

Redes de datos en instituciones de educación básica y media

Por Juan Carlos López García & Willy Figueroa Celis · 2008-03-01

La Red Escolar de Datos es un elemento de la infraestructura tecnológica que toda institución educativa que disponga de computadores, debe implementar. Este artículo explica en qué consiste, cuáles son tanto sus componentes básicos como su estructura lógica. Ofrece además, una serie de recomendaciones para administrarla: políticas de acceso de docentes, personal administrativo y estudiantes.

Una Red de Área Local (LAN, por su sigla en inglés) está compuesta por un conjunto de computadores interconectados entre sí a través de un medio (cable o medio inalámbrico) y unos equipos de transmisión (Routers, Switches y tarjetas). Esto permite que los usuarios de la Red, de acuerdo con unos perfiles establecidos, compartan archivos, aplicaciones, medios de almacenamiento de datos y dispositivos como impresoras y unidades de CD/DVD. Estas Redes se han popularizado en empresas grandes y pequeñas, gracias a la facilidad con la que se instalan y a la optimización de los recursos que se comparten.

Las Instituciones Educativas (IE) no pueden quedarse atrás en la implementación de estas redes y deben procurar convertir sus trabajos administrativos y académicos en labores cooperativas de la institución. La *Red Escolar de Datos (RED)* permite la comunicación entre usuarios de las diferentes áreas de la institución, para compartir la información que generan de forma rápida y fácil, agilizando así, tanto actividades pedagógicas y administrativas como procesos educativos, entre directivas, docentes y estudiantes.

1. OBJETIVOS DE LA RED ESCOLAR DE DATOS (RED)

El objetivo principal de una *Red Escolar de Datos (RED)* es compartir los recursos de las Tecnologías de la Información y la Comunicación (TIC) que tiene la Institución, mediante procesos de trabajo conjunto o complementario entre directivos, coordinadores académicos, docentes y estudiantes.

2. BENEFICIOS DE LAS REDES ESCOLARES DE DATOS

Los beneficios son múltiples y en la mayoría de los casos van a depender de los recursos tecnológicos (TIC) con los que cuente la IE. Algunos de estos son:

a. Centralizar la información: Agrupar en un servidor de archivos determinado todos los trabajos de los estudiantes: tareas, proyectos, exámenes, investigaciones u otros. Esto permite que los docentes realicen seguimiento académico y control de cumplimiento de tareas, desde cualquiera de los computadores conectados a la Red en la Institución.

Otra de las ventajas de la centralización es poder compartir y comunicar información entre coordinadores académicos y docentes. Esta información puede ser: directorio de estudiantes, planeación de horarios, aplicaciones de registro académico, herramientas pedagógicas que promueve la IE, etc.

b. Compartir recursos: Optimizar la cantidad de dispositivos como impresoras o unidades de almacenamiento (quemadores de DVD o de CD) que se pueden compartir a través de la red. Por ejemplo, no es necesario usar memorias USB para transferir la información que se necesita imprimir, pues si esta se encuentra en la red, se puede imprimir desde cualquier computador conectado a ella.

c. Seguridad: El administrador de la red asigna diferentes permisos para utilizar recursos compartidos (dispositivos, programas y datos) de acuerdo a las funciones de cada usuario o grupo de usuarios. De esta manera, por ejemplo, los docentes tendrán acceso al programa de registro académico, pero los estudiantes no. El administrador de la red es el encargado de velar por la seguridad tanto de los dispositivos compartidos como de los datos almacenados.

d. Acceso remoto: La información se puede consultar en cualquier momento y desde cualquier lugar. Es posible habilitar el servicio incluso, para que los docentes se comuniquen con la red de la IE desde su casa para poder así digitar o consultar información.

e. Conectividad entre Redes: En instituciones educativas grandes se puede dividir la información para que resida en varios servidores; estos últimos se pueden interconectar permitiendo a los usuarios acceder a cualquiera de esas redes, dependiendo de sus funciones.

f. Administración centralizada: Es posible habilitar opciones del sistema operativo de red para facilitar su administración. Por ejemplo, mediante la opción “distribución de software automático” de Windows Server 2003, se pueden instalar aplicaciones en forma remota desde el servidor, en todas las estaciones de trabajo de la red.

