SESIÓN

05 | CRIPTOGRAFÍA

- Criptografía
- Avance del proyecto 2

Aplica las técnicas de encriptación de la información

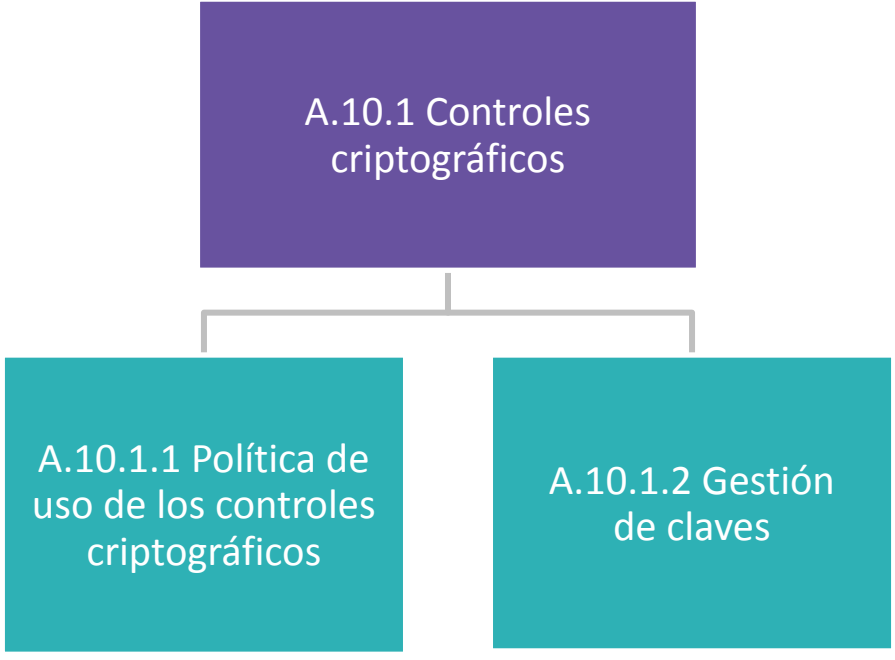
Política de uso de controles criptográficos

Gestión de Claves

/ CRIPTOGRAFÍA

AGENDA

- Objetivo
- Política
- Gestión de Claves
- Tipos de Claves
- Firma Digital



A.10.1 Controles Criptográficos

Objetivo: Garantizar un adecuado y eficaz uso de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

A.10.1.1 Política de uso de los controles criptográficos

Se debe formular e implantar una política para el uso de los controles criptográficos para proteger la información.

A.10.1.2 Gestión de claves

Se deberá elaborar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a través de todo su ciclo de vida.

- **CONCEPTO**
  Técnica que protege documentos y datos. Funciona a través del uso de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

- **CIFRADO DE DATOS**
  Medio para mantener en secreto la información.

PREGUNTAS IMPORTANTES

- ¿Qué hace la organización para utilizar la criptografía?

- ¿Qué tipos de criptografía usa el organismo, y en qué aplicaciones?

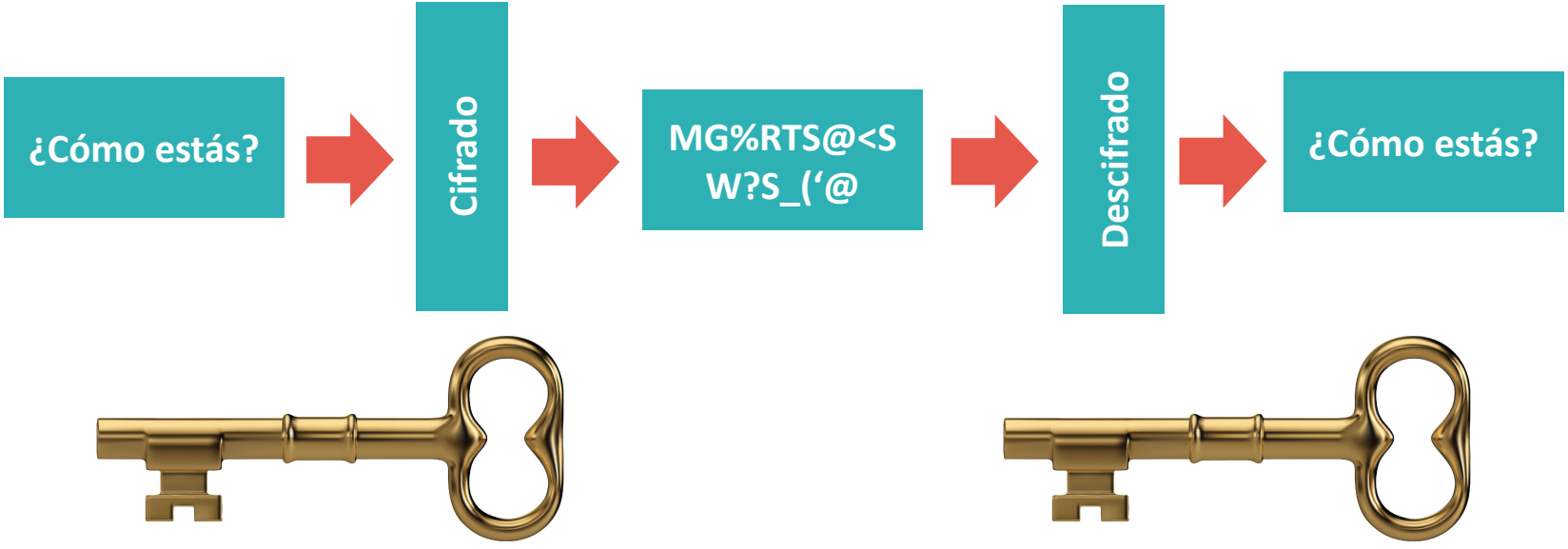
¿CÓMO DEBO GESTIONAR LAS CLAVES?

