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

Estafas en línea e ingeniería social Guía de protección

Phishing por correo electrónico, dominios suplantados, vishing, estafas de soporte técnico, verificación por un canal alternativo, BEC

RESUMEN DE APRENDIZAJE: ESTAFAS EN LÍNEA

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 defensa contra estafas online. Explorarás los sitios web de phishing falsos, las tácticas de ingeniería social, las estafas de soporte técnico, los vectores de fraude en transferencias y los métodos de verificación de pagos.

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/estafas-en-linea/

Tu hoja de ruta de aprendizaje sobre protección contra estafas en línea

- Identificar los indicadores habituales de estafas de soporte técnico y de dominios de typosquatting.
- Implantar protocolos de verificación del correo electrónico (SPF, DKIM, DMARC) contra la suplantación.
- Establece la verificación de las transacciones por un canal alternativo para evitar el fraude en las transferencias empresariales.

INSTRUCCIONES DE LA GUÍA SOBRE ESTAFAS EN LÍNEA

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 frente a estafas en línea. Termina con la actividad extra Piensa rápido.

PROTECCIÓN CONTRA ESTAFAS EN LÍNEA E INGENIERÍA SOCIAL (INTRODUCCIÓN)

Las estafas en línea explotan el comportamiento humano mediante phishing, ventanas emergentes de falso soporte, vishing y fraude por transferencia bancaria. Exigir la verificación de las transacciones por un canal independiente y aplicar las reglas de dominio SPF/DKIM/DMARC ayuda a bloquear los vectores de ingeniería social en la puerta de enlace.

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 principal indicio de una estafa de soporte técnico?

- A. Una ventana emergente que afirma que tu sistema está infectado y te exige que llames a un número de teléfono
- B. Una actualización de seguridad automática descargada de un registro oficial
- C. Un gestor de contraseñas que se niega a rellenar las credenciales en un dominio corporativo
- D. Una copia de seguridad de archivos en segundo plano configurada en una unidad externa

2. ¿Qué técnica utiliza dominios de remitente falsificados para robar datos bancarios?

- A. Phishing por correo electrónico
- B. Escaneo de puertos
- C. Inyección en memoria
- D. Borrado criptográfico

3. ¿Qué opción representa el fraude por transferencia bancaria?

- A. Engañar a las víctimas con ingeniería social para que envíen dinero a cuentas corporativas falsas
- B. Cifrar las bases de datos del sistema mediante cargas útiles de ransomware
- C. Consultar bases de datos mediante comandos de inyección SQL
- D. Hacer copias de seguridad de los archivos del sistema en discos de almacenamiento sin conexión

4. ¿Por qué los estafadores crean sitios web de compras falsos?

- A. Robar los datos de las tarjetas de crédito y las credenciales de pago de los compradores
- B. Alojar tablas de bases de datos de análisis de malware en entornos aislados
- C. Para acelerar la entrega de los pedidos en línea
- D. Para probar gratis nuevos diseños de sitios web

5. ¿Qué significa vishing?

- A. Estafas de phishing por voz a través de redes telefónicas para robar credenciales
- B. Buscar dispositivos del sistema sin proteger en las redes locales
- C. Restaurar las bases de datos del sistema tras una filtración no autorizada
- D. Ejecutar código no fiable dentro de contenedores virtuales seguros

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Las estafas de phishing solo se dirigen a usuarios finales, nunca a directivos como objetivos de whaling.

- ◯ Verdadero
- ◯ Falso

7 Pregunta 7

7. Los dominios suplantados suelen usar pequeñas erratas (como amaz0n.com) para imitar marcas de confianza.

- ◯ Verdadero
- ◯ Falso

8 Pregunta 8

8. Las estafas de soporte técnico se pueden resolver concediendo acceso remoto a quien llama.

- ◯ Verdadero
- ◯ Falso

9 Pregunta 9

9. La ingeniería social explota la psicología humana, como el miedo y la urgencia, para saltarse las normas de seguridad.

- ◯ Verdadero
- ◯ Falso

10 Pregunta 10

10. Las solicitudes de transferencia bancaria siempre deben verificarse por canales de comunicación alternativos (fuera de banda).