3. COMPONENTES BÁSICOS DE UNA RED DE DATOS

a) Servidor: Es el equipo central (computador), con características técnicas robustas (discos duros SATA o SCSI, Tarjeta RAID, unidad de respaldo, sistema operativo de Red), encargado de almacenar los datos que se comparten entre los usuarios. Se recomienda que este equipo trabaje de forma dedicada, es decir que solo se use para las tareas de compartir datos y *no como estación de trabajo*. Normalmente, el número de servidores necesarios en una institución depende de la cantidad de subredes que se necesite atender o de los servicios que se quieran prestar; ej: servidor de correo, de Internet, de datos para el área académica, de datos para el área administrativa, etc. Otra recomendación es conectar ese o esos servidor(es) a una UPS (Uninterruptible Power Supply), para evitar daños de los datos en eventos de desconexión súbita del suministro eléctrico.

b) Sistema operativo de Red: Es el software residente en un servidor dentro de una red de área local (LAN) y se encarga de administrar las solicitudes de las estaciones de trabajo conectadas a la red. Los sistemas operativos de red pueden comunicarse con los sistemas operativos de las estaciones que la conforman a través de un medio de transmisión con el objeto de intercambiar información, transferir archivos y ejecutar comandos remotos, entre otras funcionalidades.

b) Estaciones de Trabajo: Las estaciones de trabajo son computadores que cuentan con sistemas operativos que les permitan trabajar en Red (Windows, Linux, etc). Se conectan al servidor por medio de tarjetas de red. Anteriormente, se usaban terminales “brutas” así llamadas porque no tenían CPU y dependían totalmente del servidor. Ahora, debido a la reducción de costos en estos equipos, se usan computadores de escritorio (PC) que solo utilizan el servidor para almacenar y compartir datos y aplicaciones, o para acceder a dispositivos compartidos.

c) Cableado: Existen diferentes tipos de cable pero los más utilizados para armar una red son: STP, UTP, par trenzado, cable coaxial y fibra óptica. En la actualidad el de preferencia es el **par trenzado**, que consiste en hilos de cobre trenzados y aislados, esto es, independientes unos de otros, lo que le confiere ventajas sobre el coaxial; estas ventajas son tanto técnicas como económicas. La tecnología que usan estos cables ha mejorado con el paso del tiempo y además no requieren habilidades sofisticadas para instalarlos; la emisión de señales hacia el exterior es mínima y son bastante inmunes a las interferencias.

Otro medio de transmisión importante es la **fibra óptica** que tiene como desventaja su elevado costo. Normalmente se utiliza para unir redes que se encuentran separadas por grandes distancias. La fibra óptica usa como medio de transmisión la luz. Permite enviar información a gran velocidad y con menor posibilidad de interferencia que puedan afectar la calidad de los datos.

Una Tecnología cuya aceptación crece aceleradamente es la inalámbrica. Con esta no hay necesidad de tender cables para interconectar los computadores que conforman la red pues los datos se transmiten a través del espacio.

d) Switches y Routers: Son los encargados de conectar las estaciones de trabajo con el servidor. También ofrecen la posibilidad para interconectar varias redes; por ejemplo, laboratorios de idiomas y de informática. Por otro lado, maximizan el desempeño de la red y permiten mayor velocidad en la transmisión de datos.

e) Antivirus: Para la seguridad de la red es importante contar con este elemento que evita la propagación de programas informáticos dañinos (virus y spyware) que corrompen parcial o totalmente el sistema operativo, las aplicaciones instaladas y/o

los datos almacenados tanto en el servidor como en las estaciones de trabajo. No solo es importante instalar un antivirus de buena calidad, sino mantenerlo actualizado, tanto con la última versión del software escogido, como con la última definición de virus disponible de este, pues a diario aparecen nuevos virus. El correo electrónico y los dispositivos de almacenamiento removibles (memorias USB, discos flexibles) son los principales medios de propagación de los virus.

f) Backup: Este proceso, conocido también como copia de respaldo, permite realizar una copia de la información almacenada en el servidor a un dispositivo de almacenamiento externo. Uno de los beneficios del Backup, es que ante cualquier eventualidad, se pueda restaurar total o parcialmente la información afectada. Si la información a respaldar, en términos de MB, no es muy voluminosa (menos de 4500MB) y la operación no se lleva a cabo diariamente, el Backup se puede realizar en una unidad escribible de DVD. Por lo regular, las copias de seguridad se realizaban en Cintas Magnéticas especiales, pero en la actualidad se pueden ejecutar en unidades de CD o DVD.

