

✓ **¡Felicitaciones! ¡Aprobaste!**

Calificación recibida 90 % Calificación del último envío 90 % Para Aprobar 80 % o más

[Ir al siguiente elemento](#)

1. ¿Cuál es el protocolo de comunicación de Internet que permite a dos dispositivos establecer una conexión y transmitir datos?

1 / 1 punto

- ☐ Protocolo de transferencia de hipertexto seguro (HTTPS)
- ☐ Capa de conexión segura/seguridad en la capa de transporte (SSL/TLS)
- ☒ Protocolo de control de transmisión (TCP)
- ☐ Protocolo de resolución de direcciones (ARP)

✓ Correcto

2. ¿Cuáles de las siguientes afirmaciones describen correctamente los protocolos inalámbricos? Selecciona tres respuestas.

1 / 1 punto

- ☒ El acceso Wi-Fi protegido (WPA) es un protocolo de seguridad inalámbrico relacionado con la conexión a Internet.
- ☒ Los protocolos de Wi-Fi proporcionan niveles de seguridad aproximadamente iguales a los de las conexiones por cable.
- ☐ 802.11 es un identificador de dispositivo.
- ☒ El conjunto de estándares IEEE 802.11 también se conoce como Wi-Fi.

✓ Correcto

✓ Correcto

✓ Correcto

3. Un administrador de cortafuegos (firewall) configura un firewall para que realice un seguimiento de la información y filtre proactivamente las amenazas. ¿Qué clase de firewall describe este escenario?

1 / 1 punto

- ☒ Cortafuegos Stateful (gestión con estado)
- ☐ Cortafuegos de última generación (NGFW)
- ☐ Cortafuegos basado en la nube
- ☐ Cortafuegos Stateless (gestión sin estado)

✓ Correcto

4. ¿Qué tipo de cortafuegos (firewall) puede conectarse a servicios de inteligencia de amenazas basados en la nube, ofrece altos niveles de protección contra intrusiones y realiza una inspección profunda de paquetes?

1 / 1 punto

- ☐ Cortafuegos Stateless (gestión sin estado)
- ☐ Documentado
- ☒ Cortafuegos de última generación (NGFW)
- ☐ Cortafuegos Stateful (gestión con estado)

✓ Correcto

5. Un/a profesional de seguridad establece una medida de seguridad para permitir que los/as empleados/as trabajen de forma segura desde su hogar al tiempo que pueden acceder a los recursos de la red interna. ¿Qué describe este escenario?

1 / 1 punto

- ☒ Red privada virtual (VPN)
- ☐ Protocolo de resolución de direcciones (ARP)
- ☐ Cortafuegos (firewall)

☐ Proveedor de servicios en la nube (CSP)

✓ Correcto

6. Completa el espacio en blanco: Los servicios VPN realizan la encapsulación para proteger los datos confidenciales al _____ en otros paquetes de datos.

1 / 1 punto

- ☐ clasificarlos
- ☐ exhibirlos
- ☐ archivarlos
- ☒ encapsularlos

✓ Correcto

7. Completa el espacio en blanco: Una zona controlada protege la red interna de una empresa en una zona de seguridad ____.

0 / 1 punto

- ☒ desmilitarizada
- ☐ restringida
- ☐ red interna
- ☐ no controlada

✗ Incorrecto

Revisa [el video sobre las zonas de seguridad](#).

8. ¿Qué zona de red establece un perímetro de seguridad para la red interna al aislar los servidores expuestos a Internet?

1 / 1 punto

- ☐ Zona no controlada
- ☒ Zona desmilitarizada (DMZ)
- ☐ Zona restringida
- ☐ Red privada virtual

✓ Correcto

9. Un/a analista de seguridad implementa un sistema para bloquear el acceso a sitios web inseguros por parte de los usuarios/as internos/as. ¿Qué utiliza para hacerlo?

1 / 1 punto

- ☒ Servidor proxy
- ☐ Red privada virtual (VPN)
- ☐ Cortafuegos
- ☐ Router

✓ Correcto

10. ¿Cuáles de las siguientes afirmaciones describen correctamente los servidores proxy directos e inversos? Selecciona tres respuestas.

1 / 1 punto

- ☐ Los servidores proxy inversos ocultan la dirección IP de un/a usuario/a y aprueban todas las solicitudes salientes.
- ☒ Los servidores proxy directos regulan y restringen el acceso de una persona a Internet.

✓ Correcto

- ☒ Los servidores proxy inversos aceptan el tráfico de terceros, lo aprueban y luego lo reenvían a servidores internos.

✓ Correcto

- ☒ Los servidores proxy directos reciben tráfico saliente de un/a empleado/a, lo aprueban y luego lo reenvían a su destino en Internet.

✓ Correcto