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

VPN empresarial

Implantación del acceso a la red de confianza cero (Zero Trust), nodos de puerta de enlace dedicados y controles de administración corporativos centralizados.

PANORAMA DE APRENDIZAJE: REDES VPN EMPRESARIALES

ALUMNO
CONDICIÓN DE ESTUDIANTE
Itinerario de defensor de redes

SEGURO
ESTADO DE LA CONEXIÓN
Proteger los paquetes de datos

ACTIVO
PROTECCIÓN CONTRA FUGAS
Protección contra fugas de DNS e IPv6

¡Hola! Este paquete de actividades te guía por las redes VPN empresariales. Explorarás las arquitecturas de confianza cero, las pasarelas dedicadas con IP estática, las consolas de administración, el aprovisionamiento y los túneles IPsec de sitio a sitio.

PUNTOS DE CONTROL DE LA HOJA DE TRABAJO

- [ ] **Partes 1-4: Domina las configuraciones de VPN y de seguridad de redes.**
- [ ] **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 las mejores VPN de VPN.com

URL: https://www.vpn.com/es/vpn/mejor-vpn-empresas/enterprise/

Tu hoja de ruta de aprendizaje sobre redes VPN empresariales

- Implantar marcos de acceso a la red de confianza cero (ZTNA).
- Configura direcciones IP de puerta de enlace de servidor dedicadas para los filtros de listas blancas.
- Gestionar paneles de administración corporativos centralizados y listas de licencias de usuario.
- Audita los registros de acceso a la red y los historiales de conexión de los usuarios.
- Configura reglas de inicio de sesión único (SSO) y de autenticación multifactor.
- Configurar túneles IPsec de sitio a sitio entre sucursales.

INSTRUCCIONES SOBRE REDES VPN EMPRESARIALES

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 confianza cero (Zero Trust) y el IPsec de sitio a sitio. Termina con la actividad extra Piensa rápido.

ARQUITECTURAS DE CONFIANZA CERO Y PASARELAS DEDICADAS (INTRODUCCIÓN)

Las VPN empresariales protegen los activos corporativos mediante la transición a marcos de acceso a la red de confianza cero (ZTNA) y la inclusión en listas blancas de pasarelas con IP estática dedicada. Los responsables de TI usan consolas de administración centralizadas para orquestar túneles IPsec de sitio a sitio y enlaces de inicio de sesión único (SSO).

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

Punto de control 1: Reto de opción múltiple

1. ¿Qué modelo de seguridad está sustituyendo a las VPN empresariales heredadas?

- A) Zero Trust
- B) Multisalto
- C) De igual a igual (peer-to-peer)
- D) Puerta de enlace única

2. ¿Qué función se necesita para restringir el acceso a la base de datos a los servidores de la empresa?

- A) IP dedicada
- B) Enrutamiento dinámico
- C) Túnel dividido
- D) Proxy DNS

3. ¿Qué protocolo es el estándar para los túneles corporativos de sitio a sitio?

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4. ¿Qué herramienta central permite a los administradores gestionar las licencias de los empleados?

- A) Consola de administración
- B) Clave del registro
- C) Firmware del router
- D) Registro del sistema

5. ¿Qué estándar de autenticación permite iniciar sesión mediante Okta o Microsoft Entra ID?

- A) Inicio de sesión único (SSO)
- B) Secreto compartido
- C) Autenticación EPP
- D) Clave WEP

Punto de control 2: Reto de verdadero o falso

6 Pregunta 6

6. El acceso a la red de confianza cero concede la entrada a la red solo tras verificar de forma continua la confianza en el dispositivo.

○ Verdadero ○ Falso

7 Pregunta 7

7. Las pasarelas con IP dedicada encaminan el tráfico de los empleados junto con el de usuarios consumidores públicos aleatorios.

○ Verdadero ○ Falso

8 Pregunta 8

8. Las consolas de administración centralizadas permiten a los responsables de TI revocar al instante la licencia de un empleado concreto.

