

RESUMEN

La información es un bien intangible cuya criticidad e importancia para quien la genera y la recibe es de difícil cuantificación, es responsabilidad de los administradores de red ofrecer entonces un escenario de transporte y gestión de datos que ofrezca la seguridad necesaria; durante el proceso de transferencia, procesamiento y almacenamiento de los datos, la información está sujeta a riesgos de ataques por parte de elementos tanto internos como externos a la red, estos ataques se pueden presentar durante la creación de la información, la transferencia, el procesamiento o el almacenamiento de los datos, es decir el riesgo existe a lo largo de todo el proceso. Existen muchos métodos que están destinados a mejorar la seguridad en la red, la mayoría de ellos trabajan en capa aplicación, sin embargo este trabajo analiza la arquitectura de IPSec e investiga la factibilidad de su implementación sobre IPv6 en un escenario que requiere contar con altos niveles de seguridad. Inicialmente se procederá a la descripción del funcionamiento del protocolo IPSec, su arquitectura, los procesos de autenticación y encriptación. Se hará un levantamiento del estado actual de la red de datos en la Institución, el análisis de la topología física actual, se propondrá el esquema de direccionamiento, los requerimientos de infraestructura y planificación de la implementación de IPSec sobre IPv6. Se procederá al diseño lógico y físico de la propuesta de implementación, posteriormente se realizará la simulación de acuerdo a los parámetros establecidos y finalmente se hará un análisis de los resultados.

Palabras clave: UNIVERSIDAD POLITÉCNICA SALESIANA, SEGURIDADES, ENCRIPCIÓN, IPSEC, IPV6.