

✓ Laura quiere enviar un documento a Ernesto, y no queremos que otra persona pueda leerlo. El documento será cifrado con la clave (1)_____ de (2)_____.

1/1

- ☐ 1: pública 2: Laura
- ☐ 1: privada 2: Ernesto
- ☒ 1: pública 2: Ernesto
- ☐ 1: privada 2: Laura



✓ La firma digital (con clave pública certificada) permite garantizar:

1/1

- ☐ Confidencialidad
- ☐ Disponibilidad
- ☒ No repudio
- ☒ Integridad



✗ Indicar qué se transfiere entre emisor y receptor cuando se utiliza el "código de autenticación de mensajes".

0/1

- ☐ el código hash calculado a partir de la unión del mensaje y un código conocido solo por el emisor y receptor
- ☐ el código hash del mensaje.
- ☐ el mensaje cifrado con la clave pública del emisor.
- ☐ el mensaje cifrado con la clave privada del receptor.
- ☒ el mensaje cifrado con la clave privada del emisor. ✗
- ☐ el mensaje cifrado con la clave simétrica.
- ☐ el mensaje cifrado con la clave pública del receptor.
- ☐ el código hash del mensaje cifrado con la clave privada del emisor.

Respuesta correcta

- ☒ el código hash calculado a partir de la unión del mensaje y un código conocido solo por el emisor y receptor

✗ Se roban un disco rígido que tiene copia de seguridad de nuestros archivos cifrados. Qué aspectos de la seguridad informática están afectados:

0/1

- ☐ No repudio
- ☒ Confidencialidad ✗
- ☐ Integridad
- ☐ Ninguno
- ☒ Disponibilidad ✗

Respuesta correcta

- ☒ Ninguno

✓ Para soportar el protocolo de transferencia de páginas web denominado 1/1
(1) _____, es necesario instalar en el servidor (2) _____ digital,
que emitió una (3) _____.

- ☐ (1) HTTP - (2) TLS - (3) institución gubernamental
- ☐ (1) TLS - (2) una firma - (3) institución gubernamental
- ☐ (1) TLS - (2) un certificado - (3) autoridad certificante
- ☐ (1) HTTPS - (2) una firma - (3) autoridad certificante
- ☒ (1) HTTPS - (2) un certificado - (3) autoridad certificante ✓
- ☐ (1) SSL - (2) una firma - (3) institución gubernamental

✓ Indique algún comando para obtener un código hash del archivo 1/1
`pagos.pdf`:

md5sum pagos.pdf ✓

✓ En mi computadora y con mi usuario ya tengo generadas el par de claves 1/1
pública-privada de ssh. De ahora en más voy a empezar a conectarme por
ssh a un nuevo servidor. ¿Qué comando (con argumentos) debo ejecutar
para evitar que el servidor me solicite la contraseña cada vez que me
conecte? El servidor tiene la dirección IP 170.220.38.98 y mi usuario en
ese servidor es federico.

ssh-copy-id federico@170.220.38.98 ✓

✓ Alguien en el camino entre un servidor web y un cliente, modifica los paquetes que llevan la información de una página web. Indicar el mecanismo del protocolo TLS que permite identificar tal situación. 1/1

☐ Certificados digitales

☐ Cifrado simétrico

☒ Código de autenticación de mensajes



☐ Cifrado asimétrico

✓ Clasificar las siguientes afirmaciones si refieren a una vulnerabilidad, amenaza o ataque. 1-Si alguien accede a la cuenta de Juan podría modificar el stock de los productos del negocio. 2- La contraseña que Juan utiliza para ingresar a su sistema es débil. 3-Fernando adivinó la contraseña de Juan y logró modificar el stock de productos. 1/1

☒ 1: Amenaza. 2: Vulnerabilidad. 3: Ataque.



☐ 1: Amenaza. 2: Ataque. 3: Vulnerabilidad.

☐ 1: Vulnerabilidad. 2: Ataque. 3: Amenaza.

☐ 1: Ataque. 2: Vulnerabilidad. 3: Amenaza.

☐ 1: Vulnerabilidad. 2: Amenaza. 3: Ataque.

☐ 1: Ataque. 2: Amenaza. 3: Vulnerabilidad.

✗ Indicar la validez de la siguiente afirmación: "Al enviar un email por un protocolo que está por sobre el protocolo TLS, el contenido del email estará cifrado con criptografía asimétrica."

0/1

☒ Verdadero

✗

☐ Falso

Respuesta correcta

☒ Falso