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

Prevención del robo de identidad y activos
Guía de seguridad

Fugas de credenciales, MFA, vigilancia de la dark web, alertas de congelación de crédito, ingeniería social

RESUMEN DE APRENDIZAJE SOBRE LA PREVENCIÓN DEL ROBO DE IDENTIDAD

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 la prevención y la mitigación del robo de identidad. Explorarás las filtraciones de credenciales, la autenticación multifactor, la supervisión de la web oscura, las alertas de congelación del crédito y la defensa frente a la ingeniería social.

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/robo-identidad/

Tu hoja de ruta de aprendizaje sobre protección de la identidad

- Comprende los riesgos de exposición de credenciales en los foros de la dark web.
- Implantar la autenticación multifactor (MFA) y alertas de congelación de crédito.
- Diseña defensas de seguridad corporativas contra estafas dirigidas de ingeniería social.

INSTRUCCIONES DE LA GUÍA SOBRE EL ROBO DE IDENTIDAD

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

PREVENCIÓN DEL ROBO DE IDENTIDAD Y SEGURIDAD DE LOS ACTIVOS (INTRODUCCIÓN)

El robo de identidad aprovecha credenciales filtradas e inicios de sesión débiles para secuestrar cuentas personales y corporativas. Implantar MFA, congelaciones de crédito, escáneres de la dark web y los marcos SPF/DKIM/DMARC constituye una defensa fundamental contra la suplantación digital.

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 método principal que usan los ladrones de identidad para robar credenciales de inicio de sesión?

- A. Enviar alertas falsas por correo electrónico para engañar a los usuarios y que introduzcan sus contraseñas en portales falsificados
- B. Escuchar emisiones de radio cerca de la oficina corporativa de un usuario
- C. Desfragmentar la unidad de almacenamiento del servidor local de un usuario
- D. Desconectar las configuraciones de copia de seguridad en redes externas

2. ¿Qué control de seguridad ofrece la defensa más sólida frente a las filtraciones de credenciales?

- A. Autenticación multifactor con llaves de hardware
- B. Crear contraseñas largas con los formatos predeterminados del navegador
- C. Cambiar los nombres de usuario del correo cada seis meses
- D. Eliminar los historiales del navegador con cookies de rastreo almacenadas

3. ¿Qué opción representa la congelación del crédito?

- A. Bloquear los informes de crédito para impedir que los ladrones abran préstamos no autorizados
- B. Eliminar historiales de transacciones de cuentas bancarias de las bases de datos
- C. Desactivar los lectores de banda magnética de tarjetas de crédito en los escáneres
- D. Cifrar en reposo los discos duros de la base de datos local

4. ¿Por qué es útil la supervisión de la dark web?

- A. Avisa a los usuarios si sus credenciales filtradas aparecen en bases de datos ilícitas
- B. Impide que el malware activo se ejecute en entornos aislados virtuales
- C. Acelera la velocidad de enrutamiento del navegador en redes virtuales
- D. Bloquea los intentos de acceso por inyección SQL a la base de datos del servidor

5. ¿Qué significa la ingeniería social?

- A. Manipular a las personas para que revelen voluntariamente credenciales confidenciales
- B. Escanear los puertos de los servidores corporativos en busca de exploits de seguridad activos
- C. Hacer copias de seguridad de los archivos de bases de datos del sistema en discos duros sin conexión
- D. Enrutar los paquetes de red a través de tres nodos onion cifrados

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. El robo de identidad solo afecta a las cuentas digitales en línea, no al correo postal físico.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. Exigir la MFA en todas las cuentas personales bloquea la mayoría de los ataques de bots de relleno de credenciales.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. Una congelación del crédito bloquea las consultas de crédito, pero te impide acceder a tu propia cuenta bancaria.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. Los gestores de contraseñas protegen a los usuarios del phishing al negarse a autocompletar contraseñas en dominios suplantados.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. Los correos de phishing suelen usar un lenguaje urgente para provocar respuestas emocionales y rápidas.

- ○ 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 ladrones de identidad van a por las contraseñas personales y las _____ de usuario.