○ Verdadero ○ Falso

9 Pregunta 9

9. IPsec es un protocolo ligero que no admite túneles de red de sitio a sitio.

○ Verdadero ○ Falso

10 Pregunta 10

10. El inicio de sesión único (SSO) permite autenticar de forma segura a los empleados mediante proveedores de identidad corporativos.

○ 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. Las arquitecturas de seguridad modernas sustituyen los túneles heredados por el acceso de _____ .

2. Para restringir el acceso a las bases de datos, las empresas configuran una dirección de puerta de enlace con _____ .

3. Las sucursales se conectan de forma segura mediante túneles _____ **entre sedes.**

4. Los administradores de TI asignan licencias a los empleados desde la _____ **central.**

5. La integración con Okta permite a los empleados autenticarse mediante el _____ **corporativo.**

6. Para proteger los inicios de sesión, los portales empresariales exigen la autenticación _____ .

BANCO DE PALABRAS DE VOCABULARIO

ASIGNACIÓN CONFIANZA CERO CONSOLA DE ADMIN INICIO DE SESIÓN ÚNICO
IP DEDICADA IPSEC MULTIFACTOR PUERTA DE ENLACE

Escribe aquí tus respuestas:

1. **2.**

3. **4.**

5. **6.**

Punto de control 4: Relación de conceptos clave

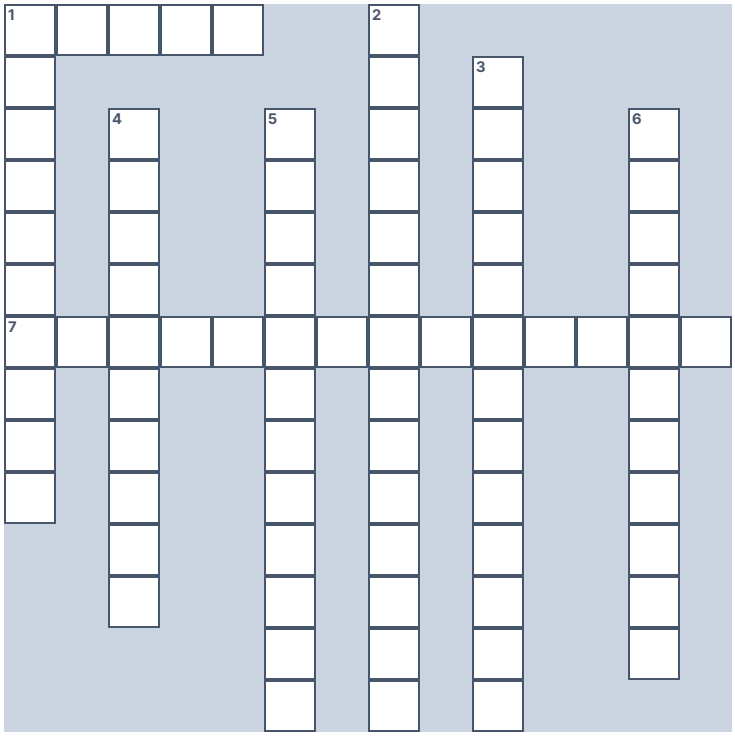
RELACIÓN DE DEFINICIONES

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. CONFIANZA CERO	A	Asignar licencias de acceso VPN a los empleados.
☐	2. IP DEDICADA	B	Vínculo de identidad con Okta y Entra ID.
☐	3. IPSEC	C	Seguridad de inicio de sesión que requiere tokens adicionales.
☐	4. CONSOLA DE ADMINISTRACIÓN	D	Dirección de pasarela de una lista blanca estática.
☐	5. INICIO DE SESIÓN ÚNICO	E	Estándar de túnel de sitio a sitio.
☐	6. MULTIFACTOR	F	Nodo de enrutamiento de entrada a la red.
☐	7. PUERTA DE ENLACE	G	Portal central de licencias para el responsable de TI.
☐	8. APROVISIONAR	H	Marco de verificación continua de la confianza.

