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

Seguridad y cifrado en redes Wi-Fi públicas

Ataques de intermediario (man-in-the-middle), puntos de acceso fraudulentos, rastreo de paquetes, túneles VPN y cifrado HTTPS.

RESUMEN DE APRENDIZAJE: SEGURIDAD EN WI-FI PÚBLICAS

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 seguridad de las redes wifi públicas. Explorarás las redes sin cifrar, los ataques de intermediario (MitM), los puntos de acceso fraudulentos, el rastreo de paquetes, los túneles VPN y la seguridad en tránsito de HTTPS.

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/seguridad-wifi-publica/

Tu hoja de ruta de aprendizaje sobre seguridad en redes wifi públicas

- Identificar los riesgos habituales de las redes Wi-Fi públicas, como el rastreo de paquetes y los puntos de acceso fraudulentos.
- Implantar túneles de cifrado VPN para proteger los datos en tránsito.
- Impón HTTPS y una configuración segura del navegador web para los trabajadores remotos.

INSTRUCCIONES DE LA GUÍA DE SEGURIDAD EN WI-FI PÚBLICAS

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

SEGURIDAD EN WI-FI PÚBLICAS Y PROTECCIÓN EN TRÁNSITO (INTRODUCCIÓN)

Los puntos de acceso wifi públicos sin cifrar dejan el tráfico de red expuesto a la captura de paquetes y a la suplantación mediante Evil Twin. Forzar el tráfico a través de túneles de cifrado VPN seguros y aplicar reglas HSTS de solo HTTPS protege las sesiones frente a la interceptación en la red local.

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

Punto de control 1: Reto de opción múltiple

1. ¿Qué es un ataque de intermediario (Man-in-the-Middle, MitM)?

- A. Interceptar y alterar las comunicaciones entre dos partes en una red compartida
- B. Una técnica de extracción de bases de datos dirigida a los registros de usuarios
- C. Saturar servidores web con peticiones de tráfico de red
- D. Borrar los volúmenes de almacenamiento del disco duro local

2. ¿Qué es un punto de acceso fraudulento (Evil Twin)?

- A. Un punto wifi malicioso configurado con el mismo SSID que una red legítima
- B. Una herramienta administrativa para supervisar las copias de seguridad de la base de datos
- C. Una configuración segura de puerta de enlace VPN
- D. Un registro DNS que indica los servidores de correo autorizados

3. ¿Cómo protege una VPN el tráfico en una red Wi-Fi pública?

- A. Envuelve todos los paquetes de red en un túnel cifrado, de modo que los sniffers no pueden leerlos
- B. Bloquea automáticamente todas las solicitudes de conexión entrantes
- C. Cambia la dirección MAC de la tarjeta de red física
- D. Elimina las cookies almacenadas en caché en el navegador web

4. ¿Qué es el rastreo de paquetes (packet sniffing)?

- A. Usar herramientas de hardware o software para capturar y registrar paquetes de red
- B. Buscar archivos duplicados en los directorios locales
- C. Restringir los privilegios de lectura de la base de datos según los roles de usuario
- D. Cifrar las unidades de almacenamiento con claves AES-256

5. ¿Qué función cumple HTTPS?

- A. Cifrar el tráfico de la sesión entre el navegador y el servidor web
- B. Filtrar los correos entrantes en la pasarela
- C. Comprimir las imágenes para que las páginas carguen más rápido
- D. Gestionar las estructuras de archivos en el almacenamiento conectado a la red

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. Los usuarios conectados pueden capturar fácilmente datos en texto plano en las redes wifi públicas abiertas.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. Los puntos de acceso no autorizados (gemelos malvados) siempre están autorizados por los administradores de red.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. Una VPN no es eficaz para proteger el tráfico frente a la captura de paquetes (sniffing) en redes públicas.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. HTTPS cifra solo la ruta de la URL y deja la carga útil del paquete en texto plano.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. Los puntos de acceso wifi con seguridad WPA3 ofrecen una protección más sólida que las redes abiertas sin contraseña.

