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

Arquitectura y seguridad de confianza cero

Verificación continua, microsegmentación de la red, gestión de identidades y accesos, mínimo privilegio y comprobaciones de postura.

RESUMEN DE APRENDIZAJE SOBRE SEGURIDAD DE CONFIANZA CERO

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 arquitectura y la seguridad Zero Trust. Explorarás la verificación continua, la microsegmentación de la red, la gestión de identidades y accesos (IAM), el mínimo privilegio y la auditoría de sesiones.

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/ciberseguridad-zero-trust/

Tu hoja de ruta de aprendizaje sobre estrategia de confianza cero

- Comprende el principio fundamental de la verificación continua.
- Implantar la microsegmentación de la red y el acceso con privilegios mínimos.
- Configura las comprobaciones de la postura de los dispositivos y la auditoría de las sesiones activas.

INSTRUCCIONES DE LA GUÍA DE SEGURIDAD DE CONFIANZA CERO

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 arquitectura de confianza cero (Zero Trust). Termina con la actividad extra Piensa rápido.

ARQUITECTURA Y SEGURIDAD DE CONFIANZA CERO (INTRODUCCIÓN)

La seguridad de confianza cero sustituye los antiguos modelos de perímetro de red por una política estricta de 'nunca confíes, verifica siempre'. Implementar la microsegmentación, la gestión de identidades y accesos (IAM), los privilegios mínimos y las comprobaciones de estado bloquea el movimiento lateral de las amenazas.

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 principio fundamental de la seguridad Zero Trust?

- A. No confiar nunca y verificar siempre cada solicitud de acceso, sea cual sea su origen
- B. Dar por hecho que todo el tráfico dentro del cortafuegos corporativo es seguro
- C. Guardar los archivos de la base de datos sin cifrar para mejorar la velocidad
- D. Exigir la autenticación del correo electrónico usando solo registros SPF

2. ¿Qué es la microsegmentación de red?

- A. Dividir las redes en zonas pequeñas y aisladas para contener el movimiento lateral
- B. Cifrar las tarjetas de red durante el tránsito de datos
- C. Conectar todos los servidores locales a una única dirección IP pública
- D. Supervisar las pulsaciones de teclas del usuario en las sesiones del navegador

3. ¿Qué es el principio de mínimo privilegio?

- A. Limitar los permisos de acceso de los usuarios a lo estrictamente necesario para su trabajo
- B. Conceder por defecto todos los privilegios del sistema a todos los usuarios
- C. Permitir inicios de sesión anónimos en los servidores de bases de datos corporativos
- D. Configurar routers wifi públicos sin contraseña

4. ¿Qué es la gestión de identidades y accesos (IAM)?

- A. Marcos que gestionan las identidades digitales y controlan los privilegios del sistema
- B. Utilidades antivirus que analizan los directorios de archivos locales
- C. Un sistema de almacenamiento de copias de seguridad en soportes aislados físicamente (air-gapped)
- D. Un protocolo de pasarela de correo electrónico que rechaza los dominios suplantados

5. ¿Qué significa la autenticación continua?

- A. Verificar repetidamente la identidad del usuario y el estado de seguridad del dispositivo durante una sesión activa
- B. Cambiar la contraseña maestra cada 10 minutos
- C. Aplicar hash a los registros de la base de datos con varios algoritmos
- D. Cifrar los paquetes de red en tránsito con claves TLS

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. La confianza cero asume que todo el tráfico dentro del cortafuegos corporativo es seguro.

- ○ Verdadero
- ○ Falso

7 Pregunta 7

7. La microsegmentación limita la capacidad de los atacantes para moverse lateralmente entre los servidores internos.

- ○ Verdadero
- ○ Falso

8 Pregunta 8

8. El mínimo privilegio concede acceso a todos los archivos de la base de datos de forma predeterminada.

- ○ Verdadero
- ○ Falso

9 Pregunta 9

9. La verificación continua valida el estado del dispositivo y las credenciales durante toda la sesión.

- ○ Verdadero
- ○ Falso

10 Pregunta 10

10. Implantar el modelo de confianza cero (Zero Trust) reduce el impacto de los inicios de sesión corporativos comprometidos.