2. Avisar a los usuarios de brechas en bases de datos permite identificar _____ de cuentas privadas.

3. Exigir un código temporal para iniciar sesión se denomina autenticación _____ .

4. Rastrear foros de hackers en busca de datos robados es la _____ de la dark web.

5. Para bloquear las consultas de crédito no autorizadas se necesita una _____ del crédito.

6. Formar a los empleados para reconocer el phishing crea una _____ de seguridad activa.

BANCO DE PALABRAS DE VOCABULARIO

CONGELACIÓN | CREDENCIALES | DEFENSA | FILTRACIONES | MONITORIZACIÓN | MULTIFACTOR | PHISHING | SUPLANTACIÓN

Escribe aquí tus respuestas:

1.
2.
3.
4.
5.
6.

Punto de control 4: Relación de conceptos de seguridad

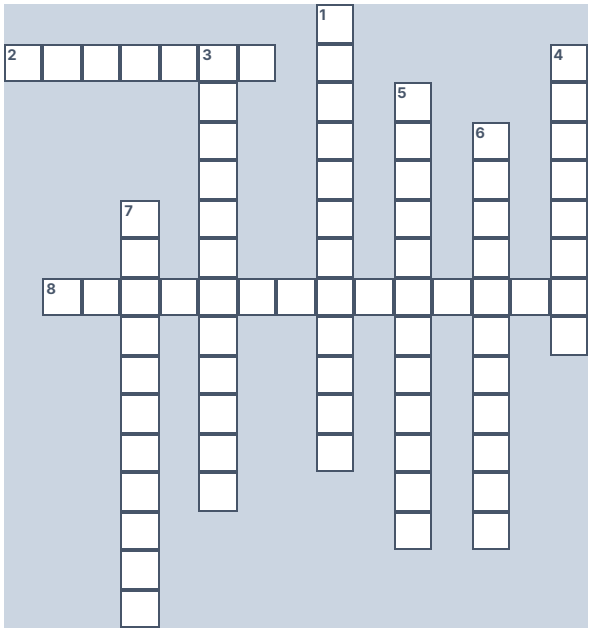
RELACIÓN DE DEFINICIONES

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. CREDENCIALES	A	Paso de verificación secundario (como las llaves de hardware) que protege el inicio de sesión en las cuentas.
☐	2. FUGAS	B	Crear un sitio web o un correo electrónico falso para imitar a una organización legítima.
☐	3. MFA	C	Restringir el acceso a los expedientes de crédito para evitar solicitudes de préstamo fraudulentas.
☐	4. SUPERVISIÓN	D	Exposición no autorizada de bases de datos privadas que contienen registros personales de usuarios.
☐	5. CONGELACIÓN	E	Formación y controles técnicos que se usan para protegerse del robo de identidad.
☐	6. DEFENSA	F	Enviar mensajes fraudulentos para engañar a los usuarios y que entreguen sus credenciales.
☐	7. SUPLANTACIÓN	G	Rastrear foros en línea y canales de hackers en busca de datos corporativos robados.
☐	8. PHISHING	H	Nombres de usuario, contraseñas y tokens privados que se usan para autenticar identidades digitales.

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. Formación y controles técnicos que se usan para protegerse del robo de identidad. (7)

8. Rastreo de foros en línea y canales de hackers en busca de datos corporativos robados. (14)

VERTICALES

1. Nombres de usuario, contraseñas y tokens privados que se usan para autenticar identidades digitales. (12)

3. Creación de un sitio web o correo electrónico falso que imita a una organización legítima. (12)

4. Envío de mensajes fraudulentos para engañar a los usuarios y que entreguen sus credenciales. (8)

5. Exposición no autorizada de bases de datos privadas que contienen registros personales de usuarios. (12)

6. Paso de verificación secundario (como las llaves de hardware) que protege el inicio de sesión en las cuentas. (11)

7. Restricción del acceso a los expedientes de crédito para evitar solicitudes de préstamos fraudulentas. (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: Formación y controles técnicos que se usan para protegerse del robo de identidad. (7 letras):

8 horizontal: Rastreo de foros en línea y canales de hackers en busca de datos corporativos robados. (14 letras):

VERTICALES

1 vertical: Nombres de usuario, contraseñas y tokens privados que se usan para autenticar identidades digitales. (12 letras):

3 vertical: Creación de un sitio web o correo electrónico falso que imita a una organización legítima. (12 letras):

4 vertical: Envío de mensajes fraudulentos para engañar a los usuarios y que entreguen sus credenciales. (8 letras):

5 vertical: Exposición no autorizada de bases de datos privadas que contienen registros personales de usuarios. (12 letras):

6 vertical: Paso de verificación secundario (como las llaves de hardware) que protege el inicio de sesión en las cuentas. (11 letras):

7 vertical: Restricción del acceso a los expedientes de crédito para evitar solicitudes de préstamos fraudulentas. (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.

