

Este test consta de 15 preguntas con un total de 15 puntos. Responde todas las preguntas, las preguntas incorrectas no restan. Sólo una opción es correcta a menos que se indique algo distinto. No está permitido el uso de calculadora.

Apellidos: \_\_\_\_\_ **SOLUCIÓN** \_\_\_\_\_ Nombre: \_\_\_\_\_ Grupo: \_\_\_\_\_

1. (1p) Comparando las cabeceras IPv4 e IPv6. ¿Cuál de las siguientes afirmaciones es falsa?  
☐ a) En IPv6, el campo TTL se denomina «límite de saltos».  
☐ b) En IPv6, el campo «protocolo» se ha reemplazado por el campo «cabecera siguiente».  
☐ c) La longitud total se ha eliminado en IPv6 y se ha reemplazado por la longitud de la carga.  
☒ d) El campo de opciones de IPv4 ha sido eliminado en IPv6.
2. (1p) ¿Cuál de las siguientes no se utiliza como estrategia de transición de IPv4 a IPv6?  
☐ a) Pila dual.  
☒ b) Traducción de datagramas.  
☐ c) Túneles.  
☐ d) Traducción de cabeceras.
3. (1p) ¿Cuál de las siguientes afirmaciones es una característica de los protocolos de enrutamiento por *vector distancia*?  
☐ a) La única métrica que utilizan es el número de saltos.  
☐ b) Sólo envían actualizaciones cuando se añade un nuevo nodo.  
☒ c) Envían sus tablas de enrutamiento a los vecinos inmediatos (directamente conectados).  
☐ d) Inundan toda la red con actualizaciones de enrutamiento.
4. (1p) ¿Cuál es el propósito de un protocolo de enrutamiento?  
☐ a) Proporciona un método para segmentar y reensamblar los paquetes de datos.  
☐ b) Se utiliza para desarrollar y mantener tablas ARP.  
☐ c) Permite que un administrador cree un esquema de direccionamiento para la red.  
☒ d) Permite que un encaminador comparta información acerca de redes conocidas con otros routers.
5. (1p) Sobre el encaminamiento basado en el estado del enlace. ¿Cuál de las siguientes afirmaciones es falsa?  
☐ a) Se crea un paquete del estado de los enlaces por cada encaminador.  
☒ b) Se define infinito para cada encaminador.  
☐ c) Se diseminan los paquetes del estado del enlace a cada encaminador.  
☐ d) Se construye el árbol del camino más corto para cada encaminador.
6. (1p) ¿Qué protocolo se utiliza para enrutar entre sistemas autónomos?  
☐ a) RIP  
☒ b) BGP  
☐ c) OSPF  
☐ d) EIGRP
7. (1p) En el algoritmo del estado del enlace (Dijkstra) cada router crea un paquete de información llamado LSP (Link State Packet) que difunde:  
☐ a) A todos sus routers vecinos.  
☐ b) Sólo a los routers hacia arriba en dirección a la raíz del árbol de rutas óptimas.  
☒ c) A todos los routers de la red, por inundación.  
☐ d) Sólo a los routers hacia abajo en el árbol de rutas óptimas.

8. (1p) El algoritmo Diffie-Hellman permite...
- ☐ a) Validar una clave pública entre dos entidades que no se han comunicado con anterioridad.
  - ☐ b) Validar las identidades de dos entidades que no se han comunicado con anterioridad.
  - ☒ c) Intercambiar una clave secreta entre dos entidades que no se han comunicado con anterioridad.
  - ☐ d) Intercambiar una clave pública sin necesidad de usar certificados digitales.
9. (1p) Cuando se crea una firma digital, ¿qué clave se utiliza para cifrar la firma?
- ☐ a) La clave privada del receptor.
  - ☐ b) La clave pública del receptor.
  - ☒ c) La clave privada del emisor.
  - ☐ d) La clave pública del emisor.
10. (1p) ¿Cuál de los siguientes servicios no proporciona el método AH de IPSec?
- ☒ a) Confidencialidad.
  - ☐ b) Integridad.
  - ☐ c) Control de acceso.
  - ☐ d) Autenticación de entidad.
11. (1p) ¿En qué capa opera SSL?
- ☐ a) Ofrece servicios de seguridad arbitrarios en cualquier capa del modelo OSI.
  - ☒ b) Proporciona «sockets TCP seguros», por tanto, opera en la capa de transporte.
  - ☐ c) Proporciona «sockets RAW seguros», por tanto opera en las capas de enlace y red.
  - ☐ d) SSL proporciona cifrado y autenticación de entidades para el protocolo HTTPS.
12. (1p) Alice quiere enviar un correo electrónico encriptado con PGP a Bob. ¿Qué hace Alice?
- ☐ a) Adjunta al correo su clave pública. Así Bob podrá desencriptar y ver el correo.
  - ☐ b) Publica su clave pública en un servidor de claves y cuando el mensaje llega a Bob, éste podrá verlo.
  - ☐ c) Adquiere un certificado digital mediante una autoridad de certificación.
  - ☒ d) Primero obtiene la clave pública de Bob desde un servidor de claves.
13. (1p) ¿Qué es un túnel IP?
- ☒ a) Un canal virtual punto a punto que transporta datagramas IP completos entre dos redes distantes
  - ☐ b) Una incidencia de seguridad que permite acceder a un puerto de un computador dentro de una red privada
  - ☐ c) Un tipo de conmutador Ethernet que permite definir enlaces entre sus puertos por medio de reglas administrativas.
  - ☐ d) Un enlace virtual punto a punto resultado de agregar varios enlaces paralelos entre 2 dispositivos dados con objeto de aumentar el ancho de banda, por ejemplo, un servidor u un conmutador.
14. (1p) ¿Qué es una VPN?
- ☐ a) Un tipo de red LAN lógica. Es posible gracias a conmutadores especiales que crean la ilusión de LANs aisladas sobre una única infraestructura de red física.
  - ☒ b) Una red privada formada por varios sitios conectados a través de túneles sobre una red ajena.
  - ☐ c) VPN significa *Valuable Public Network*, es decir, una red capaz de aplicar protocolos de aplicación arbitrarios por cada grupo de personas o servicios.
  - ☐ d) Una red privada a la que no es posible conectar si no se proporcionan credenciales válidas por cada usuario.
15. (1p) Explique brevemente qué caracteriza a una red de conmutación de paquetes.

La característica más importante de una red de conmutación de paquetes es que los nodos intermedios (encaminadores) determinan la ruta —normalmente en términos del siguiente salto— considerando individualmente cada paquete. Por tanto, paquetes con el mismo origen y destino pueden seguir rutas diferentes.