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

Ataques de phishing e ingeniería social

Spear phishing, estafas de whaling, protocolos SPF/DKIM/DMARC, suplantación del remitente y formación en seguridad para empleados.

RESUMEN DE APRENDIZAJE: ATAQUES DE PHISHING

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 ataques de phishing y la ingeniería social. Explorarás el spear phishing, el whaling, la suplantación de dominios, los protocolos SPF/DKIM/DMARC, la seguridad de los enlaces y la formación de concienciación de los empleados.

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/ataques-phishing/

Tu hoja de ruta de aprendizaje sobre mitigación del phishing

- Identificar las estafas habituales de phishing, vishing y ventanas emergentes de soporte técnico.
- Implantar procedimientos de verificación de transacciones por un canal independiente (fuera de banda).
- Configura reglas SPF, DKIM y DMARC para bloquear dominios suplantados.

INSTRUCCIONES DE LA GUÍA SOBRE ATAQUES DE PHISHING

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 autenticación del correo electrónico. Termina con la actividad extra Piensa rápido.

ATAQUES DE PHISHING E INGENIERÍA SOCIAL (INTRODUCCIÓN)

Los ataques de phishing utilizan mensajes dirigidos, estafas de whaling y suplantación de dominios para obtener las credenciales de inicio de sesión de los usuarios. Proteger los sistemas corporativos requiere implantar reglas SPF, DKIM y DMARC en la puerta de enlace junto con pasos de aprobación por un canal independiente.

LEE ATENTAMENTE CADA PUNTO DE CONTROL Y SELECCIONA O ESCRIBE LA RESPUESTA CORRECTA.

Punto de control 1: Reto de opción múltiple

1. ¿Qué es el spear phishing?

- A. Un correo de phishing dirigido y adaptado a una persona u organización concreta
- B. Un correo masivo genérico enviado a millones de direcciones aleatorias
- C. Un ataque de red que inunda de tráfico los servidores web
- D. Una técnica de extracción de bases de datos dirigida a los registros de usuarios

2. ¿Qué protocolo permite a un dominio indicar en el DNS sus direcciones IP de envío autorizadas para combatir la suplantación?

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3. ¿Qué es un ataque de whaling?

- A. Una campaña de phishing dirigida específicamente a altos directivos de empresas
- B. Un ataque de inyección SQL dirigido a las copias de seguridad de la base de datos
- C. Un robo físico del equipo de router de la red de área local
- D. Un análisis automatizado de fuerza bruta mediante relleno de credenciales

4. ¿Qué hace DKIM?

- A. Añade una firma criptográfica a los correos electrónicos para verificar la autenticidad del remitente
- B. Bloquea el tráfico de paquetes de red entrante en el cortafuegos
- C. Cifra los volúmenes de almacenamiento de la base de datos en reposo
- D. Analiza los archivos adjuntos del correo electrónico en busca de malware basado en firmas

5. ¿Qué función cumple DMARC?

- A. Indicar a los servidores de correo receptores cómo gestionar los mensajes que no superan las comprobaciones SPF/DKIM
- B. Descifrar contraseñas del sistema con tablas arcoíris precalculadas
- C. Comprimir los archivos adjuntos del correo antes de enviarlos
- D. Configurar los privilegios de acceso al enrutamiento de la red

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. El spear phishing se basa en correos masivos genéricos enviados a millones de direcciones aleatorias.

- ◯ Verdadero
- ◯ Falso

7 Pregunta 7

7. Las políticas DMARC pueden indicar a los servidores de correo que rechacen los mensajes suplantados no autorizados.

- ◯ Verdadero
- ◯ Falso

8 Pregunta 8

8. La verificación SPF funciona validando la firma criptográfica del cuerpo del correo.

- ◯ Verdadero
- ◯ Falso

9 Pregunta 9

9. Los ataques de whaling se dirigen a administradores corporativos de bajo nivel para acceder a archivos de bases de datos.

- ◯ Verdadero
- ◯ Falso

10 Pregunta 10

10. La verificación de las solicitudes de pago por un canal independiente ayuda a detener las estafas con transferencias bancarias.

- ◯ 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. Atacar a un empleado concreto con información personalizada es phishing _____ .

