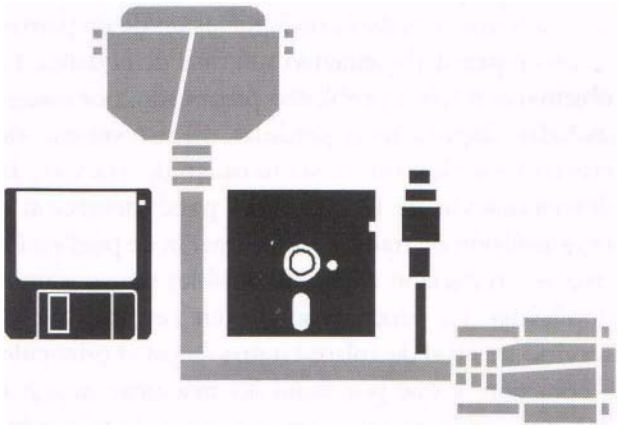
METODOLOGÍA PARA LA AUDITORIA DE UNA RED DE TRANSMISIÓN DE DATOS

(Niveles del MODELO OSI)

Carlos Alberto Vanegas*
Docente de la Facultad Tecnológica

LM información, fuente de poder de una organización, debe mantenerse protegida. Por eso debemos desarrollar técnicas de auditoría a las redes de datos, eliminando el riesgo de pérdida de la misma. Si analizamos, detectamos y corregimos la seguridad de la misma en todos los puntos críticos de una Red de Transmisión de Datos, lograremos obtener un flujo de información eficiente.



decisiones de una organización. Por su valor incalculable, es necesario protegerla.

El avance y perfeccionamiento tecnológico permanente, específicamente en el campo de las telecomunicaciones, permite a los computadores comunicarse con otros dispositivos remotos, y con otros computadores físicamente separados. Así se ha desarrollado el concepto de RED DE TRANSMISIÓN DE DATOS, elemento muy importante el diseño de sistemas de información.

Sin embargo, la información que mediante ellas se maneja sin estar debidamente protegida durante el proceso de transmisión de datos, puede generar costosas e importantes pérdidas a las organizaciones usuarias, generando riesgos e incertidumbre en la exactitud de la información manejada.

Por esto es muy importante desarrollar y/o aplicar una metodología de Auditoría a los procesos de transmisión de datos, con el fin de garantizar la seguridad en la información del sistema.

Todo sistema de comunicación se compone de tres elementos básicos a saber: fuente, destino y canal o medio de comunicación. Su objetivo es reproducir
mensaje originado en la fuente transmitiendo información, que es el elemento vital. Finalmente este proceso requiere de un medio que la transporte: la señal u onda eléctrica.

os efectos de la información sobre el sistema son los

a información puede ser transmitida por medios químicos, mecánicos, electromagnéticos o de cualquier otra índole. Cuando se utiliza el medio electromagnético, el proceso es

* Ingeniero de Sistemas Uni-INCCA de Colombia, Profesor de la Universidad Distrital "Francisco José de Caldas" adscrito a la Facultad Tecnológica.

Cuando la información no requiere grandes desplazamientos es usual la utilización de medios físicos como el sistema de cableado telefónico (multipunto, esto es, más de dos equipos terminales de datos conectados a un mismo canal), y en espacios más reducidos cableado punto a punto (sólo dos equipos terminal de datos conectados a la línea o canal).

Para establecer una comunicación entre computadores, lo mismo que para establecerla entre personas, es necesario contar con una serie de normas que regulen dicho proceso. Esas normas las fija la sociedad en general o una organización internacional de normalización.

El **MODELO OSI** es la base para la estructuración de una red de comunicaciones. Este modelo propone dividir en niveles todas las tareas que se llevan a cabo en una comunicación entre computadores.

Todos los niveles están bien definidos y no interferirán con los demás; de ese modo, si fuera necesaria una corrección o una modificación en un nivel, no se afectaría al resto.

En total se formaron siete niveles: los cuatro primeros tienen funciones de comunicación y los tres restantes de proceso. Se estudiará cada uno de ellos, explicando qué función cumplen, cuál es su objetivo, cuál debe ser el control de auditoría y cuáles son las pruebas de auditoria que deberían realizarse.