- ○ 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. Exigir credenciales en cada punto de acceso es una _____ continua.

2. Dividir la red corporativa en zonas diminutas se denomina micro- _____ .

3. Para configurar identidades digitales y el control de acceso se usa un sistema _____ .

4. Restringir los permisos de los usuarios aplica el principio de mínimo _____ .

5. Evaluar el estado de salud de los dispositivos conectados consiste en analizar su _____ .

6. Registrar y revisar las sesiones activas es una _____ de seguridad.

BANCO DE PALABRAS DE VOCABULARIO

AUDITORÍA CORTAFUEGOS IAM POSTURA PRIVILEGIO ROUTER SEGMENTACIÓN VERIFICACIÓN

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos de seguridad

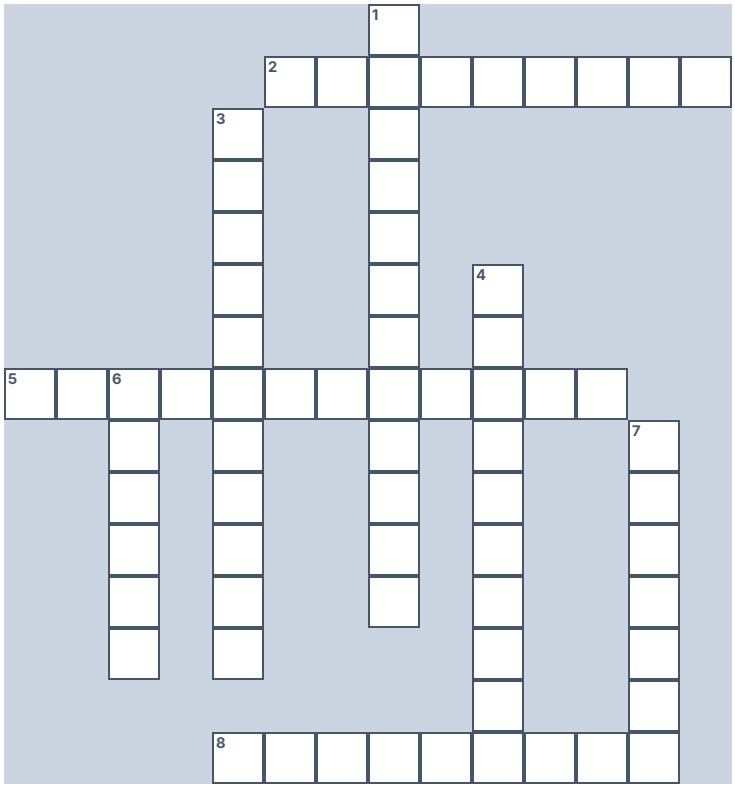
RELACIÓN DE DEFINICIONES

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. VERIFICACIÓN	A	Gestionar el acceso a las credenciales de usuario.
☐	2. SEGMENTACIÓN	B	Principio de mínimos derechos de acceso.
☐	3. IAM	C	Enrutar el tráfico de paquetes de red.
☐	4. PRIVILEGIO	D	Protección de barrera de la red externa.
☐	5. ESTADO DE SEGURIDAD	E	Revisar las sesiones de acceso registradas.
☐	6. AUDITORÍA	F	Dividir las zonas de la red interna.
☐	7. CORTAFUEGOS	G	Comprobar siempre las credenciales del usuario.
☐	8. ROUTER	H	Evaluar el estado de salud del dispositivo.

Punto de control 5: Crucigrama

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



HORIZONTALES

2. Gestión del acceso con credenciales de usuario (IAM). (9)

5. Comprobación constante de las credenciales del usuario. (12)

8. Revisión de las sesiones de acceso registradas. (9)

VERTICALES

1. División de la red interna en zonas. (12)

3. Barrera de protección frente a la red externa. (11)

4. Principio de derechos de acceso mínimos. (10)

6. Enrutamiento del tráfico de paquetes de red. (6)

7. Evaluación del estado de salud de un dispositivo. (7)

Punto de control 5, alternativa: Pistas accesibles del crucigrama

Los usuarios de lectores de pantalla y de teclado pueden escribir las respuestas del crucigrama directamente en los campos de texto de abajo.

