Nombre: _____ Fecha: _____ Puntuación: _____

Dark web frente a deep web: seguridad y Diferencias

Indexación de buscadores, bases de datos de la web profunda, enrutamiento cebolla de Tor, anonimato en la red y riesgos

RESUMEN DE APRENDIZAJE: WEB OSCURA FRENTE A WEB PROFUNDA

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 las diferencias entre la web profunda y la web oscura. Explorarás las bases de datos no indexadas, el enrutamiento onion del navegador Tor, los dominios criptográficos .onion y los riesgos de seguridad del anonimato.

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/dark-web-vs-deep-web/

Tu hoja de ruta de aprendizaje sobre estrategia ante la web profunda y la web oscura

- Contrasta la web profunda (bases de datos no indexadas) con la web oscura (servicios onion).
- Comprende cómo el enrutamiento cebolla (Onion Routing) cifra y retransmite el tráfico de red.
- Evalúa los riesgos de seguridad de acceder a sitios no verificados de la red Tor.
- Despliega políticas de pasarela segura y de aislamiento (sandboxing) para el rastreo de inteligencia de amenazas.
- Analiza el formato criptográfico de las direcciones de los dominios de servicios onion.

INSTRUCCIONES DE LA GUÍA SOBRE LA DEEP WEB Y LA DARK WEB

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 privacidad en la web profunda y la web oscura. Termina con la actividad extra Piensa rápido.

BASES DE DATOS DE LA DEEP WEB FRENTE AL ENRUTAMIENTO ONION DE LA DARK WEB (INTRODUCCIÓN)

La deep web está formada por páginas no indexadas protegidas por contraseñas e inicios de sesión, como el correo privado o los portales bancarios corporativos. La dark web es un subconjunto de la deep web que se oculta intencionadamente y requiere navegadores especializados (como Tor) y redes onion para acceder de forma anónima.

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

Punto de control 1: Reto de opción múltiple

1. ¿Qué distingue la web profunda de la web superficial?

- A. Las páginas de la web profunda no están indexadas por los buscadores públicos
- B. El tráfico de la web profunda es ilegal y está vigilado por las fuerzas del orden
- C. Para acceder a los sitios de la web profunda se necesitan navegadores especializados como Tor
- D. Las páginas de la web profunda siempre cargan más rápido que las de la web superficial

2. ¿Cómo se accede a la dark web?

- A. Mediante navegadores especializados que usan redes de enrutamiento cebolla (onion)
- B. Configurando ajustes de DNS personalizados en routers estándar
- C. A través de consolas privadas de búsqueda en la web superficial, solo por invitación
- D. Instalando una extensión de navegador estándar para bloquear anuncios

3. ¿Qué estructura constituye la mayor parte de la web profunda?

- A. Bases de datos de usuarios protegidas con contraseña y cuentas privadas
- B. Foros ilegales del mercado negro que comercian con bienes ilícitos
- C. Protocolos de intercambio de archivos entre pares sin cifrar
- D. Bases de datos de la caché de los motores de búsqueda públicos

4. ¿Qué hace el enrutamiento cebolla (Onion Routing) con el tráfico de red?

- A. Cifra los paquetes y los enruta a través de varios repetidores
- B. Aumenta las velocidades de descarga al evitar los nodos del ISP
- C. Asocia los números de serie del hardware del dispositivo con registros de IP
- D. Elimina las cookies del navegador web después de cada clic

5. ¿Qué sufijo de dominio se usa exclusivamente en las redes Tor?

- A. La extensión criptográfica de nivel superior .onion
- B. La extensión comercial clásica estándar .com
- C. La extensión descentralizada .eth de blockchain de la Web3
- D. La extensión tecnológica de código de país .ai

Punto de control 2: Reto de verdadero o falso

6 Pregunta vf 6

6. La deep web y la dark web se refieren al mismo segmento de la red.

- ○ Verdadero
- ○ Falso

7 Pregunta vf 7

7. Los portales de intranet corporativos forman parte de la web profunda.

- ○ Verdadero
- ○ Falso

8 Pregunta vf 8

8. El enrutamiento cebolla descifra por completo los paquetes de datos en cada nodo de tránsito.

- ○ Verdadero
- ○ Falso

9 Pregunta vf 9

9. Acceder a la dark web expone los dispositivos a un alto riesgo de malware.

- ○ Verdadero
- ○ Falso

10 Pregunta vf 10

10. Los buscadores web estándar rastrean e indexan los sitios onion.

- ○ 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 portales privados de los bancos se encuentran en el segmento no indexado de la _____ .
2. Nodos especializados de Tor alojan servicios ocultos de la _____ .
3. Los sitios web de Tor usan la extensión criptográfica de nivel superior _____ .
4. El trazado del tráfico cifrado en varias capas se denomina _____ .
5. Los buscadores de la web superficial rastrean el contenido _____ públicamente.
6. Las redes onion cifran las IP de los clientes para mantener el _____ del usuario.

