UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

METODOLOGÍA PARA LA CREACIÓN Y ADMINISTRACIÓN DE CENTROS DE CÓMPUTO EDUCATIVOS

TESIS PROFESIONAL

PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

FRANCISCO JAVIER PEÑA GRANADOS
ERIC ROMERO MARTÍNEZ

DIRECTOR DE TESIS
ING. CARLOS ALBERTO ROMÁN ZAMITIZ

CUIDAD UNIVERSITARIA
MÉXICO, D.F. 2010

FRANCISCO JAVIER PEÑA GRANADOS
ERIC ROMERO MARTÍNEZ

METODOLOGÍA PARA LA CREACIÓN Y ADMINISTRACIÓN DE CENTROS DE CÓMPUTO EDUCATIVOS

2010

Agradecimientos

Un agradecimiento a aquellas personas sin cuya participación no existiría este trabajo de tesis:

- Al Ing. Carlos Alberto Román Zamitiz por aceptar el dirigir la tesis y orientación durante el desarrollo de la misma.

FRANCISCO JAVIER PEÑA GRANADOS

Agradecimientos

Este trabajo es un escalón más que debo subir en este largo camino llamado *vida*, y estoy enormemente agradecido con todas aquellas personas que me han acompañado a lo largo de estos 27 años y que de alguna forma me han extendido la mano para ayudarme a seguir ascendiendo más y más.

Agradezco principalmente a mis padres Adolfo y Conchita, no solo por haberme dado el regalo de la vida, también porque son las personas que me han acompañado en todo momento de mi vida y con su gran apoyo, cariño y comprensión me han enseñado cosas invaluables que la escuela nunca me hubiera podido enseñar, a estas maravillosas personas que se han sacrificado día a día para darme cariño, salud, alimentación, techo, ropa y educación. Por enseñarme a respetar a los animales y a la naturaleza, y por enseñarme el gran valor de la humildad.

Agradezco a Martha, por estar conmigo en los momentos más difíciles y complicados que he tenido, por cada beso, abrazo y palabra de aliento que me han ayudado a comprender las cosas, por enseñarme a verme a mí mismo, a ver y corregir mis errores, por inspirarme y orientarme a ser una mejor persona en la vida, por el amor y comprensión que me ha brindado.

Agradezco a mis hermanos Edgar y Evelín, porque son una gran compañía, con ellos he podido llorar, reír, correr, jugar… compartir.

Agradezco a mis amigos y colegas Alex y Wences, quienes me enseñaron a disfrutar la vida en otro entorno, a conocer lugares, tener aventuras únicas en mi vida, enseñarme a ver lo bello de la tierra y la gente, a ver paisajes inolvidables. Pero también me enseñaron a ser ambicioso, a no conformarme con lo que tengo, a seguir luchando por todo aquello que deseo. Personas en las cuáles confío plenamente y sé que nunca me darán la espalda.

A mis sobrinas Celes y Cris, que cada día me enseñan que la sonrisa de un niño es lo más hermoso que cualquier ser humano puede ver y escuchar.

Agradezco a mi amigo Javier, no solo por ser un gran amigo, también por ser un excelente compañero de trabajo, de muy alto nivel profesional, y con la única persona que realmente he podido trabajar como equipo y con quien estoy sumamente orgulloso de presentar este trabajo que realizamos con tanto esfuerzo y dedicación.

Agradezco a todas aquellas personas que conforman mi entorno y que por motivos de límite de espacio, no pude mencionar de forma particular, pero que aún así, forman una parte muy importante en mi vida.

ERIC ROMERO MARTÍNEZ

Índice

INTRODUCCIÓN

La tesis tiene como propósito el ayudar a los administradores o futuros administradores a administrar o crear un nuevo centro de cómputo respectivamente. Debido a que las sedes educativas normalmente carecen de recursos, se propone hacerlo con software libre lo cual reduce los costos de licencias en lo posible.

La tesis es una propuesta **propia** la cual no intenta de ninguna forma ser una guía, o que la metodología deba seguirse al pie de la letra, intenta dar una guía segmentada con lo cual pueda solo usar la sección o capitulo que le interese. Seleccionamos los temas a desarrollar con el fin de tener una visión general para la administración de un centro de cómputo sin profundizar demasiado en cada uno de ellos, ya que cada uno de los temas puede ser una tesis por separado.

Tanto la metodología, aplicaciones y forma de administrar en una visión propia tratando de omitir en lo posible los procesos administrativos rigurosos que normalmente (nuevamente es nuestra opinión) es lo que hace claudicar a la mayoría de las personas al tener que hacer las cosas de una forma tan rígida. Esto no implica de ninguna forma que la metodología estándar esté incorrecta o tomemos una posición en contra, solo tratamos de hacer la administración más sencilla para que cualquier persona pueda llevarla a cabo en sus actividades diarias.

Este documento está dirigido a personas que inician o tienen conocimientos medios, siendo posible también funcionar como una guía rápida para los administradores con grandes conocimientos y experiencia.

En el capítulo 1, *Conocimientos básicos*, definimos centro de cómputo y se brinda una pequeña introducción a temas que se trataran más a detalle en el desarrollo de la tesis.

El capítulo 2, *Análisis de las necesidades específicas de un centro de cómputo educativo: limitantes, ¿qué se necesita? y ¿por qué se necesita?,* se delinean las necesidades que puede presentar un centro de cómputo dando respuesta a preguntas como: ¿Por qué construirlo?, ¿Quién o quiénes van a operar el centro de cómputo? Y ¿Cómo va a operar el centro de cómputo?

El capítulo 3, *Análisis de los Sistemas operativos*, ayuda a la selección del sistema operativo de equipos clientes y servidores de acuerdo a las necesidades de los usuarios.

El capítulo 4, *Administración de recursos y software a utilizar*, da un panorama del software que será necesario de acuerdo a las necesidades de los usuarios, además se presentan opciones del dicho software (con licencia y gratuito).

El capítulo 5, *Análisis y recomendaciones de cableado estructurado o uso de tecnología Wireless*, describe los componentes, estándares e instalación correcta de una red alámbrica e inalámbrica.

El capítulo 6, *Seguridad informática*, define las directrices sobre las que vamos a basar la seguridad informática (confidencialidad, integridad, disponibilidad y autenticación), nos ayuda a definir claramente ¿Qué debemos proteger?, ¿De quién protegernos?, ¿Con qué y cómo nos protegemos?

El capítulo 7, *Sistemas de respaldo*, explica cómo debe proteger el equipo de fallos de corriente y la forma correcta de realizar respaldo de datos.

El capítulo 8, *Selección de equipos,* brinda una explicación de los principales componentes de una computadora y en general del equipo (el más típico) que será necesario en el centro de cómputo.

El capítulo 9, *Malware y antivirus,* describe el principal malware que afecta a los equipos, se hacen recomendaciones para evitar la infección y propagación de malware en los equipos y se explica la importancia del antivirus en los equipos.

El capítulo 10, *Instalación de un equipo servidor,* describe los pasos para la instalación del software necesario para un equipo servidor.

El capítulo 11, *Políticas de un centro de cómputo,* propone lineamiento generales y ejemplos para la creación de políticas propias.

El capítulo 12, *Sistema administrativo de recursos y estadísticas,* se propone un sistema que facilite la administración de tareas y recursos de un centro de cómputo educativo.

Capítulo 1 – Conocimientos Básicos

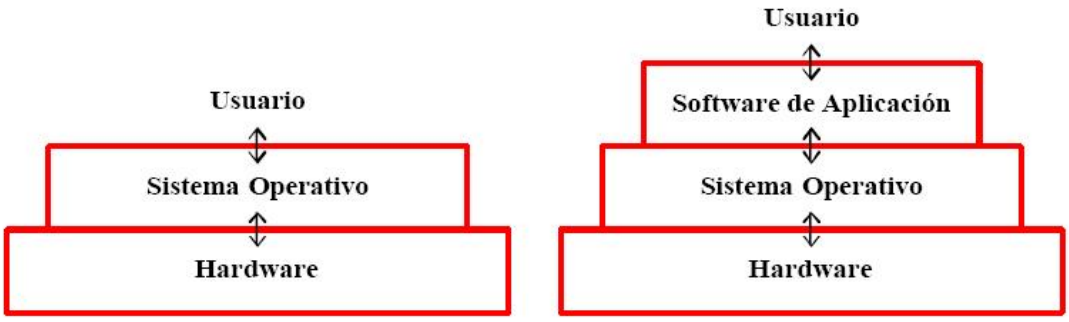
Definición de Centro de cómputo

Un centro de cómputo (hablando dentro del ámbito educativo) es aquel espacio donde se brinda el servicio de cómputo, tal y como puede ser el préstamo de un equipo de cómputo (computadora, escáner, proyector, micrófono, etc.), asesoría técnica, servicio de impresiones, etc.

Sistemas operativos: Linux y Windows

El sistema operativo es un conjunto de instrucciones que hacen uso de los recursos de la computadora para ayudar al usuario a realizar tareas específicas.

Dependiendo de la forma y el nivel de empleo de los recursos, el usuario puede trabajar directamente con el sistema operativo para comunicarse con la computadora, o puede recurrir al Software de Aplicación.



GNU/Linux

GNU/Linux fue creado originalmente por Linus Torvald en la Universidad de Helsinki en Finlandia, siendo él estudiante de informática. Linus inicio el desarrollo implementando una versión de UNIX llamada Minix, un pequeño sistema Unix desarrollado por Andy Tannenbaum. Aquella era una versión muy reducida que ha ido creciendo con los años gracias a las aportaciones de numerosos equipos de programadores. El 5 de octubre de 1991, Linus anuncio su primera versión "oficial" de Linux, versión 0.02.

Linux es un sistema operativo libre (Open Source), esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, Linux se distribuye bajo la GNU Public License: por lo tanto, el código fuente tiene que estar siempre accesible, sin embargo, hacer funcionar un sistema a partir del código fuente es bastante difícil, por lo que normalmente, Linux se distribuye en un formato binario, es decir, ya compilado. Poco

después de que apareciera el kernel Linux, comenzaron a aparecer las primeras distribuciones, que agrupaban versiones probadas de varios programas, junto con el kernel, de tal manera que formaban un sistema operativo listo para usar.

A medida que fue pasando el tiempo, algunas distribuciones se fueron haciendo más sofisticadas, otras desaparecieron, otras se hicieron comerciales y aparecieron mucha más. Existen distribuciones de muchos tipos: distribuciones que ocupan 1 diskette y distribuciones que llegan a ocupar 10 CDs; distribuciones orientadas a una finalidad en especial (redes, seguridad, etc.) y distribuciones de uso general.

Características de Linux

- Multiusuario.- Varios usuarios pueden acceder a las aplicaciones y recursos del sistema al mismo tiempo. Y, por supuesto, cada uno de ellos puede ejecutar múltiples tareas (multitareas).

- Multitarea.- Es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación. Permite alternar el uso del procesador (normalmente solo uno, aunque hoy día con varios núcleos) entre varios programas, de esta manera aunque solo se esté ejecutando un programa a la vez, da la impresión de que todos se ejecutan simultáneamente. Cuando se tienen procesadores con varios núcleos (p.e. Intel Core 2 Duo) realmente se pueden procesar dos programas a la vez.

- Shells programables

- Memoria virtual

- Acceso transparente a particiones MS-DOS (o a particiones OS/2 FAT).

Microsoft Windows

Microsoft Corporation empresa creadora de Windows fue fundada en 1975 por William H. Gates III y Paul Allen, estos primero desarrollaron MS-DOS y en 1985 lanzaron su primera versión de Windows con una interfaz gráfica (GUI) para MS-DOS el cual habían incluido en las computadoras de IBM desde 1981. De 1987 (fecha de lanzamiento de Windows 2.0) a finales de 1990 Microsoft trabajo conjuntamente con IBM para el desarrollo de Sistemas operativos. En 1990 Microsoft lanzó una nueva versión de su sistema operativo Windows 3.0 versión que fue muy popular debido a las capacidades gráficas de la PC de la época. Le siguieron Windows 3.1 y 3.11 los cuales tenían un

soporte multimedia y protocolos mejorados para las comunicaciones de red y soporte para redes punto-punto (peer-to-peer).

Después continuaron Windows NT, Windows NT 3.1, Windows NT 3.5/3.5.1, Windows NT 4.0, Windows 95, Windows 98, Windows Millenium, Windows 2000, Windows XP, Windows Vista y finalmente Windows 7 (hasta el día de hoy, abril de 2010).

Lenguajes de Programación

Un lenguaje de programación es un lenguaje artificial que puede utilizarse para definir una secuencia de instrucciones para su procesamiento por una computadora.

Lenguajes de bajo nivel.- denominado código máquina ya que es una colección muy detallada de crípticas que controlan la circuitería interna de la máquina. Éste es el dialecto natural de la computadora. Este tipo de lenguajes son específicos de cada procesador por lo que no puede ser ejecutado en otro tipo de procesador sin modificaciones importantes.

Lenguajes de alto nivel.- Se compone de instrucciones que son más compatibles con los lenguajes y la forma de pensar humanos.

Shell

El intérprete de comandos o "Shell" de UNIX es también un lenguaje de programación completo. La programación de Shell se usa mucho para realizar tareas repetidas con frecuencia. Los diseñadores de sistemas suelen escribir aplicaciones en el lenguaje de base del sistema operativo, C en el caso de UNIX, por razones de rapidez y eficiencia. Sin embargo, el Shell de UNIX tiene un excelente rendimiento en la ejecución de "scripts"; ésta es la denominación aplicada a los programas escritos en el lenguaje del Shell.

Los shells usados habitualmente son:

- sh.- Fue escrito por Steven Bourne, y es por eso que se lo suele llamar Bourne Shell. Está disponible en todas las versiones de UNIX y es lo suficientemente básico como para que funcione en todas las plataformas.

  El bourne Shell tiene las siguientes características:

  - Control de procesos.
  - Variables.
  - Expresiones regulares.

- Control de flujo.
- Control de entrada/salida.
- Soporte a funciones.

Algunos problemas que presenta son:

- No existe soporte a autocompletado de nombres de archivos.
- No existe historial de comandos ni de edición en línea.
- Dificultad para ejecutar múltiples procesos en segundo plano (background).

- bash (bourne again shell).- fue desarrollado por Brian Fox como parte del proyecto GNU y ha reemplazado el bourne Shell, en los sistemas basados en GNU. Prácticamente todas las distribuciones de Linux utilizan bash como su reemplazo de sh.

  Algunas características son:

  - Acceso al historial de comandos ejecutados.
  - Autocompletado de nombres de comando y archivos automáticamente, al presionar la tecla TAB.
  - Soporta arreglos (arrays) de tamaño ilimitado.
  - Aritmética de enteros en cualquier base numérica (entre 2 y 64).

- csh.- Fue escrito por Bill Joy y debe su nombre al lenguaje de programación C. Al hacer scripts en este Shell puede utilizarse una sintaxis similar a la de C.

- ksh.- Está basado en sh, con algunos agregados muy básicos para hacerlo más amigable.

MS-DOS

En 1980 IBM contrató a Microsoft para escribir el sistema operativo del IBM PC, que saldría al mercado al año siguiente. Presionada por el poco tiempo disponible, Microsoft compró QDOS (Quick and Dirty Operating System) a Tim Paterson, un programador de Seattle, por 50.000 dólares y le cambió el nombre a MS-DOS. El contrato firmado con IBM permitía a Microsoft vender este sistema

operativo a otras compañías. En 1984 Microsoft había otorgado licencias de MS-DOS a 200 fabricantes de equipos informáticos y, así, este sistema operativo se convirtió en el más utilizado para PC.