4. ESTRUCTURA LÓGICA DE UNA RED

Para mejorar el uso de la información y de los dispositivos compartidos se deben tener en cuenta varios elementos, a saber:

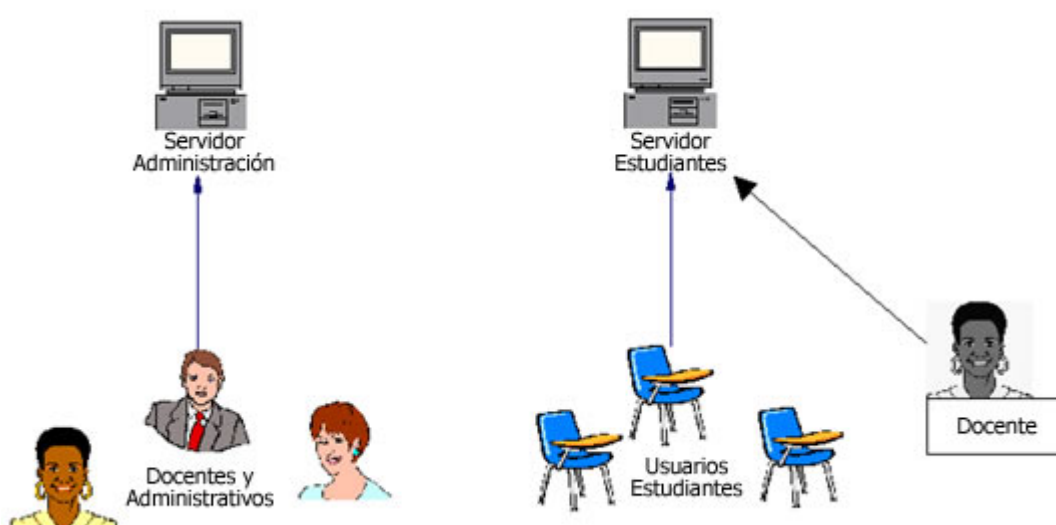
Datos compartidos del Servidor: Inicialmente se debe definir si los datos se almacenan en uno ó en varios servidores y cuáles usuarios accederán a ellos.

También se debe definir, dependiendo de los usuarios, qué datos serán de uso común y cuáles de uso restringido.

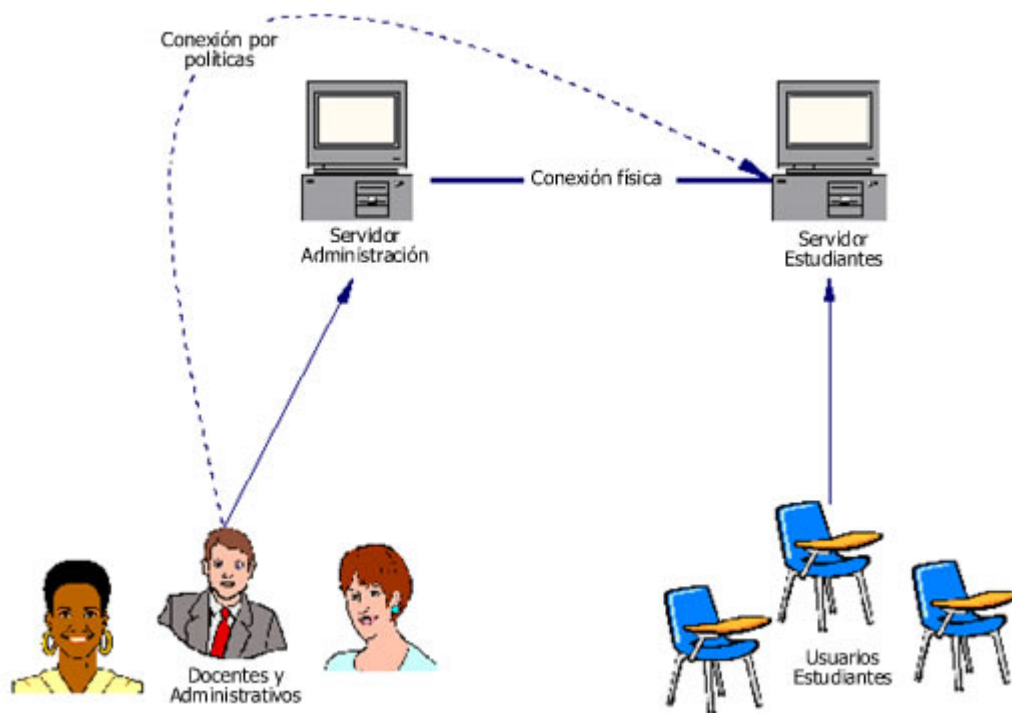
Si la información se almacena en dos servidores independientes, es decir que no están interconectados por un medio físico (cable), se ofrece mayor seguridad a la información almacenada pero se limita el acceso a los usuarios de ambos servidores. Por lo regular, en las IE se cuenta con dos tipos de información: Académica (notas, trabajos de estudiantes, horarios, etc) y administrativa (registro de estudiantes, contabilidad, nómina, cartera, etc). Es importante definir si ambos tipos de información van a almacenarse en el mismo servidor de datos o van a estar en

