1. Modifique las siguientes afirmaciones para hacerlas verdaderas.

Una Red Privada Virtual (VPN) es una red informática (privada / ~~pública~~), construida dentro de una infraestructura de red, (~~privada~~ / pública) como Internet.

El término "cifrado" significa el proceso de seguridad de las VPN con el objetivo de garantizar (confidencialidad / ~~autenticación~~) y (integridad / ~~encriptación~~) de datos.

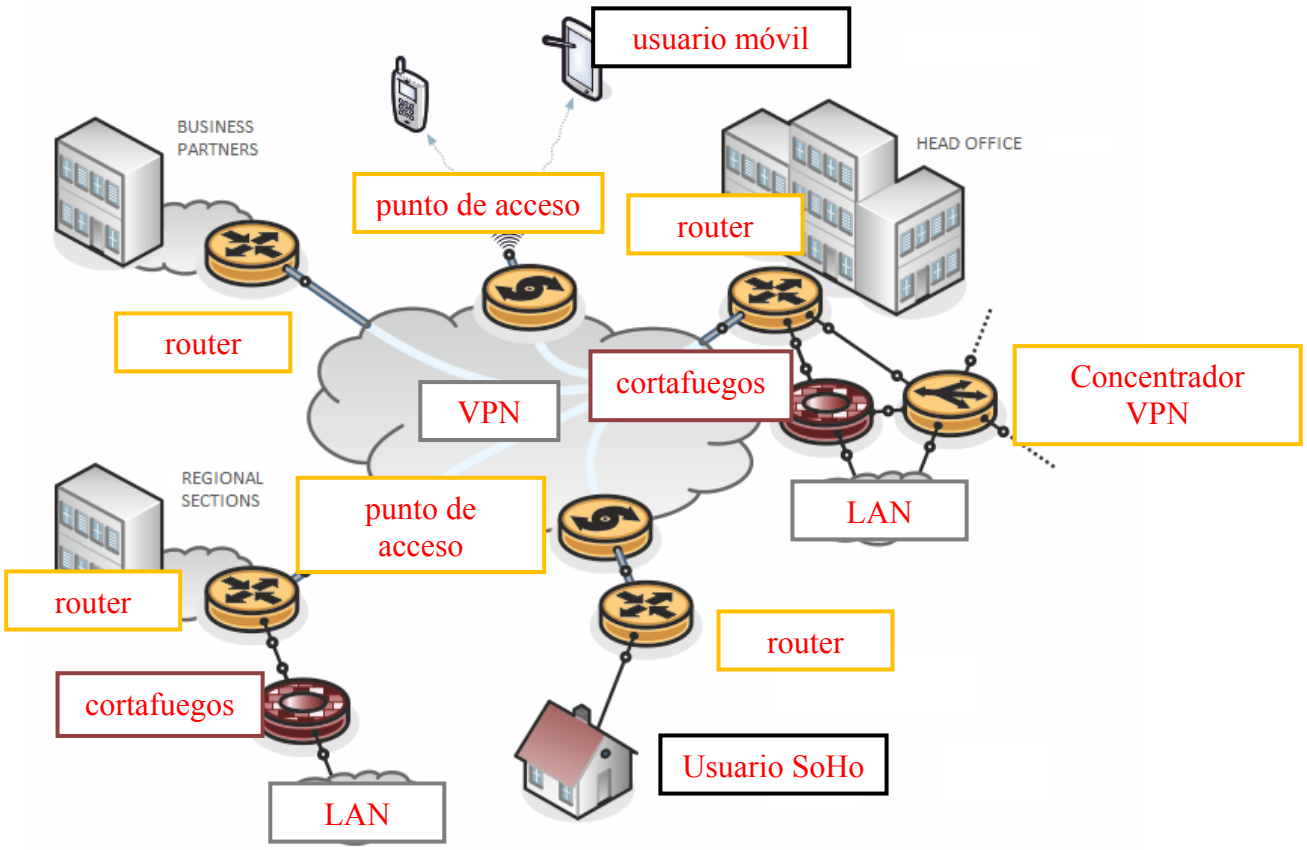
---

2. Los requisitos de seguridad en términos de diseño de VPN se resuelven mediante:

1. tunelado
2. cifrado
3. autenticación
4. control de acceso

---

3. Añada las etiquetas correctas a las partes individuales en la siguiente figura:



El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

4. Indica las sentencias correctas.

☐ IPSec no es un conjunto completo de protocolos de cifrado, autenticación, integridad de datos y tunelado.

X IPSec permite dos modos de trabajo: transporte y tunelado.

☐ El protocolo IKE tiene dos modos para configurar el túnel: modo principal y modo simple.

X Una ventaja del modo agresivo es el ahorro de ancho de banda y tiempo necesario para la transmisión de mensajes.

X Una desventaja del modo agresivo es el intercambio de información importante antes de que se establezca la conexión cifrada, que es susceptible de ser interceptada, lo que se conoce como Sniffing.

☐ El algoritmo Diffie-Hellman (algoritmo D-H) es un protocolo criptográfico que, sin embargo, no permite la creación de conexiones cifradas entre las partes comunicantes a través de un canal no seguro; es necesario establecer previamente una clave de cifrado.

X Una firma electrónica cualificada garantiza la aceptabilidad legal de los documentos firmados.

☐ Una firma electrónica es utilizada exclusivamente por una persona jurídica o una organización estatal; un sello electrónico es utilizado exclusivamente por una persona física.

---

5. Modifique las siguientes afirmaciones para hacerlas verdaderas.

El sello de calidad se basa en firma electrónica (cualificada / ~~garantizada~~), es su equivalente con respecto al área de su uso (exclusivamente para una persona (jurídica / ~~física~~)).

---

6. Una estructura de sellos de tiempo firmados electrónicamente incluye, entre otras cosas:

1. nombre del editor
2. número de serie único del sello
3. comprobación (HASH) derivada del documento
4. instante de tiempo

Erasmus+

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.