

# Punto de control: Resultado

Recuerde contestar todas las preguntas antes de finalizar.

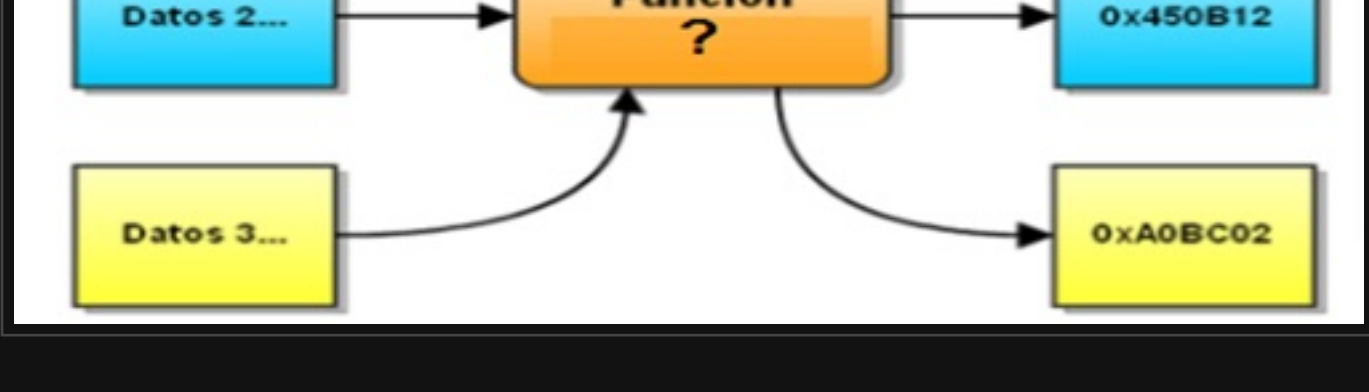
## Trabajos Prácticos de Respuesta Múltiple N°8 P1 - CORRECTAS: 10 de 10 - APROBADO

1) Existe un programa que permite verificar la ruta que realiza un conjunto de Paquetes o bloques de información a través de una Red de Internet. Dicho servicio debe estar bloqueado por nuestro Firewall para toda comunicación entrante e nuestra red. Este programa corresponde a:

```
# traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
1 192.168.0.1 (192.168.0.1) 3.038 ms 1.530 ms 1.286 ms
2 192.168.0.1 (192.168.0.1) 1.445 ms 1.544 ms 1.285 ms
3 192.168.178.1 (192.168.178.1) 56.268 ms 81.940 ms 87.898 ms
4 172.24.199.169 (172.26.199.169) 79.666 ms 64.663 ms 73.266 ms
5 79.red-81-46-37.customer.static.ccgg.telefonica.net (81.46.37.79) 189.427 ms 95.949 ms 89.762 ms
6 65.red-81-46-68.customer.static.ccgg.telefonica.net (81.46.68.68) 123.788 ms 91.384 ms 67.246 ms
7 * 97.red-81-46-68.customer.static.ccgg.telefonica.net (81.46.68.97) 72.291 ms 60.095 ms
8 109.red-88-58-186.staticip.rims-tde.net (88.58.186.189) 48.350 ms * 132.008 ms
9 174.52.253.97 (174.52.253.97) 219.846 ms * 3578.661 ms
10 6.53.1.74 (6.53.1.74) 1087.314 ms
11 72.14.219.20 (72.14.219.20) 2739.369 ms 2617.731 ms
12 * 188.170.253.225 (188.170.253.225) 946.940 ms
13 74.125.242.161 (74.125.242.161) 3796.752 ms *
12 * 74.125.253.199 (74.125.253.199) 2181.214 ms
13 dns.google (8.8.8.8) 697.794 ms 1616.121 ms 569.983 ms
```