- ○ 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. Capturar contraseñas privadas en una red wifi pública es una _____ de las comunicaciones.

2. Analizar paquetes sin procesar en una red local requiere la _____ de paquetes.

3. Un punto de acceso falso que imita la red wifi de un hotel es un _____ .

4. Proteger el tráfico web en tránsito requiere cifrarlo con _____ .

5. Para cifrar todas las salidas de red se usa un _____ .

6. Una ruta de comunicación cifrada a través de redes públicas es un _____ .

BANCO DE PALABRAS DE VOCABULARIO

CAPTURA CLIENTE VPN CORTAFUEGOS GEMELO MALVADO HTTPS INTERCEPTACIÓN TÚNEL WPA3

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

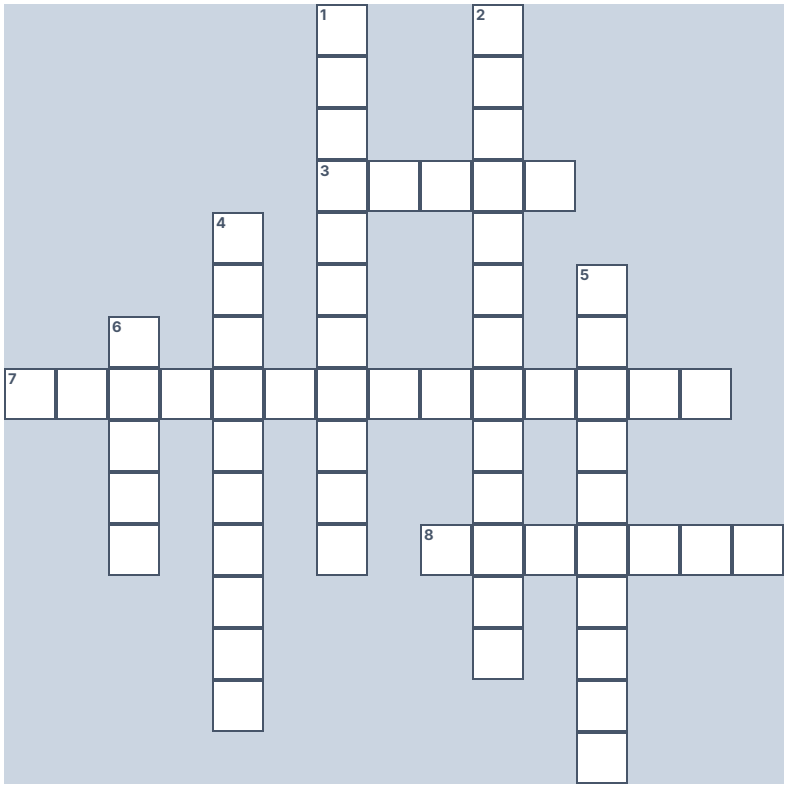
RELACIÓN DE DEFINICIONES

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. INTERCEPTACIÓN	A	Estándar moderno de seguridad Wi-Fi.
☐	2. SNIFFING	B	Ruta segura de los datos en tránsito.
☐	3. EVIL TWIN	C	Filtrar el tráfico entrante.
☐	4. HTTPS	D	Punto de acceso falso que imita una red wifi.
☐	5. VPN	E	Leer el tráfico en tránsito.
☐	6. TÚNEL	F	Capturar paquetes de datos de la red.
☐	7. WPA3	G	Red privada virtual cifrada.
☐	8. CORTAFUEGOS	H	Transmisión web segura.