BANCO DE PALABRAS DE VOCABULARIO

ANONIMATO BASE DE DATOS DARK WEB DEEP WEB ENRUTAMIENTO CEBOLLA INDEXADO NODO DE ENTRADA ONION

Escribe aquí tus respuestas:

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

Punto de control 4: Relación de conceptos de seguridad

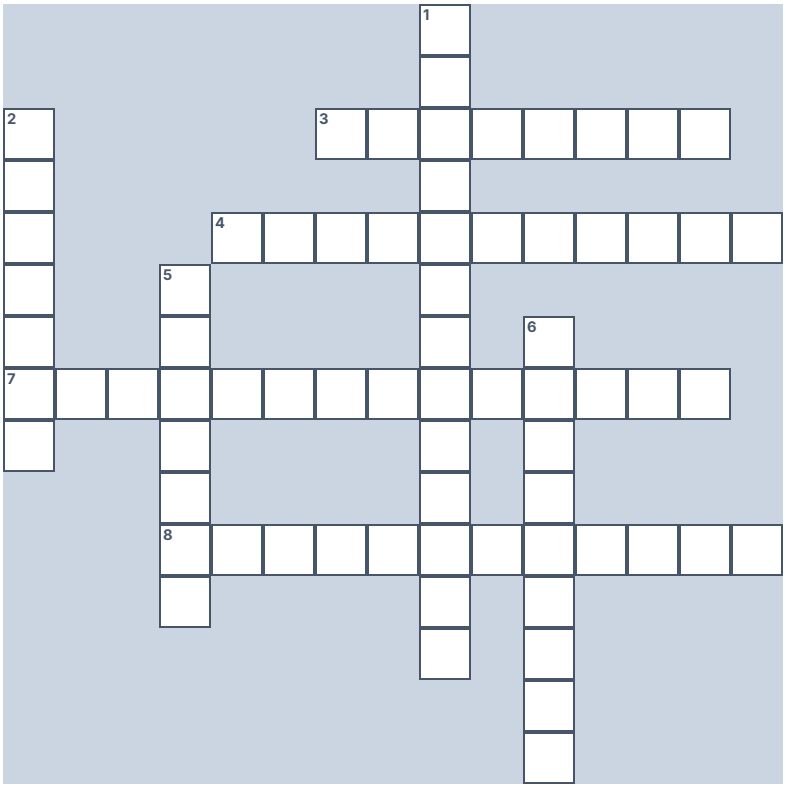
RELACIÓN DE DEFINICIONES

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. Segmento de la web profunda	**A**	Segmento de red cifrado al que solo se puede acceder con navegadores especiales.
☐	2. Portal de la web oscura	**B**	Cifrar los datos en capas y retransmitirlos a través de tres nodos.
☐	3. Extensión onion	**C**	Almacenamiento de backend seguro que aloja registros del sistema no indexados.
☐	4. Enrutamiento Tor	**D**	Sufijo de dominio de nivel superior criptográfico que se usa en las redes Tor.
☐	5. Páginas indexadas	**E**	El nodo de punto de entrada que se usa para acceder a la red Tor.
☐	6. Anonimato del usuario	**F**	Contenido de la web superficial recopilado y que se puede buscar en Google.
☐	7. Base de datos privada	**G**	Mantener ocultas a los servidores las direcciones IP públicas de los clientes.
☐	8. Puerta de enlace de entrada	**H**	Contenido web no indexado, como inicios de sesión privados, correos electrónicos y registros de bases de datos.

