

## Taller - Introducción a la Encriptación de Datos

Julian Andres Garcia Acuña

- 1) ¿Qué es la encriptación de datos?  
**RTA:** Es un proceso el cual lo que hace es encriptar datos mediante alguna clave para que estos no sean de fácil acceso
- 2) Diferencia entre encriptación, hash y firmas digitales.  
**RTA:** La encriptación se puede revertir o desencriptar con la clave, el hash no puede revertirse, pero si puede verificar la integridad de los datos y la firma digital criptografía para probar la identidad.
- 3) ¿Por qué ciframos los datos en las bases de datos?  
**RTA:** Para evitar que alguien sin su debido permiso lea o robe la información o datos.
- 4) ¿cuáles podría ser posibles causas de la filtración de datos?  
**RTA:** Poner la misma contraseña en todo lado, que sea algún dato de la persona como su nombre, contraseñas débiles o también puede ser por algún virus o malware.
- 5) ¿Qué significa encriptar los datos almacenados en la base de datos?  
**RTA:** Esto quiere decir que la información guardada se transforma en un formato que no se puede acceder de ningún modo sin la clave correspondiente.
- 6) ¿Qué tipo de encriptación es más adecuado para bases de datos en reposo?  
**RTA:** El que se a usado el AES ya que es bastante eficiente y rápido y no tiene gran complejidad para la encriptación.
- 7) ¿Cómo manejarías la rotación de claves en un sistema en producción?  
**RTA:** Con un sistema que automatice las claves es decir que las ande cambiando periódicamente sin afectar claro el acceso de los usuarios.
- 8) Explica los riesgos de no cifrar los datos en tránsito.  
Pueden ser robados o tomados por atacantes o gente no deseada.
- 9) Si tu base de datos contiene datos sensibles, pero también datos públicos, ¿cómo decidirías qué datos cifrar y qué datos no?  
**RTA:** Se cifran solamente los datos sensibles como documentos, cédulas, datos que no deban ser de conocimiento público.
- 10) En un escenario en el que un atacante obtiene acceso a la base de datos, pero no tiene acceso a las claves de encriptación, ¿qué tipo de protección adicional necesitas para mitigar el riesgo?  
**RTA:** Agregaría una autenticación de doble factor para que con ello no solo se dependa de una sola cosa para el acceso del usuario y con ello evitar intentos sospechosos de acceso a la cuenta.