Punto de control 5: Crucigrama

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



HORIZONTALES

3. Ruta segura de los datos en tránsito. (5)

7. Lectura del tráfico en tránsito. (14)

8. Recogida de los paquetes de datos que circulan por la red (sniffing). (7)

VERTICALES

1. Filtrado del tráfico entrante. (11)

2. Punto de acceso falso que imita una red wifi. (13)

4. Estándar moderno de seguridad wifi (WPA3). (10)

5. Software de red privada virtual cifrada. (10)

6. Transmisión web segura. (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

3 horizontal: Ruta segura de los datos en tránsito. (5 letras):

7 horizontal: Lectura del tráfico en tránsito. (14 letras):

8 horizontal: Recogida de los paquetes de datos que circulan por la red (sniffing). (7 letras):

VERTICALES

1 vertical: Filtrado del tráfico entrante. (11 letras):

2 vertical: Punto de acceso falso que imita una red wifi. (13 letras):

4 vertical: Estándar moderno de seguridad wifi (WPA3). (10 letras):

5 vertical: Software de red privada virtual cifrada. (10 letras):

6 vertical: Transmisión web segura. (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.

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

LISTA DE PALABRAS DE VOCABULARIO

INTERCEPTACION CAPTURA GEMELOMALVADO HTTPS CLIENTEVPN TUNEL CIFRADOWPA CORTAFUEGOS

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. INTERCEPTACION	_____ 1. Estándar moderno de seguridad wifi (WPA3).
B. CAPTURA	_____ 2. Punto de acceso falso que imita una red wifi.
C. GEMELOMALVADO	_____ 3. Recogida de los paquetes de datos que circulan por la red (sniffing).
D. HTTPS	_____ 4. Ruta segura de los datos en tránsito.
E. CLIENTEVPN	_____ 5. Filtrado del tráfico entrante.
F. TUNEL	_____ 6. Lectura del tráfico en tránsito.
G. CIFRADOWPA	_____ 7. Software de red privada virtual cifrada.
H. CORTAFUEGOS	_____ 8. Transmisión web segura.

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. CCPAETNTIIONRE
2. DLEOMGAMOLVAE
3. CTPELNNEVI
4. DPAARWOCIF
5. UATPCRA
6. PHTST
7. ELTNU
8. GUSFRCAOOET

Actividad extra: Piensa rápido

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

1	Razones para actualizar el software			
2	Dispositivos que se conectan automáticamente al Wi-Fi			
3	Información que nunca deberías compartir			
4	Hábitos seguros que puedes empezar hoy			
5	Formas de mantenerte seguro en una cafetería			
6	Dispositivos que pueden ser hackeados			
7	Cosas que un hacker puede ver en una red Wi-Fi abierta			
8	Señales de una red Wi-Fi falsa			
9	Alternativas a las redes Wi-Fi públicas			
10	Señales de alerta en un correo electrónico			
11	Cosas que no haces en una red Wi-Fi pública			
12	Lugares con Wi-Fi gratis			
13	Formas de proteger tus cuentas			
14	Señales de que un ordenador está infectado			
15	Nombres de Wi-Fi que parecen sospechosos			

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: CONTENCIÓN DE LA INTERCEPTACIÓN DE PAQUETES EN WIFI PÚBLICA



Escenario: Un directivo de ventas en remoto conectado a la red Wi-Fi pública de un aeropuerto observa que varios correos de empresa confidenciales se filtran poco después de enviarlos en texto plano.

Pregunta de debate: Analiza los riesgos de las redes públicas y describe una solución de cifrado del tráfico.

CASO PRÁCTICO 2: DEFENSA FRENTE A PUNTOS DE ACCESO FALSOS (EVIL TWIN)



Escenario: Unos atacantes despliegan un punto de acceso inalámbrico falso llamado 'CoffeeShop_Guest' que imita el punto de acceso legítimo de una cafetería y capturan el tráfico de red de clientes desprevenidos.

Pregunta de debate: Detalla los pasos de verificación para detectar y bloquear los puntos de acceso falsos.

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

3	9	6	19	1		5	12		21	19	1	6	9	3	16		4	5		12	1			
24	9	6	9		17	22	2	12	9	3	1		3	16	14		22	14	1					
									23	17	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: ¿Por qué el Wi-Fi público no es seguro?