- ◯ 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 correos fraudulentos que engañan a los usuarios se llaman _____ .

2. Una dirección web que imita a una marca de confianza es un sitio _____ .

3. Las estafas telefónicas para robar datos bancarios se llaman _____ .

4. Una ventana emergente que exige dinero por eliminar un virus es una _____ de soporte técnico.

5. Confirmar una solicitud de pago requiere una _____ por un canal independiente.

6. Desviar las transacciones de una empresa a las cuentas de un ladrón es un fraude de _____ .

BANCO DE PALABRAS DE VOCABULARIO

ESTAFA FALSIFICADO PHISHING SMISHING TRANSFERENCIA BANCARIA VERIFICACIÓN VISHING WHALING

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

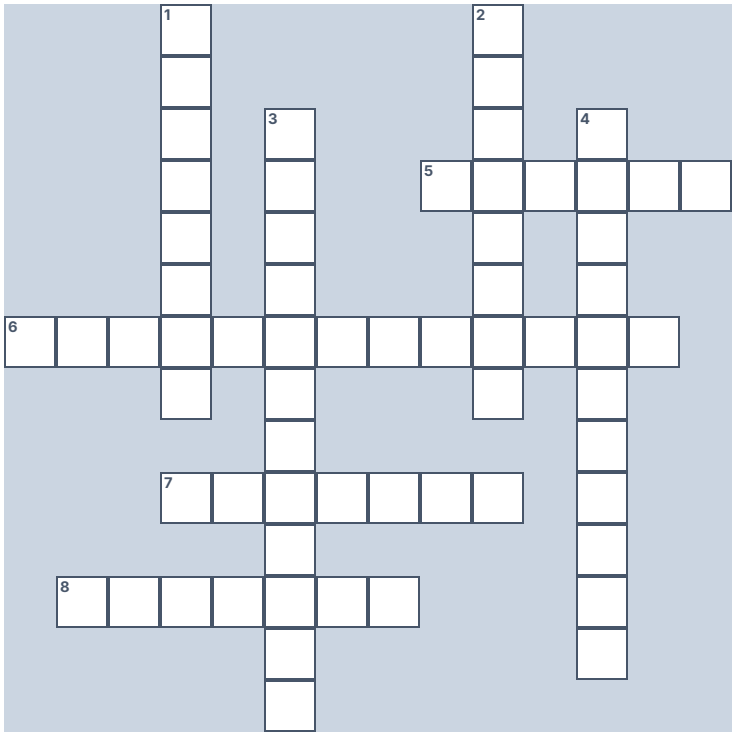
RELACIÓN DE DEFINICIONES

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. PHISHING	A	Desvío fraudulento de transacciones bancarias a cuentas de delincuentes.
☐	2. SUPLANTADO	B	Estafa diseñada para robar dinero o credenciales de acceso a las víctimas.
☐	3. VISHING	C	Enviar mensajes de texto fraudulentos para robar credenciales de cuentas móviles.
☐	4. ESTAFA	D	Llamadas de voz fraudulentas diseñadas para robar credenciales y datos de cuentas.
☐	5. VERIFICACIÓN	E	Ataques de phishing dirigidos que buscan robar las credenciales de los altos directivos.
☐	6. CABLE	F	Dirección de remitente de correo o de sitio web imitada para que parezca legítima.
☐	7. WHALING	G	Campañas de correo fraudulentas diseñadas para robar credenciales de inicio de sesión y contraseñas.
☐	8. SMISHING	H	Confirmar los datos de pago mediante un método de contacto secundario de confianza.

Punto de control 5: Crucigrama

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



HORIZONTALES

5. Plan fraudulento diseñado para robar dinero o credenciales de acceso a las víctimas. (6)

6. Desvío fraudulento de transacciones bancarias a cuentas de delincuentes. (13)

7. Ataques de phishing dirigidos a robar credenciales de altos directivos. (7)

8. Llamadas de voz fraudulentas diseñadas para robar credenciales y datos de cuentas. (7)

VERTICALES

1. Envío de mensajes de texto fraudulentos para robar credenciales de cuentas móviles. (8)

2. Campañas de correo fraudulentas diseñadas para robar credenciales de inicio de sesión y contraseñas. (8)

3. Confirmación de los datos de pago mediante un segundo método de contacto de confianza. (12)

4. Remitente de correo o dirección web imitados para parecer legítimos. (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