Nivel **1: capa de enlace físico**

En este nivel se definen las características eléctricas y mecánicas de la red, necesarias para establecer y mantener la conexión física. Se incluyen las dimensiones físicas de los conectores, los cables y los tipos de señales que van a circular por ellos. Por consiguiente, se ocupa de la transmisión de bits a lo largo de un canal de comunicaciones. Su objetivo es controlar el acceso físico a los cables de conexión y a los modems. El control consiste en proteger físicamente los cables de conexión, modems y circuitos de comunicación. La prueba que se realiza es la verificación física de los lugares en donde están conectados todos los alambres y cables de comunicación.

Todas las líneas de abonados locales que salen del edificio deben asegurarse físicamente y colocarse fuera del alcance de los usuarios, para evitar un daño físico ó una derivación telefónica. Para ello deben aplicarse procedimientos formales que ayudan a identificar amenazas a la seguridad o entradas ilegales al sistema cuando se efectúen en la capa física.

Por último la protección física de los circuitos telefónicos (canal IC) es responsabilidad de la empresa de comunicaciones (Compañía Telefónica).

Nivel 2: capa de enlace de datos

Este nivel se encarga del empaquetamiento de datos en tramas o paquetes. La creación y reconocimiento de una trama se realiza con la inclusión de un patrón de bits especial al comienzo y al final de la trama. El objetivo es resolver problemas provocados por tramas .dañadas, duplicadas o perdidas. El mecanismo de control es el conteo secuencial de tramas, la determinación de la capacidad para detección y retransmisión de tramas, identificación de pérdida de tramas y reducción a cero de posibles transmisiones duplicadas. La prueba consiste en verificar que el servicio de nivel de enlace en una red es el orientado a conexión, y que por tanto las máquinas origen y destino establecen una conexión antes de transmitir datos.

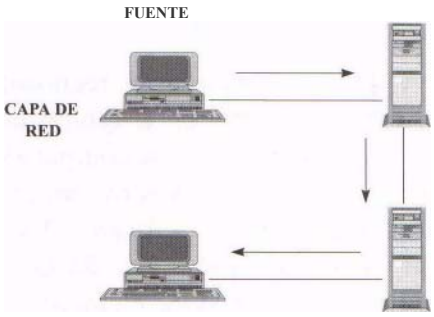


Figura 1. Nivel 3

Cada una de las tramas transmitidas a través de la conexión se numera, y el nivel de enlace garantiza que cada trama transmitida sea, en efecto, recibida exactamente una vez y en un orden correcto.

Nivel 3: capa de red

Este nivel se ocupa del control de la operación de la SubRed, convirtiendo direcciones lógicas (nombres) en direcciones físicas (nodos o dispositivos).

Un punto de suma importancia en su diseño es la determinación de como encaminar los paquetes del origen al destino. También se incluyen la administración y gestión de datos, la emisión de mensajes y la regulación del tráfico en la red. El objetivo de este nivel es elegir la mejor ruta del circuito. El propósito del control es asegurar que todos los paquetes sean recibidos correctamente en los destinos y se controle la existencia de demasiados paquetes en un canal. La prueba consiste en verificar que existan rutinas para la emisión de cuentas para los usuarios. Estas deben revisarse en cuanto a posibles problemas como errores, robo de tiempo o cargos incorrectos para mensajes, (ver Figura 1. Nivel 3).

Nivel 4: capa de transporte

Este nivel se encarga de que el transporte de datos se realice en forma segura y económica, desde la máquina fuente hasta la máquina destino.

Su función principal consiste en aceptar los datos de la capa de sesión (dividirlos siempre que sea necesario), en unidades más pequeñas, pasarlas a la capa de red y asegurar que todos ellos lleguen correctamente al otro e

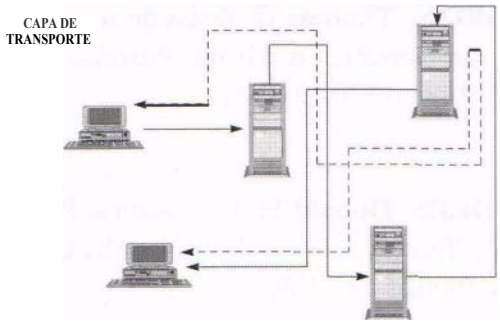


Figura 2. Nivel 4

En síntesis el objetivo es controlar el transporte de datos entre la fuente y el destino. El propósito del control es el direccionamiento de la máquina fuente/ destino y el control de flujo de mensajes. El software a este nivel determina qué máquina pertenece a qué conexión. La prueba en este nivel consiste en comprobar que un programa en una máquina fuente dialoga con un programa similar en la máquina destino mediante el empleo de encabezados y mensajes de control.