Java - Sun Microsystems

El lenguaje Java fue desarrollado por Sun Microsystems en 1991. Nace como parte de un proyecto de investigación para desarrollar software para comunicación entre aparatos electrónicos de consumo como videos, televisores, equipos de música, etc. Durante la fase de investigación surgió un problema que dificultaba enormemente el proyecto iniciado: cada aparato tenía un microprocesador diferente y muy poco espacio de memoria; esto provoco un cambio en el rumbo de la investigación que desemboco en la idea de escribir un nuevo lenguaje de programación independiente del dispositivo que fue bautizado inicialmente como Oak.

La explosión de Internet en 1994 gracias al navegador grafico Mosaic para la Word Wide Web (WWW), no paso desapercibida por el grupo investigador de Sun. Se dieron cuenta de que los logros alcanzados con el proyecto eran perfectamente aplicables a Internet. Básicamente Internet es una red que conecta múltiples computadoras con diferentes sistemas operativos y diferentes arquitecturas de microprocesadores, pero todos tienen en común un navegador que utilizan para comunicarse entre sí. Esta idea hizo que el grupo investigador abandonara el proyecto de desarrollar un lenguaje que permitiera la comunicación entre aparatos y dirigiera sus investigaciones hacia el desarrollo de un lenguaje que permitiera crear aplicaciones que se ejecutaran en cualquier ordenador de Internet con el único soporte de un navegador.

A partir de aquí de empezó a hablar de Java y de sus aplicaciones conocidas como Applets. Un Applet es un programa escrito en Java que se ejecuta en el contexto de una página Web en cualquier computadora, independientemente de su sistema operativo y de la arquitectura de su procesador. Para ejecutar el Applet solo es necesario un navegador que soporte la maquina virtual de Java.

Existen dos principales ambientes:

- Java 2 Software Development Kit (J2SDK) .- Contiene las clases básicas, clases para interfaz grafica, colecciones avanzadas y lo necesario para desarrollar aplicaciones Java (javac que es el compilador de Java)

- Java Runtime Enviroment (JRE).- Provee el intérprete de Java, el cual te permite ejecutar aplicaciones Java.

Las principales características de Java son:

- Simple.- Ofrece toda la funcionalidad de un lenguaje potente, pero sin las características menos usadas y confusas de éstos.

- Orientado a Objetos.- Trabaja con sus datos como objetos y con interfaces a esos objetos. Soporta tres características propias del paradigma de la orientación a objetos: encapsulación, herencia y polimorfismo.

- Distribuido.- Tiene extensas capacidades de interconexión, esto permite acceder a la información a través de la red con mucha facilidad. Java en sí no es distribuido, sino que proporciona librerías y herramientas para que los programas puedan ser distribuidos.

- Seguro.- El código pasa por muchas comprobaciones antes de ejecutarse en una maquina, pasa por un verificador de ByteCode (archivo .class) que lo comprueba; el cargador de clases mantiene la seguridad separando el espacio de nombres del sistema de archivos locales de los recursos procedentes de la red.

- Portable.- Debido a que la ejecución de la aplicación se lleva a cabo en una maquina virtual se puede ejecutar en cualquier computadora que tenga esta máquina virtual.

- Multitarea.- Permite realizar muchas actividades simultáneas en un programa.

Bases de datos

Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su uso posterior. Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

Modelos de bases de datos

Un modelo es básicamente una descripción del contenedor de datos, así como el método de almacenar y recuperar información. Los modelos de datos no son cosas físicas: son abstracciones que permiten la implementación de un sistema eficiente de base de datos; por lo general se refieren a algoritmos y conceptos matemáticos.

Algunos modelos son (solo se mencionaran algunas):

- Base de datos relacional (comúnmente la más utilizada).- Su idea fundamental es el uso de "relaciones", las cuales pueden considerarse en forma lógica como conjuntos llamados tuplas. Cada relación de la tabla está compuesta por registros (filas de una tabla), que representan las tuplas y los campos columnas de la tabla.

  En este modelo la forma y lugar donde se almacenan los datos no tiene relevancia, lo que facilita el entender y utilizar este modelo. La información puede recuperarse e insertarse

mediante “consultas” lo que ofrece una amplia flexibilidad para administrar la información. Estas “consultas” se llevan a cabo con SQL (Structured Query Language o Lenguaje Estructurado de Consultas) el cual es un lenguaje estándar en los principales motores y sistemas de gestión de este tipo de modelos.

- Base de datos jerárquica.- La información esta almacenada de forma jerárquica, está organizada como en forma de árbol invertido y los nodos padres puede tener varios hijos, no así los nodos hijos, los cuales no pueden tener varios padres. Como en cualquier árbol el nodo que no tiene padre se le llama raíz y el nodo que no tiene hijos hoja.

  Son útiles cuando se tiene gran cantidad de información y esta es muy compartida, sin embargo es poco eficiente en cuanto a la información redundante.

- Base de datos de red.- Es similar a la base jerárquica (mencionada anteriormente), la diferencia fundamental es que los nodos pueden tener varios padres, lo que soluciona el problema de redundancia que presenta el modelo jerárquico. Sin embargo presenta muchos problemas al administrar la información lo que ocasiona que no sea muy usada.

- Bases de datos orientadas a objetos.- Es un modelo reciente el cual permite almacenar en la base objetos completos (estado y comportamiento). Este modelo soporta encapsulación, herencia y polimorfismo.

Ventajas del uso de bases de datos

Globalización de la información.- La misma información es utilizada por todos los usuarios de la base, de esta manera al realizar un usuario alguna modificación en la información todos tendrán acceso a ésta.

Eliminación de información inconsistente.- Debido a que al diseñar la base de datos debe cuidarse este aspecto en un buen diseño no se tendrá información la cual no tenga sentido de acuerdo a las necesidades de la empresa. P.e. podemos tener un campo en la base de datos de edad en la cual se especifique que debe ser un entero y no la edad con letras o un número negativo (nótese que el ejemplo es solo demostrativo, ya que para una necesidad así es mejor tener la fecha de nacimiento, ya que de esta forma se sabrá la edad de las personas en cualquier año).

Servidores de Bases de Datos (Sistema de gestión de base de datos)

Los Sistemas de Gestión de bases de datos es un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. Debe permitir crear y mantener una Base de Datos, asegurando su integridad, confidencialidad y seguridad. Ejemplos de sistemas manejadores de Bases de Datos son:

- Access.- Programado por Microsoft.
- MySQL.- Base de datos con licencia GPL.
- SQL Server.
- PostgreSQL (manejador que se usara en la aplicación demo).

Arquitectura cliente-servidor

Puede definirse a ésta arquitectura como:

> "Sistema distribuido donde hay clientes que solicitan servicios y servidores que los proporcionan."

Aunque la arquitectura puede verse en sola computadora donde esta ofrezca un servicio y la misma máquina lo solicite (imaginemos un gestor de bases de datos instalado en una maquina sin conexión de red, la misma computadora puede acceder al gestor, convirtiéndose así la misma computadora en cliente y servidor). Esta arquitectura es más ventajosa en un ambiente de red, donde una computadora denominada servidor ofrece algún servicio y otra computadora el cliente los solicita.

Características del cliente

- El inicia la comunicación haciendo peticiones y espera hasta tener respuestas.

Características del servidor

- Normalmente es una computadora con muchos recursos.
- No interactúa con los usuarios finales.
- Tiene una interfaz única y definida.
- Sus cambios no afectan al cliente.

Ventajas de la arquitectura

- Recursos centralizados.- Debido a que el servidor contiene toda la información.
- Mejor seguridad.- Ya que solo debe cuidarse el servidor, los puntos de entrada del sistema se reducen.

Cableado estructurado y Wireless

Hoy en día, el avance tecnológico avanza con más rapidez en todo instante, es por ello que distintas entidades, tanto lucrativas como no lucrativas, se ven en la necesidad de comunicarse a gran distancia y de diversas formas, algo muy importante es la velocidad con la que se hace la comunicación y la disponibilidad que se tienen a ella. Para ello se cuenta con un sistema de cableado estructurado.

Implementar sistemas de cableado estructurado en las organizaciones lucrativas genera mayor producción, pero en instituciones educativas ayudan al desarrollo profesional, no solo como una herramienta más para realizar tareas o investigaciones, sino que gracias a los avances tecnológicos en las telecomunicaciones, se cuenta con la educación a distancia, con la cual se puede preparar profesionalmente a un estudiante sin importar donde se encuentre y también se puede realizar la difusión de la cultura.

¿Qué es un cableado estructurado?

Un cableado estructurado es aquella infraestructura de medios físicos que proporcionan la comunicación en áreas limitadas, está integrada por dispositivos pasivos que cumplen con ciertas características.

Para llevar a cabo la ardua tarea de crear un sistema de cableado estructurado es necesario seguir una serie de normas y estándares, tanto locales del lugar donde se instalará dicho cableado así como internacionales.

Las normas del cableado estructurado son aquellas reglas escritas que estamos obligados a seguir si es que deseamos tener un sistema de este tipo.

Los estándares son documentos que nos proporcionan consejos o sugerencias a seguir para homogeneizar criterios de comparación en la industria y establecer parámetros comunes de desempeño, calidad y seguridad para los productos y servicios en los diferentes mercados y ramas industriales. No estamos obligados a acatarlos, pero es una buena práctica.

Al establecerse marcos legales de soporte se convierten en referencias obligadas o recomendatorias sobre las cuales cada fabricante se debe apegar en la fabricación de sus productos, así como en las prácticas de instalación y puesta en marcha.

Para los sistemas de cableado estructurado se utilizan medios como son los cables de cobre y de fibra óptica, en sus distintas modalidades dependiendo el área al cual se van a aplicar.

Algunas veces se opta por usar redes inalámbricas en lugar de usar un sistema de cableado, esto puede ser debido a: que el usuario de la red no tiene a su disposición un medio físico para conectarse; el usuario requiere de frecuente movilidad; que el área de trabajo no sea apta para instalar un sistema de cableado o bien por simple comodidad.

Una conexión de red inalámbrica nos ofrece:

- Movilidad: nos permite una conexión sin importar el lugar donde nos encontremos (siempre y cuando estemos dentro del alcance de la señal) e incluso en movimiento (puede depender del dispositivo de conexión de cada usuario).
- Identidad: el diseño de la red no está basada en puertos de red, si no que estaría basado en la identidad del usuario y/o del equipo.
- Fácil y rápida instalación.
- Gran facilidad de mantenimiento y crecimiento de la red.
- En algunos casos, el costo se podría ver reducido en vez de hacer una instalación de cableado estructurado.

En el año 1997, la IEEE (The Institute of Electrical and Electronics Engineers, El Instituto de Ingenieros Eléctricos y Electrónicos) publicó el estándar para las redes inalámbricas, el estándar 802.11. Este estándar (mejor conocido como Wi-Fi) fue diseñado para soportar 2 Mbps de ancho de banda y trabajó en la banda de los 2.4 GHz. Hoy en día se han derivado mayores características que satisfacen distintas necesidades de conexiones wireless.

El usar tecnología inalámbrica pone en riesgo la red ante ataques de intercepción de datos, intrusión de la red, interferencias y ataques de denegación de servicios. (Detalles en el capítulo 5).

Clasificación de redes de acuerdo a la cobertura

Según su cobertura, se pueden clasificar en diferentes tipos:

- WPAN (Wireless Personal Area Network).- En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth (protocolo que sigue la especificación IEEE 802.15.1) y ZigBee (basado en la especificación IEEE 802.15.4, que

requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo); RFID, sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

- WLAN (Wireless Local Area Network).- En las redes de área local podemos encontrar tecnologías inalámbricas basadas en HiperLAN (del inglés, High Performance Radio LAN), un estándar del grupo ETSI, o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.

- WMAN (Wireless Metropolitan Area Network, Wireless MAN).- Para redes de área metropolitana se encuentran tecnologías basadas en WiMax (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMax es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service).

- WWAN (Wireless Wide Area Network, Wireless WAN).- En estas redes encontramos tecnologías como UMTS (Universal Mobile Telecommunications System), utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología GSM (para móviles 2G), o también la tecnología digital para móviles GPRS (General Packet Radio Service).

Bibliografía

Introducción a los sistemas operativos. Deitel, H.M. Addison Wesley Iberoamericana, 2000.

Teoría de autómatas y lenguajes formales. Kelley, Dean. Prentice-Hall, 1195.

Fundamentos de sistemas de Bases de Datos. Elmasri Ramaez A., Navathe Shamkant B. Pearson Prentice Hall, 2003.

Capítulo 2 - Análisis de las necesidades específicas de un centro de cómputo educativo

Para poder saber las necesidades de un centro de cómputo (cualquiera, no solo sesgado al centro de cómputo educativo) debe tenerse como primer punto la función del centro y los servicios que se quieren prestar. Para este caso específico (centro de cómputo educativo) partiremos de nuestra definición:

> "Un centro de cómputo (hablando dentro del ámbito educativo) es aquel espacio donde se brinda el servicio de cómputo, tal y como puede ser el préstamo de un equipo de cómputo (computadora, escáner, proyector, micrófono, etc.), asesoría técnica, servicio de impresiones, etc."

Nótese que se quiere prestar computadoras, equipo (escáner, proyector, etc. esto variará de acuerdo a los recursos con los que se cuenten o los que se quiera invertir en el caso de estar creando un centro), dar asesoría técnica, servicios de impresión y algunos otros servicios. Al reestructurar y al crear un centro es recomendable dejar abiertas las funciones de nuestro centro de cómputo ya que podríamos omitir detalles importantes. En este caso la definición ha quedado abierta a propósito con el fin de que englobe el mayor número de casos.

Teniendo listados los servicios y funciones del centro, pasamos en forma a la planeación en la cual se tendrán que responder preguntas como: ¿Qué?, ¿Quién?, ¿Dónde?, ¿Cuándo? ¿Cómo? y ¿Por qué?

- El ¿Por qué construirlo? podría corresponder a una "planeación estratégica" ya que identificaríamos sistemáticamente las oportunidades y riesgos que surgirán en el futuro. Con el listado hecho anteriormente es muy sencillo responder la pregunta ¿Por qué?, lo complicado radica en localizar los puntos de riesgo, por ejemplo: necesitamos servicio de impresión, ¿Contamos o contaremos con los recursos (económicos y/o materiales) para atender a toda aquella persona que requiera del servicio?, ¿El personal que dará la asesoría técnica estará en constante capacitación a fin de poder prestar un servicio adecuado?

  Hacer lo anterior no implica adivinar el futuro o tomar decisiones futuras, sólo pretende seleccionar entre posibles sucesos futuros.

- ¿Quién o quiénes van a operar el centro de cómputo? Una planeación de personal es necesaria para saber cuántas personas serán necesarias que laboren y cuáles serán sus funciones.

Aquí debe considerarse personal para cubrir las funciones de administradores, préstamo de los equipos, asesoría técnica, etc. Debe considerarse personal para cubrir todos los servicios que se pretenda brindar. Debe notarse que una sola persona puede realizar varias funciones, sin embargo, es necesario que esté muy claro que hará cada persona tanto para el buen funcionamiento del centro, como para tener el personal que cumpla el perfil y nivel de conocimientos que se requerirán para ocupar el puesto.

- ¿Cómo va a operar el centro de cómputo? (planeación operativa). Qué software y hardware requerirá el centro de acuerdo a los servicios e igual de importante en esta sección es considerar los usuarios, su nivel de conocimientos, necesidades específicas que puedan presentar y qué operaciones les será permitido realizar.

Hardware

Para hacer la petición de compra de equipos (en caso de crear un centro) o bien en hacer una buena distribución (en caso hacer una reestructuración) primero debe considerarse que los equipos con más recursos (procesador, disco duro y memoria RAM) y/o servidor se destinen a aquellas computadoras que prestarán un servicio a los usuarios, ya sea servidor NAT (Network Address Translation - Traducción de Dirección de Red), servidor Web, servidor de base de datos, o cualquier otro servicio que se quiera o sea necesario para los usuarios.