Las redes Wi-Fi públicas abiertas no cifran el tráfico inalámbrico, por lo que otras personas cercanas pueden capturar cualquier dato sin proteger. [2]

Q2: ¿Qué es la captura de paquetes (packet sniffing)?

Un sniffer de paquetes captura los datos sin procesar que circulan por una interfaz de red y expone contraseñas en texto plano y detalles del tráfico.

Q3: ¿Qué es un gemelo malvado (Evil Twin)?

Un punto de acceso falso creado por hackers que imita el nombre y la configuración de un punto wifi local de confianza.

Q4: ¿Cómo me protege una VPN?

Enruta tu tráfico a través de un túnel cifrado y oculta tu actividad de navegación a los rastreadores de la red local.

Q5: ¿Me protege HTTPS en una Wi-Fi pública?

Sí, cifra los datos intercambiados entre tu navegador y el sitio web, y una VPN añade otra capa de protección.

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 WPA3?

El estándar moderno Wi-Fi Protected Access, que ofrece un cifrado más fuerte y protección frente a ataques de diccionario sin conexión. [1]

Q7: ¿Puede una Wi-Fi pública transmitir malware?

Sí, los atacantes pueden interceptar el tráfico e inyectar en tu sesión del navegador avisos de descarga maliciosos (descargas drive-by).

Q8: ¿Qué riesgo tiene compartir archivos?

Si el uso compartido de archivos está activado, otros usuarios de la red pública pueden leer o modificar tus carpetas locales.

Q9: ¿Qué es un portal cautivo?

La página de inicio de sesión que usan las redes de hoteles o cafeterías para conceder acceso a internet, que a veces los atacantes pueden suplantar.

Q10: ¿Debo desactivar el Wi-Fi cuando no lo uso?

Sí, desactivar el wifi impide que tu dispositivo se conecte automáticamente a redes no fiables.

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 explota un ataque de intermediario el DNS?

Usando la suplantación de DNS en un router malicioso para dirigir los navegadores objetivo a páginas de phishing de aspecto similar en lugar de a los dominios reales.

Q2: ¿Qué es el secuestro de sesión?

Un atacante que captura una cookie de sesión sin cifrar en una red wifi pública y la importa para eludir el inicio de sesión con credenciales.

Q3: ¿Qué es el SSL stripping?

Un ataque MitM en el que el atacante degrada la solicitud HTTPS segura de un usuario a HTTP sin cifrar y captura los datos de inicio de sesión en texto plano.

Q4: ¿Cómo protege HSTS contra el SSL stripping?

HTTP Strict Transport Security obliga a los navegadores a conectarse solo mediante HTTPS y rechaza el recurso a HTTP sin cifrar. [3]

Q5: ¿Qué es una VPN de túnel dividido?

Una configuración que enruta solo el tráfico corporativo a través de la VPN y envía directamente los datos de internet pública, lo que puede crear riesgo de rutas de fuga.

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: ¿Por qué WPA2 es vulnerable a KRACK?

El ataque de reinstalación de claves explota el protocolo de enlace de cuatro vías de WPA2 para descifrar paquetes sin la contraseña de la wifi.

Q7: ¿Qué es el aislamiento de clientes?

Un ajuste de seguridad del router que impide que los dispositivos wifi conectados se comuniquen directamente entre sí, lo que bloquea la captura de paquetes local.

Q8: ¿Cómo usan los atacantes servidores DNS falsos?

Configuran routers fraudulentos para asignar servidores DNS falsos a los clientes, lo que les permite interceptar y reescribir todas las búsquedas web.

Q9: ¿Puede una VPN ocultar mi dirección MAC local?

No. Las direcciones MAC son identificadores locales de capa 2; en su lugar, usa la opción de aleatorización de MAC (dirección privada) integrada en tu dispositivo.

Q10: ¿Qué es un ataque de suplantación de portal cautivo?

Un atacante que aloja un portal de autenticación falso en un punto de acceso fraudulento para robar credenciales con la excusa de ofrecer wifi gratis.

