

## ✓ ¡Felicitaciones! ¡Aprobaste!

Calificación recibida 100 % Para Aprobar 75 % o más

[Ir al siguiente elemento](#)

1. ¿Cuáles de los siguientes elementos son necesarios cuando se utiliza el cifrado? Selecciona todas las opciones que correspondan.

1 / 1 punto

☐ Token

☒ Clave

✓ **Correcto**

El cifrado requiere un código y una clave. Esto permite el intercambio seguro de información.

☐ Certificado

☒ Código

✓ **Correcto**

El cifrado requiere un código y una clave. Esto permite el intercambio seguro de información.

2. ¿Qué tecnologías se utilizan en la infraestructura de clave pública (PKI)? Selecciona tres respuestas.

1 / 1 punto

☐ Texto cifrado

☒ Cifrado asimétrico

✓ **Correcto**

La PKI intercambia información cifrada mediante cifrado asimétrico, cifrado simétrico y certificados digitales.

☒ Cifrado simétrico

✓ **Correcto**

La PKI intercambia información cifrada mediante cifrado asimétrico, cifrado simétrico y certificados digitales.

☒ Certificados digitales

✓ **Correcto**

La PKI intercambia información cifrada mediante cifrado asimétrico, cifrado simétrico y certificados digitales.

3. Completa el espacio en blanco: El cifrado \_\_\_\_\_ produce un par de claves pública y privada.

1 / 1 punto

☒ asimétrico

☐ hashing

☐ salting

☐ simétrico

✓ **Correcto**

El cifrado asimétrico produce un par de claves, pública y privada, que se utilizan para cifrar y descifrar información. La clave pública se comparte con otros, mientras que el propietario de los datos gestiona la clave privada.

4. Un atacante obtiene acceso a una base de datos en la que las contraseñas de los usuarios están protegidas con el algoritmo hash SHA-256. ¿Puede el atacante descifrar estas contraseñas?

1 / 1 punto

☐ Sí. Los algoritmos hash producen una clave de descifrado.

☒ No. Los algoritmos hash no producen claves de descifrado.

✓ **Correcto**

El atacante no puede descifrar las contraseñas de los usuarios porque se almacenan como un valor hash que es irreversible. Solo los algoritmos de cifrado simétrico y asimétrico producen claves de descifrado.

5. ¿Qué término describe la imposibilidad de negar la autenticidad de una información?

1 / 1 punto

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

✓ **Correcto**

El no repudio significa que no se puede negar la autenticidad de la información. También confirma que el remitente de los datos es quien dice ser.