Punto de control 5: Crucigrama

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



HORIZONTALES

1. Estándar de túnel entre sedes (site-to-site) (5)

7. Portal central donde TI gestiona las licencias de los usuarios (14)

VERTICALES

1. Dirección de puerta de enlace estática para listas blancas (10)

2. Nodo de enrutamiento de entrada a la red (14)

3. Marco de verificación continua de la confianza (13)

4. Reparto de licencias de acceso VPN entre los empleados (10)

5. Vínculo de identidad con Okta y Entra ID (12)

6. Seguridad de inicio de sesión que exige tokens adicionales (11)

Punto de control 5, alternativa: Pistas accesibles del crucigrama

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

HORIZONTALES

1 horizontal: Estándar de túnel entre sedes (site-to-site) (5 letras):

7 horizontal: Portal central donde TI gestiona las licencias de los usuarios (14 letras):

VERTICALES

1 vertical: Dirección de puerta de enlace estática para listas blancas (10 letras):

2 vertical: Nodo de enrutamiento de entrada a la red (14 letras):

3 vertical: Marco de verificación continua de la confianza (13 letras):

4 vertical: Reparto de licencias de acceso VPN entre los empleados (10 letras):

5 vertical: Vínculo de identidad con Okta y Entra ID (12 letras):

6 vertical: Seguridad de inicio de sesión que exige tokens adicionales (11 letras):

Punto de control 6: Sopa de letras

Encuentra los 8 términos clave del vocabulario ocultos en la cuadrícula de abajo. Las palabras pueden estar en horizontal, en vertical o en diagonal.

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

LISTA DE PALABRAS DE VOCABULARIO

CONFIANZACERO IPDEDICADA IPSEC CONSOLADEADMIN SINGLESIGNON
MULTIFACTOR PUERTADEENLACE ASIGNACION

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. CONFIANZACERO	_____ 1. Dirección de puerta de enlace estática para listas blancas.
B. IPDEDICADA	_____ 2. Nodo de enrutamiento de entrada a la red.
C. IPSEC	_____ 3. Reparto de licencias de acceso VPN entre los empleados.
D. CONSOLADEADMIN	_____ 4. Seguridad de inicio de sesión que exige tokens adicionales.
E. SINGLESIGNON	_____ 5. Estándar de túnel entre sedes (site-to-site).
F. MULTIFACTOR	_____ 6. Marco de verificación continua de la confianza.
G. PUERTADEENLACE	_____ 7. Vínculo de identidad con Okta y Entra ID.
H. ASIGNACION	_____ 8. Portal central donde TI gestiona las licencias de los usuarios.

Punto de control 7: Reto de palabras desordenadas

Ordena las letras de abajo para descubrir conceptos clave de esta hoja de trabajo. Escribe tus respuestas en los campos proporcionados.

1. NNARAOZCCE OIF
2. ICESP
3. SIISOGNENLN G
4. UDCNREAEEA LPET
5. AIAPECDIDD
6. LADONMDIAC OENS
7. CIMUARTOLF T
8. OGANANSCII

Actividad extra: Piensa rápido

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

1	Herramientas que una empresa usa todos los días			
2	Cosas que una VPN puede ocultar			
3	Puestos de un departamento de TI			
4	Palabras que describen Zero Trust			
5	Formas de iniciar sesión de forma segura			
6	Razones para dar una VPN a los empleados			
7	Cosas que hacer tras una brecha de seguridad			
8	Razones para usar una VPN cuando viajas			
9	Normas para teletrabajar de forma segura			
10	Datos que una empresa debe proteger			
11	Cosas que pueden interrumpir una videollamada			
12	Dispositivos que pueden usar una VPN			
13	Programas de oficina que conoces			
14	Lugares desde los que trabajan los empleados			
15	Dispositivos que podría tener un empleado			

Punto de control 8: Casos prácticos de VPN y redes

Aplica los conceptos que has aprendido para resolver los escenarios reales que aparecen a continuación.

CASO PRÁCTICO 1: MIGRACIÓN A CONFIANZA CERO



Escenario: Una empresa quiere proteger sus servidores locales verificando continuamente los certificados de cumplimiento de los dispositivos, el estado del cortafuegos y la ubicación de los usuarios, en lugar de confiar en cualquiera que esté dentro de la red.