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. Contenido de la web superficial recopilado y que se puede buscar en Google (8)

4. Almacenamiento backend seguro que aloja registros del sistema no indexados (11)

7. Sufijo de dominio de nivel superior criptográfico que se usa en las redes Tor (14)

8. Cifrado de los datos en capas y retransmisión a través de tres nodos (12)

VERTICALES

1. Primer punto de acceso que se usa para entrar en la red Tor (13)

2. Segmento de red cifrado al que solo se accede con navegadores especiales (7)

5. Contenido web no indexado, como accesos privados, correos electrónicos y registros de bases de datos (7)

6. Mantener ocultas las direcciones IP públicas de los clientes ante los servidores (9)

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: Contenido de la web superficial recopilado y que se puede buscar en Google (8 letras):

4 horizontal: Almacenamiento backend seguro que aloja registros del sistema no indexados (11 letras):

7 horizontal: Sufijo de dominio de nivel superior criptográfico que se usa en las redes Tor (14 letras):

8 horizontal: Cifrado de los datos en capas y retransmisión a través de tres nodos (12 letras):

VERTICALES

1 vertical: Primer punto de acceso que se usa para entrar en la red Tor (13 letras):

2 vertical: Segmento de red cifrado al que solo se accede con navegadores especiales (7 letras):

5 vertical: Contenido web no indexado, como accesos privados, correos electrónicos y registros de bases de datos (7 letras):

6 vertical: Mantener ocultas las direcciones IP públicas de los clientes ante los servidores (9 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.

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

LISTA DE PALABRAS DE VOCABULARIO

DEEPWEB DARKWEB EXTENSIONONION ENRUTAMIENTO INDEXADO
ANONIMATO BASEDEDATOS NODODEENTRADA

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. DEEPWEB**
- **B. DARKWEB**
- **C. EXTENSIONONION**
- **D. ENRUTAMIENTO**
- **E. INDEXADO**
- **F. ANONIMATO**
- **G. BASEDEDATOS**
- **H. NODODEENTRADA**

DEFINICIONES Y CAMPOS DE RELACIÓN

_____ 1. Mantener ocultas las direcciones IP públicas de los clientes ante los servidores.

_____ 2. Almacenamiento backend seguro que aloja registros del sistema no indexados.

_____ 3. Cifrado de los datos en capas y retransmisión a través de tres nodos.

_____ 4. Contenido web no indexado, como accesos privados, correos electrónicos y registros de bases de datos.

_____ 5. Segmento de red cifrado al que solo se accede con navegadores especiales.

_____ 6. Sufijo de dominio de nivel superior criptográfico que se usa en las redes Tor.

_____ 7. Primer punto de acceso que se usa para entrar en la red Tor.

_____ 8. Contenido de la web superficial recopilado y que se puede buscar en Google.

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. **PEDWBEE** _____
2. **NXSTIOEIONONNE** _____
3. **ENIXAODD** _____
4. **DOSESDTABAE** _____
5. **WBKRDEA** _____
6. **OTENATIENMRU** _____
7. **MATOANNIO** _____
8. **TDDEANANEODRO** _____

Actividad extra: Piensa rápido

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

1	Razones para mantenerte alejado de la dark web			
2	Cosas que un buscador no puede encontrar			
3	Dispositivos que pueden ser hackeados			
4	Razones legales para usar Tor			
5	Razones para actualizar el software			
6	Señales de alerta en un correo electrónico			
7	Cosas que se venden ilegalmente en la dark web			
8	Personas a las que puedes pedir ayuda informática			
9	Hábitos seguros que puedes empezar hoy			
10	Cosas que hacer tras una filtración de datos			
11	Cosas que forman parte de la deep web			
12	Sitios que usas con inicio de sesión			
13	Palabras relacionadas con el anonimato			
14	Información que nunca deberías compartir			
15	Cosas que están 'bajo la superficie'			

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: IDENTIFICACIÓN DE FUGAS DE DATOS



Escenario: Una auditoría de seguridad corporativa descubre que se están comerciando registros confidenciales de la base de datos de clientes en un mercado onion. Los datos no están indexados en Google.

Pregunta de debate: Explica qué segmentos de la web están implicados y cómo se produjo esta filtración.

CASO PRÁCTICO 2: ANONIMATO FRENTE A RIESGOS DE MALWARE



Escenario: Una analista quiere consultar fuentes de inteligencia sobre amenazas en un sitio web de Tor. Descarga el navegador Tor y accede al sitio.

Pregunta de debate: Evalúa las ventajas en cuanto a anonimato y describe los pasos para mitigar el malware.

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

13 1 14 21 5 14 5 12 1 14 16 14 9 13 1 21 16

3 16 14 5 14 19 22 21 1 13 9 5 14 21 16

3 5 2 16 12 12 1

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 la deep web?

La deep web está formada por todas las páginas web que los motores de búsqueda no pueden indexar, como la banca en línea, las bases de datos de correo electrónico y las revistas de pago.

Q2: ¿Qué es la dark web?