5 horizontal: Plan fraudulento diseñado para robar dinero o credenciales de acceso a las víctimas. (6 letras):

6 horizontal: Desvío fraudulento de transacciones bancarias a cuentas de delincuentes. (13 letras):

7 horizontal: Ataques de phishing dirigidos a robar credenciales de altos directivos. (7 letras):

8 horizontal: Llamadas de voz fraudulentas diseñadas para robar credenciales y datos de cuentas. (7 letras):

VERTICALES

1 vertical: Envío de mensajes de texto fraudulentos para robar credenciales de cuentas móviles. (8 letras):

2 vertical: Campañas de correo fraudulentas diseñadas para robar credenciales de inicio de sesión y contraseñas. (8 letras):

3 vertical: Confirmación de los datos de pago mediante un segundo método de contacto de confianza. (12 letras):

4 vertical: Remitente de correo o dirección web imitados para parecer legítimos. (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.

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

LISTA DE PALABRAS DE VOCABULARIO

PHISHING FALSIFICADO VISHING ESTAFA VERIFICACION TRANSFERENCIA WHALING SMISHING

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. PHISHING**
- **B. FALSIFICADO**
- **C. VISHING**
- **D. ESTAFA**
- **E. VERIFICACION**
- **F. TRANSFERENCIA**
- **G. WHALING**
- **H. SMISHING**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Remitente de correo o dirección web imitados para parecer legítimos.

_____ 2. Confirmación de los datos de pago mediante un segundo método de contacto de confianza.

_____ 3. Desvío fraudulento de transacciones bancarias a cuentas de delincuentes.

_____ 4. Envío de mensajes de texto fraudulentos para robar credenciales de cuentas móviles.

_____ 5. Ataques de phishing dirigidos a robar credenciales de altos directivos.

_____ 6. Llamadas de voz fraudulentas diseñadas para robar credenciales y datos de cuentas.

_____ 7. Campañas de correo fraudulentas diseñadas para robar credenciales de inicio de sesión y contraseñas.

_____ 8. Plan fraudulento diseñado para robar dinero o credenciales de acceso a las víctimas.

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. NSHPIHGI
2. VSGNIHI
3. VEACOCRINFI I
4. GHILNWA
5. AACILOIFFDS
6. FAETAS
7. NCRFTRESAIA EN
8. SMHGSNII

Actividad extra: Piensa rápido

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

1	Dispositivos que pueden ser hackeados			
2	Frases que suelen usar los estafadores			
3	Métodos de pago que piden los estafadores			
4	Tipos de estafas en línea			
5	Ofertas demasiado buenas para ser verdad			
6	Lugares donde denunciar una estafa			
7	Palabras relacionadas con la ciberseguridad			
8	Personas a las que puedes avisar sobre estafas			
9	Cosas de las que haces copia de seguridad			
10	Señales de alerta en un correo electrónico			
11	Señales de que un ordenador está infectado			
12	Formas de comprobar una tienda en línea			
13	Formas de proteger tus cuentas			
14	Cosas que hacer si te estafan			
15	Cosas que hacer tras una filtración de datos			

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: PREVENCIÓN DE ESTAFAS CON TRANSFERENCIAS BANCARIAS CORPORATIVAS

👷

Escenario: El departamento financiero recibe un correo urgente desde una dirección suplantada de un proveedor en el que se pide que las futuras transferencias de facturas se envíen a un nuevo número de ruta bancaria.

Pregunta de debate: Describe la política de verificación contra el fraude en transferencias y especifica los bloqueos de autenticación del correo electrónico.

CASO PRÁCTICO 2: INCIDENTE DE PHISHING DE TIPO WHALING CONTRA DIRECTIVOS

👷

Escenario: Un directivo hizo clic en un enlace de phishing que decía contener un documento seguro de una reunión del consejo e introdujo sus credenciales corporativas principales en un portal suplantado.

Pregunta de debate: Detalla los pasos de respuesta al incidente y explica cómo auditar los inicios de sesión de los directivos.