- Las claves criptográficas deben ser protegidas contra la alteración, pérdida y destrucción.
- Las claves secretas y personales tienen que ser protegidas contra la divulgación no autorizada.
- Se debe proteger físicamente, el equipo que se utiliza para generar, almacenar y archivar las claves.
- ¿Cuándo expira una clave?
- ¿Qué se debe hacer cuando una clave ha sido comprometida?

TIPOS DE CLAVE

- Clave Simétrica
- Clave Asimétrica

Clave Simétrica

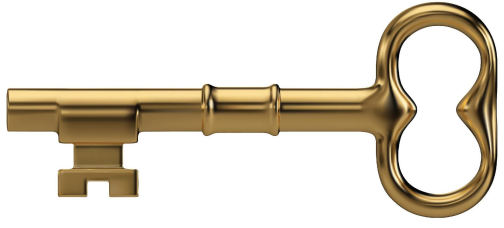


Clave Secreta Compartida

Clave Asimétrica

¿Cómo estás? → Cifrado → MG%RTS@<S W?S_('@ → Descifrado → ¿Cómo estás?

Diferentes claves se usan para cifrar y descifrar



Clave Pública del Destinatario

Clave Privada del Destinatario

FIRMA DIGITAL

- Las firmas digitales se crean mediante el uso de criptografía asimétrica.
- Una firma digital es un método para confirmar si la información digital se ha producido o enviado por quien dice.
- Consta generalmente de dos algoritmos.

Certificado Digital

/ AVANCE DEL PROYECTO 2

ANÁLISIS DE C I D

Objetivo

- Del avance de proyecto 1 , realizar una análisis de confidencialidad, integridad y disponibilidad por cada uno de los activos identificados.
- El análisis debe ser realizado en una herramienta que permita visualizar el mapa de calor correspondiente.
- Si se asigna el valor uno (1) verde.
- Si se asigna el valor dos (2) amarillo.
- Si se asigna el valor tres (3) rojo.

TAREA GRUPAL

Objetivo

- Conocimiento y aplicación del procedimiento de criptografía de información.

TAREA GRUPAL

En grupos de 5 participantes trabajar lo siguiente:

- Los participantes deberán elaborar un algoritmo de cifrado e información.
- Generar una frase corta a la que se le deberá aplicar el algoritmo.
- El texto cifrado será compartido en clase a otro grupo para que sea decodificado.

TAREA GRUPAL

Instrucciones para la entrega de la tarea.

- La tarea deberá ser realizada y descifrada en clase, por todos los miembros del grupo.

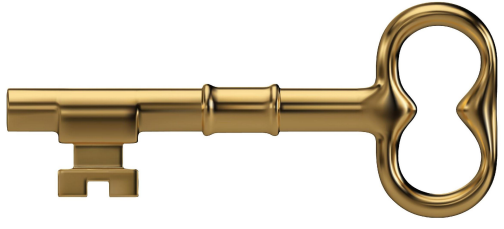
/ RESUMEN

Criptografía.

Clave Asimétrica

¿Cómo estás? → Cifrado → MG%RTS@<S W?S_('@ → Descifrado → ¿Cómo estás?

Diferentes claves se usan para cifrar y descifrar



Clave Pública del Destinatario

Clave Privada del Destinatario