La dark web es un pequeño subconjunto de la deep web, oculto intencionadamente y accesible solo mediante navegadores especializados que usan redes onion.

Q3: ¿Cómo indexan las páginas los motores de búsqueda?

Los buscadores ejecutan programas automatizados (arañas) que siguen los enlaces públicos e indexan las páginas que no bloquean el rastreo mediante directivas para robots.

Q4: ¿Por qué se considera la banca en línea parte de la web profunda?

Los portales bancarios están protegidos por inicios de sesión y contraseñas, lo que impide que los buscadores públicos indexen las páginas de extractos de cuenta.

Q5: ¿Qué es el enrutamiento cebolla (Onion Routing) del navegador Tor?

El enrutamiento cebolla es un método de transmisión que cifra el tráfico en capas y lo pasa por varios relés para ocultar las direcciones IP de los usuarios.

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

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

Q6: ¿Es ilegal acceder a la web oscura?

No. Acceder a la dark web es legal en la mayoría de los países, aunque está prohibido participar en mercados ilegales o en actividades cibernéticas ilícitas.

Q7: ¿Por qué los sitios de la web oscura tardan en cargar?

El tráfico se enruta y se descifra a través de al menos tres repetidores repartidos por el mundo (de entrada, intermedio y de salida), lo que aumenta la latencia de transmisión.

Q8: ¿Qué significa el sufijo de dominio .onion?

Es un sufijo de dominio de nivel superior especializado que se usa en las redes Tor y apunta a direcciones generadas criptográficamente en lugar de a servidores DNS estándar.

Q9: ¿Qué riesgos tienen los enlaces de la web oscura?

Los sitios no tienen ningún control de seguridad, lo que expone a los usuarios a altas tasas de infección por malware, scripts de phishing y estafas en las transacciones.

Q10: ¿Quién creó el protocolo de enrutamiento de la red Tor?

La tecnología la desarrolló originalmente el Laboratorio de Investigación Naval de EE. UU. en la década de 1990 para proteger las comunicaciones del gobierno.

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 protegen los nodos intermedios el anonimato en Tor?

Cada nodo descifra solo una capa de los datos de enrutamiento y conoce únicamente el salto anterior y el siguiente, nunca el origen y el destino a la vez.

Q2: ¿Qué función cumple el nodo de salida?

El nodo de salida descifra la última capa de cifrado y envía el tráfico al servidor de destino público o al servidor onion.

Q3: ¿Qué es una pasarela de puentes de Tor?

Los puentes son relés de entrada de Tor no listados que se usan para eludir los bloqueos del ISP y la censura en regiones que restringen el acceso al navegador Tor.

Q4: ¿Cómo explotan las criptomonedas los actores de la web oscura?

Los delincuentes usan criptomonedas anónimas para realizar operaciones financieras en mercados de la dark web y eludir los controles habituales de las transacciones bancarias.

Q5: ¿Por qué los motores de búsqueda estándar no consiguen rastrear las bases de datos profundas?

Los rastreadores no pueden introducir credenciales de inicio de sesión, resolver CAPTCHA de seguridad ni ejecutar los scripts de consultas SQL del servidor necesarios para acceder a las bases de datos profundas.

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 servidor de directorio en las redes Tor?

Es un servidor de confianza que mantiene la lista de repetidores de entrada, intermedios y de salida activos que usan los clientes para construir las rutas.

Q7: ¿Cómo husmean los actores maliciosos en los nodos de salida (exit node sniffing)?

Los operadores de nodos de salida maliciosos pueden interceptar el tráfico HTTP sin cifrar cuando sale de la red Tor y robar nombres de usuario y cookies.

Q8: ¿Cuál es la diferencia entre Tor e I2P?

Tor usa un directorio centralizado de repetidores y nodos de salida para acceder a la web pública, mientras que I2P usa una estructura descentralizada entre pares para el alojamiento interno.

Q9: ¿Cómo rastrean las fuerzas de seguridad los mercados de la web oscura?

Las autoridades usan el análisis de blockchain, localizan las instalaciones físicas de alojamiento de los servidores y realizan operaciones encubiertas para identificar a los operadores.

Q10: ¿Cómo compromete una fuga de DNS el anonimato del cliente?

Las fugas de DNS se producen cuando las consultas DNS del navegador se envían directamente a través del ISP local en lugar de encaminarse por la red cifrada de Tor.

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

La deep web es mucho más grande que la web superficial que se puede buscar, ya que la mayor parte del contenido está detrás de inicios de sesión y bases de datos.