Software

Aquí primero debe considerarse qué operaciones podrán realizar los usuarios y dependiendo de ello se instalarán aplicaciones que les ayuden a realizar sus tareas, así como otras que impedirán que realicen operaciones no permitidas, como pudiera ser un firewall que no permita el acceso a ciertas paginas o bien tener máquinas que funcionen con firewall y que no permitan la comunicación de ciertos protocolos como UDP el cual bloquearía el uso de mensajeros instantáneos (Messenger, amsn, y todos aquellos que se comuniquen con estos protocolos), debe considerarse que al cerrar puertos o protocolos en algunas ocasiones los usuarios puedan tener restringido el uso de ciertas aplicaciones las cuales les sean necesarias y tengamos la obligación de proporcionarles estos servicios. Por lo anterior debe sensibilizarse a las personas que sean los responsables de administrar este software y solo cerrar los puertos y protocolos que representen un peligro a las computadoras o bien a la información que contiene nuestra red.

Ahora bien, qué software deberá instalarse en cada computadora puede ser dividido en 3 grandes ramas:

- Equipos que prestarán servicios: Este tipo de equipos debe tener el software necesario para los servicios que se quieran prestar así como aplicaciones extras para asegurar la integridad de los equipos ante intrusos.

- Equipos que serán usados por los administradores: Tendrán las aplicaciones que los administradores consideren necesarios para cumplir sus funciones y puedan comunicarse con los servidores.

- Equipos que serán usados por los usuarios.

  Las instalaciones son de vital importancia y normalmente no se tiene suficiente presupuesto para construir aquellas que cumplan con todos los requerimientos o bien lo que se desee. Es común que se tengan que hacer adecuaciones para adaptarlas.

  Debe considerarse:

  - Sección de equipo para préstamo a usuarios: contendrá las computadoras que son prestadas a los usuarios.

  - Sección para los administradores: se tiene las computadoras del administrador y en algunas ocasiones y debido a falta de espacio servidores que prestan servicios a los usuarios. Esto aunque normal, dependiendo del número de servidores y que tan sensible sea la información que contengan los servicios que prestan debieran tener su propia sección. A lo anterior debe aunarse que este tipo de equipos desprenden mucho calor y podrían necesitar ventilación adecuada o algún tipo de control de temperatura.

  - Sección para el equipo que se necesite prestar (proyector, micrófono, etc.): Mantiene seguro y en condiciones optimas el equipo extra que será prestado a los usuarios.

  - Debe también considerarse la ventilación y salidas de emergencias.

Al considerar todos los puntos anteriores queda la pregunta que posiblemente más interesa ya que es uno de los principales limitantes: ¿Cuál será el monto de la inversión?

Para responder esta pregunta debe haberse seguido los puntos anteriores con lo que ya se tendrá una clara idea de qué será necesario, con lo cual podremos adecuar el presupuesto y prorratearlo en diferentes etapas para concluir con el centro de cómputo que sea el adecuado de acuerdo a nuestras necesidades.

Bibliografía

1. http://www.monografias.com/trabajos11/cenco/cenco.shtml, Niveles de planeación.

Capítulo 3 - Análisis de los Sistemas Operativos.

Un Sistema Operativo (SO) es un conjunto de instrucciones informáticas capaces de ejecutar programas para realizar una tarea en común, sin embargo, cada SO puede realizar o ejecutar de forma distinta sus instrucciones para llegar al mismo resultado. Por ejemplo, existen distinto software para hojas de cálculo capaces de realizar las mismas tareas (incluso leer los mismos archivos), dicho software pueden ser compatible con distintos SO o pueden ser exclusivos de un sólo SO (véase la figura 3.1).

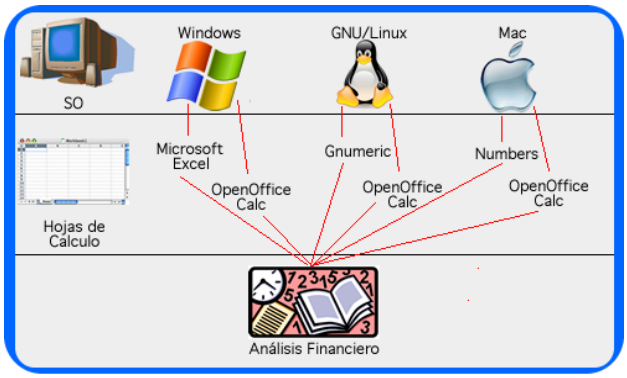


Figura 3.1

Los Sistemas Operativos más populares a utilizar son: GNU/Linux, Mac OS y Microsoft Windows, al ser los más populares los hace buenos candidatos para que los usuarios del centro de cómputo hagan uso de ellos.

Clientes

Microsoft Windows

La elección de un sistema operativo depende del uso que se le va a dar y del lugar donde será instalado, normalmente se utilizará Microsoft Windows, éste es el SO más popular y sencillo de utilizar, por lo que es muy probable que los equipos destinados al préstamo para usuarios tengan este SO. Ahora bien, es muy importante no confundir popularidad y sencillez con eficiencia. Los sistemas operativos de Microsoft Windows son los menos eficaces, ya que tienen un alto consumo de recursos, gran problema de virus, vulnerabilidad e inestabilidad, además de que es de licencia comercial.

Este tipo de sistemas operativos por sí solos no sirven de mucho (a excepción de equipo servidores, los cuales se mencionarán posteriormente), requieren que se les instale por separado software adicional (véase capítulo 4) para la protección del equipo y su uso.

Las desventajas de Microsoft Windows son:

- Se debe pagar la licencia del SO.
- El equipo requiere grandes recursos (equipo muy costoso).
- Comprar software extra (como antivirus, Secure Shell, procesadores de palabras, etc.).

Mac OS

El siguiente candidato es Mac OS, el uso de este software es casi tan sencillo como Microsoft Windows. Una de las cualidades de Mac OS es su casi invulnerabilidad a virus, sin embargo, es posible encontrar virus que pueden afectar al sistema si el mismo usuario da su consentimiento (Ingeniería Social).

Anteriormente Mac Os utilizaba procesadores Power PC (ppc), que son de tipo RISC, lo cual los hacía equipos muy eficientes, hoy en día, Apple decidió cambiar sus núcleos por Intel (arquitectura CISC), los cuales son de mayor capacidad pero menos eficientes que los RISC. Con estos nuevos procesadores los equipos de Apple pueden tener instalado Microsoft Windows.

Este SO fue elaborado para el desarrollo multimedia y cuestiones de diseño. Cuando se instala un equipo Mac, por defecto ya tiene aplicaciones para la edición de video, imágenes y audio, lo cual no sucede con Sistemas Microsoft o Linux.

Las desventajas de Mac son:

- Difícil mantenimiento en caso de avería.
- Los equipos diseñados para este SO son más costosos que las PCs.
- Menos diversidad de software.
- Licencia comercial.

GNU/Linux

El tercer candidato son Sistemas GNU/Linux (comúnmente llamado Linux), hay que hacer énfasis en que la interfaz gráfica no es Linux, Linux es el núcleo del Sistema, cuando se aprende a usar el núcleo se es capaz de manejar cualquier distribución de Linux.

Las distintas versiones de Linux se les llama distribuciones, cada distribución de Linux varía en las aplicaciones y diseño que tienen, y esto debido a que las distribuciones tienen fines diferentes

(o mejor dicho, están pensadas para distintos tipos de usuarios). Sin embargo, el kernel[1] es el mismo.

Por ejemplo, las distribuciones Red Hat, Mandriva y Ubuntu, son distribuciones orientadas al usuario, es decir, tienen pre-cargadas el software más comúnmente utilizado y una interfaz gráfica que le brinde al usuario mayor facilidad para su instalación y uso; la distribución Salux tiene pocas aplicaciones y tiene entorno de red, está elaborada específicamente para uso en hospitales, no tiene muchas aplicaciones por que debe ser un sistema rápido y capaz de comunicarse en red; la distribución Debian está orientada a servidores, su uso e instalación es un poco más complejo, sin embargo se tiene completo control en la administración de recursos y dispone de una gran variedad de paquetes opcionales (antes o después de ser instalado) para brindar distintos servicios (Web, Correo, DNS, etc.).

¿Qué sistema operativo se instalará para los usuarios?

Lo primero es conocer el entorno donde será utilizado el equipo, es decir, cual es el interés o a que se dedican las personas que utilizaran el equipo.

- Si la institución se dedica al desarrollo multimedia y/o diseño gráfico y además cuenta con los recursos necesarios, es conveniente el uso de Mac OS. En su defecto utilizar Microsoft Windows, ya que muchos de los programas de diseño son para estos sistemas operativos, por ejemplo Macromedia.

- Si la institución se dedica a la enseñanza informática, es buena idea tener instalado Sistemas Linux y Windows. Linux por cuestiones de que puedan aprender a usar el SO (tanto en su administración, uso de paquetes, programación, etc.) y aprovecharlo al máximo, y Windows porque a pesar de que la enseñanza sea de informática, puede que los objetivos de los alumnos no sean los mismos y que para algunos no sea necesario (o indispensable) usar Linux, y por sencillez, prefieran usar Windows.

- Si la institución tiene objetivos ajenos a los mencionados anteriormente, lo más aconsejable es usar SO Microsoft Windows.

[1] Parte fundamental de un sistema parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

Servidores

Hasta ahora se han descrito las características, ventajas y desventajas de los equipos clientes, sin embargo, todo centro de cómputo requiere brindar uno o más servicios. Para brindar dichos servicios se requiere de uno o más equipos servidores, de los cuales se habla a continuación.

Los servicios que se pueden brindar son:

- Préstamo de equipos (Administración de cuentas y accesos de usuarios).
- Cuota (o también conocido como Quota) de disco (Almacenamiento de archivos).
- Impresiones.
- NAT (Network Address Translation - Traducción de Dirección de Red).
- Servidor Web.
- Base de datos.
- Correo electrónico.
- DNS (Domain Name System - Sistema de Nombres de dominio).

Implicaciones del uso de Microsoft Windows en servidores

Usar este tipo de Servidores implica, en primer instancia, adquirir equipos de altos recursos y, obviamente, de alto costo, ya que entre más reciente sea la versión (2000, 2003, 2008, etc.) mayor es el requerimiento de los recursos.

El segundo costo de gran importancia son las licencias. Una licencia es el permiso que se otorga a una persona u organización a utilizar un software en específico, ya sea de forma parcial o total.

Los servidores Windows requieren dos tipos de licencias, la primera de ellas es para el uso del propio SO. El segundo tipo de licencia es para el número de equipos clientes que se conectarán de forma simultánea al servidor. Es decir, entre más equipos clientes se tengan, mayor será el costo de esta licencia.

El tercer costo a considerar (que no es obligatorio, pero es muy recomendable) es invertir en software para la protección del equipo y de la información, como lo es software antivirus, antiespías y firewall.

La administración del acceso de los usuarios al servidor es administrado con Active Directory, el cual presenta las siguientes características:

Ventajas:

- Fácil instalación.
- Asistente para configurar distintos servicios.
- Fácil mantenimiento.
- Fácil administración de recursos de cuentas.

Desventajas:

- Se debe pagar una licencia extra para que se puedan conectar ciertos equipos al servidor de forma simultánea, por defecto, viene una licencia para 5 equipos.
- Las reservaciones se tienen que hacer desde el mismo equipo servidor.
- Su uso lo tiene que hacer personal con cierto nivel de conocimientos.
- Susceptible a virus.
- En general, se debería tener un equipo servidor por cada uno de los servicios brindados, por lo que usar servidores Windows tendría un costo muy alto.
- Si el equipo es usado de forma personal, podría congelar el sistema y esto afectaría a todos los usuarios.
- Los servidores Windows tienen retraso considerablemente alto para que se brinden todos los servicios cuando se encienda el equipo (tiempo en que tarda en levantar el servidor).
- El proceso de administración de cuentas puede llegar a ser más lento que las llegadas de los usuarios solicitando servicios, y esto tendría como consecuencia la generación de colas de espera.

Implicaciones del uso de Linux en servidores

El uso de alguna distribución libre de Linux representa un ahorro ya que no es necesaria la compra de licencias, ni para el uso de software o para el número de usuarios conectados al servidor. Además Linux tiene un excelente uso de los recursos de los equipos, sin importar que sean equipos con pocos recursos o bien supercomputadoras.

La distribución Debian es orientada a servidores ya que cuenta con un gran número de paquetes (software) lo que le permite brindar innumerables servicios, además de contar con una estricta seguridad.

Aunado a lo anterior Linux presenta las siguientes características:

Ventajas:

- Utiliza memoria de intercambio (swap). La memoria swap es el equivalente a la memoria virtual de un sistema Windows, y consiste en la porción de disco duro destinado a guardar imágenes de procesos que no se mantienen en la memoria Ram[2].
- Software necesario para prestar servicios gratuitos.
- Seguridad. Linux cuenta con: autenticación de usuarios, sistema completo de permisos para realizar las operaciones de lectura, escritura y ejecución de archivos, firewall integrado, por mencionar algunas características de seguridad.
- Manejo de conexiones remotas.
- Sistema vulnerable a muy pocos virus.

Desventajas:

- Para su administración y uso se requiere una persona con conocimientos de este sistema operativo. Lo cual en ocasiones resulta costoso ya que se requiere capacitar al personal (Este costo no es obligatorio ya que existen una gran cantidad de tutoriales sobre el uso y administración).

Implicaciones del uso de sistemas Unix en servidores

Sólo mencionará BSD (Berkeley Software Distribution - Distribución de Software Berkeley) que es un sistema operativo derivado de Unix nacido a partir de los aportes realizados a ese sistema por la Universidad de California en Berkeley.

FreeBSD ofrece toda la estabilidad y fiabilidad de un sistema Unix. Dispone de una única distribución, por lo que el esfuerzo de miles de desarrolladores y programadores de todo el mundo se ve reflejado en esta. Contrario a Linux el cual tiene muchas distribuciones y el trabajo se ve "repartido" en cada una de ellas

Permite sacar el máximo rendimiento de equipos basados en procesador Intel (a partir de 386SX y 5 Mb de RAM), recomendándose equipos con procesador 486DX o superiores y 8 Mb o más de

[2]http://informatica-practica.net/wordpress/index.php/2007/09/28/el-tamano-ideal-para-la-memoria-swap-de-linux/

memoria RAM. El sistema mínimo requiere 60 Mb de espacio en disco y 340 Mb la instalación completa.

Características de FreeBSD:

- Amplia gama de hardware soportado. Tarjetas gráficas, de sonido, de red, multipuerto, capturadoras de vídeo, controladoras IDE y SCSI, CDROMs, streamers, comunicaciones analógicas, RDSI, Frame Relay, ATM, etc.
- Permite convivir con otros sistemas operativos como Windows NT, Linux, Solaris, etc., en la misma máquina e incluso en el mismo disco, utilizando su propio gestor de arranque o el de otro sistema. Permite incluso acceder a particiones con sistemas de archivos de distinta naturaleza (FAT, FAT32, NTFS, EXT2, UFS, NFS).
- Versatilidad. Este sistema permite utilizarlo como ordenador personal, estación de trabajo, servidor de ficheros, aplicaciones, bases de datos, comunicaciones e Internet, además de router, gateway o firewall. Permite ejecutar programas de otros sistemas operativos como DOS, Windows, Linux, SCO, etc.
- También permite el uso del sistema como firewall, es decir no admita conexiones de usuarios con lo cual disminuye enormemente su vulnerabilidad a los ataques de intrusos.

Implicaciones del uso de sistemas MAC OS en servidores

Los sistemas Mac están basados en Unix, por lo que su administración es muy similar.