Pregunta de debate: ¿Qué marco debería implantar el director de seguridad de TI para lograrlo?

CASO PRÁCTICO 2: RESTRICCIÓN DE LA PUERTA DE ENLACE



Escenario: Una empresa aloja bases de datos financieras privadas en la nube. Quiere bloquear todo el acceso público desde internet a los paneles de administración y permitir inicios de sesión solo desde equipos verificados de la empresa.

Pregunta de debate: ¿Qué configuración de red debería establecer el administrador de bases de datos en el cortafuegos de la nube?

Punto de control 9: Descifrar el código

Un ingeniero de redes protege los canales de enrutamiento y los túneles de los clientes. 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	16	14	6	9	1	14	27	1	3	5	19	16	
23	5	19	9	6	9	3	1	3	1	4	1	5	18	22	9	17	16
3	16	14	5	3	21	1	4	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 VPN (Parte A)

Repasa las preguntas y respuestas más habituales sobre las redes privadas virtuales (VPN) y la tunelización.

Q1: ¿Qué es una VPN corporativa?

Un túnel de red seguro diseñado para empresas, que permite a los teletrabajadores acceder a las redes corporativas con una gestión centralizada.

Q2: ¿En qué se diferencia Zero Trust de las VPN tradicionales?

Las VPN tradicionales confían en cualquiera que esté dentro del túnel, mientras que Zero Trust verifica continuamente cada dispositivo y cada conexión de usuario.

Q3: ¿Qué es una IP dedicada en las VPN para empresas?

Una dirección IP estática reservada exclusivamente para tu empresa, que te permite incluirla en una lista blanca para acceder de forma segura a bases de datos en la nube.

Q4: ¿Por qué es importante el SSO para las VPN para empresas?

El inicio de sesión único (SSO) permite a los empleados usar sus credenciales corporativas (como Okta o Microsoft Entra ID) para iniciar sesión de forma segura.

Q5: ¿Qué es una VPN de sitio a sitio?

Un túnel que conecta dos oficinas físicas (como una sucursal y la sede central) a través de internet pública mediante IPsec.

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

Repasa las preguntas y respuestas más habituales sobre las redes privadas virtuales (VPN) y la tunelización.

Q6: ¿Cuál es la función de una consola de administración?

Un panel para que los administradores de TI añadan o eliminen puestos de empleados, asignen puertas de enlace y supervisen las conexiones activas.

Q7: ¿Cómo protege la MFA las VPN para empresas?

Exigiendo un código secundario (como un token de una aplicación de autenticación) para evitar accesos no autorizados con contraseñas comprometidas.

Q8: ¿Puedo auditar el historial de conexiones de los empleados?

Sí, las VPN empresariales registran las marcas de tiempo de conexión, la duración y las IP asignadas para las auditorías de cumplimiento.

Q9: ¿Qué es ZTNA?

Acceso a la red de confianza cero, un modelo de seguridad que concede acceso solo a aplicaciones concretas en lugar de a toda la red.

Q10: ¿Qué función cumplen los nodos de puerta de enlace?

Sirven como puntos de entrada seguros para el tráfico remoto y enrutan los datos directamente a los servidores corporativos privados.

Punto de control 10: Preguntas frecuentes avanzadas sobre VPN (Parte C)

Explora aspectos técnicos avanzados de los protocolos de tunelización VPN, las integraciones con clientes móviles y el despliegue empresarial.

Q1: ¿Cómo protege IPsec las comunicaciones corporativas de sitio a sitio?

IPsec cifra el tráfico en la capa de red mediante Encapsulating Security Payload (ESP) para garantizar la confidencialidad y la integridad de los datos.

Q2: ¿Por qué está fallando la seguridad tradicional basada en el perímetro para las plantillas que trabajan en remoto?

Porque los empleados acceden a los datos desde varias ubicaciones y dispositivos, lo que deja obsoleto un único perímetro de cortafuegos de red.

Q3: ¿Cómo implementan los responsables de TI el aprovisionamiento automatizado?

Asignando los protocolos SCIM entre los proveedores de identidad (Okta) y la consola de administración de la VPN para sincronizar los directorios de usuarios.

