**UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA**

**UNAN-León**

****

**FACULTAD DE CIENCIAS Y TECNOLOGÍA**

**DEPARTAMENTO DE COMPUTACIÓN**

**INGENIERÍA EN TELEMÁTICA**

**COMPONENTE:** Seguridad de Redes

**DOCENTE:** Aldo Martínez

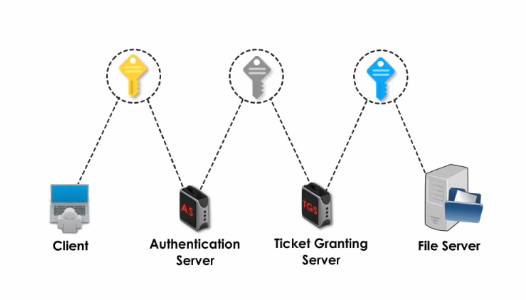
**TEMA:** Programación de Kerberos.

**FECHA:** 27/07/19

**INTEGRANTE:** Jonathan Eduardo Ochoa Velasquez 15-01898-0

¡A la libertad por la Universidad!

**¿Cuál es la arquitectura y funcionamiento de Kerberos?**



R= Kerberos es un sistema de autenticación de usuarios. Se basa en una arquitectura cliente servidor, la cual añade una 3ra entidad (Kerberos) que proporciona 2 servicios: el de autenticación (AS, Authentication Service) y el de tickets (TGS, Ticket Granting Service). Kerberos se base es criptografía simétrica, y este tiene las claves privadas de los clientes y de los servidores, los 2 servicios de Kerberos comparten una clave privada. Si un cliente quiere comunicarse con un servidor, primero debe de autenticarse, para realizar la autenticación realiza lo siguiente:

* El cliente envía una solicitud de autenticación cifrado con su clave privada al AS.
* El servicio AS recibe la petición y la descifra con la clave privada del cliente, de esta manera se asegura que el cliente es quien dice ser.
* El AS le envía al cliente un boleto cifrado con la clave compartida por los servidores Kerberos.
* El cliente le envía este boleto al TGS y le indica que quiere establecer una conexión con un servidor, el TGS así se asegura que el cliente es quien dice ser.
* El TGS le envía un token al cliente cifrado con la clave privada del servidor al que el cliente se desea conectar y una clave privada para que el cliente use con el servidor que se desea conectar, esta clave privada es enviada en el token y en otro mensaje cifrado con la clave del cliente.
* El cliente le envía ese token al servidor, el servidor descifra el token con su clave privada, asegurándose que el cliente es quien dice ser, y ya se pueden intercambiar información de forma segura por un periodo de tiempo limitado, que está indicado en el token.