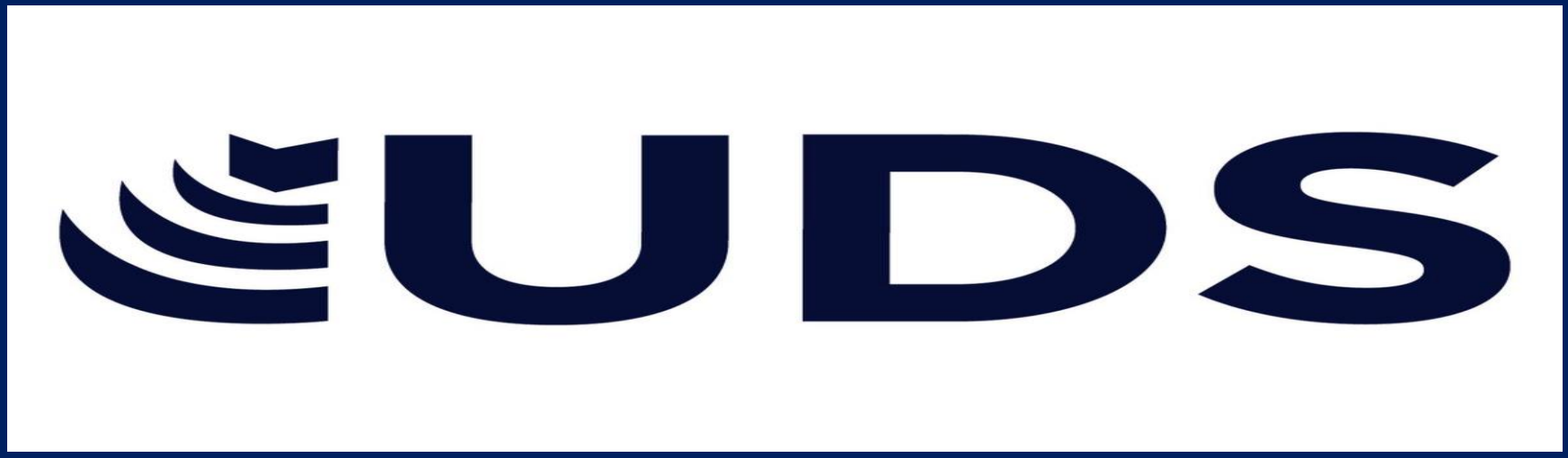


NOMBRE DEL LALUMNO: JOSE CARLOS TOLEDO PEREZ

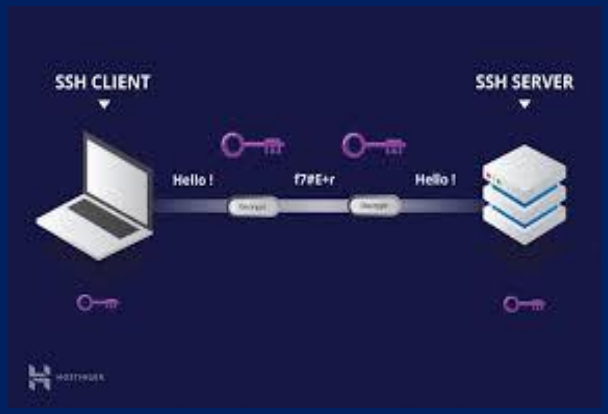
NOMBRE DEL PROFESOR: JORGE SEBASTIAN DOMINGUEZ TORRES

MATERIA: SEGURIDAD EN LA INFORMACION

MODULO: 2

CARRERA: INGENIERIA EN SISTEMAS COMPUTACIONALES

TIPO DE TRABAJO: SUPER NOTA



SSH (Secure SHell) es un programa que nos permite comunicarnos, mediante una línea de comandos, con un servidor remoto de forma segura

Y lo hace, como en el caso anterior, basándose en la criptografía para cifrar las comunicaciones intercambiadas con el servidor, de forma que nadie pueda sacar la información de los paquetes que se cruzan entre ambos

PKI (infraestructura de clave pública)

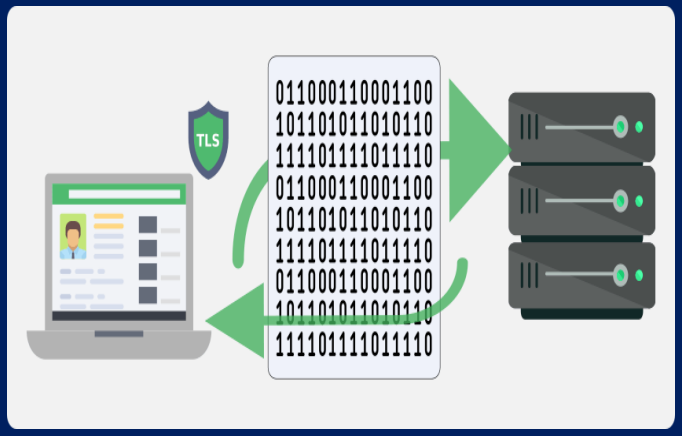
es un conjunto de elementos de infraestructura necesarios para la gestión de forma segura de todos los componentes de una o varias Autoridades de Certificación. Por tanto, una PKI incluye los elementos de red, servidores, aplicaciones, etc. Ahora vamos a identificar algunos de los componentes lógicos básicos de una infraestructura de clave pública.

TLS 1.0 es una reimplementación mejorada de SSL 3.0, con suficientes diferencias para que ambos sean incompatibles entre ellos.

Las diferencias entre TLS y SSL es que la primera mejora al segundo corrigiendo vulnerabilidades de seguridad que se han ido encontrando en SSL, y que en TLS se autentifica al cliente, mientras que en SSL no.

la criptografía es un método de protección de la información y las comunicaciones mediante el uso de códigos, de modo que solo aquellos a quienes está destinada la información puedan leerla y procesarla.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas).



SSL

Lo que hacía el SSL (Secure Sockets Layer) y continúa haciendo TLS (Transport Layer Security) de forma más eficiente, es cifrar las comunicaciones mediante el uso de criptografía en diversos servicios online, como el correo electrónico o la web.

HTTPS

Cuando un usuario hace clic en un enlace o confirma una entrada de URL en la barra de direcciones con el botón Enter, el navegador establece una conexión. El servidor presenta un certificado que lo autentica como un proveedor genuino y confiable. Una vez que el cliente ha verificado la autenticidad, envía una clave de sesión que sólo puede leer el servidor.