2. PERSPECTIVA SOBRE SEGURIDAD

La dark web es una parte pequeña e intencionadamente oculta de la deep web, a la que se accede con herramientas como Tor.

3. PERSPECTIVA SOBRE SEGURIDAD

El enrutamiento de Tor cifra los paquetes de datos tres veces y va retirando las capas de cifrado, como las de una cebolla, en cada nodo de retransmisión.

4. PERSPECTIVA SOBRE SEGURIDAD

Tor surgió del proyecto de enrutamiento cebolla (onion routing) del Laboratorio de Investigación Naval de EE. UU., y su código se publicó como software libre. [1]

5. PERSPECTIVA SOBRE SEGURIDAD

Las direcciones onion son cadenas alfanuméricas de 56 caracteres generadas criptográficamente a partir de pares de claves públicas.

6. PERSPECTIVA SOBRE SEGURIDAD

Los nodos de salida pueden leer el tráfico en texto claro, por lo que TLS/HTTPS sigue siendo necesario en Tor para proteger los datos de la sesión.

7. PERSPECTIVA SOBRE SEGURIDAD

Los sitios de intranet, las unidades en la nube y las bases de datos privadas constituyen los mayores segmentos de almacenamiento de datos de la deep web.

8. PERSPECTIVA SOBRE SEGURIDAD

Buscadores especializados como DuckDuckGo tienen portales onion que permiten hacer búsquedas anónimas en la red Tor.

9. PERSPECTIVA SOBRE SEGURIDAD

Más de 2 millones de usuarios se conectan cada día a la red Tor para sortear la censura y mantener la privacidad de sus comunicaciones.

10. PERSPECTIVA SOBRE SEGURIDAD

Las operaciones policiales internacionales (como la Operación Bayonet) han cerrado grandes mercados de la dark web incautando el hardware de alojamiento.

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] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

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

[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

Clave de respuestas: Punto de control 1 – Opción múltiple

1 **Indexación de buscadores** DEEP WEB — **Respuesta correcta: A**

NOTA PARA DOCENTES

Las páginas de la deep web están tras muros de inicio de sesión y bases de datos, lo que impide que las arañas de los buscadores las rastreen. Cita: IETF RFC 3986.

2 **Acceso a Tor** WEB OSCURA — **Respuesta correcta: A**

NOTA PARA DOCENTES

La dark web está formada por servicios onion ocultos a los que solo se puede acceder con navegadores como Tor. Cita: IETF RFC 3986.

3 **Bases de datos profundas** BASES DE DATOS — **Respuesta correcta: A**

NOTA PARA DOCENTES

Las cuentas protegidas con contraseña y los registros corporativos forman el segmento más grande de la deep web. Cita: NIST Digital Identity.

4 **Enrutamiento cebolla** RED TOR — **Respuesta correcta: A**

NOTA PARA DOCENTES

El enrutamiento cebolla cifra los paquetes de datos en capas y los retransmite a través de varios nodos para garantizar el anonimato. Cita: IETF RFC 3986.

5 **Dominio onion** SUFIJO — **Respuesta correcta: A**

NOTA PARA DOCENTES

El sufijo de dominio criptográfico.onion enruta el tráfico internamente en Tor sin DNS público. Cita: IETF RFC 3986.

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

6 **Segmentos web** ESTRUCTURA — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

La deep web abarca todas las páginas no indexadas, mientras que la dark web es un pequeño subsegmento onion cifrado. Cita: IETF RFC 3986.

7 **Intranets corporativas** DEEP WEB — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los sitios de intranet están protegidos por portales con contraseña y no están indexados, lo que significa que forman parte de la deep web. Cita: NIST Digital Identity.

8 **Cifrado por capas** REPETIDORES — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Los relés onion solo descifran una capa de enrutamiento para proteger el anonimato del usuario, nunca el paquete completo. Cita: IETF RFC 3986.

9 **Exposición al malware** AMENAZAS — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los mercados de la dark web no tienen ningún filtrado de seguridad, por lo que conllevan un riesgo extremo de infección por malware. Cita: Center for Internet Security (CIS).

10 **Pregunta 10** — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

Los rastreadores de los buscadores normales no usan Tor, por lo que no pueden acceder a los sitios .onion ni indexarlos.