HORIZONTALES

2 horizontal: Gestión del acceso con credenciales de usuario (IAM). (9 letras):

5 horizontal: Comprobación constante de las credenciales del usuario. (12 letras):

8 horizontal: Revisión de las sesiones de acceso registradas. (9 letras):

VERTICALES

1 vertical: División de la red interna en zonas. (12 letras):

3 vertical: Barrera de protección frente a la red externa. (11 letras):

4 vertical: Principio de derechos de acceso mínimos. (10 letras):

6 vertical: Enrutamiento del tráfico de paquetes de red. (6 letras):

7 vertical: Evaluación del estado de salud de un dispositivo. (7 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 A A E Ñ E F P H I D R Q M E

O I I R Z S F R Q V I F A A Q

I R E T U O R I O N D P T X Q

C O K R T R D V N Y E B G R X

A T W J A R Z I Y Y N L G C I

T I N Q K M M L T O T H P O Q

N D H Z A O V E G U I C Y R R

E U Y B H M Z G G K D Ñ P T Ñ

M A W C M Z Y I G Y A O W A U

G L U P B Ñ V O T M D H U F D

E V E R I F I C A C I O N U Y

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

D A P O S T U R A D K Q V G W

W L J I T I G B F I L T R O V

Q Z E I F R C A L P C Z M S K

LISTA DE PALABRAS DE VOCABULARIO

VERIFICACION SEGMENTACION IDENTIDAD PRIVILEGIO POSTURA AUDITORIA CORTAFUEGOS ROUTER

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. VERIFICACION	_____ 1. Barrera de protección frente a la red externa.
B. SEGMENTACION	_____ 2. Revisión de las sesiones de acceso registradas.
C. IDENTIDAD	_____ 3. Principio de derechos de acceso mínimos.
D. PRIVILEGIO	_____ 4. División de la red interna en zonas.
E. POSTURA	_____ 5. Enrutamiento del tráfico de paquetes de red.
F. AUDITORIA	_____ 6. Evaluación del estado de salud de un dispositivo.
G. CORTAFUEGOS	_____ 7. Gestión del acceso con credenciales de usuario (IAM).
H. ROUTER	_____ 8. Comprobación constante de las credenciales del usuario.

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. CIAFECIVORNI
2. DIANDIDTE
3. TPUASRO
4. UOSFRAGECOT
5. EIATNGECNSOM
6. IIVEGPRLOI
7. OAIARIUTD
8. URRETO

Actividad extra: Piensa rápido

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

1	Información que nunca deberías compartir			
2	Hábitos seguros que puedes empezar hoy			
3	Cosas que se comprueban en un dispositivo			
4	Cosas que quedan registradas			
5	Palabras relacionadas con la ciberseguridad			
6	Cosas que comprueba Zero Trust			
7	Lugares donde enseñas tu documento de identidad en la vida diaria			
8	Formas de demostrar que eres realmente tú			
9	Cosas que hacer tras una filtración de datos			
10	Señales de que un ordenador está infectado			
11	Razones para actualizar el software			
12	Niveles de acceso en una empresa			
13	Herramientas de seguridad que conoces			
14	Zonas en las que se puede dividir una red			
15	Refranes sobre la confianza			

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: TRANSICIÓN A UNA ARQUITECTURA DE RED DE CONFIANZA CERO



Escenario: Una gran empresa usa actualmente una red interna plana en la que cualquier dispositivo de la red local puede acceder a todos los servidores y bases de datos de la empresa.

Pregunta de debate: Diseña una estrategia de microsegmentación de la red para limitar el movimiento lateral.