Q4: ¿Qué ventaja tiene el túnel dividido en entornos corporativos?

Enruta el tráfico de SaaS local (como Microsoft 365) fuera del túnel VPN, lo que preserva el ancho de banda de la puerta de enlace corporativa para las bases de datos privadas.

Q5: ¿Cómo validan las comprobaciones de postura del dispositivo la seguridad de los endpoints?

El cliente VPN analiza el dispositivo antes de conectarse para verificar que el cortafuegos esté activo, el antivirus esté en funcionamiento y los parches del sistema operativo estén al día.

Punto de control 10: Preguntas frecuentes avanzadas sobre VPN (Parte D)

Explora aspectos técnicos avanzados de los protocolos de tunelización VPN, las integraciones con clientes móviles y el despliegue empresarial.

Q6: ¿Qué papel desempeña el NAT traversal en las configuraciones de VPN para empresas?

NAT-T encapsula los paquetes IPsec en UDP para que puedan atravesar los routers domésticos y los cortafuegos sin que se corte la conexión.

Q7: ¿Cómo evitan las empresas la saturación del ancho de banda en la pasarela?

Desplegando varios nodos de puerta de enlace regionales y repartiendo el tráfico entrante de los usuarios entre ellos con balanceadores de carga.

Q8: ¿Por qué se prefieren las listas blancas de IP estáticas a las dinámicas?

Las listas blancas estáticas impiden que IP externas no autorizadas intenten el handshake de conexión, lo que reduce drásticamente la superficie de ataque.

Q9: ¿Qué papel desempeña la autenticación basada en certificados en las VPN empresariales?

Valida certificados digitales únicos instalados en los dispositivos gestionados por la empresa, lo que bloquea los ordenadores personales no gestionados.

Q10: ¿Cómo reduce ZTNA el riesgo de movimiento lateral?

Aislando las sesiones de los usuarios en recursos autorizados concretos, lo que impide que los hackers recorran la red si se vulnera un nodo.

Parte 11: 10 datos reales sobre las VPN y su aplicación

Repasa datos reales sobre velocidades de cifrado de VPN, auditorías de protocolos, conectividad móvil y teletrabajo en empresas.

1. PERSPECTIVA SOBRE VPN

Las arquitecturas de confianza cero verifican continuamente el estado de seguridad de cada dispositivo que intenta conectarse a la red.

2. PERSPECTIVA SOBRE VPN

Las pasarelas con IP dedicada permiten a las empresas blindar sus bases de datos en la nube incluyendo direcciones estáticas en listas blancas.

3. PERSPECTIVA SOBRE VPN

IPsec es el protocolo estándar del sector para configurar túneles seguros de sitio a sitio entre las redes de las oficinas.

4. PERSPECTIVA SOBRE VPN

Las consolas de administración permiten a los departamentos de TI asignar, gestionar y auditar los puestos de acceso VPN de los empleados.

5. PERSPECTIVA SOBRE VPN

El inicio de sesión único (SSO) integra el acceso a la VPN con proveedores de identidad corporativos como Okta y Entra ID.

6. PERSPECTIVA SOBRE VPN

La autenticación multifactor bloquea los intentos de conexión no autorizados que se originan con contraseñas robadas.

7. PERSPECTIVA SOBRE VPN

El túnel dividido optimiza el ancho de banda corporativo al excluir del túnel cifrado el tráfico de SaaS públicos.

8. PERSPECTIVA SOBRE VPN

Las comprobaciones del estado del dispositivo verifican la configuración de seguridad local antes de conceder acceso a los servidores corporativos.

9. PERSPECTIVA SOBRE VPN

La sincronización de directorios SCIM automatiza los controles de acceso en las altas y bajas de empleados.

10. PERSPECTIVA SOBRE VPN

El acceso a la red de confianza cero limita el acceso de los usuarios a aplicaciones autorizadas concretas, lo que impide el movimiento lateral en la red.

Referencias técnicas y fuentes

La guía de estudio y los pasatiempos interactivos se han elaborado a partir de estándares técnicos, especificaciones y marcos normativos internacionales.