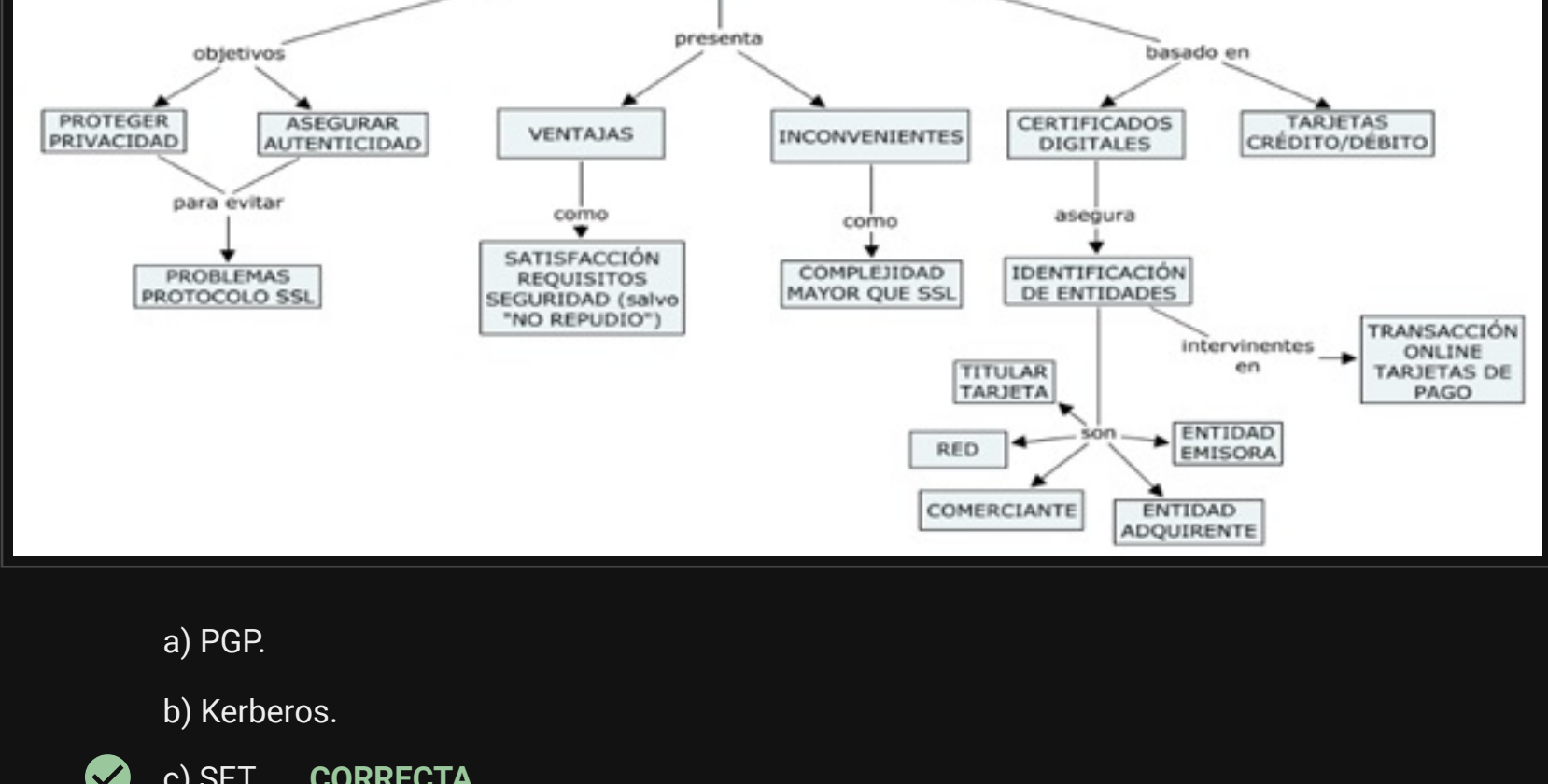
- a) WHOIS.
- b) ICMP.
- ☒ c) TraceRoute. CORRECTA
- d) Finger.
- e) Spoofing.
- f) Ninguna de las Anteriores es correcta.