CASO PRÁCTICO 2: IMPLANTAR CONTROLES DE ACCESO DE MÍNIMO PRIVILEGIO



Escenario: Los registros de auditoría revelan que usuarios temporales de la base de datos y empleados de nivel bajo tienen permisos globales de lectura y escritura en bases de datos contables críticas.

Pregunta de debate: Audita y restringe los privilegios IAM de la base de datos para aplicar el mínimo privilegio.

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

23	5	19	9	6	9	3	1		20	9	5	13	17	19	5		3	16	14
3	16	14	6	9	1	14	27	1		3	5	19	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 Zero Trust?

La confianza cero es un marco de seguridad que asume que existen amenazas tanto fuera como dentro del perímetro de la red, por lo que exige verificar cada solicitud. [1]

Q2: ¿Cuál es la regla fundamental de Zero Trust?

Nunca confíes, verifica siempre.

Q3: ¿Qué es la microsegmentación?

Dividir una red en segmentos lógicos pequeños y seguros para controlar el tráfico y contener las intrusiones.

Q4: ¿Qué es el mínimo privilegio?

Conceder a los usuarios solo los derechos de acceso mínimos necesarios para realizar sus tareas de trabajo específicas. [2]

Q5: ¿Qué significa IAM?

Gestión de identidades y accesos.

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

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

Q6: ¿Cómo ayuda la comprobación de postura del dispositivo?

Verifica que un dispositivo tiene los parches aplicados, ejecuta un antivirus activo y es seguro antes de permitir el acceso.

Q7: ¿Qué es el movimiento lateral?

El proceso que usan los atacantes para desplazarse por una red desde un nodo comprometido inicial hasta sistemas de mayor valor.

Q8: ¿Sustituye la confianza cero (Zero Trust) a los cortafuegos?

No, los refuerza añadiendo comprobaciones centradas en la identidad y cortafuegos de segmentación interna.

Q9: ¿Qué es la autenticación continua?

Verificación continua de la identidad del usuario durante toda la sesión activa, no solo al iniciar sesión.

Q10: ¿Por qué es peligrosa una red plana?

En las redes planas, un solo nodo comprometido permite a los atacantes acceder fácilmente a cualquier base de datos de la red.

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 aborda Zero Trust el modelo perimetral?

Sustituye el anticuado modelo de «castillo y foso» y traslada la defensa del perímetro de la red a las identidades y los recursos concretos de los usuarios.

Q2: ¿Qué es un punto de decisión de políticas (PDP)?

El componente del sistema que evalúa las solicitudes de autorización según las reglas de seguridad para decidir si se concede el acceso.

Q3: ¿Qué es un punto de aplicación de políticas (PEP)?

El nodo del sistema (como una puerta de enlace o un proxy) que permite o bloquea físicamente las solicitudes de conexión según la decisión del PDP.

Q4: ¿Cómo respalda el control de acceso basado en roles (RBAC) la confianza cero (Zero Trust)?

El RBAC agrupa los permisos en roles concretos, lo que ayuda a evitar que los usuarios hereden privilegios administrativos excesivos.

Q5: ¿Qué es el control de acceso contextual?

Evaluar las solicitudes de inicio de sesión mediante pistas secundarias como la ubicación geográfica, el estado del dispositivo y la hora de inicio de sesión para valorar el riesgo.

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: ¿En qué se diferencia la microsegmentación de las VLAN estándar?

Las VLAN dividen las redes en grandes segmentos lógicos en la capa 2, mientras que la microsegmentación usa políticas de software para aislar cargas de trabajo individuales.

Q7: ¿Qué es el acceso justo a tiempo (JIT)?

Conceder temporalmente permisos administrativos elevados y revocarlos automáticamente una vez terminada la tarea.

Q8: ¿Cómo se protegen las API en un marco de confianza cero (Zero Trust)?

Exigiendo tokens OAuth firmados criptográficamente y auditando las firmas de las solicitudes en cada pasarela de API.

Q9: ¿Qué es un cliente de acceso a la red de confianza cero (ZTNA)?

Un agente de software que establece conexiones salientes seguras y cifradas con aplicaciones concretas en lugar de con subredes completas.