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		5	12		17	8	9	20	8	9	14	7

3	16	14		23	5	19	9	6	9	3	1	3	9	16	14

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 una estafa en línea?

Un plan fraudulento que usa canales digitales para engañar a las víctimas y que envíen dinero o entreguen sus credenciales personales.

Q2: ¿Cuál es el principal indicio de un correo de phishing?

Un mensaje que alega urgencia (como la suspensión de una cuenta) y te dirige a un enlace que no coincide con el dominio oficial.

Q3: ¿Qué es el typosquatting?

Registrar dominios con errores tipográficos habituales de marcas populares (como amaz0n.com) para alojar sitios falsos de phishing.

Q4: ¿Qué es una estafa de soporte técnico?

Una ventana emergente que afirma que tu PC está infectado y te indica que llames a un número y pagues por un falso software de limpieza o por servicios de acceso remoto. [1]

Q5: ¿Qué es el vishing?

Ataques de phishing que usan llamadas telefónicas para engañar a las víctimas y que faciliten sus datos bancarios o de inicio de sesión.

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 fraude electrónico (wire fraud)?

Desvío de transacciones de pago a cuentas fraudulentas suplantando a proveedores o directivos.

Q7: ¿Qué es el whaling?

Una forma muy dirigida de spear phishing que apunta directamente a objetivos de alto valor, como los altos directivos de una empresa.

Q8: ¿Qué es el smishing?

Mensajes de texto fraudulentos enviados a dispositivos móviles, con enlaces a portales falsos o a supuestas actualizaciones de seguimiento.

Q9: ¿Por qué es fundamental la verificación fuera de banda?

Confirma los detalles de la transacción por un canal de comunicación independiente (como una llamada telefónica), evitando los hilos de correo comprometidos.

Q10: ¿Cómo funciona una estafa con un falso depósito en garantía (escrow)?

Los estafadores crean un sitio falso de depósito en garantía (escrow), afirman que los fondos están a buen recaudo y luego roban la transferencia del comprador.

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 usan los estafadores el BEC (compromiso del correo electrónico empresarial) para cometer fraude por transferencia bancaria?

Secuestran la cuenta de correo electrónico de un empleado legítimo, vigilan los hilos de facturas y envían datos de facturación actualizados con cuentas bancarias fraudulentas.

Q2: ¿Qué riesgo suponen los ataques homográficos IDN en las estafas en línea?

Usar caracteres no ASCII que parecen idénticos a las letras normales (p. ej., la 'a' cirílica) para registrar dominios falsos que imitan a marcas reales.

Q3: ¿Por qué es importante inspeccionar los encabezados de correo electrónico para detectar estafas?

Revela la IP real del servidor de origen y el estado de validación SPF/DKIM, lo que muestra si el dominio del remitente está falsificado.

Q4: ¿Cómo explotan los estafadores de soporte técnico el software de escritorio remoto?

Usan herramientas como AnyDesk o TeamViewer para conectarse al dispositivo de la víctima, instalar malware y robar las contraseñas guardadas.

Q5: ¿Cuál es el objetivo de las estafas de pago por adelantado?

Engañar a las víctimas para que paguen por adelantado gastos de tramitación a cambio de una gran recompensa económica que no existe.

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 usan los estafadores la elaboración de perfiles en redes sociales para el phishing dirigido?

Recopilan las estructuras organizativas de las empresas y los nombres de los empleados para redactar correos de spear phishing convincentes.

Q7: ¿Por qué las tiendas web falsas ofrecen grandes descuentos?

Para atraer a los compradores a introducir los datos de su tarjeta de crédito y capturar las credenciales para reutilizarlas o revenderlas en foros de carding.

Q8: ¿Cómo bloquean los registros DMARC las estafas de phishing?

DMARC permite a los propietarios de dominios pedir a los receptores que pongan en cuarentena o rechacen el correo que no supera las comprobaciones alineadas de SPF y DKIM, bloqueando la suplantación directa. [5]

Q9: ¿Qué amenaza suponen los portales de robo de credenciales?

Páginas de destino falsificadas diseñadas para parecer exactamente iguales a Microsoft 365 o Google Workspace, que roban las credenciales de acceso a medida que se introducen.