Ventajas:

- Rendimiento.
- Tiempo de vida más largo que las PCs.
- Gran invulnerabilidad ante los virus informáticos.
- Terminal desde la cual se puede manipular todo el sistema (similar al Shell de Linux).

Desventajas:

- Costo y su complejidad. El costo es muy elevado, ya que solo pueden ser instalados en equipos especiales Mac.
- Mantenimiento y reparación complicada y costosa.

Bibliografía

1. http://www.jerocu.net/articulos/02/index.html

Capítulo 4 - Administración de recursos y software a utilizar

Al llegar a este punto ya debemos conocer cuáles son las necesidades especificas de nuestro centro de computo, qué servicios se requieren o se desean prestar y sobre todo cual es el perfil de los usuarios y cuáles son los programas y/o sistemas que requieren.

Otro punto muy importante a considerar para seleccionar el software (y en general cualquier recurso) es el presupuesto con el que se cuenta, ya que el costo del software puede ser superior al de algunos de los equipos. Solo como ejemplo el costo de "Adobe Illustrator CS4" para diseño gráfico tiene un costo aproximado de US $599[1], como puede observarse el costo es muy elevado, sin embargo, si es necesario para el funcionamiento del centro deberá adquirirse.

Se pueden establecer convenios entre diversas organizaciones de software de cómputo para la adquisición de licencias institucionales, dichas licencias son negociadas cuando el uso del software es con fines educativos no lucrativos.

Las licencias para el uso del software pueden ser de uso temporal o permanente. Ejemplo de licencias temporales son los antivirus, los cuales permiten el uso del software por periodos anuales (1, 2, 3 años, etc.). Ejemplo de licencias permanentes son procesadores de texto y hojas de cálculo.

La adquisición de software original permite actualizar el software para obtener nuevos módulos y herramientas del programa, correcciones a errores de programación y actualizaciones de seguridad.

En este tema puede entrar la gran discusión si la piratería de software es buena o mala, y sobre todo con el lema "Que la pague el que la pueda pagar", este tema puede ser sumamente extenso, es por ello que este tema no será discutido en esta tesis.

También debe considerarse la política que quiere seguirse en el centro de computo, el ir comprando software bajo licencia o bien adquirir software libre (Free[2]) lo cual significaría un ahorro monetario. Aunque hay que considerar que el software libre utilizado puede ser de menor, mayor o igual eficiencia.

No obstante el punto anterior debe seleccionarse software cuyo proveedor tenga prestigio, el soporte técnico y con adecuada documentación para su uso eficiente.

[1] Costo obtenido de https://store1.adobe.com el 14 de mayo de 2009.

[2] Free o libre significa que no es necesario comprar una licencia, se puede usar y en algunos casos distribuir, sin embargo, no significa la ausencia de una, siempre hay términos de uso para el software y se deben respetar. Por otro lado existe el software de código abierto u "open source", los cuales se caracterizan por distribuir el software junto el código fuente. Por lo anterior todo software de código abierto es libre, pero no todo software libre es de código abierto.

Respecto a soporte técnico, el giro de algunas organizaciones de software libre consta de ofrecer gratuitamente la distribución y uso del software, pero el servicio de soporte técnico es cobrado de forma independiente por periodos de tiempo, por ejemplo, Red Hat Enterprise (distribución de Linux).

Tomando en cuenta lo mencionado anteriormente, se dará software general (puede ser usado en todas las aéreas) y tres diferentes perfiles (estos se mencionaron en el capítulo 3), además de opciones licenciadas (L) y libres (F) con esto se podrá elegir la mejor opción para cada caso:

- Software general: Aquí se incluye el software de paquetería básica para cualquier institución. La función principal de este software es la lectura y modificación de los archivos con los principales formatos, además de permitir el acceso a internet y estar protegidos contra intrusos y virus.

Función	Opción comercial (L)	Opción libre (F)
Procesador de texto	Microsoft Word Pages	Open Office Writer Google Docs
Hoja de cálculo	Microsoft Excel Numbers	Open Office Calc Google Docs
Presentaciones	Microsoft Power Point Keynote	Open Office Impress Google Docs
Lector de documentos PDF		Acrobat Reader Perfect PDF Reader
Conversor de documentos PDF	Acrobat	doPDF
Navegador de Internet		Mozilla Firefox Internet Explorer Safari Opera Google Chrome
Antivirus	Nod32 Kaspersky	AVG Free Avast

Firewall		Sygate Personal Firewall ZoneAlarm
Antiespías		Lavasoft Spybot
Suite de seguridad (Antivirus, antiespías, firewall, etc.)	AVG Inter. Security Norton Inter. Security	
Compresor de archivos	Winzip	Winrar

Tabla 4.1 Software de propósito general.

- Institución dedicada al desarrollo multimedia y/o diseño gráfico. Este software está dirigido a la creación y edición de imágenes, video o posiblemente audio, todo de acuerdo a las necesidades de la institución:

Herramienta	Opción comercial (L)	Opción libre (F)
Editor de imagen	Adobe Photoshop	Gimp
Dibujo	Adobe Fireworks	Open Office Draw
Películas SWF	Adobe Flash	
Diseño de páginas Web	Adobe Dreamweaver Frontpage	
Editor de audio	Adobe Audition	

Tabla 4.2 Software para desarrollo multimedia y/o diseño gráfico.

- Institución dedicada a la enseñanza informática. Este software es muy especializado, dedicado a la programación (hay software especializado para cada lenguaje de programación y software elaborado para múltiples lenguajes de programación), brindar servicios y resolución de problemas matemáticos:

Herramienta	Opción comercial (L)	Opción libre (F)
Editor de programación	Visual Studio	Netbeans Eclipse
Compiladores	C Sharp	C C++ Java
Servidores Web	IIS	Apache Tomcat
Manejadores de Bases de Datos	SQL Server Oracle	MySql Postgresql
Conexión remota	Tectia Secure Shell	Open SSH Putty

Tabla 4.3 Software para enseñanza informática.

- Instituciones que tienen otros objetivos: Para la selección del software de esta institución se deberá conocer las necesidades específicas y evaluar las posibles opciones, aquí mencionaremos algunas posibilidades:

  - Institución dedicada a la enseñanza arquitectónica y de construcción (Ingeniería civil y arquitectura), se requiere de software especializado para la elaboración de diagramas, dibujo técnico, planos y dibujos e 3D.

Herramienta	Opción comercial (L)	Opción libre (F)
Diagramas	Microsoft Visio	ArgoUML
Planos	Autocad	Dia
Dibujos en 3D	Autocad	

Tabla 4.4 Software para enseñanza arquitectónica y de construcción.

- Institución dedicada a la enseñanza financiera (por ejemplo contaduría y economía).

Herramienta	Opción comercial (L)	Opción libre (F)
Administración de recursos	Aspel	

Tabla 4.5 Software para enseñanza financiera.

- Institución dedicada a la enseñanza estadística y psicoanalítica.

Herramienta	Opción comercial (L)	Opción libre (F)
Análisis estadístico	Spss Eviews	
Elaboración de bibliografías	Endnote	

Tabla 4.6 Software para enseñanza estadística y psicoanalítica.

- La institución tiene otros objetivos: Para la selección del software de esta institución se deberá conocer las necesidades específicas y evaluar las posibles opciones.

A todo lo anterior nunca debe olvidarse que a fin de brindar un buen servicio se debe monitorear las necesidades de los usuarios para mantener instalado y actualizado el software necesario.

El hardware puede ser adquirido o seleccionado previamente a la elección del software, sin embargo, eso puede causar que se tenga equipo que no cumpla con los mínimos requerimientos del software o bien su ejecución no sea la adecuada, por lo anterior es recomendable primero saber cuál será el uso que tendrá el equipo. Aquí también debe considerarse que otro equipo va a coexistir, previendo la expansión, interconexión o capacidad.

Bibliografía

Se consultó el sitio Web oficial del software mencionado en este capítulo.

Capítulo 5 - Análisis y Recomendaciones de Cableado estructurado y tecnologías Wireless

Redes alámbricas (Cableado Estructurado)

Un sistema de cableado estructurado (también conocido como Sistemas de Transporte de Información) es aquella infraestructura de medios físicos que proporcionan la comunicación en áreas limitadas, está integrado por dispositivos pasivos que cumplen ciertas características.

El objetivo del cableado estructurado es permitir a las telecomunicaciones un desempeño óptimo de acuerdo a las necesidades del usuario. Se basan en normas o códigos y estándares tanto internacionales como nacionales (de acuerdo al lugar donde se instalará el sistema).

Durante el desarrollo de este capítulo, se mencionarán los códigos y estándares que hay que cubrir para un sistema de cableado estructurado, tomando en cuenta sólo la transmisión de datos y no de voz.

Hay que tener en cuenta que los recursos pueden ser escasos en las instituciones educativas, es por ello que no es obligatorio seguir los estándares y códigos mencionados a continuación, pero en caso de que los recursos así lo permitan, es muy recomendable seguirlos.

¿Qué son los códigos y los estándares?

Los **códigos** son reglas que estamos obligados a seguir, ya que estos aseguran la calidad de la construcción y protegen la propiedad y aún más importante, protegen la salud y la vida de las personas. Los códigos no sirven para proteger las telecomunicaciones, como lo es una intrusión, ruido inducido o eventos que interrumpan o alteren el flujo de la información.

Los **estándares** son aquellas "sugerencias" que nos aseguran que cumplirán ciertos requisitos mínimos, pero que no estamos obligados a cumplir. Los estándares son usados para analizar el flujo de la información, estos son establecidos como una base para comparar y juzgar: capacidad, cantidad, contenido, grado, valor y calidad.

Las principales organizaciones y códigos que existen para el cableado estructurado son:

- NEC, National Electrical Code - Código Nacional Eléctrico: El NEC de México fue creado para protección dentro de los edificios, es conocido como Norma Oficial Mexicana (NOM-001) y fue emitido para establecer las especificaciones y lineamientos de carácter técnico que deben satisfacer las instalaciones destinadas a la utilización de la energía eléctrica, a fin de que ofrezcan condiciones adecuadas de seguridad para las personas y sus propiedades, en lo referente a la protección contra:

- Choques eléctricos.
- Efectos térmicos.
- Sobrecorrientes.
- Falla de corriente.
- Sobretensiones.

Define los siguientes términos utilizados en telecomunicaciones:

- Plenum: Cámara plena: Área designada utilizada para transportar aire externo como parte del sistema de distribución.
- Riser: Una corrida vertical en un pozo, o de piso a piso, sellado de manera independiente al resto del edificio.
- Unión: la unión permanente de partes metálicas para formar una trayectoria eléctricamente conductiva con la capacidad de conducir de manera segura cualquier corriente que corra por ella.
- Aterrizaje: conexión internacional a tierra para prevenir altos voltajes que puedan resultar peligrosos ya sea para los equipos conectados o para las personas.

El NEC se encuentra divido en 9 capítulos (año 2005), y cada capítulo contiene una cantidad variada de artículos, sin embargo los artículos que pertenecen al cableado de comunicaciones son:

- 100: Definiciones
- 250: aterrizajes y uniones.
- 300: métodos para cablear.
- 770: Cables y canalizaciones de Fibra Óptica.
- 800: Circuitos de comunicaciones.

- ANSI, American National Standard Institute - Instituto Americano Nacional de Estándares: Compila y publica los estándares nacionales para los sistemas de cableado estructurado de telecomunicaciones.
- TIA, Telecommunications Industry Association - Asociación de Industrias de Telecomunicaciones: Escribe los estándares de cableado en conjunto con EIA.
- EIA, Electronics Industries Alliance - Alianza de Industrias Electrónicas: Escribe los estándares para el equipo electrónico.
- FCC, Federal Communications Commission - Comisión Federal de las Comunicaciones.
- IEEE, Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos.
- NESC, National Electrical Safety Code - Código Nacional de Seguridad Eléctrico: Fue publicado por IEEE, este código aplica para el exterior (en la línea de entrada al edificio y entre edificios).
- NFPA, National Fire Protection Association - Asociación Nacional de Protección contra incendios.

Los estándares para telecomunicaciones son:

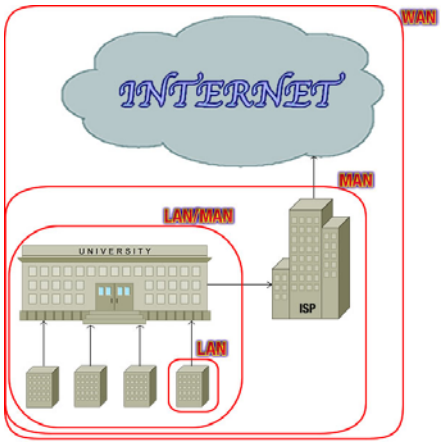
- ANSI/TIA/EIA-568-B: Estándar para el cableado de telecomunicaciones para edificios comerciales.
- ANSI/TIA/EIA-569-A: Rutas y espacios.
- TIA-569-B: Estándar para las Canalizaciones y Espacios de Telecomunicaciones para edificios comerciales (rutas y espacios).
- ANSI/TIA/EIA-606-A: Estándar para la administración de la infraestructura de Telecomunicaciones para edificios comerciales. Establecen los requerimientos para los registros que se deben tener y la información disponible para administrar debidamente los sistemas de telecomunicaciones en los edificios comerciales.
- ANSI-J-STD-607-A: Requerimientos de Aterrizaje y Unión a Tierra de Telecomunicaciones para edificios comerciales. Especifica los requerimientos de aterrizaje y los requerimientos de interconexión entre la tierra de telecomunicaciones y otros componentes para edificios comerciales.

- ANSI/TIA/EIA-570-B: Estándar para el cableado de Telecomunicaciones Residencial. Establece dos grados de servicio:
  - Grado 1. Sistema de cableado genérico que cumple con los requerimientos básicos de los sistemas de telecomunicaciones.
  - Grado 2. Sistema de cableado genérico que cumple con los requerimientos básicos, avanzados y de multimedia de los sistemas de telecomunicaciones.

Para el caso de una institución educativa, se deben seguir los estándares para edificios comerciales (ya que existen estándares definidos para uso doméstico o dentro del hogar).

Componentes de un Sistema de Transporte de Información

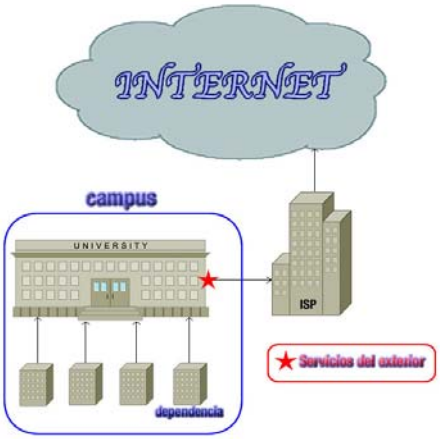
El sistema de transporte de información se compone de los siguientes elementos:



I. Servicios del exterior
II. Acceso al edificio
III. Requerimientos de espacios
IV. Requerimientos de canalización
V. Hardware de terminación
VI. Salidas en el área de trabajo
VII. Cables
VIII. Documentación
IX. Esquema final de red

Figura 5.1 Sistema de Transporte de Información para una institución educativa.

I. Servicios del exterior



Los servicios del exterior se componen de:

1) Servicios de Larga distancia y/o Local
2) Acceso a Internet mediante una puerta de enlace (Gateway) y un ISP (Proveedor de Servicios de Internet).
3) Wide Área Network (WAN).
4) Circuitos especiales.
5) Enlaces de campus.

Figura 5.2. Servicios del exterior.