servidores separados. Por ejemplo: Si se configuran dos servidores, uno con información Administrativa y otro con información Académica , los usuarios del servidor Administrativo no pueden revisar, desde su equipo, de tipo académico de los estudiantes.

Esta situación demanda de parte de los usuarios del servidor Administrativo, desplazarse a un equipo conectado al servidor Académico y usar un perfil de usuario y una contraseña, diferentes al los que manejan en el otro servidor, como se muestra en la siguiente gráfica:



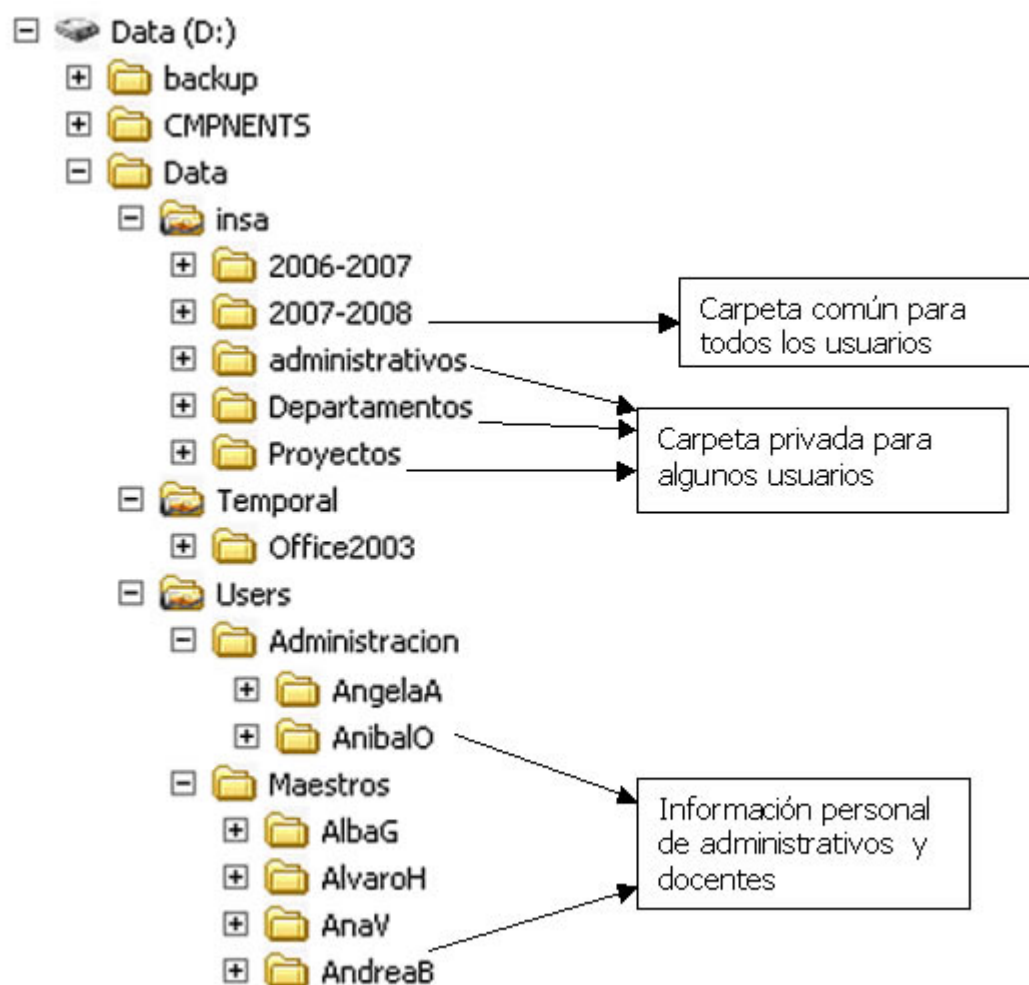
Si se interconectan los dos servidores , como lo muestra la siguiente imagen, un usuario podría tener acceso a ambos. Por medio de políticas de seguridad, se comparte o se restringe el accesos de diferentes usuarios o grupos de estos a cada uno de los servidores. Por ejemplo: un usuario con perfil de docente puede tener acceso al programa de notas, a consultar su nómina y a la información de todos los estudiantes de grado cuarto; sin embargo, un usuario con perfil de estudiante de grado cuarto solo tendría acceso a su propia información, no tendría acceso a la información de sus compañeros de clase y mucho menos a aplicaciones o datos que se encuentran en el servidor de administración.



