Unidad I

Introducción a la administración de redes

1.1. Definición de la administración de redes según la ISO.

Los términos **administrador de red**, **especialista de red** y **analista de red** se designan a aquellas posiciones laborales en las que los ingenieros se ven involucrados en redes de computadoras, o sea, las personas que se encargan de la **administración de la red**.

Los administradores de red son básicamente el equivalente de red de los administradores de sistemas: mantienen el hardware y software de la red.

Esto incluye el despliegue, mantenimiento y monitoreo del engranaje de la red: switches, routers, cortafuegos, etc. Las actividades de administración de una red por lo general incluyen la asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de ruteo así como, configuración de autenticación y autorización de los servicios.

Frecuentemente se incluyen algunas otras actividades como el mantenimiento de las instalaciones de red tales como los controladores y ajustes de las computadoras e impresoras. A veces también se incluye el mantenimiento de algunos tipos de servidores como VPN, sistemas detectores de intrusos, etc.

Los analistas y especialistas de red se concentran en el diseño y seguridad de la red, particularmente en la Resolución de problemas o depuración de problemas relacionados con la red. Su trabajo también incluye el mantenimiento de la infraestructura de autorización a la red.

1.2. Funciones de la administración de redes definidas por ISO.

Que implica la administración de redes?, para poder dar una definición más apegada a la realidad, nos basaremos en un modelo de administración de redes creado por la ISO (International Standards Organization) donde se definen 5 áreas donde se especifican claramente las funciones de los sistemas administradores de redes.

1.3. Criptografía:

1.3.1. Criptografía simétrica,

La **criptografía simétrica** (en inglés *symmetric key cryptography*), también llamada **criptografía de clave secreta** (en inglés *secret key cryptography*) o

criptografía de una clave[1] (en inglés*single-key cryptography*), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

1.3.2. Criptografía asimétrica,

La **criptografía asimétrica** (en inglés *asymmetric key cryptography*), también llamada **criptografía de clave pública** (en inglés *public key cryptography*) o **criptografía de dos claves**[1] (en inglés *two-key cryptography*), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

1.4. Rendimiento:

1.4.1. de fallas,

Cuando hay problemas en las redes eléctricas es necesario encontrar la secuencia de la anomalía rápidamente y, para ello, expertos de la UN desarrollaron una herramienta que optimiza el proceso hasta en dos minutos.

Se trata del Diagnóstico Automático de Eventos (DAE), un sistema que permite procesar ágilmente fallas de un sistema interconectado como el de la electrificadora ISA.

Tales problemas se identifican, normalmente, con fuentes y equipos registradores de información que, una vez estudiados por analistas, dan el diagnóstico. Sin embargo, ese paso se puede evitar con la innovación de la UN que obtiene los datos dinámicamente.

Investigadores del Grupo de Teleinformática y Teleautomática (T y T) de la UN en Medellín, explican que hay varias causas para que se den fallas en las redes. Por ejemplo, las hay de origen natural, como descargas eléctricas atmosféricas que caen sobre el sistema, vientos muy fuertes que generan algún descontrol. Otras de tipo técnico, como una mala operación de los equipos y/o desgaste de alguna línea. Además de las que provienen de actos malintencionados, como los terroristas, cuando tumban las torres.

Para cualquiera de estas causas se debe conocer el origen general del problema, y eso es lo que hace el DAE, que consta de tres módulos: el que se encarga de las fuentes digitales, el que reúne la información análoga y el que junta la información de los dos primeros para finalmente hacer las verificaciones de coherencia de la información.

1.4.2. de contabilidad,

Después de la reseña histórica, de la Contabilidad y los Costos, el investigador considera oportuno exponer los conceptos, funciones, clasificaciones, relaciones y comparaciones de la plataforma que sirve de soporte a este trabajo de grado.

1.4.3. de seguridad

La **seguridad informática** o **seguridad de tecnologías de la información** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El concepto de seguridad de la información no debe ser confundido con el de «seguridad informática», ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Puesto simple, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quien y cuando se puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización a organización. Independientemente, cualquier compañía con una red debe de tener una política de seguridad que se dirija a conveniencia y coordinación.