

ENCRIPTACIÓN DE LA INFORMACIÓN

La encriptación es un mecanismo para ocultar un mensaje o información, como resultado produce un texto que solo puede ser leído por el destinatario si este cuenta con la clave para el cifrado correspondiente.

La encriptación utiliza esquemas de cifrado con clave generada por un algoritmo. Esta clave debe ser suficientemente robusta para evitar recuperar la información por terceros no autorizados.

En diferentes ambientes y dispositivos tales como: teléfonos móviles, comunicaciones en red, computadoras, archivos y otros, el cifrado no impide la interferencia, captura o acceso a la información encriptada, sin embargo, su interpretación está limitada ante un posible interceptor no autorizado.

RECOMENDACIONES PARA EL CIFRADO DE INFORMACIÓN, SI CORRESPONDE:

- Use las claves de cifrado de la mayor longitud posible. Usar las longitudes de clave máximas posibles dificulta acceso a la información, con el objetivo de que no se rompa fácilmente su encriptación. Por ejemplo, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.
- Cifrado en capas. Se recomienda generar la mayor cantidad de capas de cifrado que sea posible. Por ejemplo, si se desea encriptar una base de datos procure cifrar cada campo, cada tabla y luego la base de datos completa.
- Almacenar claves de cifrado de forma segura. Un ciberdelincuente podría descifrar de forma simple la información encriptada, si logra acceder a las claves que lo protegen. Recuerde que el cifrado en sí mismo, es solo una parte del proceso para asegurar su información, sin embargo la clave debe ser robusta.

DÓNDE APLICAR EL CIFRADO DE INFORMACIÓN EN ALGUNOS CASOS:

- Cualquier tipo de archivos
- Particiones de disco y memorias USB
- Partición donde esté instalado el sistema operativo.

ALGUNAS TÉCNICAS DE CIFRADO DISPONIBLES:

- Tecnologías de llave pública y privada tales como firma digital son muy seguras.
- Encriptación directa de archivos (PGP).