II. Acceso al edificio

Para realizar un enlace desde el exterior a un edificio, hay 3 formas distintas de hacerlo:

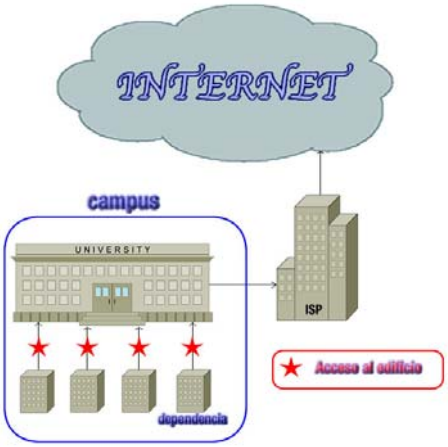
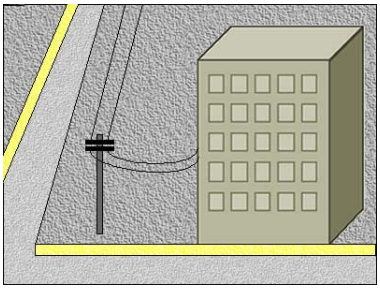


Figura 5.3.a. Acceso al edificio

1. Aéreo



Es el enlace más económico, ya que no requiere de mayor inversión para su instalación, el cable es económico, sencillo para mantenimiento, movimientos, cambios y adiciones.

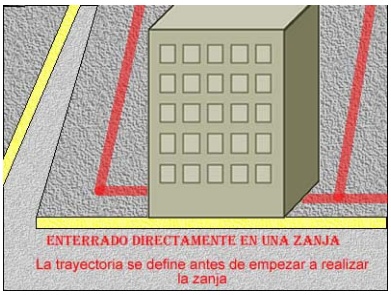
Figura 5.3.b. Acceso al edificio (aéreo).

Cuando se coloca cable aéreo hay que dejar alturas mínimas de acuerdo al tránsito que habrá en el lugar:

- Calles con vehículos: 4.7 m.
- Calles con peatones: 3 m.
- Otros techos 2.4 m.
- Ferrocarriles: 7.2 m.

Las desventajas que se tiene es que visualmente es muy notorio y está sujeto a daños de personas, animales y al clima.

2. Enterrado directo



Consiste en enterrar directamente en el subsuelo los medios de comunicación, con lo cual se mantendría escondido de la vista, es económico de instalar y la ruta a trazar es flexible.

Figura 5.3.c.1. Acceso al edificio (enterrado directo).

Para este tipo de método, es necesario utilizar una armadura que proteja a nuestro medio contra roedores y/o aplastamiento.

Para realizar este tipo de acceso, el cable es colocado directamente en una zanja, la cual debe tener al menos 60 cm. de profundidad, a 45 cm. de altura de donde está ubicado el cable se debe colocar una cinta de advertencia para evitar que el cable sea dañado al momento de realizar excavaciones o querer hacer movimientos sobre el medio ya instalado.

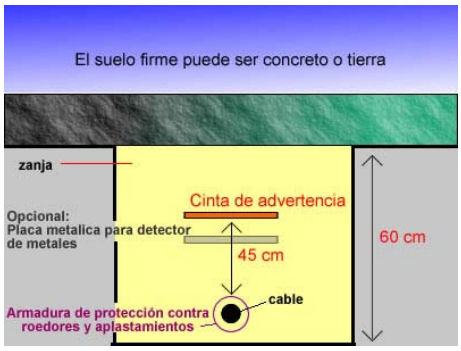


Figura 5.3.c.2. Acceso al edificio (enterrado directo).

Si el suelo que cubre la zanja es tierra, opcionalmente, se puede agregar una placa metálica la cual permitirá, mediante un detector de metales, saber la ubicación de la instalación del medio.

Las desventajas que tendría realizar este tipo de acceso al edificio es que está expuesto a daños por roedores, agua o excavaciones, realizar movimientos, cambios o adiciones puede costar mucho tiempo y dinero, es difícil de acceder y el mantenimiento del cable utilizado es muy costoso.

3. Subterráneo

Este tipo de acceso consta de un sistema canalizado debajo del suelo (por ejemplo, dentro de un túnel, sistema de drenaje, el metro, etc.), lo cual, deja el cableado oculto de la vista, lo protege contra daños y es muy fácil realizar movimientos, adiciones o cambios.

Sin embargo, este tipo de acceso es el más costoso y difícil de instalar, ya que requiere de la coordinación con las autoridades locales y compañías de electricidad, gas, agua, drenaje, telefonía, etc. Esto para prevenir hacer daños a instalaciones ajenas. Además de que la re-localización del sistema es igualmente compleja y costosa.

III. Requerimientos de Espacios.

Los espacios de un Sistema de Información están dedicados a componentes de telecomunicaciones como lo son el cable, equipo y terminaciones.

Existen 4 tipos de espacios en un Sistema de Información:

1. Acometida (EF- Entrante Facility).
2. Sala de Equipos (ER- Equipment Room).
3. Cuarto de Telecomunicaciones (TR- Telecommunications Room).
4. Área de Trabajo (WA- Work Area).

1. Acometida (EF- Entrance Facility)

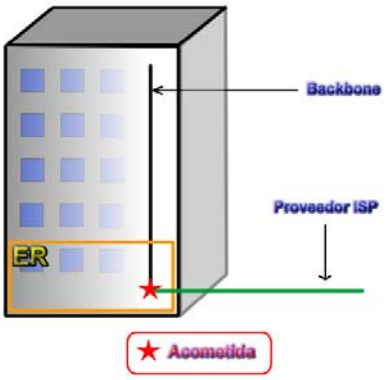


Figura 5.4.a. Acometida (ubicación).

Es la conexión que se realiza para hacer el cambio entre el cable del exterior proporcionado por el servidor de internet (ISP) y cable interior que es el inicio de nuestra red.

Normalmente la acometida está en una Sala de Equipos la cual será la encargada de proveer internet a la organización o institución.

La acometida está conformada por:

- Cables de entrada (proveniente del proveedor de servicio).
- Mangas de empalme.
- Protección eléctrica: Se basa en los códigos nom001 para la protección eléctrica (artículo 250). Para la protección eléctrica puede ser necesario que el proveedor de acceso y el cliente se pongan de acuerdo para determinar las necesidades y las políticas a cubrir.
- Punto de demarcación: Es el punto donde se unen y se hace el cambio de cable exterior a cable interior mediante una manga de empalme.
- Campos de terminación.
- Cables verticales (Backbone).
- Cables de conexión cruzada (Cross Connect).
- Aterrizaje a tierra: Estos requerimientos se siguen de acuerdo a ANSI/TIA/EIA-607: Requerimientos para Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales.

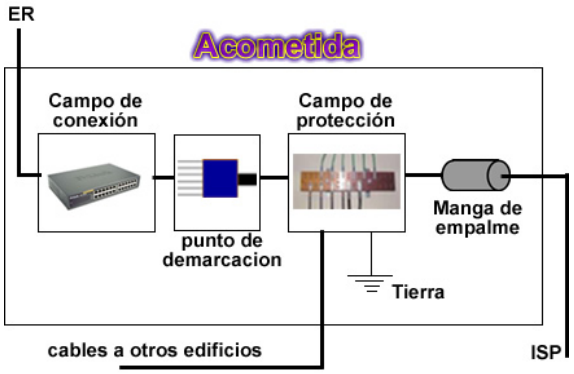


Figura 5.4.b. Acometida (componentes).

Para realizar el registro de la acometida se debe hacer sobre una pared cubierta por un triplay con ¾" de grosor y pintado con 2 capas de pintura retardante al fuego.

La puesta a tierra de la acometida debe ser con una Barra Principal de Tierra (TMGB) y usar cable #6 AWG (mínimo) con forro verde, la TMGB debe estar muy bien sujeta, ya que un "golpe" eléctrico podría desprenderlo y convertirlo en riesgo de incendio.

2. Sala de Equipos (ER – Equipment Room).

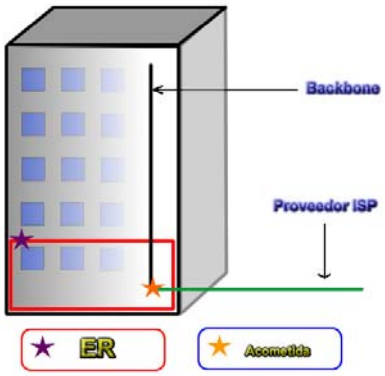


Figura 5.5.a. Sala de equipos (ubicación).

Su diseño está sujeto al estándar ANSI/TIA/EIA-569-A. La sala de equipos contiene el equipo necesario que proveerá la comunicación al edificio o a un campus por lo que su tamaño debe ser suficiente para albergarlo y es conveniente tener un ambiente controlado para hospedar equipos de telecomunicaciones (equipo que es utilizado para la comunicación a distancia), panel de parcheo (Patch Panel), empalmes, conexión y unión a tierra, así como dispositivos de protección donde se requiera.

El ER debe tener una localización centralizada con respecto al edificio o campus, ser de fácil acceso para el movimiento de equipo de gran tamaño (como el UPS), estar por encima del suelo (normalmente con piso falso que soporte el equipo pesado) y alejado de fuentes de agua, procurar

que este lejos de fuentes de emisión de interferencia magnética (transformadores, motores, generadores, transmisores de radio, elevadores, copiadoras, etc.).

Su función es mantener la comunicación con los cuartos de telecomunicaciones.

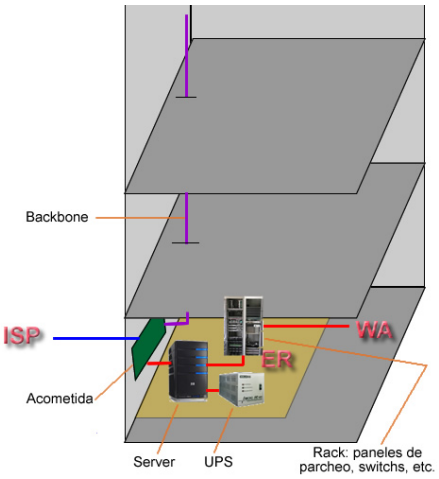


Figura 5.5.b. Sala de equipos (componentes)

3. Cuarto de telecomunicaciones (TR – Telecommunications Room).

El diseño de un TR está sujeto al estándar ANSI/TIA/EIA-569-A.

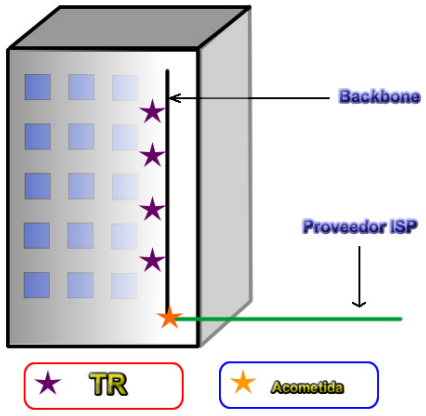


Figura 5.6.a. Sala de telecomunicaciones (ubicación).

de

Su principal función es hacer compatibles las terminaciones del cableado horizontal y del Backbone con el hardware de conexión (paneles parcheo, transceiver, switch, etc.). El uso de paneles de parcheo permite una conectividad flexible.

Un TR puede contener paneles de parcheo en cada piso o un solo panel de parcheo en el ER para distintas partes del sistema de cableado del Backbone.

El TR proporciona un ambiente controlado para albergar equipo de telecomunicaciones, hardware de conexión y terminaciones de empalme que sirven a una porción del edificio (puede ser a un área de trabajo o un piso completo). También provee la administración y distribución de los cables de equipos desde la conexión cruzada horizontal hasta el equipo de telecomunicaciones. En algunos casos, el punto de demarcación (ver acometida) y los dispositivos de protección pueden estar ubicados en el TR.

El cableado horizontal y el Backbone deben terminar en el hardware de conexión basados en los requerimientos del estándar ANSI/TIA/EIA-568-B.2 (componentes de cableado de par trenzado) y ANSI/TIA/EIA-568-B.3 (componentes de cableado de Fibra Óptica), estas terminaciones de cables no deben ser reubicados para implementar movimientos al sistema de cableado, adiciones o cambios. Todas las conexiones entre los cables de la horizontal y el backbone deben ser a través de conexiones cruzadas.

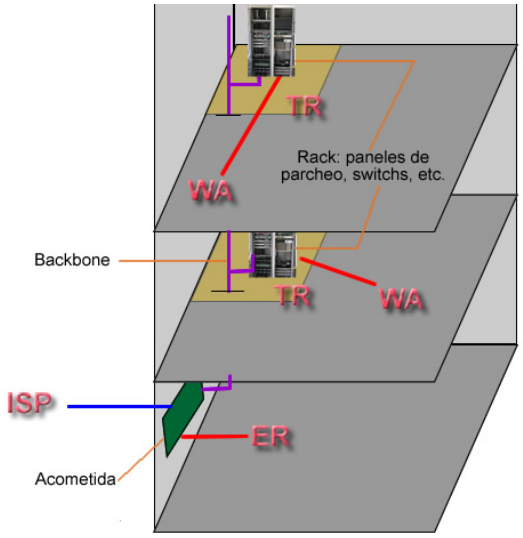


Figura 5.6.b. Sala de telecomunicaciones (componentes).

Un edificio debería contar con al menos un TR por cada piso, debe estar tan centrado como sea posible al área de servicio y alejado de transformadores, motores, generadores de electricidad o radio transmisores. Un TR y sus respectivos racks deben tener su puesta a Tierra.

4. Área de Trabajo (WA – Work Area)

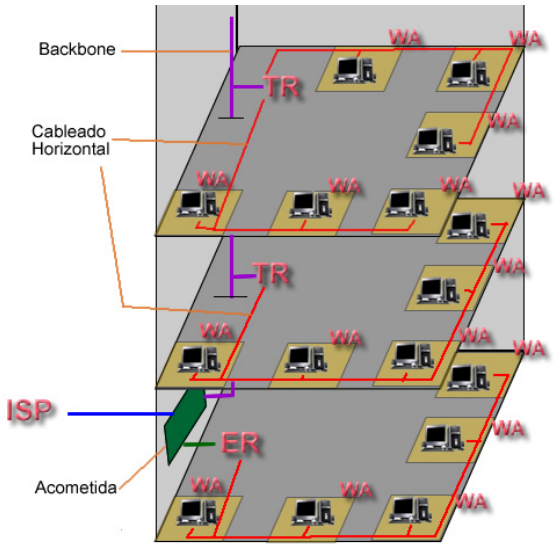


Figura 5.7. Áreas de trabajo

El área de trabajo es el espacio físico destinado al usuario final, en ésta área se encuentran las salidas de telecomunicaciones (tapas o faceplate) y los cables de equipo.

Se recomienda que durante la planeación se considere la instalación de 2 puntos de red por cada espacio asignado a los usuarios.

En caso de que se encuentre en construcción el edificio se debe estimar que cada espacio individual (WA) debe medir $2m^2$ aproximadamente.

IV. Requerimientos de canalización.

A continuación se mencionará las características y las distintas formas de realizar las canalizaciones necesarias tanto para cableado vertical como horizontal.

- Cableado vertical (backbone):

  La función del Backbone es proveer la interconexión entre los TR, ER y EF. Consiste en cables tipo riser[1] o fibra óptica, panel de parcheo intermedio (panel ubicado en TR) y panel de parcheo principal (ubicado en ER). El Backbone también incluye al cableado entre edificios (campus).

  Es proyectado para atender las necesidades de los ocupantes del edificio por uno o varios periodos, cada periodo puede ser pensado entre 3 y 10 años de servicio. Y en cada periodo se debe tener la flexibilidad para el crecimiento y los cambios necesarios en la instalación sin tener que hacer un re-cableado del sistema. La duración de cada periodo está basada en la estabilidad y el crecimiento del usuario final de la organización.