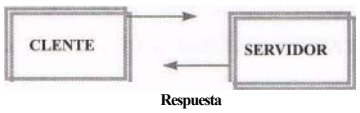
De este modo, algunos de los controles podrían ubicarse en los programas de aplicación, (ver Figura 2. Nivel 4).

Nivel 5: capa de sesión

Este nivel permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos, apoya la sesión del usuario y enciende y apaga la comunicación entre dos estaciones de trabajo. Uno de los servicios de la capa de sesión consiste el control del diálogo

Así su objetivo es permitir sesiones entre la fuente y el destino. La función del control es proporcionar secuenciación de mensaje cuando el nivel de transporte no lo haga. Finalmente para la realización de la prueba se deben analizar controles relacionados con una Terminal (especializado o de marcación) como contraseñas, procedimientos de entrada, direccionamiento de Terminal, (ver Figura 3. Nivel 5).

CAPA DE SESIÓN



MODELO CLÍENTE-SERVIDOR

Figura 3. Nivel 5

Nivel 6: capa de presentación

Este nivel realiza ciertas funciones que se necesitan bastante a menudo, para dar una solución general de ellas, más que dejar que cada uno de los usuarios resuelva problemas a su manera.

También realiza codificación de datos y traduce órdenes del nivel de aplicación, proporcionando una sintaxis (lenguaje) que sea comprendida por los dispositivos a través de la red.

Se incluye además el control de impresoras, emulación de terminales y los sistemas de codificación.

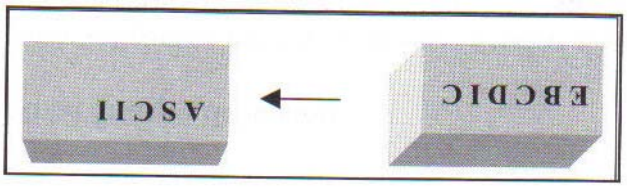


Figura 4. Capa de presentación

En general su objetivo es controlar las posibles fallas, para que estas sean transparentes al usuario. El control pretende la conversión de archivos y formatos de archivos incompatibles, de modo que sea posible la comunicación entre dos sistemas. La prueba consiste en verificar que existen seguridades en las conexiones de las redes tales como:

- Proteger los datos para que no puedan ser leídos por personas que no tiene autorización para hacerlo
- Impedir que las personas sin automación inserten o borren mensajes
- Verificar al emisor de cada uno de los mensajes :
- Hacer posibles que los usuarios transmitan electrónicamente documentos firmados.

Nivel 7: capa de aplicación

Este nivel realiza funciones como transferencia de archivos y correo electrónico, la entrada de trabajos a distancia, servicios de directorio, entre otras. Su objetivo es aislar los programas de aplicación de la tarea de transmitir mensajes. Los controles deben asegurar que este nivel de Software no dirija erróneamente ningún mensaje. Estos también están relacionados con los programas de aplicación de los sistemas administrativos, el software de comunicación también debe contener controles internos.

La prueba consiste en verificar los controles lógicos que se encuentran integrados en el sistema mismo de la aplicación, e identificar el software de comunicación que se esté utilizando.

Bibliografía

GONZÁLEZ SAÍN, Néstor. Comunicaciones y Redes de Procesamiento de Datos. Editorial Me. Graw Hill. 1,993, México.

ILLINGWORTH, Valerie. Diccionario de Informática. Segunda Edición, Editorial Me. Graw Hill.

LEVINE GUTIÉRREZ, Guillermo. Introducción a la Computación y a la Programación Estructurada. Segunda Edición. Editorial Me. Graw Hill. Grupo Micrológica. Universidad Autónoma Metropolitana. Iztapalapa, México.

MADRON, Thomas W. Redes de Área Local. La siguiente Generación. Grupo Noriega Editores. 1,992. Páginas 170,191,211.

SANDERS, Donald H. Informática, Presente Y Futuro. Tercera Edición, Editorial Me. Graw Hill, 1,983. Páginas 127-150.

WOLFGANG, R. Redes Locales Practico Y Conciso. Desde la Solución Monousuario Hasta la Estructura de la Red, Editorial Datanet.