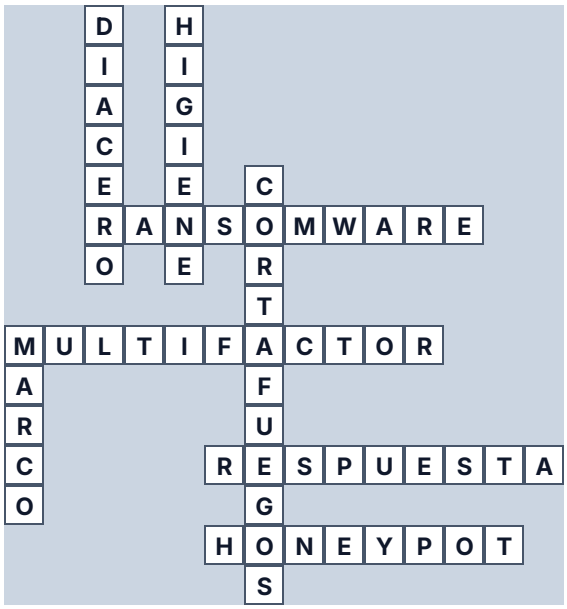
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS



SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

4 horizontal: RANSOMWARE Malware que cifra los datos y exige un pago económico para descifrarlos (10 letras)

5 horizontal: MULTIFACTOR Validación de seguridad que exige dos o más factores de autenticación (11 letras)

6 horizontal: RESPUESTA Plan estructurado para gestionar y mitigar las brechas de seguridad (9 letras)

7 horizontal: HONEYPOT Sistema señuelo creado para atraer y analizar a los actores maliciosos (8 letras)

VERTICALES

1 vertical: DIACERO Explotación de una vulnerabilidad antes de que el fabricante publique un parche (7 letras)

2 vertical: HIGIENE Buenas prácticas para gestionar credenciales y claves de autenticación (7 letras)

3 vertical: CORTAFUEGOS Barrera de red que filtra el tráfico según reglas de seguridad (11 letras)

5 vertical: MARCO Directrices estructuradas, como las del NIST, que se usan para gestionar los riesgos cibernéticos (5 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. RWMOARAESN — **RANSOMWARE**
2. DAORECI — **DIACERO**
3. CUFEROOSAGT — **CORTAFUEGOS**
4. EIEINHG — **HIGIENE**
5. TUCALRIFMOT — **MULTIFACTOR**
6. OTEPHYON — **HONEYPOT**
7. ERTASPEUS — **RESPUESTA**
8. OMRCA — **MARCO**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"PROTEGE TU SISTEMA CON AUTENTICACION MULTIFACTOR"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Estrategia de recuperación frente al ransomware

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: la red de una empresa está infectada con ransomware que bloquea bases de datos críticas. Los atacantes exigen un pago de $100,000 en criptomonedas. La empresa tiene copias de seguridad sin conexión de hace 24 horas.
- Estrategia y solución recomendadas: Riesgos de pagar: pagar no garantiza el descifrado de los archivos, marca a la empresa como un objetivo que paga y financia actividades delictivas. Estrategia de recuperación: el equipo debe aislar los equipos infectados, borrar los servidores comprometidos y restaurar los datos desde copias de seguridad sin conexión. Debe corregir el vector de acceso inicial (phishing o exploit) para evitar una reinfección inmediata.

B Caso práctico 2: Defensas contra el relleno de credenciales

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Un servicio online sufre un ataque de relleno de credenciales (credential stuffing): los hackers prueban millones de pares de usuario y contraseña robados de otros sitios.
- Estrategia y solución recomendadas: Mecanismo: los atacantes aprovechan la reutilización de contraseñas entre sitios usando bots automatizados para entrar en las cuentas de los usuarios. Defensas: 1. La autenticación multifactor (MFA) bloquea los intentos de inicio de sesión aunque la contraseña sea correcta. 2. Implantar limitación de frecuencia y CAPTCHA bloquea el tráfico de bots automatizados que satura los puntos de inicio de sesión.