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

LISTA DE PALABRAS DE VOCABULARIO

CREDENCIALES FILTRACIONES MULTIFACTOR MONITORIZACION CONGELACION
DEFENSA SUPLANTACION PHISHING

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. CREDENCIALES**
- **B. FILTRACIONES**
- **C. MULTIFACTOR**
- **D. MONITORIZACION**
- **E. CONGELACION**
- **F. DEFENSA**
- **G. SUPLANTACION**
- **H. PHISHING**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Envío de mensajes fraudulentos para engañar a los usuarios y que entreguen sus credenciales.

_____ 2. Nombres de usuario, contraseñas y tokens privados que se usan para autenticar identidades digitales.

_____ 3. Creación de un sitio web o correo electrónico falso que imita a una organización legítima.

_____ 4. Formación y controles técnicos que se usan para protegerse del robo de identidad.

_____ 5. Rastreo de foros en línea y canales de hackers en busca de datos corporativos robados.

_____ 6. Restricción del acceso a los expedientes de crédito para evitar solicitudes de préstamos fraudulentas.

_____ 7. Exposición no autorizada de bases de datos privadas que contienen registros personales de usuarios.

_____ 8. Paso de verificación secundario (como las llaves de hardware) que protege el inicio de sesión en las cuentas.

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. ANIERCLCEESD
2. IRUMOFLTCAT
3. CALCNOONEIG
4. OAAPTNNICSUL
5. INICSLROAFET
6. ORCTNIIOAMOZNI
7. DSNAEEF
8. SHHGPNII

Actividad extra: Piensa rápido

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

1	Cosas que hacer si te roban la identidad			
2	Cosas que no compartir en redes sociales			
3	Cosas de las que haces copia de seguridad			
4	Tarjetas o documentos de identidad de tu cartera			
5	Documentos que deberías proteger			
6	Cosas que hacer tras una filtración de datos			
7	Razones para actualizar el software			
8	Información que quiere un ladrón de identidad			
9	Dispositivos que pueden ser hackeados			
10	Lugares por los que se pueden filtrar tus datos			
11	Hábitos seguros que puedes empezar hoy			
12	Señales de que un ordenador está infectado			
13	Formas de demostrar quién eres			
14	Señales de robo de identidad			
15	Señales de alerta en un correo electrónico			

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: PROTECCIÓN FRENTE A LA SUPLANTACIÓN DE IDENTIDAD DE DIRECTIVOS



Escenario: Un alto directivo de perfil destacado ha sido objetivo de nombres de dominio con errores tipográficos (typosquatting) que imitan su correo personal para estafar a clientes. Diseña un plan de protección de la marca.

Pregunta de debate: Analiza los riesgos de suplantación de la marca y detalla los controles SPF/DKIM/DMARC y de autenticación.

CASO PRÁCTICO 2: EXPOSICIÓN DE CREDENCIALES CORPORATIVAS EN LA DARK WEB



Escenario: Un volcado de base de datos en la dark web contiene varios cientos de credenciales corporativas de administradores de sistemas de una empresa. Diseña una estrategia de mitigación.

Pregunta de debate: Describe el proceso de limpieza de credenciales y planifica la implantación de un gestor de contraseñas.

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 9 4 5 14 21 9 4 1 4

4 9 7 9 21 1 12 3 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: ¿Qué es el robo de identidad?

Un delito en el que un atacante roba datos personales (como contraseñas o números de la Seguridad Social) para suplantar a otra persona y obtener un beneficio económico.

Q2: ¿Cuál es la causa más habitual del robo de identidad?

El phishing es una de las principales formas en que los ladrones obtienen contraseñas, atrayendo a los usuarios a sitios web falsos y suplantados.

Q3: ¿Cómo protege la autenticación multifactor (MFA) las identidades?