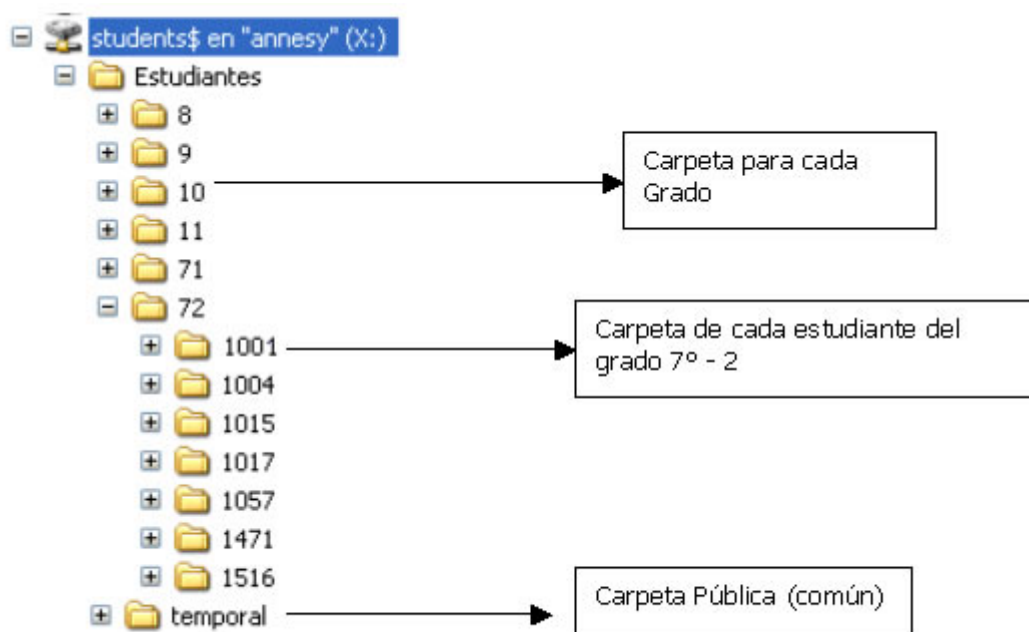
Esta solución requiere realizar una configuración avanzada de los servicios de seguridad del sistema operativo de la red, pero beneficia a docentes, coordinadores académicos y directivos permitiéndoles el acceso a los datos de los estudiantes y brindando conectividad total desde cualquier estación de la red sin necesidad de desplazarse de un servidor a otro, como lo harían en el modelo anterior.

Datos: Son la información que se almacena en carpetas compartidas. Por ejemplo: en el servidor Administrativo, se puede crear una carpeta pública (común), esto es a la que todos los usuarios con el perfil adecuado puedan ingresar acceder a la información que contiene; además, se puede crear una carpeta personal en la cual cada usuario guarde su información privada (personal) y, una o varias carpetas compartidas para grupos de usuarios. Estas carpetas se asignan según el perfil de cada uno de los usuarios o grupos de estos ; Ej: directivos ó docentes de una misma área.

En el caso de los estudiantes, cada uno de ellos tiene su carpeta personal con subcarpetas para almacenar trabajos correspondientes a los diferentes periodos académicos del año escolar y una carpeta Pública (común) en la cual los docentes pueden guardar y almacenar los talleres o trabajos que los estudiantes deben realizar.