  Los medios de comunicación que se pueden usar para el sistema de cableado de Backbone son:

  - Par trenzado de 100 Ω (definido en el estándar ANSI/TIA/EIA-568-B.2).
  - Fibra óptica Multimodal 62.5/125 μ o 50/125 μ (definido en el estándar ANSI/TIA/EIA-568-B.3).
  - Fibra óptica Mono modo (definido en el estándar ANSI/TIA/EIA-568-B.3).

  Para la selección adecuada del medio de comunicación a utilizar se toman en cuenta 3 puntos:

  1. Flexibilidad con respecto a los servicios que se brindará.
  2. Tiempo de vida útil del cableado de Backbone.
  3. Tamaño del lugar y de la población que será atendida.

  Nótese que no está mencionado el costo monetario del medio de comunicación, y esto es debido a que no debe considerarse como limitante para la instalación de un sistema de cableado. Siempre y cuando la organización o institución cuente con los recursos necesarios.

[1] Cable de par trenzado con el forro más rígido de lo normal, por lo que es menos susceptible a daños físicos, sin embargo es menos flexible causando que sea más difícil manipularlo en curvas, además al incendiarse el forro de este tipo de cable produce humo más tóxico que un cable de par trenzado de uso general.

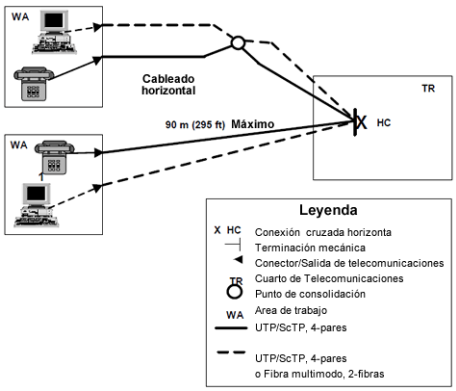
Si la instalación del Backbone se hace con:

- Cables: deben fijarse (o soportarse) cada metro, para ello, puede hacerse mediante una charola colgada verticalmente, soporte o cuerda de soporte.
- Fibra óptica: se debe utilizar ducto interno que proteja a la fibra óptica, ya que es muy susceptible a daños físicos.

En ambos casos (cables o fibra óptica) para pasar el Backbone entre pisos debe utilizarse masilla contra fuego (Fire stopping), ya que es un requerimiento de seguridad mencionado en la nom001 artículo 300-21[2].

Es importante notar que todos los elementos utilizados para la instalación del Backbone deben tener su correspondiente conexión a tierra.

- Cableado horizontal:



Comunica las áreas de trabajo (WA) con las salas de telecomunicaciones (TR), está compuesto por los cables horizontales, los conectores de telecomunicaciones del (WA) y paneles de parcheo alojados en el TR.

El cableado horizontal no debe tener más de un punto de transición o punto de consolidación entre el conector de telecomunicaciones y la conexión cruzada horizontal.

Figura 5.8. Diagrama de cableado horizontal.

- Punto de consolidación:

Es la unión de dos tramos de cables largos mediante una roseta (por ejemplo, al querer reparar un cable que fue mordido por un roedor), en la imagen 5.9 se muestra un punto de consolidación para dos cables mediante rosetas (roseta abierta y roseta cerrada).

[2] Nom001, 300-21. Propagación de fuego o de productos de combustión.

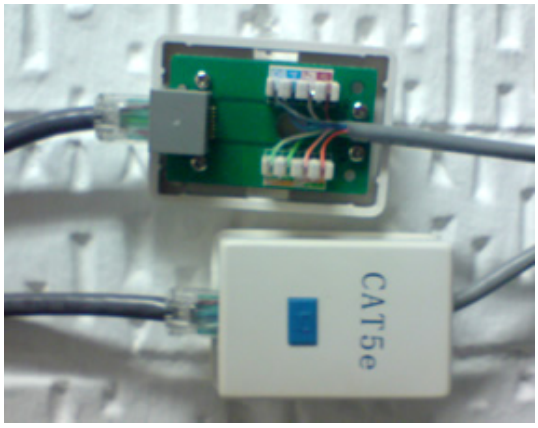


Figura 5.9. Fotografía de dos puntos de consolidación mediante el uso de rosetas.

Al realizar remodelaciones del área o espacio, podría ser necesario mover de lugar las terminaciones de red lo que ocasionaría que se requiera consolidar un gran número de cables, en este caso pueden usar dispositivos específicos para esta finalidad.

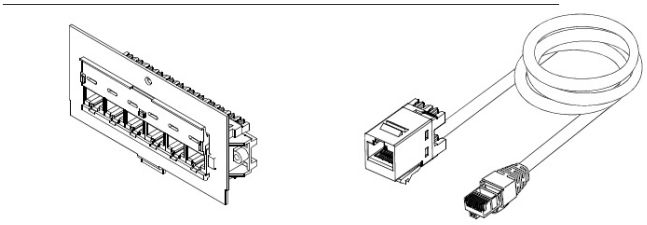


Figura 5.10. Hardware para múltiples puntos de consolidación

La topología a utilizar para el cableado horizontal es de tipo estrella, cada conector de telecomunicaciones del WA debe ser conectado al TR usando cable horizontal y el TR debe estar ubicado en el mismo piso que las WA a la cuales brindará servicio.

- Canalización:

La canalización del cableado horizontal puede hacerse de 4 formas:

1. Bajo piso: Es una instalación que se hace durante la construcción del edificio, son ductos localizados en la losa de concreto con puntos de acceso predeterminados.

En cableado horizontal con Fibra Óptica, debe usarse innerduct (tubo metálico) para proteger la fibra.

Durante la construcción del edificio, el orden de instalación de distintos servicios es el siguiente:

a) Aire acondicionado.

b) Plomería.

c) Eléctrico.

d) Telecomunicaciones.

Este orden es considerado por la dificultad y flexibilidad de instalación de cada servicio, los ductos del aire acondicionado son muy grandes y poco flexibles, es por ello que debe ser lo primero en instalar, las canalizaciones de telecomunicaciones son muy flexibles, por ello, es lo mas recomendado de instalar al final.

2. Por el plafón: Para este tipo de cableado se utilizan soportes especiales instalados sobre la estructura del edificio, los cuales deben quedar por arriba del plafón.

   Como soporte pueden utilizarse charolas, escalerillas o red plástica para cable de cobre.

   Al instalar una charola, debe haber un soporte como máximo cada 1.5 metros, de acuerdo a la nom001. El tamaño es dado de acuerdo a la cantidad de cables que pasarán por ella y debe utilizarse el 40% de la charola. Un uso del 50% o mayor se considera muy lleno, por el contrario utilizarlo al 25% o menos se considera muy sobrado, esto dado que debe considerarse un plan de crecimiento.

   Para explicar lo anterior se propone el siguiente ejemplo:

   Conocer el ancho de una charola por la cual pasarán 500 cables categoría 6.

   Solución:

   El diámetro del cable se puede conocer como dato del fabricante o incluso se puede medir directamente, para este ejemplo, diámetro por cable = 6mm.

   $Superficie_{cable}$ = (Π * d2) / 4

   $Superficie_{cable}$ = (3.14 * (6mm)2) / 4

   $Superficie_{cable}$ = 113.04mm2 / 4

   $Superficie_{cable}$ = 28.26 mm2

   Para conocer la superficie total de todos los cables, se multiplica la superficie utilizada por cada cable por el número de cables a instalar.

Para este caso, el número de cables a instalar es de 500.

$Superficie_{cables}$ = Superficiecable * 500

$Superficie_{cables}$ = 28.26 mm2 * 500

$Superficie_{cables}$ = 14130 mm2

Se conoce la superficie a utilizar que será utilizable al 40%

$Superficie_{charola}$ = Superficiecables / 0.40

$Superficie_{charola}$ = 14230 mm2 / 0.40

$Superficie_{charola}$ = 35 325 mm2

Las dimensiones de la charola se definen por la altura y el ancho, la altura es un dato proporcionado por el fabricante, para este caso de ejemplo, es de 75 mm. El ancho es el dato a obtener, y por medio del cual se deberá comprar la charola.

$Superficie_{charola} = Altura_{charola} * Ancho_{charola}$

$Ancho_{charola} = Superficie_{charola} / Altura_{charola}$

$Ancho_{charola}$ = 35 325mm2 / 75 mm

$Ancho_{charola}$ = 471 mm

Normalmente, las unidades utilizadas para las charolas son en pulgadas…

$Ancho_{charola}$ = 471 mm ≈ 18.54”

Sin importar que tipo de soporte se instale hay que asegurarse de que los soportes están aterrizados a conexión a tierra. Si no realiza dicho aterrizaje, la energía atrapada puede causar daños o mal funcionamiento.

3. Canaleta sobrepuesta: Son conductos plásticos que se sujetan a muros o particiones de tabla roca, se encuentran expuestas al personal ocupante del cuarto.
   Este tipo de instalación se lleva a cabo cuando el edificio ya está construido y no se hizo una planeación de estructura de red durante su construcción. Al sujetar la canaleta a la pared se debe tener cuidado con las esquinas ya que no debe haber esquinas con ángulos de 90 grados.

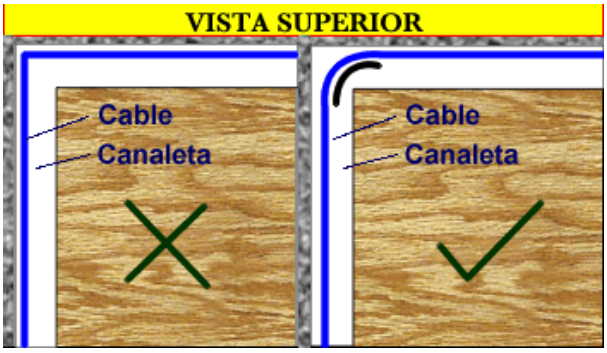


Figura 5.11. Vuelta incorrecta/correcta de un cableado horizontal.

4. Piso falso: Al poner este tipo de canalización, se utilizan soportes al igual que una instalación de plafón.

V. Hardware de terminación

El hardware de terminación se encuentra en dos espacios: TR (paneles de parcheo y racks) y WA (tapas o faceplate y conectores jacks).

El Hardware de terminación es el siguiente:

- Paneles de parcheo (patch panel): Pueden instalarse montados en muros (con soportes abisagrados) o racks y su terminación se hace con cables de parcheo (patch cords).

  Ventajas de su uso:

  - Tiene terminación directa en el equipo permite velocidades de transmisión de datos más alta, los cables de parcheo permiten a los usuarios hacer movimientos, adiciones y cambios sin necesidad de herramientas especiales.

Figura 5.12. Paneles de Parcheo.

Desventajas de uso:

- Su costo es más alto que las regletas.
- Requiere más espacio para la terminación.
- Un Rack de montaje en pared o en el piso.

- Requiere administración.
- Son más costosos que las regletas, se requiere más espacio para la terminación, un rack para montaje en pared o en el piso y de una administración de los cables de parcheo.

- Racks: Tienen la capacidad de soportar equipo, regletas, paneles de parcheo y la administración del cableado.

  Cada espacio que hay en los Racks se llaman unidades, dependiendo el elemento que se vaya a instalar (Switch, panel de parcheo, organizador, etc.), será el número de unidades a utilizar. Una unidad tiene aproximadamente 1.75" de altura (4.44 cm).

  Para decidir la altura del Rack que se va a instalar, se debe basar en el número de usuarios a los que se dará servicio y considerar un crecimiento del al menos 50%.

  Normalmente se tienen hasta 192 nodos de red en cada Rack, aunque máximo se puede contener hasta 240 nodos (utilizando Switch de 48 puertos).

  Ventajas de uso:

  - Todos los cables, campos de terminación y equipo electrónico pueden ser montados en el mismo espacio.
  - Se pueden instalar dentro de gabinete especializados para mantener una ventilación adecuada.
  - Se tiene acceso frontal y posterior del equipo.

  Desventajas de uso:

  - El costo del rack y/o gabinete.
  - Deben estar fijos al sueño o techo.
  - Utilizan espacio.

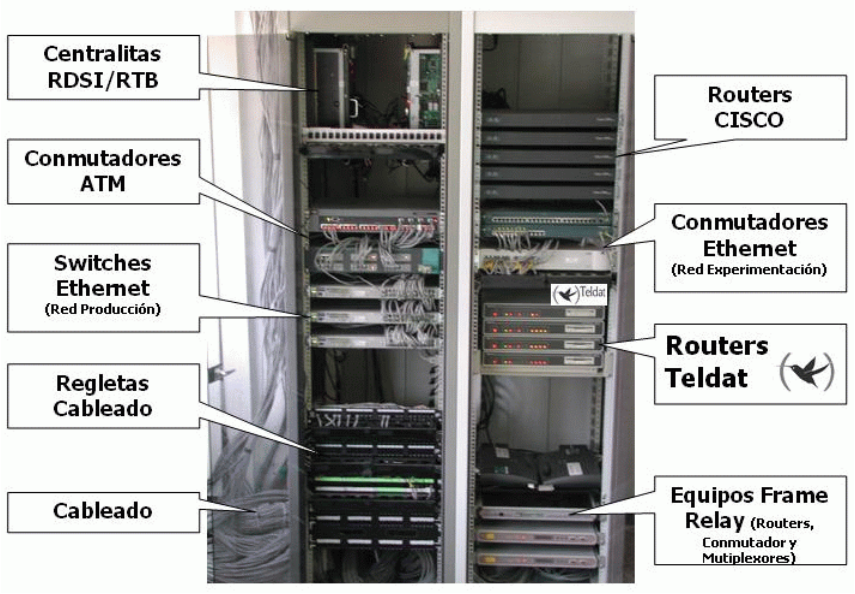


Figura 5.13. Organización de un rack

La instalación de los Racks está basada en el estándar EIA-310-D (Gabinetes, Racks, Paneles y Equipos relacionados). Este estándar provee al usuario los requisitos de diseño para Gabinetes, Racks y Paneles. Cuando las especificaciones están basadas con este estándar, el acuerdo por cada unidad del rack debe realizarse entre el cliente y el proveedor. Todo Rack instalado debe estar aterrizado a Tierra.

VI. Salidas en el área de trabajo

Las tapas protegen y soportan los conectores hembras (jacks) y machos (plugs) del WA, existen distintos modelos y colores los cuales permiten una mejor identificación de los puntos de terminación (nodos de red).

Los campos de terminación del WA (salidas de telecomunicaciones) tienen la función de conectar el equipo del WA (teléfonos, fax, computadoras y modem) al cableado horizontal.

Las salidas de comunicaciones deben ser instaladas a la misma altura que las salidas eléctricas, y debe haber como mínimo una en cada WA.

Por cuestiones de crecimiento, se debe instalar como mínimo dos cables en cada salida de telecomunicaciones y cada salida debe ser instalada por cada 7 a 10 m^2 de espacio de oficina.

VII. Cables.

Hay distintos tipos de cables a utilizar, dependiendo del uso que tendrán. Los distintos tipos de cables son:

- Cable horizontal: Cable entre el WA y el TR, el cuál provee los medios para transportar las señales de telecomunicaciones. Su distancia máxima es de 90 m. entre el campo de terminación y la salida de telecomunicaciones.

- Cable vertical (Backbone): Cable entre el TR, la ER, la EF por dentro y entre edificios. La distancia máxima de este cable es de 90 metros en el caso de cable de cobre y 2Km y 3Km en caso de fibra óptica multimodo y monomodo respectivamente.

- Cable de parcheo (Patch Cords): Conecta los paneles de parcheo horizontales a verticales o al equipo electrónico que genere señal. Su distancia máxima es de 5 metros entre paneles de parcheo.

- Cables de equipo: Cables usados para conectar equipos (computadoras, teléfonos, impresoras, fax, etc.) a la salida de telecomunicaciones. Su distancia máxima es de 5 metros entre una salida de telecomunicaciones y un equipo.