La MFA exige una segunda prueba (como una llave de hardware) para iniciar sesión, lo que bloquea a los atacantes aunque roben tu contraseña.

Q4: ¿Qué es una congelación de crédito?

Un servicio gratuito que impide que las agencias de crédito compartan tu expediente de crédito, de modo que los ladrones no puedan abrir nuevos préstamos a tu nombre. [2]

Q5: ¿Qué es la supervisión de la web oscura?

Software que revisa foros de hackers en busca de correos, contraseñas y datos personales filtrados y te avisa si tus datos quedan expuestos.

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 relleno de credenciales (credential stuffing)?

Bots automatizados que prueban listas de contraseñas filtradas en cientos de sitios web para apoderarse de cuentas activas.

Q7: ¿Por qué es peligrosa la suplantación de correo electrónico (email spoofing)?

Permite a los atacantes falsificar el nombre del remitente en los correos electrónicos, de modo que los mensajes de phishing parezcan enviados por compañeros de confianza.

Q8: ¿Cómo frenan los gestores de contraseñas el robo de identidad?

Guardan contraseñas complejas y únicas para cada cuenta y se niegan a autocompletar las credenciales en dominios de phishing falsos.

Q9: ¿Qué es el spear phishing?

Un ataque de phishing muy dirigido, personalizado con el nombre y los datos de la víctima para aumentar las posibilidades de engaño.

Q10: ¿En qué se diferencia una alerta de crédito de una congelación?

Una alerta indica a los prestamistas que verifiquen tu identidad antes de abrir cuentas, mientras que una congelación bloquea por completo el acceso a tu expediente de crédito. [2]

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 conduce el SIM swapping al robo de identidad?

Los atacantes convencen al personal del operador para que transfiera el número de teléfono de la víctima a una nueva tarjeta SIM y así secuestran los códigos 2FA enviados por SMS.

Q2: ¿Qué función cumple DMARC en la prevención del robo de identidad?

DMARC permite a los propietarios de dominios impedir que los correos suplantados lleguen a las bandejas de entrada, frenando los correos falsos que imitan dominios corporativos.

Q3: ¿Por qué es difícil detectar el robo de identidad sintética?

Los ladrones combinan números de la Seguridad Social (SSN) reales con nombres y fechas de nacimiento falsos para crear perfiles crediticios totalmente nuevos, eludiendo las alertas básicas de fraude.

Q4: ¿Cómo explotan los intermediarios de datos las identidades personales?

Los intermediarios de datos recopilan registros públicos, comportamiento en la web e historiales de compra para elaborar expedientes de perfiles, que pueden filtrarse o venderse.

Q5: ¿Por qué se considera vulnerable la MFA basada en SMS?

El tráfico SMS es vulnerable a la interceptación, al phishing y a los ataques de SIM swapping a nivel del operador.

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 bloqueo del expediente de crédito?

Un servicio comercial parecido a una congelación, que permite a los usuarios desbloquear o bloquear al instante su expediente de crédito desde una aplicación móvil.

Q7: ¿Cómo alimentan las filtraciones de datos corporativas el robo de identidad?

Las bases de datos filtradas exponen millones de credenciales en texto plano y dan a los ladrones los datos en bruto necesarios para cometer fraudes de identidad dirigidos.

Q8: ¿Qué riesgo tiene compartir demasiado en las redes sociales?

Compartir públicamente nombres de mascotas, lugares de nacimiento y apellidos de soltera de la madre da a los ladrones las respuestas a las preguntas habituales de recuperación de cuentas.

Q9: ¿Cómo protegen los inicios de sesión biométricos los perfiles de identidad?

La biometría vincula los inicios de sesión a rasgos como las huellas dactilares o el rostro; guardados en el dispositivo son difíciles de robar, pero los datos biométricos almacenados pueden filtrarse.

Q10: ¿Cómo combate la Red Flags Rule el robo de identidad?

Una normativa federal que obliga a las entidades financieras a elaborar programas escritos para detectar las señales de alerta de robo de identidad y responder a ellas.