2. Falsificar la cabecera de un correo para que los mensajes parezcan legítimos es la _____ del remitente.

3. La lista del DNS con las IP de los servidores de correo autorizados es el registro _____ .

4. El estándar de firma de correo electrónico que permite verificar al remitente es _____ .

5. Para establecer políticas que rechacen los mensajes que no superan las comprobaciones SPF/DKIM se usa _____ .

6. Una campaña de phishing contra altos directivos se llama _____ .

BANCO DE PALABRAS DE VOCABULARIO

DIRIGIDO DKIM DMARC PHISHING SPF SUPLANTACIÓN VISHING WHALING

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

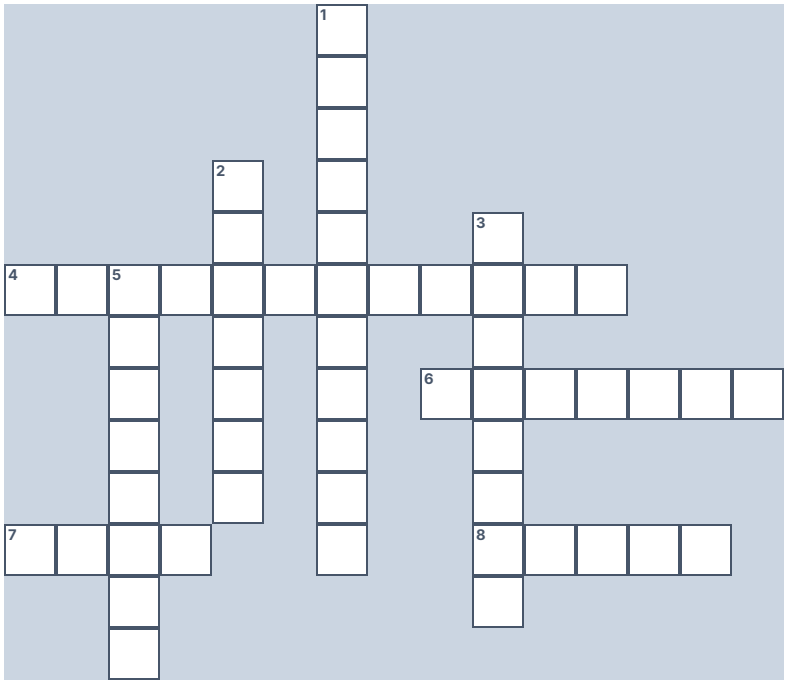
RELACIÓN DE DEFINICIONES

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. SPEAR PHISHING	A	Llamadas fraudulentas por voz.
☐	2. SUPLANTACIÓN	B	Dirigido a altos directivos.
☐	3. SPF	C	Instrucciones de rechazo de la política.
☐	4. DKIM	D	IP de remitentes autorizados en el DNS.
☐	5. DMARC	E	Correo de ingeniería social.
☐	6. WHALING	F	Correo electrónico dirigido y personalizado.
☐	7. PHISHING	G	Falsificación de la dirección de correo del remitente.
☐	8. VISHING	H	Firma criptográfica en el correo electrónico.

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. Falsificación de la dirección del remitente de un correo. (12)

6. Llamadas fraudulentas por voz. (7)

7. Firma criptográfica en el correo electrónico. (4)

8. Política con instrucciones de rechazo. (5)

VERTICALES

1. IP de remitentes autorizados publicadas en el DNS. (11)

2. Ataque dirigido a altos directivos. (7)

3. Correo personalizado contra un objetivo concreto. (8)

5. Correo de ingeniería social. (8)

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: Falsificación de la dirección del remitente de un correo. (12 letras):

6 horizontal: Llamadas fraudulentas por voz. (7 letras):

7 horizontal: Firma criptográfica en el correo electrónico. (4 letras):

8 horizontal: Política con instrucciones de rechazo. (5 letras):

VERTICALES

1 vertical: IP de remitentes autorizados publicadas en el DNS. (11 letras):

2 vertical: Ataque dirigido a altos directivos. (7 letras):

3 vertical: Correo personalizado contra un objetivo concreto. (8 letras):

5 vertical: Correo de ingeniería social. (8 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.

D M A R C I N P N L Q P H N N

F Q R S T T G H C S W P Ñ I R

P G B V D M S I Z U H C Z V G

S N K H I Z D S N E A Q X P C

O I U K B A Z H Ñ D L L A D E

R H D Ñ E F H I I D I R Q I M

T S E I R Z S N F Q N V F R A

S I A Q O N P G T X G Q K I R

I V T R D N Y B G R X W J G A

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

E S U P L A N T A C I O N D O

R H P Q H Z A O V G U C Y O R

Y B H M Z G K Ñ P Ñ W C M Z Y

G Y O W U L U P B Ñ V T M H U

D Y U K R B W Z Y M R Q X I O

LISTA DE PALABRAS DE VOCABULARIO

DIRIGIDO SUPLANTACION REGISTROSPF DKIM DMARC WHALING PHISHING VISHING

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	DEFINICIONES Y CAMPOS DE RELACIÓN
A. DIRIGIDO	_____ 1. Falsificación de la dirección del remitente de un correo.
B. SUPLANTACION	_____ 2. Correo personalizado contra un objetivo concreto.
C. REGISTROSPF	_____ 3. Llamadas fraudulentas por voz.
D. DKIM	_____ 4. IP de remitentes autorizados publicadas en el DNS.
E. DMARC	_____ 5. Correo de ingeniería social.
F. WHALING	_____ 6. Política con instrucciones de rechazo.
G. PHISHING	_____ 7. Firma criptográfica en el correo electrónico.
H. VISHING	_____ 8. Ataque dirigido a altos directivos.

