Actividad 17. Infraestructura de clave públca PKI

Infraestructura de clave pública

El modelo de confianza basado en Terceras Partes Confiables es la base de la definición de **las Infraestructuras de Clave Pública (ICPs o PKIs, Public Key Infrastructures).**

Una infraestructura de Clave Pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.

Algunos de los servicios ofrecidos por una **ICP** son los siguientes:

- Registro de claves: emisión de un nuevo certificado para una clave pública.
- Revocación de certificados: cancelación de un certificado previamente emitido.
- Selección de claves: publicación de la clave pública de los usuarios.
- Evaluación de la confianza: determinación sobre si un certificado es válido y qué operaciones están permitidas para dicho certificado.
- Recuperación de claves: posibilitación de recuperar las claves de un usuario.

Las **ICPs** están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:

- Autoridad de Certificación
- Autoridad de Registro Otras Terceras Partes Confiables como por ejemplo las Autoridades de Fechado Digital.

En los siguientes artículos se habla de las Infraestructuras de clave pública (KPI):

- PKI: ¿Qué es La Infraestructura de Claves Públicas?
- ¿Qué es la PKI?
- Infraestructura clave pública (PKI)

En los siguientes vídeos se habla de las Infraestructuras de clave pública (KPI), certificado digital, el sello de tiempo:

- La firma PKI basada en certificados o sello electrónico emitidos por servicios de confianza
- La identificación PKI
- El certificado digital
- El sello de tiempo

Se pide:

1. Elabora un documento explicando el funcionamiento de una infraestructura de clave pública (PKI)