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

IdentityTheft.gov, gestionado por la FTC, permite a las víctimas de EE. UU. denunciar el robo de identidad y obtener un plan de recuperación personalizado. [1]

2. PERSPECTIVA SOBRE SEGURIDAD

Las llaves de seguridad físicas son una MFA resistente al phishing, el tipo de MFA más robusto que recomienda encarecidamente CISA. [4]

3. PERSPECTIVA SOBRE SEGURIDAD

Las contraseñas comprometidas son una vía de entrada habitual en las filtraciones de datos y alimentan después el fraude de identidad.

4. PERSPECTIVA SOBRE SEGURIDAD

Una congelación del crédito es gratuita por ley federal e impide que los prestamistas consulten tu expediente de crédito hasta que lo desbloquees. [2]

5. PERSPECTIVA SOBRE SEGURIDAD

DMARC permite a los propietarios de dominios indicar a los servidores de correo que rechacen o pongan en cuarentena el correo suplantado que no supera las comprobaciones. [7]

6. PERSPECTIVA SOBRE SEGURIDAD

El SIM swapping permite a los hackers burlar la autenticación en dos pasos por SMS en los portales bancarios.

7. PERSPECTIVA SOBRE SEGURIDAD

El fraude de identidad sintética mezcla datos reales y falsos, lo que dificulta que los prestamistas lo detecten.

8. PERSPECTIVA SOBRE SEGURIDAD

Muchas personas reutilizan la misma contraseña en varias cuentas en línea, por lo que una sola filtración puede exponer varias de ellas.

9. PERSPECTIVA SOBRE SEGURIDAD

Los corredores de datos recopilan expedientes detallados sobre un gran número de consumidores, lo que crea un riesgo concentrado para la privacidad.

10. PERSPECTIVA SOBRE SEGURIDAD

Recuperarse de un robo de identidad puede suponer meses de trabajo, como reclamar cargos y corregir informes de crédito.

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] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Clave de respuestas: Punto de control 1 – Opción múltiple

1 Pregunta 1

Respuesta correcta: A

NOTA PARA DOCENTES

¿Cuál es el método principal que usan los ladrones de identidad para robar credenciales de inicio de sesión? → Enviar alertas falsas por correo electrónico para engañar a los usuarios y que introduzcan sus contraseñas en portales falsificados

2 Pregunta 2

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué control de seguridad ofrece la defensa más sólida frente a las filtraciones de credenciales? → Autenticación multifactor con llaves de hardware

3 Pregunta 3

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué opción representa la congelación del crédito? → Bloquear los informes de crédito para impedir que los ladrones abran préstamos no autorizados

4 Pregunta 4

Respuesta correcta: A

NOTA PARA DOCENTES

¿Por qué es útil la supervisión de la dark web? → Avisa a los usuarios si sus credenciales filtradas aparecen en bases de datos ilícitas

5 Pregunta 5

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué significa la ingeniería social? → Manipular a las personas para que revelen voluntariamente credenciales confidenciales

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

6 **Pregunta 6**

Respuesta correcta: Falso

NOTA PARA DOCENTES

El robo de identidad también puede empezar fuera de internet, por ejemplo con correo o documentos robados.

7 **Pregunta 7**

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Exigir la MFA en todas las cuentas personales bloquea la mayoría de los ataques de bots de relleno de credenciales.

8 **Pregunta 8**

Respuesta correcta: Falso

NOTA PARA DOCENTES

Una congelación del crédito impide nuevas consultas de crédito, pero no afecta a tus cuentas existentes.

9 **Pregunta 9**

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Los gestores de contraseñas protegen a los usuarios del phishing al negarse a autocompletar contraseñas en dominios suplantados.

10 **Pregunta 10**

Respuesta correcta: Verdadero

NOTA PARA DOCENTES

Los correos de phishing suelen usar un lenguaje urgente para provocar respuestas emocionales y rápidas.

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

H 1. CREDENCIALES	D 2. FUGAS	A 3. MFA	G 4. SUPERVISIÓN
C 5. CONGELACIÓN	E 6. DEFENSA	B 7. SUPLANTACIÓN	F 8. PHISHING

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 CREDENCIALES	2 FILTRACIONES	3 MULTIFACTOR	4 MONITORIZACIÓN
5 CONGELACIÓN	6 DEFENSA		

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

1 H – PHISHING	2 A – CREDENCIALES	3 G – SUPLANTACION	4 F – DEFENSA
5 D – MONITORIZACION	6 E – CONGELACION	7 B – FILTRACIONES	8 C – MULTIFACTOR

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar CREDENCIALES, FUGAS y MFA 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.