REFERENCIAS ACADÉMICAS Y DEL SECTOR

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

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

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

Clave de respuestas: Punto de control 1 – Opción múltiple

1 **Confianza cero** MODELO ZTNA **Respuesta correcta: A**

NOTA PARA DOCENTES

Los modelos de confianza cero verifican continuamente el cumplimiento de los dispositivos antes de permitir la entrada a la red. Cita: NIST Zero Trust.

2 **IP dedicada** IP ESTÁTICA **Respuesta correcta: A**

NOTA PARA DOCENTES

Las direcciones IP dedicadas permiten que las pasarelas con listas blancas bloqueen el tráfico público. Cita: Dedicated IP Guide.

3 **Estándar IPsec** TÚNEL IPSEC **Respuesta correcta: A**

NOTA PARA DOCENTES

IPsec es el protocolo estándar que se utiliza para los túneles de sitio a sitio entre sucursales. Cita: IPsec Tunneling.

4 **Asignación de TI** CONSOLA DE ADMINISTRACIÓN **Respuesta correcta: A**

NOTA PARA DOCENTES

Los paneles de administración centralizados permiten a los responsables de TI asignar licencias por usuario. Cita: CISA Guidelines.

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

NOTA PARA DOCENTES

¿Qué estándar de autenticación permite iniciar sesión mediante Okta o Microsoft Entra ID? → Inicio de sesión único (SSO)

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

6 **Confianza cero** COMPROBACIONES ZTNA — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los modelos de confianza cero verifican continuamente el cumplimiento de los dispositivos antes de permitir la entrada a la red. Cita: NIST Zero Trust.

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

NOTA PARA DOCENTES

Las IP dedicadas se reservan para una sola empresa, por lo que su tráfico no se mezcla con el de otros usuarios.

8 **Asignación de TI** PUESTO DE ADMINISTRADOR DE TI — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

Los paneles de administración centralizados permiten a los responsables de TI asignar licencias por usuario. Cita: CISA Guidelines.

9 **Estándar IPsec** SITIO A SITIO — **Respuesta correcta: Falso**

NOTA PARA DOCENTES

IPsec es el protocolo estándar que se utiliza para los túneles de sitio a sitio entre sucursales. Cita: IPsec Tunneling.

10 **Enlace SSO de Okta** INICIO DE SESIÓN SSO — **Respuesta correcta: Verdadero**

NOTA PARA DOCENTES

El inicio de sesión único (SSO) integra los inicios de sesión de la VPN con directorios corporativos como Okta. Fuente: Okta SSO.

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. CONFIANZA CERO	D 2. IP DEDICADA	E 3. IPSEC	G 4. CONSOLA DE ADMINISTRACIÓN
B 5. INICIO DE SESIÓN ÚNICO	C 6. MULTIFACTOR	F 7. PUERTA DE ENLACE	A 8. APROVISIONAR

PUNTO DE CONTROL 3: SOLUCIÓN DE LOS TÉRMINOS CLAVE

1 CONFIANZA CERO	2 IP DEDICADA	3 IPSEC	4 CONSOLA DE ADMIN
5 INICIO DE SESIÓN ÚNICO	6 MULTIFACTOR		

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

1 B – IPDEDICADA	2 G – PUERTADEENLACE	3 H – ASIGNACION	4 F – MULTIFACTOR
5 C – IPSEC	6 A – CONFIANZACERO	7 E – SINGLESIGNON	8 D – CONSOLADEADMIN

NOTAS DE DEBATE PARA DOCENTES

Términos clave:
Comprueba que los estudiantes saben explicar CONFIANZA CERO, IP DEDICADA y IPSEC 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.