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. DIGDIIOR
2. SFERPTGSORI
3. ADCRM
4. SNGIHPHI
5. UIATNPACNSOL
6. IMDK
7. WNIGHLA
8. IHGVNIS

Actividad extra: Piensa rápido

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

1	Dispositivos que pueden ser hackeados			
2	Señales de un correo de phishing			
3	Señales de que un ordenador está infectado			
4	Palabras que crean una falsa urgencia			
5	Formas de comprobar un remitente			
6	Personas a las que puedes pedir ayuda informática			
7	Cosas de las que haces copia de seguridad			
8	Peces o criaturas marinas que conoces			
9	Empresas por las que se hacen pasar los estafadores			
10	Hábitos seguros que puedes empezar hoy			
11	Cosas que hacer tras hacer clic en un enlace falso			
12	Cosas que hacer tras una filtración de datos			
13	Canales por los que se produce el phishing			
14	Cosas que nunca envías por correo electrónico			
15	Formas de proteger tus cuentas			

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: RESPUESTA A UN ATAQUE DE WHALING CONTRA LA ALTA DIRECCIÓN



Escenario: Un director financiero recibe un correo muy personalizado que dice proceder del director ejecutivo y en el que se pide una transferencia urgente de $50,000 para cerrar la compra confidencial de un dominio.

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

CASO PRÁCTICO 2: IMPLANTAR POLÍTICAS DE PASARELA SPF/DKIM/DMARC



Escenario: Una empresa no supera las auditorías de seguridad porque sus correos de marketing salientes se marcan a menudo como spam y los hackers están suplantando activamente el dominio de la marca de la empresa.

Pregunta de debate: Establece controles técnicos y administrativos para verificar la autenticidad del correo electrónico.

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		12	1		9	14	7	5	14	9	5	19	9	1
20	16	3	9	1	12		1	22	4	9	21	1	14	4	16		5	12		
						3	16	19	19	5	16									

Mensaje descifrado:

CONSEJO: CADA NÚMERO REPRESENTA LA POSICIÓN DE ESA LETRA EN EL ALFABETO (P. EJ., 1 = A, 2 = B, 27 = Z).

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

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

Q1: ¿Qué es el phishing?

El phishing es un ataque de ingeniería social en el que los delincuentes envían mensajes fraudulentos para engañar a los usuarios y que compartan datos confidenciales.

Q2: ¿Qué diferencia hay entre el phishing y el spear phishing?

El phishing se dirige a grupos amplios con contenido genérico, mientras que el spear phishing se dirige a víctimas concretas usando detalles personalizados.

Q3: ¿Qué es el whaling?

El whaling es un ataque de phishing muy dirigido contra directivos de alto perfil que tienen poder administrativo.

Q4: ¿Qué es la suplantación de correo electrónico (email spoofing)?

La suplantación de correo electrónico consiste en crear mensajes con una dirección de remitente falsificada para engañar al destinatario y que confíe en el origen.

Q5: ¿Cómo evita SPF la suplantación?

Publica en el DNS una lista de direcciones IP autorizadas para enviar correo, lo que permite a los servidores receptores verificar el origen del correo. [1]

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 es DKIM?

DomainKeys Identified Mail añade una firma criptográfica a los encabezados del correo, lo que demuestra que un dominio asumió la responsabilidad y que el mensaje no se alteró.

Q7: ¿Qué significa DMARC?

Autenticación, notificación y conformidad de mensajes basada en dominios. [2]

Q8: ¿Qué es una política DMARC?

Una política que indica a los servidores de correo cómo tratar los mensajes que no superan SPF/DKIM (none, quarantine o reject). [2]

Q9: ¿Qué es el vishing?

Phishing por voz, en el que los atacantes usan llamadas telefónicas fraudulentas para obtener datos administrativos o financieros.

Q10: ¿Cómo ayudan los escáneres de enlaces?

Analizan y reescriben los enlaces de los correos entrantes para verificar la seguridad de las páginas web de destino en el momento del clic.