2) Dentro de la firma digital, La función o algoritmo aplicada a un mensaje de M bits, que da como resultado un Función de N bits y que constituye un resumen del mensaje original a transmitir dentro del sobre digital se la denomina:



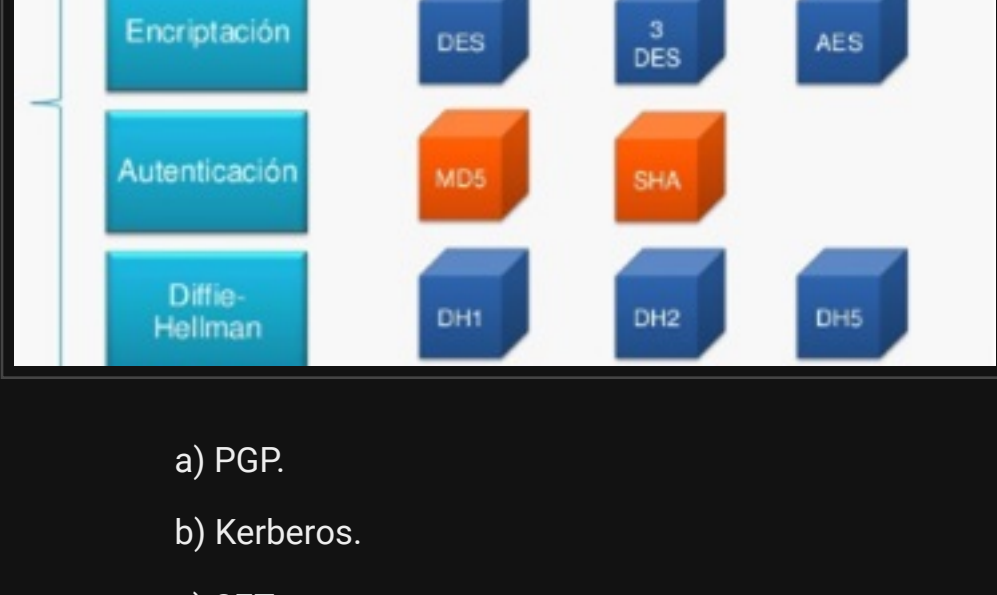
- a) RSA.
- b) DSA.
- ☒ c) HASH. CORRECTA
- d) X509.
- e) Ambas a y c.
- f) Ninguna de las Anteriores es correcta.

3) La Norma técnica anunciada por VISA y MASTERCARD que incluye el uso de Certificados Digitales, que asegura y autentica la integridad de los participantes en una operación económica y su código aplica técnicas de criptografía manteniendo el carácter confidencial de la información se la denomina



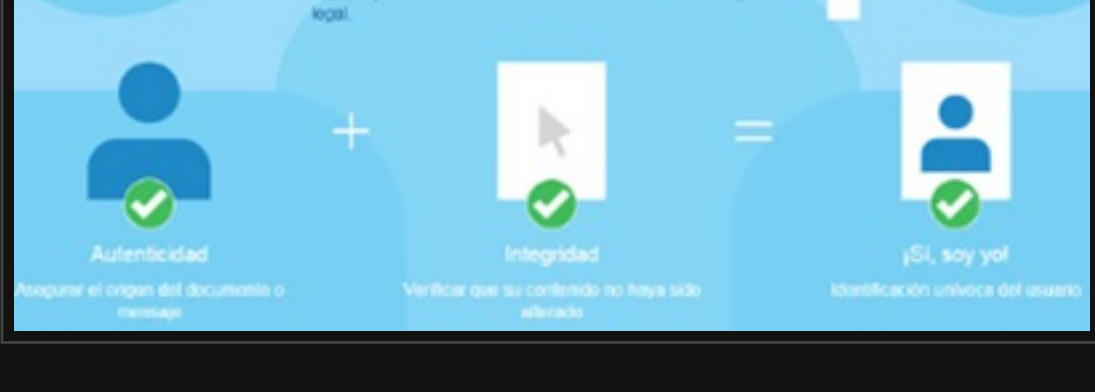
- a) PGP.
- b) Kerberos.
- ☒ c) SET. CORRECTA
- d) SSL.
- e) IP Sec.
- f) S/MIME.
- g) Todas las Anteriores son correctas.
- h) Ninguna de las Anteriores es correcta.