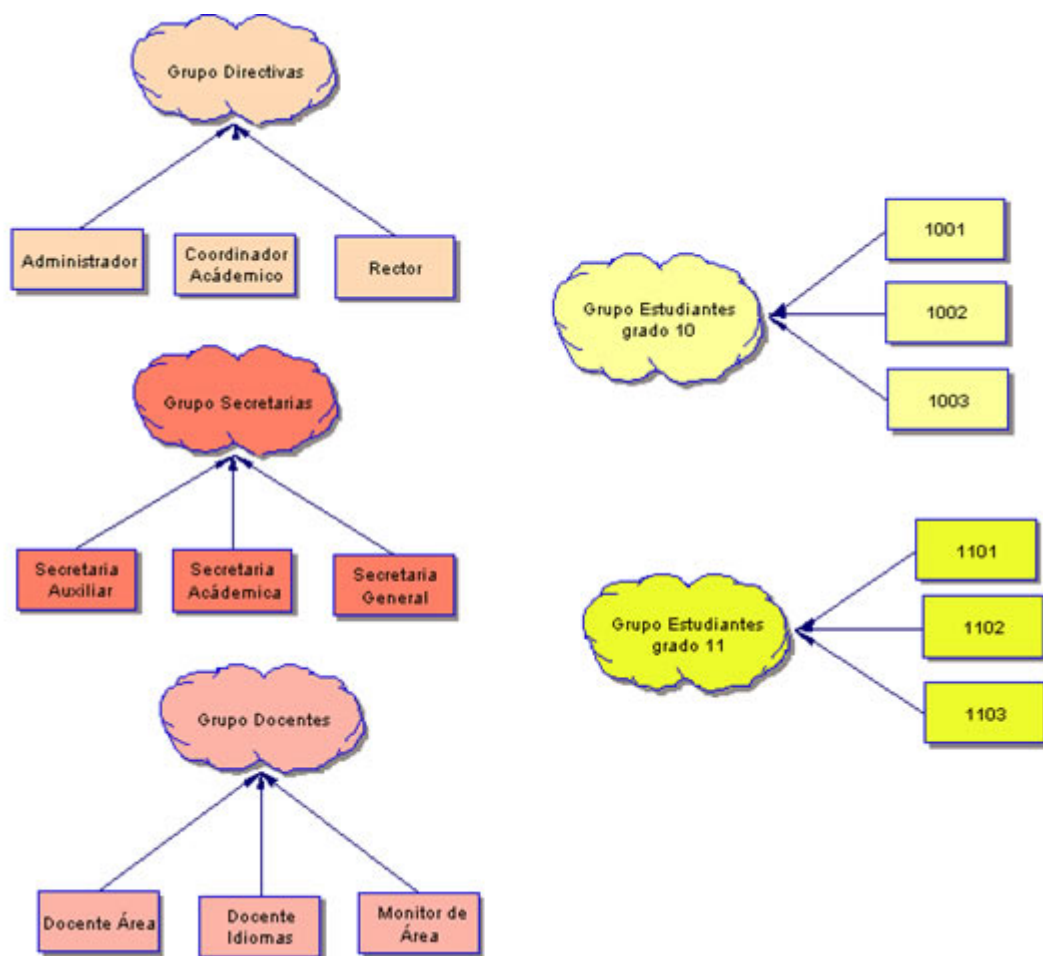


Ejemplo de la estructura de carpetas configuradas en un servidor administrativo.



Ejemplo de la estructura de carpetas configuradas en un servidor de estudiantes.

Usuarios y grupos de trabajo. Hace referencia a la definición de las personas que ingresan a la red para usar datos y dispositivos compartidos y también, a los grupos de trabajo a los que ellas pertenecen. Un ejemplo de usuario sería: el rector, el coordinador académico, la secretaria académica, el docente de matemáticas y los estudiantes, estos últimos considerados individualmente. Los grupos de trabajo se conforman por usuarios que tienen algo en común; Ej: estudiantes del mismo grado, directivos ó docentes que participen en el mismo proyecto pedagógico, etc.



Cada uno de los usuario anteriores debe tener las restricciones que el administrador de la red considere necesarias o apropiadas. Ej: para evitar que los usuarios almacenen demasiada información, se puede limitar la capacidad en MB que se les asigna. En el caso de los estudiantes, esta se puede restringir además para ciertos tipos de archivos tales como videos ó archivos MP3.

Políticas de seguridad. Se refiere a los permisos especiales a usuarios y a grupos de usuarios para el uso de dispositivos compartidos y para el acceso y manejo de la información almacenada en la red.