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 funciona un ataque homográfico?

Los atacantes registran nombres de dominio con caracteres Unicode no ASCII de aspecto similar para imitar visualmente un nombre de dominio legítimo.

Q2: ¿Qué es una representación punycode?

Una codificación que convierte los nombres de dominio Unicode en cadenas compatibles con ASCII que empiezan por 'xn--' para que el DNS pueda gestionarlas.

Q3: ¿Por qué 'p=reject' es el estado de DMARC más seguro?

Pide a los servidores receptores que rechacen durante la sesión SMTP el correo que no supere DMARC (SPF/DKIM alineados), lo que bloquea la suplantación directa. [2]

Q4: ¿Cómo eluden los atacantes las reglas SPF?

Aprovechando dominios de aspecto similar (typosquatting) o usando cuentas comprometidas en servicios de correo legítimos de terceros.

Q5: ¿Qué es el compromiso del correo electrónico empresarial (BEC)?

Una estafa corporativa en la que los atacantes secuestran o suplantan cuentas de correo electrónico de empresas para autorizar pagos fraudulentos.

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 frena el phishing la autenticación multifactor?

Requiere tokens secundarios (como llaves físicas) que no se pueden robar solo mediante páginas de destino falsas que imitan a las auténticas.

Q7: ¿Qué es una página de destino para el robo de credenciales?

Un portal de inicio de sesión de imitación diseñado para capturar en tiempo real los nombres de usuario, las contraseñas y los tokens MFA introducidos.

Q8: ¿Qué es el secuestro de subdominios?

Un atacante que toma el control de un puntero DNS de subdominio en desuso para alojar páginas de phishing bajo un dominio principal de confianza.

Q9: ¿Cómo funciona la comprobación de alineación de DKIM?

Verifica que el dominio del encabezado 'From' coincide con el dominio que firmó criptográficamente el mensaje en el encabezado DKIM.

Q10: ¿Qué función cumple una pasarela de correo electrónico?

Filtrar el correo entrante, auditar los enlaces, ejecutar los archivos adjuntos en un entorno aislado (sandbox) y validar el cumplimiento de SPF/DKIM/DMARC.

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. [4]

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. [4]

3. PERSPECTIVA SOBRE SEGURIDAD

Los ataques homográficos utilizan letras cirílicas de aspecto similar para duplicar visualmente en los navegadores dominios de marca de coincidencia exacta.

4. PERSPECTIVA SOBRE SEGURIDAD

Con 'p=reject', un dominio pide a los receptores que rechacen durante la entrega el correo que no supere la verificación, en lugar de archivarlo como spam. [2]

5. PERSPECTIVA SOBRE SEGURIDAD

Los ataques de whaling dirigidos a directores ejecutivos suelen solicitar pagos urgentes para fusiones confidenciales o compras de dominios.

6. PERSPECTIVA SOBRE SEGURIDAD

Los portales de robo de credenciales copian páginas de inicio de sesión reales para que las víctimas escriban sus contraseñas directamente en el formulario del atacante.

7. PERSPECTIVA SOBRE SEGURIDAD

La guía conjunta de la CISA sobre phishing recomienda formar a los usuarios, además de usar DMARC, SPF, DKIM y MFA resistente al phishing. [3]

8. PERSPECTIVA SOBRE SEGURIDAD

La evaluación SPF está limitada a 10 términos que consultan el DNS; superar el límite devuelve un resultado 'permerror'. [1]

9. PERSPECTIVA SOBRE SEGURIDAD

Las llaves de seguridad físicas FIDO2 ofrecen una protección respaldada criptográficamente contra la recolección remota de credenciales.

10. PERSPECTIVA SOBRE SEGURIDAD

El phishing es una de las formas más habituales en que los atacantes acceden por primera vez a una organización, por eso la formación periódica de concienciación es una defensa eficaz.

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

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

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

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

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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

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

Clave de respuestas: Punto de control 1 – Opción múltiple

1 Pregunta 1

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué es el spear phishing? → Un correo de phishing dirigido y adaptado a una persona u organización concreta

2 Pregunta 2

Respuesta correcta: A

NOTA PARA DOCENTES

SPF publica en el DNS los hosts de envío autorizados de un dominio para que los receptores puedan comprobar el remitente del sobre.

3 Pregunta 3

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué es un ataque de whaling? → Una campaña de phishing dirigida específicamente a altos directivos de empresas

4 Pregunta 4

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué hace DKIM? → Añade una firma criptográfica a los correos electrónicos para verificar la autenticidad del remitente

5 Pregunta 5

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué función cumple DMARC? → Indicar a los servidores de correo receptores cómo gestionar los mensajes que no superan las comprobaciones SPF/DKIM

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

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

NOTA PARA DOCENTES

Falso: el spear phishing se adapta a personas concretas, a diferencia del phishing masivo genérico.