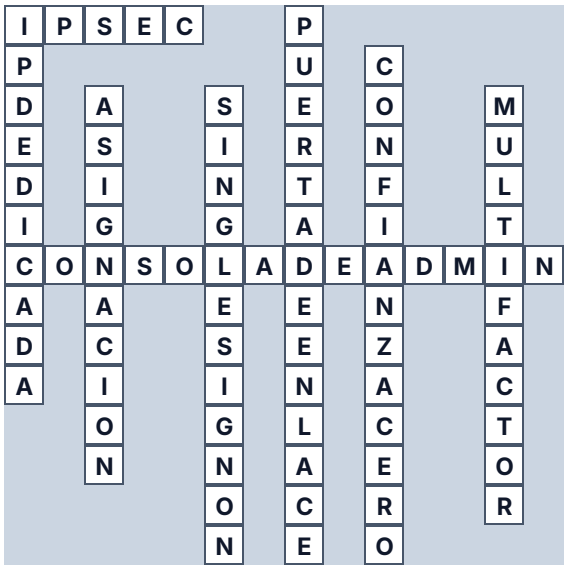
Evaluación de fuentes:
Haz que los estudiantes comprueben al menos una afirmación con las fuentes de la hoja de trabajo y comenta con ellos por qué las cifras, los precios y las normas pueden cambiar con el tiempo.

Claves de los pasatiempos y notas para docentes

SOLUCIÓN DE LA SOPA DE LETRAS

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

SOLUCIÓN DEL CRUCIGRAMA



GUÍA PARA DOCENTES CON LAS SOLUCIONES DEL CRUCIGRAMA

HORIZONTALES

1 horizontal: IPSEC Estándar de túnel entre sedes (site-to-site) (5 letras)

7 horizontal: CONSOLADEADMIN Portal central donde TI gestiona las licencias de los usuarios (14 letras)

VERTICALES

1 vertical: IPDEDICADA Dirección de puerta de enlace estática para listas blancas (10 letras)

2 vertical: PUERTADEENLACE Nodo de enrutamiento de entrada a la red (14 letras)

3 vertical: CONFIANZACERO Marco de verificación continua de la confianza (13 letras)

4 vertical: ASIGNACION Reparto de licencias de acceso VPN entre los empleados (10 letras)

5 vertical: SINGLESIGNON Vínculo de identidad con Okta y Entra ID (12 letras)

6 vertical: MULTIFACTOR Seguridad de inicio de sesión que exige tokens adicionales (11 letras)

Clave de soluciones de palabras desordenadas y del cifrado

Clave de calificación de la actividad de ordenar letras del vocabulario y del Reto del código secreto.

CLAVE DE LAS PALABRAS DESORDENADAS

1. NNARAOZCCEOIF — **CONFIANZACERO**
2. ICESP — **IPSEC**
3. SIISOGNENLNG — **SINGLESIGNON**
4. UDCNREAEEALPET — **PUERTADEENLACE**
5. AIAPECDIDD — **IPDEDICADA**
6. LADONMDIACOENS — **CONSOLADEADMIN**
7. CIMUARTOLFT — **MULTIFACTOR**
8. OGANANSCII — **ASIGNACION**

CLAVE DEL RETO DEL CÓDIGO SECRETO

"CONFIANZA CERO VERIFICA CADA EQUIPO CONECTADO"

Clave de respuestas de los casos prácticos

A Caso práctico 1: Migración a confianza cero

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis de escenario: Una empresa quiere proteger sus servidores locales verificando de forma continua los certificados de cumplimiento de los dispositivos, el estado del cortafuegos y la ubicación del usuario, en lugar de confiar en cualquiera que esté dentro de la red.
- Estrategia y solución recomendadas: el director debe migrar a un modelo de acceso a la red de confianza cero (ZTNA), que aplica comprobaciones de seguridad continuas basadas en el contexto.

B Caso práctico 2: Restricción de la puerta de enlace

Solución para docentes

PAUTA DE CALIFICACIÓN

Las respuestas del alumnado deben abordar los siguientes puntos:

- Análisis del escenario: una empresa aloja bases de datos financieras privadas en la nube. Quiere bloquear todo acceso público desde internet a los paneles de administración y permitir el inicio de sesión solo desde equipos verificados de la empresa.
- Estrategia y solución recomendadas: el administrador debe configurar una pasarela de IP dedicada en la VPN empresarial y añadir esta dirección estática a la lista de permitidos del cortafuegos de la base de datos en la nube.