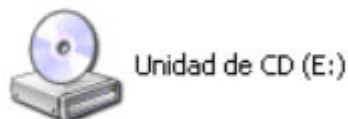
Al momento de diseñar las políticas de seguridad, se debe tener en cuenta cuáles son los permisos y restricciones requeridos por los usuarios para manejar tanto datos compartidos como el software (programas) con los que cuenta la IE. Ej: No permitir a los usuarios instalar o desinstalar programas en los computadores.

En las estaciones de trabajo, se debe estandarizar: el escritorio (fondo de pantalla, íconos de acceso, tamaño y fuente de letra, resolución de pantalla, salva pantallas, etc.); las unidades de almacenamiento que se les asignan (ver imagen) y los dispositivos compartidos como las impresoras.

Unidades de disco duro



Dispositivos con almacenamiento extraíble



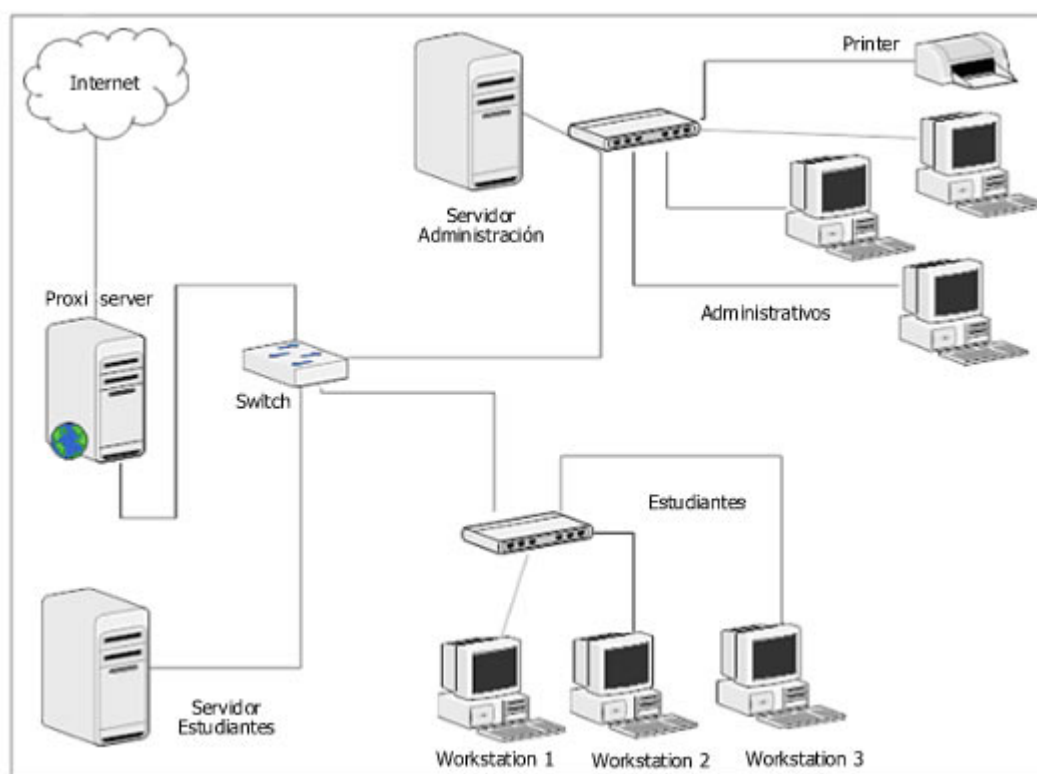
Unidades de red



Todas las políticas de seguridad deben apuntar a un diseño de red para uso exclusivamente académico y no público, situación esta última en la que los usuarios puedan realizar cualquier tipo de trabajo o consulta.

Internet. Es no solo deseable sino necesario que el acceso a Internet se realice mediante un servidor diferente al de *datos*. Un Servidor de Internet, con antivirus actualizado, ofrece mayor seguridad a la red, porque crea una barrera contra virus, spywares y adwares que pueden entrar por su conducto y además, permite restringir el acceso de los usuarios a sitios improcedentes de la Web.

A continuación se propone el diagrama de una red compuesta por 3 servidores con los puntos a tener en cuenta en ese tipo de diseño:



RECOMENDACIONES GENERALES:

- Instalar en la red escolar de datos dos servidores interconectados: uno para *Estudiantes* y otro para personal *Administrativo*, en este último se deben incluir directivos y docentes.
- Restringir por completo el acceso de los estudiantes al servidor *Administrativo*.