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

NOTA PARA DOCENTES

Las políticas DMARC pueden indicar a los servidores de correo que rechacen los mensajes suplantados no autorizados.

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

NOTA PARA DOCENTES

Falso: SPF compara la IP de envío con el DNS; DKIM es el que verifica una firma criptográfica.

9 **Pregunta 9** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Falso: el whaling se dirige a altos directivos, que pueden aprobar pagos y acceder a datos sensibles.

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

NOTA PARA DOCENTES

Verdadero: confirmar las solicitudes de pago por un canal independiente y conocido ayuda a detener el fraude en transferencias.

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

F 1. SPEAR PHISHING	G 2. SUPLANTACIÓN	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. PHISHING	A 8. VISHING

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 DIRIGIDO	2 SUPLANTACIÓN	3 SPF	4 DKIM
5 DMARC	6 WHALING		

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

1 B – SUPLANTACION	2 A – DIRIGIDO	3 H – VISHING	4 C – REGISTROSPF
5 G – PHISHING	6 E – DMARC	7 D – DKIM	8 F – WHALING

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar SPEAR PHISHING, SUPLANTACIÓN y SPF 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.

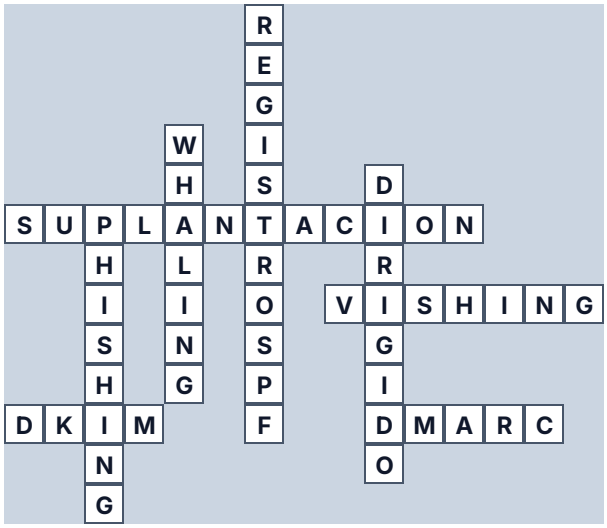
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

4 horizontal: SUPLANTACION Falsificación de la dirección del remitente de un correo. (12 letras)

6 horizontal: VISHING Llamadas fraudulentas por voz. (7 letras)

7 horizontal: DKIM Firma criptográfica en el correo electrónico. (4 letras)

8 horizontal: DMARC Política con instrucciones de rechazo. (5 letras)

VERTICALES

1 vertical: REGISTROSPF IP de remitentes autorizados publicadas en el DNS. (11 letras)

2 vertical: WHALING Ataque dirigido a altos directivos. (7 letras)

3 vertical: DIRIGIDO Correo personalizado contra un objetivo concreto. (8 letras)

5 vertical: PHISHING Correo de ingeniería social. (8 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. DIGDIIOR	DIRIGIDO	5. UIATNPACNSOL	SUPLANTACION
2. SFERPTGSORI	REGISTROSPF	6. IMDK	DKIM
3. ADCRM	DMARC	7. WNIGHLA	WHALING
4. SNGIHPHI	PHISHING	8. IHGVNIS	VISHING

CLAVE DEL RETO DEL CÓDIGO SECRETO

"DETECTA LA INGENIERIA SOCIAL AUDITANDO EL CORREO"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Respuesta a un ataque de whaling contra la alta dirección

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un director financiero recibe un correo muy personalizado que dice ser del consejero delegado y pide una transferencia urgente de $50,000 para cerrar una compra confidencial de un dominio.
- Estrategia y solución recomendadas: configurar DMARC con una política 'p=reject' para bloquear los dominios de remitentes suplantados. Añadir en la pasarela banners de advertencia para remitentes externos y exigir una confirmación verbal fuera de banda para todas las transacciones financieras.

B Caso práctico 2: Implantar políticas de pasarela SPF/DKIM/DMARC

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Una empresa no supera las auditorías de seguridad porque sus correos de marketing salientes se marcan a menudo como spam y unos hackers están suplantando activamente el dominio de su marca.
- Estrategia y solución recomendadas: publicar un registro TXT de SPF que detalle las IP de remitentes autorizadas. Configurar claves de firma DKIM en los servidores de correo saliente y analizar los informes XML de DMARC recibidos para detectar abusos.