4) El Conjunto de Protocolos para soportar seguridad de intercambio de paquetes en VPNs estandarizado en IPv6 Se lo denomina:



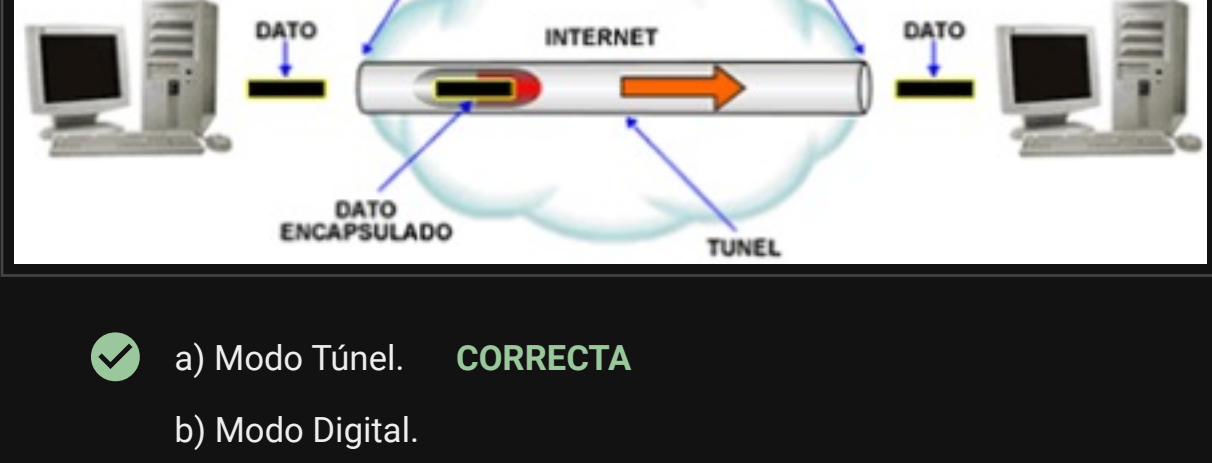
- a) PGP.
- b) Kerberos.
- c) SET.
- d) SSL.
- ☒ e) IP Sec. CORRECTA
- f) DH5.
- g) AES.
- h) Ninguna de las Anteriores es correcta.

5) Dentro de los Beneficios del uso de la Firma Digital podemos destacar:



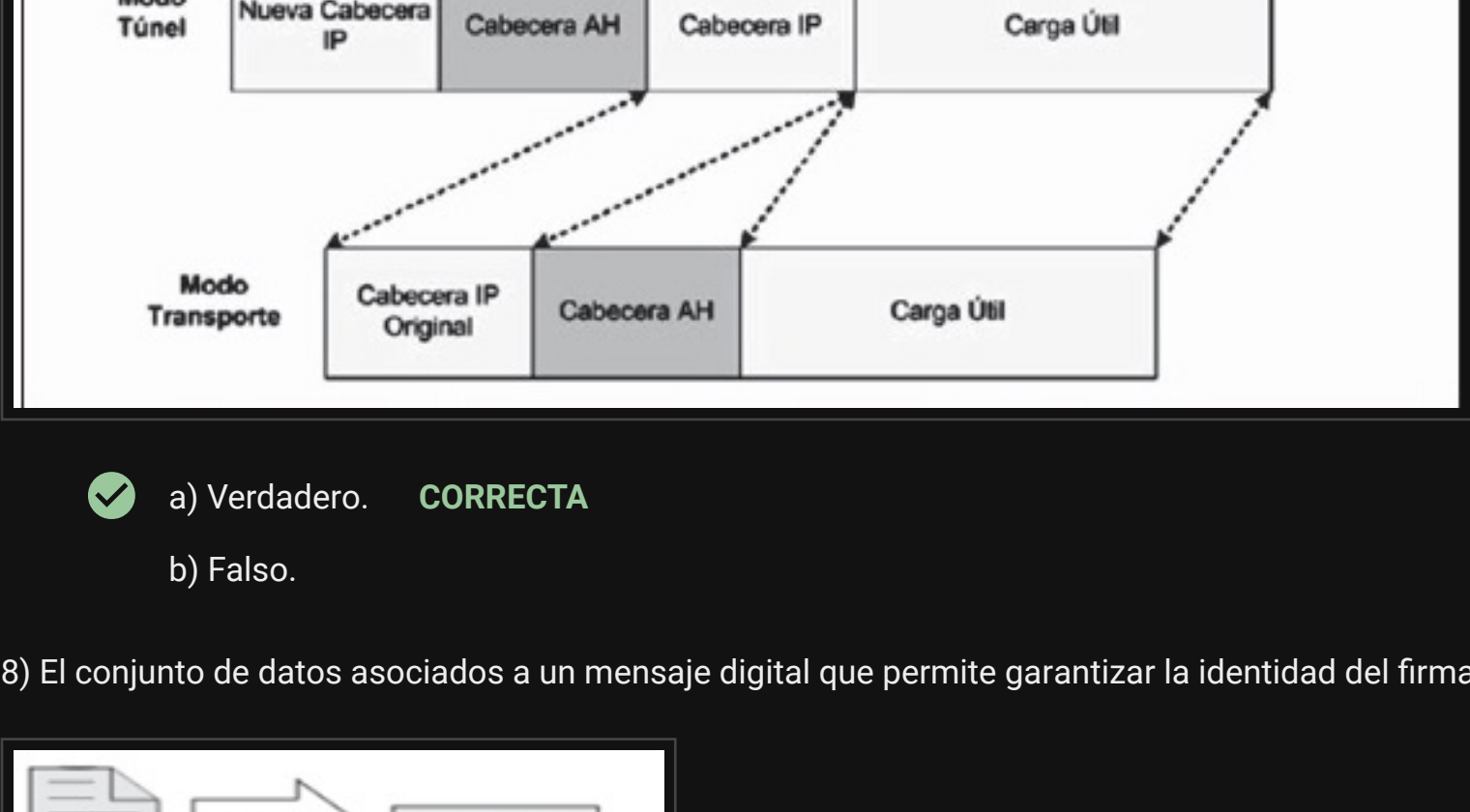
- a) Garantía de Procedencia.
- b) Capacidad de Virtualizar.
- c) Seguridad de no Intervención.
- d) Identificación del firmante.
- e) Todas las anteriores son correctas.
- ☒ f) Hay más de una respuesta correcta. CORRECTA
- g) Ninguna de las Anteriores es Correcta.

6) El Protocolo IP Sec utilizado para realizar encriptación de datos aplicable a redes remotas y heterogéneas puede ser configurado como:



- ☒ a) Modo Túnel. CORRECTA
- b) Modo Digital.
- c) Modo Transporte.
- d) Modo Analógico.
- e) Ambas A y C.
- f) Ambas B y C.
- g) Todas las anteriores son correctas.
- h) Ninguna de las Anteriores es correcta.

7) El protocolo IP Sec cuando es configurado para transportar datos dentro de una red homogénea de tipo LAN en modo transporte encripta exclusivamente datos.



- ☒ a) Verdadero. CORRECTA
- b) Falso.

8) El conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje se lo denomina:



- a) Certificado.
- b) Firma Electrónica.
- c) Firma Holográfica.
- d) X509.
- ☒ e) Firma Digital. CORRECTA
- a) Ninguna de las anteriores es correcta.

9) El ataque Syn Flood se basa con el comienzo de cientos de conexiones a un servidor, e interrumpiéndola inmediatamente. Corresponde a un tipo de ataque:



- a) Fuerza Bruta.
- b) Spoofing.
- c) Autenticación.
- ☒ d) Denegación de Servicio. CORRECTA
- e) Escaneo de Puertos.
- f) Ninguna de las Anteriores es correcta.

10) La Pieza electrónica que prueba la identidad de su propietario, así como el derecho a acceder a la información están basados en la norma estándar para los certificados digitales que corresponde a:

Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issuer Unique ID
Subject Unique ID
Extensions

- a) RSA.
- b) HASH.
- c) DSA.
- d) PGP.
- ☒ e) X509. CORRECTA
- f) Ninguna de las Anteriores es correcta.