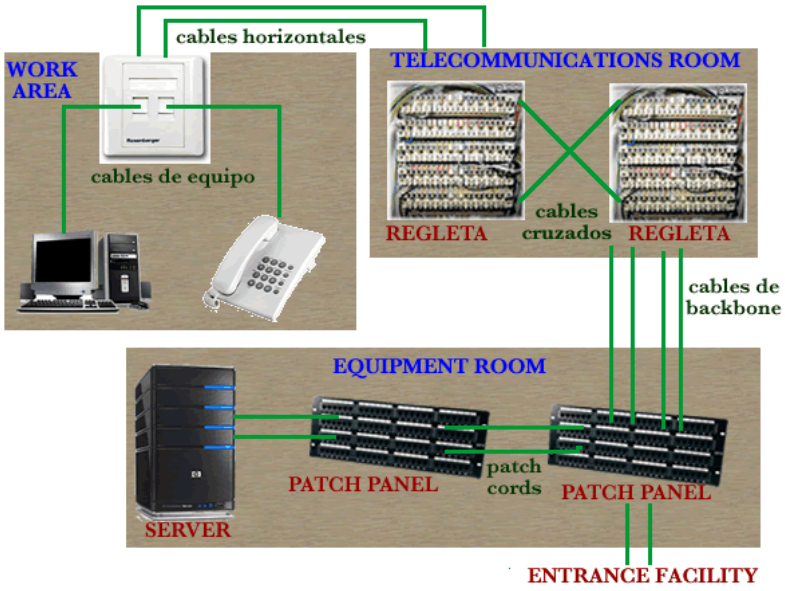


Figura 5.14. Uso y ubicación de los distintos tipos de cable.

Medios de comunicación

Los medios a usar son:

- Cable de par trenzado sin blindaje (UTP: Unshielded Twisted Pair): Es el más utilizado para voz y datos, es el medio de cobre más económico y cumple con los estándares. El Ancho de banda del UTP se denota por la categoría del cable.

Este tipo de cable usa conectores (Plugs) RJ45. Para cualquier categoría tiene una limitación de 90 metros.

Figura 5.15.a. Cable UTP.

Las categorías más utilizadas (para datos) son:

  - Categoría 5e: desempeño hasta los 100 MHz soporta aplicaciones grandes para LAN 1000 Base T.
  - Categoría 6: desempeño hasta 250 MHz soporta aplicaciones más grandes para LAN 1000 Base TX.

- Cable de par trenzado apantallado (FTP: Foiled Twisted Pair y STP: Shielded Twisted Pair): El cable FTP posee una pantalla (cubierta metálica) que protege a todos los pares del cable contra el efecto de interferencia. Su costo es mayor que el UTP y usa el mismo tipo de conector RJ45, sin embargo su instalación es un poco más compleja que el UTP.

Figura 5.15.b. Cable FTP.

La pantalla del cable FTP debe estar aterrizada a tierra para que la pantalla funcione de forma correcta.

El cable STP cuenta con una pantalla por cada uno de los pares del cable, lo cual protege a los pares contra interferencias y contra el efecto de diafonía producido entre pares. Su costo

es mayor que el FTP y su instalación es más compleja. Este tipo de cable usa conectores RJ49.

Figura 5.15.c. Cable FTP

En ambos casos FTP y STP para que las pantallas funcionen correctamente deben estar aterrizadas a tierra.

- Cable coaxial: El cable coaxial cumple con el estándar ANSI 570-B para CATV (Community Antenna Television - Televisión por Cable) y sistemas de video.

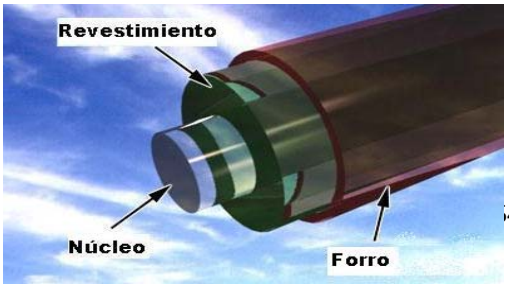
  Su ancho de banda depende del grosor del conductor central de cobre, con un desempeño superior a los 500 MHz

  Este cable consiste en un conductor central de cobre cubierto por un material aislante, seguido por una malla para blindar, una pantalla y finalmente por un recubrimiento.

  Su capacidad contra interferencias es muy superior a los cables de par trenzado, sin embargo es poco flexible, muy pesado, grueso, caro (dependiendo del BW) y su recubrimiento produce humos tóxicos.

  Este tipo de cable también es usado cuando se requiere hacer transferencia de información en lugares donde existen múltiples fuentes de interferencia (motores industriales o generadores eléctricos).

- Fibra óptica: Está hecha de un solo hilo de vidrio el cual está compuesto de dos partes: Núcleo (core) y revestimiento (cladding). Para transmitir la información se utiliza una emisión de luz, la cual es contenida dentro del núcleo y el revestimiento es la parte que refleja y confina la luz en el núcleo.



Para llevar a cabo la transmisión de información se requieren de equipos especiales para la emisión y recepción de la luz, el emisor (o

transmisor) se encarga de convertir las señales eléctricas del cable de cobre a impulsos de luz, y el receptor realiza el proceso inverso.

Su nomenclatura indica el diámetro del núcleo y revestimiento (núcleo/revestimiento), por ejemplo, una fibra óptica multimodo 50/125 indica que tiene 50 micrómetros en el diámetro del núcleo y 125 micrómetros de diámetro en el revestimiento.

Existen dos tipos de fibra óptica:

1) Multimodo: Disponible en 62.5/125, usa un LED como fuente de luz y 50/125, puede usar un diodo láser VCSEL como fuente de luz. Es usada como Backbone tanto dentro de los edificios y en el campus. De acuerdo a las normas del cableado estructurado, el límite de distancia es de 2 km para campus y 90 metros para horizontal, tiene un ancho de banda de 1 Gigahertz (1 GHz).

2) Monomodo: Tiene un núcleo de 8 a 9 micrómetros y revestimiento de 125. Es utilizada para grandes distancias y gran cantidad de envío de información, su límite de distancia es de 3 km para campus y 90 metros en horizontal, tiene un BW cercano a 300 GHz.

Nomenclatura de los medio de comunicación.

El cable de cobre y fibra óptica cuentan en su revestimiento con una leyenda la cual indica características como: fabricante, marca, tipo, longitud, etc. Las de mayor importancia son las siguientes:

- OF- Fibra Óptica (Optical fiber).
- N- No conductiva (Nonconductive): No contiene elementos metálicos.
- C- Conductiva (Conductive): Contiene elementos metálicos.
- P- Clasificación Plenum: Áreas con ambientes controlado (Ambiente con control de temperatura y humedad) y componentes resistentes al fuego y baja producción de humo.
- R- Clasificación Riser.
- G- General.

Por ejemplo una fibra óptica con la leyenda "OFNP" indica que es una fibra óptica Plenum no conductiva, la cuál es usada en ambientes en Plenum.

Por otro lado la leyenda OFCG, es una fibra óptica conductiva para usarse en propósitos generales, a excepción de Plenum, Riser y de espacios que necesiten ambientes libres de incendios.

La nomenclatura para cables de cobre es la siguiente:

- CM- Comunicaciones.
- MP- Multipropósito.
- P- Plenum.
- R-Riser.
- G-General.

Ejemplo: CMP, indica un cable de comunicaciones Plenum adecuado para usarse en ductos y Plenum. Tiene características de resistencia al fuego y baja producción de humo.

La leyenda CMR, indica cable de comunicaciones Riser adecuado para usarse en ductos verticales o de piso a piso, tiene la característica de resistencia al fuego y tiene la capacidad de prevenir la dispersión del fuego de un piso a otro.

VIII. Documentación

Después de la instalación del sistema de red, se debe hacer una documentación en la cual se describan los esquemas o diagramas de red de los edificios, el material utilizado, notas acerca de los registros, el etiquetado de los cables y las pruebas de campo (o pruebas de cables).

- Diagramas de red: Se deben realizar los planos donde se haga indicación de las instalaciones del edificio, ubicaciones de las terminaciones de telecomunicaciones, estructura de red y la nomenclatura usada para el etiquetado de las salidas de telecomunicaciones.

- El etiquetado: Se debe hacer un correcto etiquetado de los cables, paneles de parcheo y campos de terminación de cada área de trabajo (WA), con el fin de dar mantenimiento o realizar una reparación de forma rápida y fácil. El etiquetado puede ser mediante colores y/o un código personalizado el cual debe quedar detallado dentro de la documentación para futuros administradores y/o referencias.

  Prueba de campo: Al instalar un nuevo cable o reparar uno existente, la prueba del cable juega un rol muy importante[3], ya que las compañías u organizaciones invierten mucho dinero en equipos de telecomunicaciones muy complejos tratando de estar a la vanguardia tecnológica, sin considerar en la mayoría de las ocasiones, la infraestructura de red con la que se cuenta. El inverso del error anterior también puede suceder, contar con una infraestructura de red muy grande considerando el uso y/o aplicaciones utilizados. En cualquiera de los casos anteriores se tiene una pérdida de recursos y eficiencia de los equipos.

[3] http://www.flukenetworks.com/fnet/en-us/learnAbout/Cable+Testing.htm

Con el fin de asegurar que la infraestructura de red y el equipo de telecomunicaciones sea el adecuado, debe invertirse recursos primeramente en realizar un análisis para seleccionar el equipo apropiado a nuestras necesidades y que aproveche la red adecuadamente, también se recomienda realizar pruebas a la estructura de la red, las cuales tienen un alto costo en equipo y capacitación para realizarlas, por lo que debe considerarse contratar alguna empresas especializada que las lleve a cabo[4].

A continuación se mencionan las pruebas realizadas sobre cable de cobre (Sólo se mencionaran algunas ya que existes un gran numero).

- Mapa de cableado (Wire Map):

  Se verifican que la conexión de cada hilo sea correcta, es decir, se verifica la continuidad de cada hilo y que su configuración (correspondencia de cada hilo) sea la correcta.

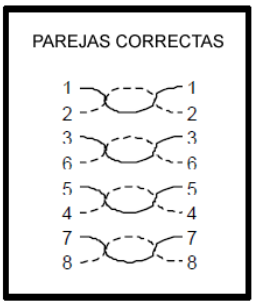


Figura 5.16.a. Prueba de WireMap correcta

Una mala conectividad puede ser:

- Reverse Pair: Un par de hilos esta invertido en un extremo del cable.
- Transposed Pairs: dos hilos están conectados en pares diferentes.
- Split Pairs: un par de hilos, físicamente está separado.

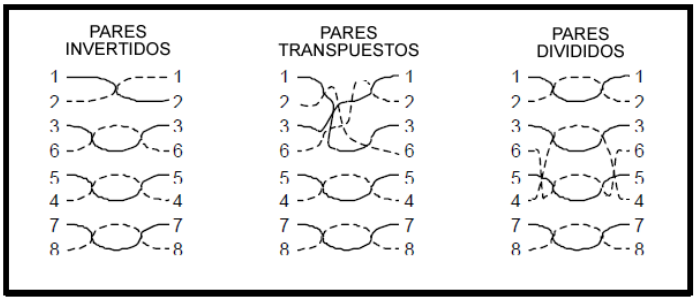


Figura 5.16.b. Pruebas de WireMap incorrectas.

[4] La empresa Fluke Network brinda este servicio, es una empresa reconocida internacionalmente para cableado estructurado.

En caso de que se utilice cable apantallado (cable FTP o STP), también se debe verificar la continuidad de la pantalla.

- Longitud (Length): El cableado debe ser medido para asegurarse que se está respetando los límites de distancia, para un canal es de 100 m. y para un enlace permanente es de 90 m.

  Un canal está constituido por el cableado horizontal, máximo un punto de consolidación, el cable de equipo del WA, las salidas de telecomunicaciones y dos conexiones en TR. La longitud de total de los cables de equipos, cables de parcheo dentro del canal no deben exceder los 10 m.

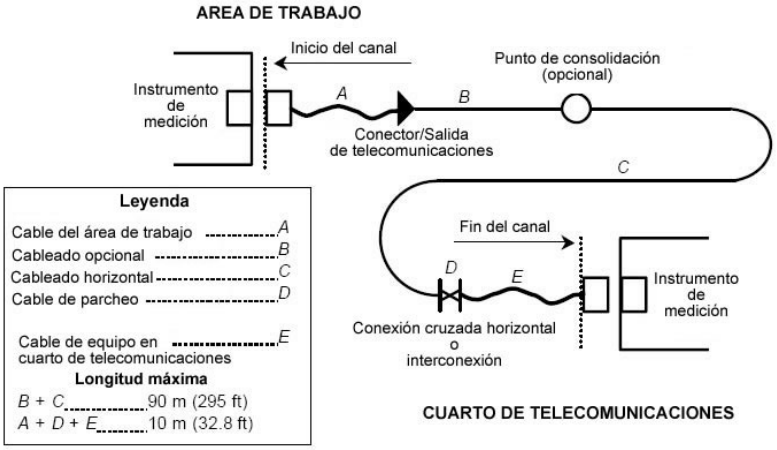


Figura 5.17.a. Canal

El enlace permanente consta del cableado horizontal (max. 90 metros) y una conexión en cada extremo del cableado, opcionalmente puede tener un punto de consolidación como máximo.

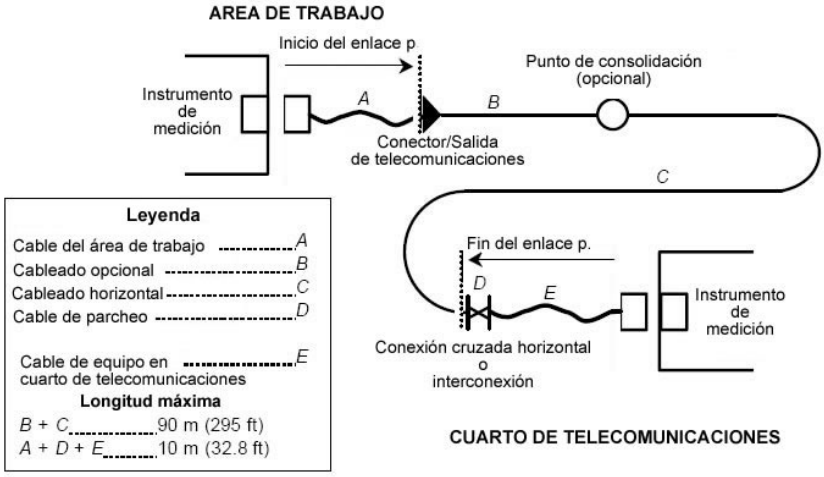


Figura 5.17.b. Enlace Permanente

Existen dos formas de obtener la distancia de un cableado:

- Física: se hace mediante las marcas de distancia en el revestimiento del cable.

- Eléctricamente: se realiza midiendo el retraso de la propagación de una señal, dicho retraso depende de la construcción y de las propiedades del material con el cual está fabricado.

La señal se propaga en cada par trenzado y se realizan los cálculos con aquel par que la señal haya obtenido el menor retraso. Lo anterior se debe a cada par esta trenzado de forma distinta y el par menos trenzado es el adecuado para hacer la estimación de la longitud real del cable.

o Pérdida de inserción o atenuación (Insertion loss): Las señales eléctricas transmitidas pierden un poco de su energía cuando viajan a lo largo de cable, siendo mayor ésta perdida en señales de frecuencia altas.

Esta prueba o medida puede aplicarse a canal o enlace permanente. En el caso de un canal, se debe medir la pérdida de 4 conectores, el enlace permanente, cables de equipo y cables de parcheo del área de trabajo. Para el caso de un enlace permanente se mide

la perdida en 3 conectores y el cable horizontal. La medición debe realizarse a 20 ºC, la temperatura es un factor que altera la pérdida de inserción.