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. Segmento de la web profunda	A 2. Portal de la web oscura	D 3. Extensión onion	B 4. Enrutamiento Tor
F 5. Páginas indexadas	G 6. Anonimato del usuario	C 7. Base de datos privada	E 8. Puerta de enlace de entrada

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 DEEP WEB	2 DARK WEB	3 ONION	4 ENRUTAMIENTO CEBOLLA
5 INDEXADO	6 ANONIMATO		

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

1 F – ANONIMATO	2 G – BASEDEDATOS	3 D – ENRUTAMIENTO	4 A – DEEPWEB
5 B – DARKWEB	6 C – EXTENSIONONION	7 H – NODODEENTRADA	8 E – INDEXADO

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar Segmento de la web profunda, Portal de la web oscura y Extensión onion 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.

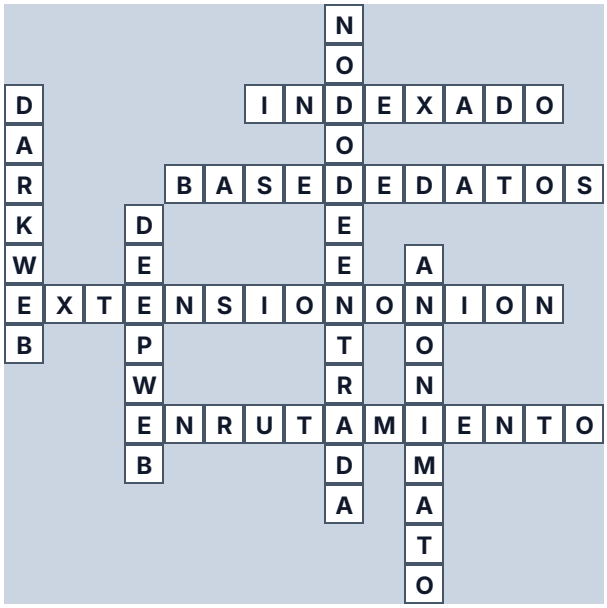
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

3 horizontal: INDEXADO Contenido de la web superficial recopilado y que se puede buscar en Google (8 letras)

4 horizontal: BASEDEDATOS Almacenamiento backend seguro que aloja registros del sistema no indexados (11 letras)

7 horizontal: EXTENSIONONION Sufijo de dominio de nivel superior criptográfico que se usa en las redes Tor (14 letras)

8 horizontal: ENRUTAMIENTO Cifrado de los datos en capas y retransmisión a través de tres nodos (12 letras)

VERTICALES

1 vertical: NODODEENTRADA Primer punto de acceso que se usa para entrar en la red Tor (13 letras)

2 vertical: DARKWEB Segmento de red cifrado al que solo se accede con navegadores especiales (7 letras)

5 vertical: DEEPWEB Contenido web no indexado, como accesos privados, correos electrónicos y registros de bases de datos (7 letras)

6 vertical: ANONIMATO Mantener ocultas las direcciones IP públicas de los clientes ante los servidores (9 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. PEDWBEE — **DEEPWEB**
2. NXSTIOEIONONNE — **EXTENSIONONION**
3. ENIXAODD — **INDEXADO**
4. DOSESDTABAE — **BASEDEDATOS**
5. WBKRDEA — **DARKWEB**
6. OTENATIENMRU — **ENRUTAMIENTO**
7. MATOANNIO — **ANONIMATO**
8. TDDEANANEODRO — **NODODEENTRADA**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"MANTEN EL ANONIMATO CON ENRUTAMIENTO CEBOLLA"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Identificación de fugas de datos

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: una auditoría de seguridad corporativa descubre que se están vendiendo registros confidenciales de la base de datos de clientes en un mercado onion. Los datos no están indexados en Google.
- Estrategia y solución recomendadas: Segmentos implicados: la base de datos privada pertenece a la web profunda (no indexada pero segura). El mercado que comercia con los datos robados está en la web oscura (red onion). Cómo ocurrió: los hackers burlaron las defensas del servidor, robaron la base de datos de la web profunda y la pusieron a la venta de forma anónima en la web oscura para eludir el rastreo de las fuerzas del orden.

B Caso práctico 2: Anonimato frente a riesgos de malware

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: un analista quiere consultar fuentes de inteligencia de amenazas en un sitio web de Tor. Descarga el navegador Tor y accede al sitio.
- Estrategia y solución recomendadas: Ventajas: Tor enruta el tráfico a través de tres nodos y enmascara la IP corporativa del analista. Riesgos y mitigación: los enlaces de la web oscura no tienen filtrado de reputación. Los analistas deben ejecutar Tor dentro de máquinas virtuales (VM) aisladas, desactivar JavaScript en la configuración de Tor y evitar descargar archivos para proteger la red corporativa.