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 teletrabajadores suelen usar la wifi de cafeterías, hoteles y aeropuertos, donde no pueden controlar la seguridad de la red.

2. PERSPECTIVA SOBRE SEGURIDAD

Un punto de acceso falso Evil Twin puede copiar el nombre exacto y la dirección MAC de una red de confianza y confundir a los dispositivos.

3. PERSPECTIVA SOBRE SEGURIDAD

El software de captura de paquetes como Wireshark es gratuito y puede mostrar en texto claro las contraseñas HTTP sin cifrar.

4. PERSPECTIVA SOBRE SEGURIDAD

La seguridad WPA3 utiliza la autenticación simultánea de iguales (SAE) para proteger frente a ataques locales de fuerza bruta.

5. PERSPECTIVA SOBRE SEGURIDAD

Los ataques de SSL stripping burlan las protecciones HTTPS básicas interceptando en la pasarela las redirecciones HTTP iniciales.

6. PERSPECTIVA SOBRE SEGURIDAD

Las cabeceras de respuesta HTTP Strict Transport Security (HSTS) impiden que los navegadores recurran a conexiones HTTP sin cifrar. [3]

7. PERSPECTIVA SOBRE SEGURIDAD

Desactivar la conexión automática ('Auto-Connect') impide que los smartphones se conecten a redes fraudulentas de apariencia similar en espacios públicos.

8. PERSPECTIVA SOBRE SEGURIDAD

Las configuraciones empresariales de VPN 'siempre activa' obligan a que todo el tráfico de red de los trabajadores remotos pase por los cortafuegos corporativos.

9. PERSPECTIVA SOBRE SEGURIDAD

Los puntos de acceso no autorizados pueden dar respuestas DNS falsificadas y redirigir los dominios objetivo a servidores de phishing.

10. PERSPECTIVA SOBRE SEGURIDAD

Sin una VPN, otros usuarios de un punto de acceso abierto pueden ver con qué sitios y servidores se comunica tu dispositivo.

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] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[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 un ataque de intermediario (Man-in-the-Middle, MitM)? → Interceptar y alterar las comunicaciones entre dos partes en una red compartida

2 Pregunta 2

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué es un punto de acceso fraudulento (Evil Twin)? → Un punto wifi malicioso configurado con el mismo SSID que una red legítima

3 Pregunta 3

Respuesta correcta: A

NOTA PARA DOCENTES

¿Cómo protege una VPN el tráfico en una red Wi-Fi pública? → Envuelve todos los paquetes de red en un túnel cifrado, de modo que los sniffers no pueden leerlos

4 Pregunta 4

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué es el rastreo de paquetes (packet sniffing)? → Usar herramientas de hardware o software para capturar y registrar paquetes de red

5 Pregunta 5

Respuesta correcta: A

NOTA PARA DOCENTES

¿Qué función cumple HTTPS? → Cifrar el tráfico de la sesión entre el navegador y el servidor web

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

6 **Pregunta 6** — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los usuarios conectados pueden capturar fácilmente datos en texto plano en las redes wifi públicas abiertas.

7 **Pregunta 7** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Falso: un Evil Twin es un punto de acceso no autorizado que un atacante configura para imitar uno real.

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

NOTA PARA DOCENTES

Falso: una VPN cifra el tráfico en un túnel, por lo que los rastreadores locales no pueden leerlo.

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

NOTA PARA DOCENTES

Falso: HTTPS cifra todo el intercambio HTTP, incluidos la ruta de la URL y el contenido de la página.

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

NOTA PARA DOCENTES

Los puntos de acceso wifi con seguridad WPA3 ofrecen una protección más sólida que las redes abiertas sin contraseña.