Q10: ¿Cómo denuncian y desactivan los equipos de seguridad los dominios fraudulentos?

Enviando pruebas del fraude al correo de abusos del registrador, al proveedor de alojamiento y al registro de Google Safe Browsing.

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

El phishing y la suplantación fueron el tipo de delito más denunciado al IC3 del FBI en 2025, con 191,561 denuncias. [2]

2. PERSPECTIVA SOBRE SEGURIDAD

El compromiso del correo electrónico empresarial (BEC) causó más de $3 mil millones en pérdidas notificadas al IC3 del FBI en 2025. [2]

3. PERSPECTIVA SOBRE SEGURIDAD

Los dominios con typosquatting se diferencian de los nombres de marca reales en uno o dos caracteres, por lo que un vistazo rápido puede pasarlos por alto.

4. PERSPECTIVA SOBRE SEGURIDAD

Las estafas de soporte técnico causaron más de $2.1 mil millones en pérdidas denunciadas al IC3 del FBI en 2025. [2]

5. PERSPECTIVA SOBRE SEGURIDAD

Los ataques homográficos parecen idénticos en la barra de direcciones del navegador, a menos que este muestre la configuración punycode.

6. PERSPECTIVA SOBRE SEGURIDAD

Las estafas por mensajes SMS (smishing) usan mensajes cortos y urgentes con enlaces, que dejan a las víctimas poco contexto para detectar el fraude.

7. PERSPECTIVA SOBRE SEGURIDAD

Los ataques de whaling se dirigen a los correos de los directivos porque estos controlan el acceso a grandes transferencias de pago.

8. PERSPECTIVA SOBRE SEGURIDAD

Verificar los cambios de pago llamando a un número de teléfono conocido y guardado es una defensa clave contra el fraude por transferencia BEC.

9. PERSPECTIVA SOBRE SEGURIDAD

Los sitios web falsos de depósito en garantía (escrow) son una estafa habitual en los mercados en línea: parecen un servicio de pago seguro, pero roban la transferencia bancaria del comprador.

10. PERSPECTIVA SOBRE SEGURIDAD

Google Safe Browsing avisa a los usuarios antes de que abran sitios que ha marcado como phishing o malware.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

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

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

[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. (n.d.). Malware, Phishing, and Ransomware.

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

[5] 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 principal indicio de una estafa de soporte técnico? → Una ventana emergente que afirma que tu sistema está infectado y te exige que llames a un número de teléfono

2 **Pregunta 2** — **Respuesta correcta: A**

NOTA PARA DOCENTES

¿Qué técnica utiliza dominios de remitente falsificados para robar datos bancarios? → Phishing por correo electrónico

3 **Pregunta 3** — **Respuesta correcta: A**

NOTA PARA DOCENTES

¿Qué opción representa el fraude por transferencia bancaria? → Engañar a las víctimas con ingeniería social para que envíen dinero a cuentas corporativas falsas

4 **Pregunta 4** — **Respuesta correcta: A**

NOTA PARA DOCENTES

¿Por qué los estafadores crean sitios web de compras falsos? → Robar los datos de las tarjetas de crédito y las credenciales de pago de los compradores

5 **Pregunta 5** — **Respuesta correcta: A**

NOTA PARA DOCENTES

¿Qué significa vishing? → Estafas de phishing por voz a través de redes telefónicas para robar credenciales

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

6 **Pregunta 6** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Falso: el phishing también se dirige a directivos; el whaling es phishing dirigido a altos cargos.

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

NOTA PARA DOCENTES

Los dominios suplantados suelen usar pequeñas erratas (como amaz0n.com) para imitar marcas de confianza.

8 **Pregunta 8** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Falso: dar acceso remoto a un estafador que se hace pasar por soporte técnico le permite instalar malware y robar datos.

9 **Pregunta 9** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

La ingeniería social explota la psicología humana, como el miedo y la urgencia, para saltarse las normas de seguridad.

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

NOTA PARA DOCENTES

Las solicitudes de transferencia bancaria siempre deben verificarse por canales de comunicación alternativos (fuera de banda).