Q10: ¿Cómo ayuda la auditoría de registros al modelo Zero Trust?

El registro continuo permite que las herramientas automatizadas de análisis de seguridad detecten anomalías y suspendan de inmediato los inicios de sesión fraudulentos.

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

Las arquitecturas de confianza cero sustituyen el antiguo modelo de castillo y foso por reglas de verificación centradas en la identidad.

2. PERSPECTIVA SOBRE SEGURIDAD

La microsegmentación de la red reduce la superficie a la que puede llegar el malware aislando las cargas de trabajo en pequeñas zonas protegidas.

3. PERSPECTIVA SOBRE SEGURIDAD

La confianza cero se centra en proteger recursos como activos, servicios y cuentas, en lugar de segmentos de red. [1]

4. PERSPECTIVA SOBRE SEGURIDAD

Las políticas de acceso de mínimo privilegio reducen el riesgo de que amenazas internas extraigan datos de las bases de datos principales.

5. PERSPECTIVA SOBRE SEGURIDAD

La validación del estado del dispositivo comprueba en tiempo real el nivel de parches del sistema operativo y el estado activo del antivirus.

6. PERSPECTIVA SOBRE SEGURIDAD

Los intermediarios de acceso a la red de confianza cero (ZTNA) pueden sustituir o complementar las VPN corporativas para restringir el alcance del acceso de los usuarios.

7. PERSPECTIVA SOBRE SEGURIDAD

La delegación de privilegios administrativos Just-in-Time (JIT) reduce el riesgo de robo de credenciales en los controladores de dominio.

8. PERSPECTIVA SOBRE SEGURIDAD

La validación continua registra y audita el comportamiento de las sesiones y suspende a los usuarios que muestran patrones anómalos de ejecución de scripts.

9. PERSPECTIVA SOBRE SEGURIDAD

Las defensas perimetrales tradicionales no logran bloquear los ataques laterales una vez que se filtra una credencial de administrador.

10. PERSPECTIVA SOBRE SEGURIDAD

La publicación especial NIST 800-207 (2020) ofrece una definición abstracta de la arquitectura Zero Trust, con modelos de implantación. [1]

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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Clave de respuestas: Punto de control 1 – Opción múltiple

1 Pregunta 1 — **Respuesta correcta: A**

NOTA PARA DOCENTES

¿Cuál es el principio fundamental de la seguridad Zero Trust? → No confiar nunca y verificar siempre cada solicitud de acceso, sea cual sea su origen

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

NOTA PARA DOCENTES

¿Qué es la microsegmentación de red? → Dividir las redes en zonas pequeñas y aisladas para contener el movimiento lateral

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

NOTA PARA DOCENTES

¿Qué es el principio de mínimo privilegio? → Limitar los permisos de acceso de los usuarios a lo estrictamente necesario para su trabajo

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

NOTA PARA DOCENTES

¿Qué es la gestión de identidades y accesos (IAM)? → Marcos que gestionan las identidades digitales y controlan los privilegios del sistema

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

NOTA PARA DOCENTES

¿Qué significa la autenticación continua? → Verificar repetidamente la identidad del usuario y el estado de seguridad del dispositivo durante una sesión activa

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

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

NOTA PARA DOCENTES

Falso: Zero Trust no concede confianza implícita en función de la ubicación en la red, ni dentro ni fuera.

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

NOTA PARA DOCENTES

Verdadero: las zonas pequeñas y aisladas limitan hasta dónde puede moverse un intruso entre servidores.

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

NOTA PARA DOCENTES

Falso: el mínimo privilegio concede solo el acceso mínimo que necesita cada función.

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

NOTA PARA DOCENTES

La verificación continua valida el estado del dispositivo y las credenciales durante toda la sesión.

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

NOTA PARA DOCENTES

Implantar el modelo de confianza cero (Zero Trust) reduce el impacto de los inicios de sesión corporativos comprometidos.