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

E 1. INTERCEPTACIÓN	F 2. SNIFFING	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TÚNEL	A 7. WPA3	C 8. CORTAFUEGOS

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 INTERCEPTACIÓN	2 CAPTURA	3 GEMELO MALVADO	4 HTTPS
5 CLIENTE VPN	6 TÚNEL		

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

1 G – CIFRADOWPA	2 C – GEMELOMALVADO	3 B – CAPTURA	4 F – TUNEL
5 H – CORTAFUEGOS	6 A – INTERCEPTACION	7 E – CLIENTEVPN	8 D – HTTPS

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar INTERCEPTACIÓN, SNIFFING y EVIL TWIN 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.

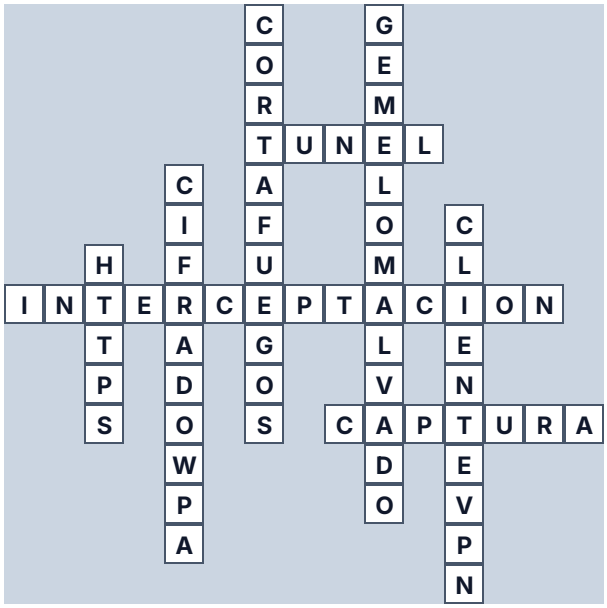
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

3 horizontal: TUNEL Ruta segura de los datos en tránsito. (5 letras)

7 horizontal: INTERCEPTACION Lectura del tráfico en tránsito. (14 letras)

8 horizontal: CAPTURA Recogida de los paquetes de datos que circulan por la red (sniffing). (7 letras)

VERTICALES

1 vertical: CORTAFUEGOS Filtrado del tráfico entrante. (11 letras)

2 vertical: GEMELOMALVADO Punto de acceso falso que imita una red wifi. (13 letras)

4 vertical: CIFRADOWPA Estándar moderno de seguridad wifi (WPA3). (10 letras)

5 vertical: CLIENTEVPN Software de red privada virtual cifrada. (10 letras)

6 vertical: HTTPS Transmisión web segura. (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. CCPAETNTIIONRE — **INTERCEPTACION**
2. DLEOMGAMOLVAE — **GEMELOMALVADO**
3. CTPELNNEVI — **CLIENTEVPN**
4. DPAARWOCIF — **CIFRADOWPA**
5. UATPCRA — **CAPTURA**
6. PHTST — **HTTPS**
7. ELTNU — **TUNEL**
8. GUSFRCAOOET — **CORTAFUEGOS**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"CIFRA EL TRAFICO DE LA WIFI PUBLICA CON UNA VPN"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Contención de la interceptación de paquetes en wifi pública

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: una ejecutiva de ventas conectada a la wifi pública de un aeropuerto descubre que varios correos de negocio delicados se filtraron poco después de enviarlos en texto plano.
- Estrategia y solución recomendadas: exigir el uso de un cliente VPN empresarial en todos los equipos remotos. Imponer extensiones de navegador solo HTTPS y bloquear los protocolos sin cifrar (como HTTP y FTP) en el cortafuegos del cliente.

B Caso práctico 2: Defensa frente a puntos de acceso falsos (evil twin)

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Unos atacantes despliegan un punto de acceso inalámbrico falso llamado 'CoffeeShop_Guest' que imita el wifi legítimo de una cafetería y capturan el tráfico de red de clientes desprevenidos.
- Estrategia y solución recomendadas: auditar las direcciones MAC BSSID de los puntos de acceso para verificar la autenticidad de la red. Aplicar la validación de la postura del cliente para bloquear la conexión a redes abiertas y exigir puntos de acceso móviles (hotspots) para el trabajo sensible.