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

G 1. PHISHING	F 2. SUPLANTADO	D 3. VISHING	B 4. ESTAFA
H 5. VERIFICACIÓN	A 6. CABLE	E 7. WHALING	C 8. SMISHING

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 PHISHING	2 FALSIFICADO	3 VISHING	4 ESTAFA
5 VERIFICACIÓN	6 TRANSFERENCIA BANCARIA		

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

1 B – FALSIFICADO	2 E – VERIFICACION	3 F – TRANSFERENCIA	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – ESTAFA

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar PHISHING, SUPLANTADO y VISHING 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.

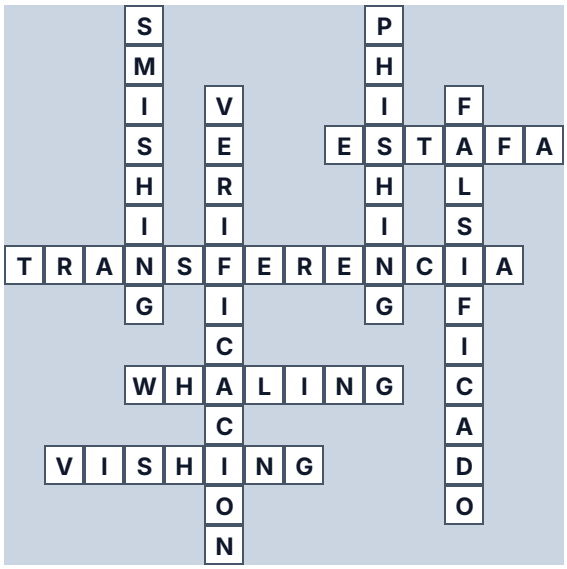
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

5 horizontal: ESTAFA Plan fraudulento diseñado para robar dinero o credenciales de acceso a las víctimas. (6 letras)

6 horizontal: TRANSFERENCIA Desvío fraudulento de transacciones bancarias a cuentas de delincuentes. (13 letras)

7 horizontal: WHALING Ataques de phishing dirigidos a robar credenciales de altos directivos. (7 letras)

8 horizontal: VISHING Llamadas de voz fraudulentas diseñadas para robar credenciales y datos de cuentas. (7 letras)

VERTICALES

1 vertical: SMISHING Envío de mensajes de texto fraudulentos para robar credenciales de cuentas móviles. (8 letras)

2 vertical: PHISHING Campañas de correo fraudulentas diseñadas para robar credenciales de inicio de sesión y contraseñas. (8 letras)

3 vertical: VERIFICACION Confirmación de los datos de pago mediante un segundo método de contacto de confianza. (12 letras)

4 vertical: FALSIFICADO Remitente de correo o dirección web imitados para parecer legítimos. (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.	NSHPIHGI	PHISHING	5.	AACILOIFFDS	FALSIFICADO
2.	VSGNIHI	VISHING	6.	FAETAS	ESTAFA
3.	VEACOCRINFII	VERIFICACION	7.	NCRFTRESAIAEN	TRANSFERENCIA
4.	GHILNWA	WHALING	8.	SMHGSNII	SMISHING

CLAVE DEL RETO DEL CÓDIGO SECRETO

"DETECTA EL PHISHING CON VERIFICACION"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Prevención de estafas con transferencias bancarias corporativas

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un departamento financiero recibe un correo urgente desde una dirección suplantada de un proveedor, que pide que las futuras transferencias de facturas se envíen a un nuevo número de cuenta.
- Estrategia y solución recomendadas: aplicar una política de doble autorización para todos los pagos. Implementar una verificación fuera de banda mediante un número de teléfono guardado previamente y bloquear en la pasarela los correos de dominios suplantados.

B Caso práctico 2: Incidente de phishing de tipo whaling contra directivos

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Un directivo hizo clic en un enlace de phishing que decía contener un documento seguro de una reunión del consejo e introdujo sus credenciales corporativas principales en un portal falsificado.
- Estrategia y solución recomendadas: aislar el dispositivo del directivo. Restablecer todos los tokens de sesión y credenciales corporativos. Revisar los registros de acceso en busca de salida de datos e implantar MFA por hardware en todos los inicios de sesión.