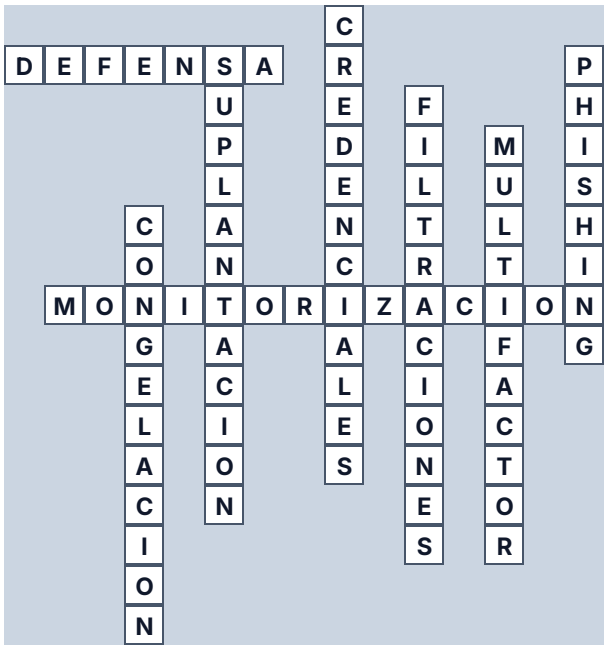
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

2 horizontal: DEFENSA Formación y controles técnicos que se usan para protegerse del robo de identidad. (7 letras)

8 horizontal: MONITORIZACION Rastreo de foros en línea y canales de hackers en busca de datos corporativos robados. (14 letras)

VERTICALES

1 vertical: CREDENCIALES Nombres de usuario, contraseñas y tokens privados que se usan para autenticar identidades digitales. (12 letras)

3 vertical: SUPLANTACION Creación de un sitio web o correo electrónico falso que imita a una organización legítima. (12 letras)

4 vertical: PHISHING Envío de mensajes fraudulentos para engañar a los usuarios y que entreguen sus credenciales. (8 letras)

5 vertical: FILTRACIONES Exposición no autorizada de bases de datos privadas que contienen registros personales de usuarios. (12 letras)

6 vertical: MULTIFACTOR Paso de verificación secundario (como las llaves de hardware) que protege el inicio de sesión en las cuentas. (11 letras)

7 vertical: CONGELACION Restricción del acceso a los expedientes de crédito para evitar solicitudes de préstamos fraudulentas. (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. ANIERCLCEESD — **CREDENCIALES**
2. IRUMOFLTCAT — **MULTIFACTOR**
3. CALCNOONEIG — **CONGELACION**
4. OAAPTNNICSUL — **SUPLANTACION**
5. INICSLROAFET — **FILTRACIONES**
6. ORCTNIIOAMOZNI — **MONITORIZACION**
7. DSNAEEF — **DEFENSA**
8. SHHGPNII — **PHISHING**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"PROTEGE TU IDENTIDAD DIGITAL CON MULTIFACTOR"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Protección frente a la suplantación de identidad de directivos

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un alto directivo muy conocido ha sido objeto de nombres de dominio con errores tipográficos (typosquatting) que imitan su correo personal para estafar a clientes. Diseña un plan de protección de marca.
- Estrategia y solución recomendadas: registrar todas las variantes ortográficas habituales del nombre del directivo. Implantar protocolos de autenticación de correo (DMARC, DKIM, SPF) para evitar la suplantación del dominio. Imponer MFA por hardware en todos los inicios de sesión corporativos de la alta dirección.

B Caso práctico 2: Exposición de credenciales corporativas en la dark web

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un volcado de base de datos en la web oscura contiene varios cientos de credenciales corporativas de los administradores de sistemas de una empresa. Diseña una estrategia de mitigación.
- Estrategia y solución recomendadas: realizar un restablecimiento de contraseñas en toda la empresa. Exigir el uso de un gestor de contraseñas empresarial. Aplicar la MFA en todos los portales del sistema y configurar alertas automatizadas y continuas de supervisión de la web oscura.