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. VERIFICACIÓN	F 2. SEGMENTACIÓN	A 3. IAM	B 4. PRIVILEGIO
H 5. ESTADO DE SEGURIDAD	E 6. AUDITORÍA	D 7. CORTAFUEGOS	C 8. ROUTER

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 VERIFICACIÓN	2 SEGMENTACIÓN	3 IAM	4 PRIVILEGIO
5 POSTURA	6 AUDITORÍA		

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

1 G – CORTAFUEGOS	2 F – AUDITORIA	3 D – PRIVILEGIO	4 B – SEGMENTACION
5 H – ROUTER	6 E – POSTURA	7 C – IDENTIDAD	8 A – VERIFICACION

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar VERIFICACIÓN, SEGMENTACIÓN y IAM 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.

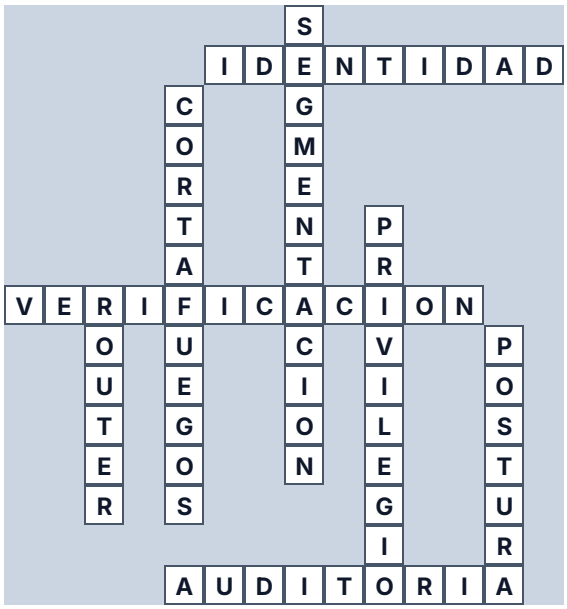
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

2 horizontal: IDENTIDAD Gestión del acceso con credenciales de usuario (IAM). (9 letras)

5 horizontal: VERIFICACION Comprobación constante de las credenciales del usuario. (12 letras)

8 horizontal: AUDITORIA Revisión de las sesiones de acceso registradas. (9 letras)

VERTICALES

1 vertical: SEGMENTACION División de la red interna en zonas. (12 letras)

3 vertical: CORTAFUEGOS Barrera de protección frente a la red externa. (11 letras)

4 vertical: PRIVILEGIO Principio de derechos de acceso mínimos. (10 letras)

6 vertical: ROUTER Enrutamiento del tráfico de paquetes de red. (6 letras)

7 vertical: POSTURA Evaluación del estado de salud de un dispositivo. (7 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. C I A F E C I V O R N I — **VERIFICACION**
2. D I A N D I D T E — **IDENTIDAD**
3. T P U A S R O — **POSTURA**
4. U O S F R A G E C O T — **CORTAFUEGOS**
5. E I A T N G E C N S O M — **SEGMENTACION**
6. I I V E G P R L O I — **PRIVILEGIO**
7. O A I A R I U T D — **AUDITORIA**
8. U R R E T O — **ROUTER**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"VERIFICA SIEMPRE CON CONFIANZA CERO"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Transición a una arquitectura de red de confianza cero

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: una gran empresa usa actualmente una red interna plana en la que cualquier dispositivo de la red local puede acceder a todos los servidores y bases de datos corporativos.
- Estrategia y solución recomendadas: segmentar la red plana en zonas departamentales aisladas. Instalar cortafuegos internos para controlar el tráfico entre zonas y exigir la validación de tokens de conexión para todo acceso.

B Caso práctico 2: Implantar controles de acceso de mínimo privilegio

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Los registros de auditoría revelan que usuarios temporales de la base de datos y empleados de bajo nivel tienen permisos globales de lectura y escritura sobre bases de datos contables críticas.
- Estrategia y solución recomendadas: revocar todos los privilegios administrativos globales. Implantar el control de acceso basado en roles (RBAC) para ajustarlo exactamente a cada puesto y establecer revisiones automáticas semanales de los permisos.