- Habilitar el ingreso a los usuarios del servidor *Administrativo* desde las salas de informática que utilizan los estudiantes.
- Instalar un Software administrador de acceso a Internet como *firewall* para toda la red.
- Controlar tanto el acceso de los estudiantes a servicios públicos de Chat, como a la instalación de aplicaciones que manejen el protocolo P2P.
- Instalar en el servidor dedicado a Internet dos tarjetas de red: Una para el acceso a Internet y otra para la red LAN.
- Controlar, si es necesario y estableciendo límites de tiempo (horarios), el acceso a Internet de los usuarios. Ej: conexión a Internet de 7:00am a 5:00pm.
- Asignar a los usuarios administrativos un espacio de almacenamiento en el servidor. Ej: 10 MB para cada uno.
- Crear una carpeta pública (común), en el dominio *Administrativo*, que permita total acceso a todos los usuarios.
- Crear una relación de *confianza* de una vía entre los dos dominios para que desde el dominio *Administrativo* se pueda ingresar al dominio *Estudiantes*.

POLÍTICAS PARA ESTUDIANTES:

- Restringir a los usuarios la administración local de las estaciones, esto significa que no pueden manipular la configuración de la máquina.
- En caso de tener dudas sobre la efectividad del antivirus, deshabilitar los puertos USB para evitar la transferencia de virus y solo dejar activos los que el docente

de informática pueda controlar.

- Tener una interfaz única en las estaciones que incluya un fondo de pantalla institucional diseñado por la IE.
- Configurar el navegador de Internet para que siempre inicie en una página Web definida.
- Programar el apagado automático de las estaciones de trabajo (computadores).
- Si está utilizando Windows, deshabilitar en las estaciones el icono “Entorno de Red”.
- Establecer para los usuarios, cuando ingresen a la red, la conexión automática de sus unidades de red.
- Restringir a los usuarios la instalación y desinstalación de programas a no ser que tengan previa autorización escrita.
- Restringir que los usuarios puedan compartir entre ellos carpetas locales.
- Limitar a los estudiantes el espacio de almacenamiento en el servidor. Por ejemplo, almacenamiento de solo 6 MB y controlar, de acuerdo con la extensión de los archivos, los tipos de información que ellos pueden guardar.
- Crear en el servidor de Estudiantes una carpeta Publica (común) con capacidad restringida de almacenamiento que permita acceso total a los usuarios.

POLÍTICAS PARA USUARIOS ADMINISTRATIVOS

- Definir para los usuarios administrativos un fondo de pantalla institucional, único.

- Resulta útil estandarizar el nombre de los usuarios: código ó iniciales de nombre y apellido de cada uno (Ej: jualop para Juan López).
- Renombrar las cuentas de administrador de red y las contraseñas de Administración local en las estaciones para evitar propagación de virus y mejorar la seguridad de la información almacenada en la red.
- Crear una cuenta con derechos para administración de usuarios, impresoras, creación de cuentas de máquina, permisos de carpetas, etc, diferente a la cuenta del administrador de red.
- Crear un archivo de inicio de red para los usuarios en donde se identifiquen las unidades de la siguiente manera :

En el caso de estudiantes: T:> Para acceso a TEMPORAL S:> Para acceso a Carpeta Personal

En el caso de directivos y docentes: T:> Para acceso a TEMPORAL H:> Para acceso a Carpeta Personal X:> Para acceso a los DATOS del servidor estudiantes

ACCESO A INTERNET

- Configurar el servidor para permitir el acceso a usuarios individuales o a grupos de usuarios.
- Para mejorar el control y poder monitorear el acceso a Internet, configurar todos los registros de entrada a Internet y guardarlos durante un período de tiempo dado como política que establece el administrador de la red o la IE.

- Crear políticas que permitan el acceso, sin restricción, a grupos de usuarios que así lo requieran.
- Restringir el acceso a páginas Web que no ofrezcan ningún beneficio académico.
- Instalar un Antivirus/Antispyware/Antiadware centralizado (en el servidor) y mantenerlos actualizados.
- Establecer una política de seguridad que estipule la periodicidad para realizar la copia de seguridad (backup) de todos los datos almacenados en la red.

CRÉDITOS:

Artículo elaborado por EDUTEKA.

*Publicación de este documento en EDUTEKA: Marzo 01 de 2008.

Última modificación de este documento: Marzo 01 de 2008.*