- Perdida por diafonía (NEXT loss, Near-End Cross Talk): Se debe a una fracción de señal que aparece en el extremo cercano de un par adyacente.

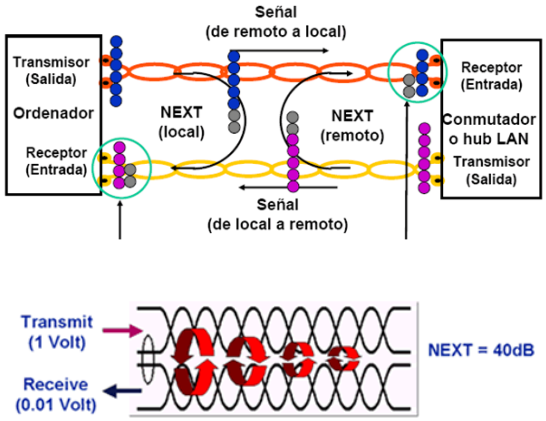


Figura 5.18. Prueba de NEXT loss.

Para la fibra óptica el único parámetro que se requiere medir es la atenuación, el ancho de banda y la dispersión son otras características muy importantes de la F.O., pero no son considerados en las pruebas de campo porque estas características no se ven afectadas durante la instalación.

El estándar ANSI TIA-EIA-568-B.2, trata a mayor detalle la forma de realizar las pruebas de cableado y la evaluación necesaria para decir si un cableado tiene el rendimiento mínimo aceptable para la transmisión de información.

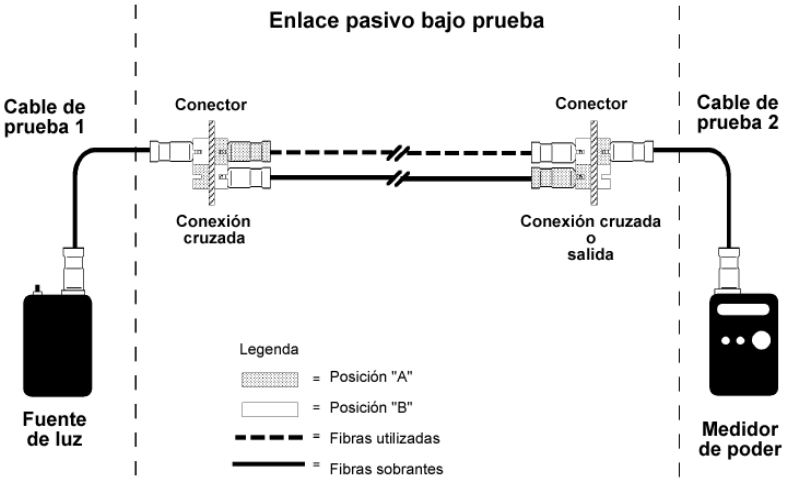


Figura 5.20. Enlace pasivo de fibra óptica.

IX. Esquema final de red

Aquí se muestra el esquema de un sistema de cableado estructurado obtenido de la documentación del estándar ANSI-TIA-EIA-568-B.1.

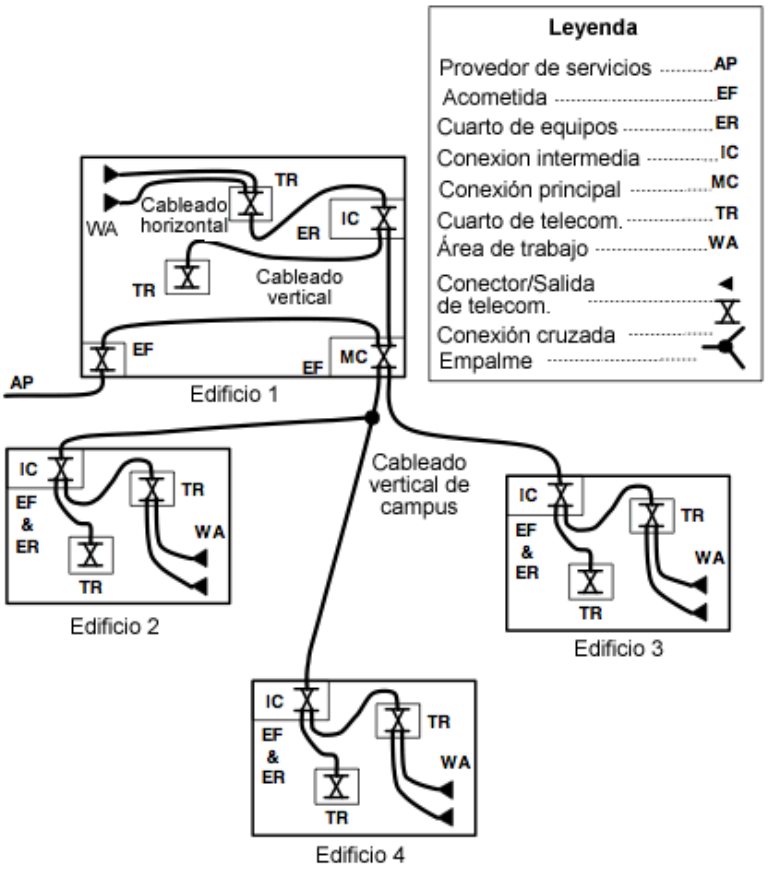


Figura 5.21. Diagrama de un típico sistema de cableado estructurado

Este esquema no hace referencia a que todos los sistemas de cableado estructurado deban estar de esta forma, solo es una representación de un caso típico.

Redes Inalámbricas (Wireless)

Un poco de historia

- 1979 unos ingenieros en Suiza publican sus resultados a sus experimentos de crear una red local en una fabrica a través de infrarrojos.
- 1985 la FCC (Federal Communications Comision – Comisión Federal de Comunicaciones) (Nota: FCC es una agencia del gobierno de Estados Unidos encarga de regular y administrar en materia de telecomunicaciones) asignó la IMS (banda para uso comercial sin licencia. Industrial, Scientific and Medical – Industria, Científica y Médica) 902-928 MHz, 2,400-2,4835 GHz; 5,725-5,850 GHz a las redes inalámbricas basadas en spread spectrum (Espectro Disperso).
- Entre 1986 – 1990 la asignación de la banda propicio una mayor actividad en la industria.
- En 1991 Se publicaron varios trabajos referentes a WLAN que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.
- 1997 Surge el primer estándar, el 802.11 el cual sienta las bases tecnológicas para el resto de la familia 802.11.
- 1998 Primeros sistemas de 11 Mb/s a 2,4 GHz. Preestándar 802.11b.
- 1999 Se publica el estándar 802.11b y el 802.11a.
- 2001 Primeros productos comerciales 802.11ª. Borrador 802.11e (QoS en WLANs)

- 2003 Es publicado el estándar 802.11g.
- 2006-2007 el nuevo estándar 802.11n.

Definición Wireless

Se denomina Wireless a las comunicaciones en la que no se utiliza un medio de propagación físico alguno, se utiliza modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión[5].

Wi-Fi (802.11: Wireless LAN Medium Access Control and Physical Layer Specifications)

Conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11 (especialmente la 802.11b), creado para redes locales inalámbricas, pero que también se utiliza para acceso a internet.

El término fue acuñado por la Wi-Fi Alliance[6]. Todo producto que ha sido probado y aprobado por la Wi-Fi Alliance lleva el texto "Wi-Fi Certified", lo que garantiza su interoperatibilidad.

El termino Wi-fi proviene de Wireless Fidelity (Fidelidad Inalámbrica), sin embargo el significado nada tiene que ver con la realidad, ya que la WECA contrato a una empresa publicitaria para que diera nombre a su estándar, de tal manera que fuera fácil de identificar y recordar.

Surgió para resolver el problema de compatibilidad que existía entre los productos de los principales fabricantes de soluciones inalámbricas. De esta forma, la marca WiFi asegura que el usuario tiene la garantía de que los equipos con sello WiFi pueden trabajar juntos sin problemas independientemente del fabricante de cada uno de ellos.

WiMax (802.16: BroadBandWireless Access Method and Physical Layer Specifications) (Este tema queda fuera del punto principal que es para centros de cómputo, por lo que sólo se mencionara la tecnología)

WIMAX (Worldwide Interoperability for Microwave Access - Interoperabilidad Mundial para Acceso por Microondas) es una coalición dedicada a la certificación de productos de acuerdo a la norma 802.16 de la IEEE, la cual es una especificación para redes metropolitanas inalámbricas

[5] http://es.wikipedia.org/wiki/Wi-Fi

[6] (nota*:Nokia y Symbol Technologies crearon en 1999 una asociación conocida como WECA (Wireless Ethernet Compatibility Alliance, Alianza de Compatibilidad Ethernet Inalámbrica). Esta asociación pasó a denominarse Wi-Fi Alliance en 2003. El objetivo de la misma fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos: http://es.wikipedia.org/wiki/Wi-Fi)

(WMAN) de banda ancha y alcanzaran conexiones de velocidades similares al ADSL o al cable módem y hasta una distancia de 50-60 km.

Tecnologías Wireless

No obstante a lo anterior no solo existe Wifi y WiMax como tecnologías Wireless, aquí una tabla con los estándares de las tecnologías ya mencionadas y algunas más:

Tecnología	Estándar	Uso	Capacidad de proceso	Alcance	Frecuencia
UWB	802.15.3a	WPAN	De 100 a 480 Mbps	Hasta 10 metros	7.5 GHz
Bluetooth	802.15.1	WPAN	Hasta 720 Kbps	Hasta 10 metros	2.4 GHz
Wi-fi*	802.11a	WLAN	Hasta 54 Mbps	Hasta 100 metros	5 GHz
Wi-fi*	802.11b	WLAN	Hasta 11 Mbps	Hasta 100 metros	2.4 GHz
Wi-fi*	802.11g	WLAN	Hasta 54 Mbps	Hasta 100 metros	2.4 GHz
Wi-fi*	802.11n	WLAN	100 – 540 Mbps	----------	5 GHz
WiMax*	802.16d	WMAN fija	Hasta 75 Mbps (20 MHz AB)	Aprox. de 6 a 10 Km.	Sub 11 GHz
WiMax*	802.16e	WWAN	Hasta 30 Mbps (10 MHz AB)	Aprox. de 1.5 a 5 Km.	De 2 a 6 GHz
Edge	2.5G	WWAN	Hasta 384 Kbps	Aprox. de 1.5 a 8 Km.	1900 MHz
CDMA2000/1x EV-DO	3G	WWAN	Hasta 2.4 Mbps (aprox. de 300 a 600 Kbps)	Aprox. de 1.5 a 8 Km.	400, 800, 900, 1700, 1800, 1900, 2100

					MHz
WCDMA/UMTS	3G		Hasta 2 Mbps (hasta 10 Mbps con tecnología HSDPA)	Aprox. de 1.5 a 8 Km.	1800, 1900, 2100 MHz

Tabla 5.1 Tecnologías inalámbricas

* La velocidad de transmisión decrece con la distancia, si hay varios ordenadores enviando o recibiendo datos al punto de acceso o Router a la vez y si existen obstáculos, entre el Acces Point y el cliente.

Ámbito de aplicación (campos de utilización)

Las aplicaciones más comunes de este tipo de redes son:

- Edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.
- En entornos cambiantes que necesitan una estructura de red flexible que se adapte a los cambios.
- Redes que permitan el acceso a la información mientras el usuario se encuentra en movimiento (no llegando a WMAN).
- Reuniones de grupos de trabajo eventuales, en cuyos casos no sea conveniente instalar una red cableada.*
- Ambientes de trabajo industriales con condiciones severas.
- Interconexión de redes de área local que se encuentren en distintos lugares físicos.*
- Aquellos lugares donde se quiera prestar un servicio a los usuarios (aeropuertos, hoteles, cafés, escuelas, etc.)*
- En un escenario residencial, donde se usa un router ADSL (Asymmetric Digital Subscriber Line - Línea de Suscripción Digital Asimétrica; consiste en una transmisión de datos digitales (la

transmisión es analógica) apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado)

** Nos interesan para nuestros fines.*

Ventajas

- Movilidad.- puedes tener acceso a la WLAN y/o internet en cualquier lugar (se debe tener cerca un Access Point)
- Costo.- El costo y el tiempo de instalación disminuyen ya que no es necesario realizar una.

Principales elementos que componen una red Wireless

Los elementos básicos para hacer una pequeña red Wireless son:

- Access Point (punto de acceso).- Equipo de conexión central entre la red cableada y los dispositivos inalámbricos. Un Access Point recibe y emite datos, tanto a través de la conexión Ethernet cableada como de forma inalámbrica.

Figura 5.22. Router inalámbrico

- Antenas.- Es un componente de suma importancia en un sistema RF (Radio Frecuencia). Convierte la onda guiada por la línea de transmisión (el cable o guía de onda) en ondas electromagnéticas que se pueden transmitir por el espacio libre. El tamaño de una antena depende de la frecuencia: a mayor frecuencia, menor tamaño. El tamaño mínimo a cualquier frecuencia es ½ de la longitud de onda.

Existen dos tipos de antenas: la omnidireccional y la direccional.

- Una antena omnidireccional (Figura 5.23a), envían y reciben información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. Sin embargo su alcance es poco (comparados con las direccionales). Puede comparase con una bombilla emitiendo luz en todas direcciones.

Figura 5.23a. Antenas omnidireccionales

Con este tipo de antena la tarjeta inalámbrica puede tener acceso a la red sin importar si la antena está apuntando hacia esta.

- Una antena direccional (Figura 5.23b), envían y reciben información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

Figura 5.23b Antena direccional

En redes 802.11 se usan normalmente antenas omnidireccionales en los extremos del enlace, aunque también es posible utilizar antenas direccionales cuando se desean cubrir distancias mayores.

- Tarjeta inalámbrica o adaptador de red inalámbrico.- es una expansión que constituye la conexión física entre un equipo y una red.

  Existen muchos tipos de adaptadores, entre ellos:

  - Las tarjetas PCMCIA para equipos portátiles (que son tarjetas que encajan en una ranura de su equipo, igual que cuando se instala una tarjeta de sonido o una tarjeta de módem)

Figura 5.24. Tarjeta de red inalámbrica PCMCIA.

  - Tarjetas integradas, algunos sistemas nuevos tienen un adaptador de red incorporado al sistema de la tarjeta madre.

  - Adaptadores USB, debido a las características propias del puerto USB, pueden ser usados indistintamente, ya sea en PCs de escritorio o portátiles.

Figura 5.25. Tarjeta de red inalámbrica USB.

- Las tarjetas PCI, si instalan en una ranura de expansión del equipo de escritorio (es necesario abrir el equipo de cómputo).

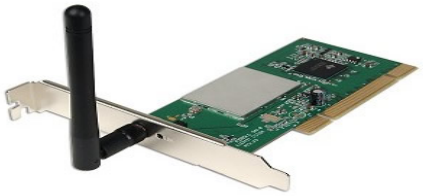


Figura 5.26. Tarjeta de red inalámbrica PCI

- Computadoras que tengan las tarjetas inalámbricas y posiblemente algún equipo para configurar el Access Point.

Estos son solo los elementos básicos más adelante se hablara de las características que deben tener de acuerdo a nuestros fines.

Qué debe considerarse para tener una red segura (véase capitulo 6)

Existen riesgos adicionales al tener este tipo de redes (Partimos de que ya consideramos los riesgos de una red cableada).

Las ondas de radio tienen en sí mismas la posibilidad de propagarse en todas las direcciones dentro de un rango relativamente amplio. Es por esto que es muy difícil mantener las transmisiones de radio dentro de un área limitada. La propagación radial también se da en tres dimensiones. Por lo tanto, las ondas pueden pasar de un piso a otro en un edificio (con un alto grado de atenuación).

La consecuencia principal de esta "propagación desmedida" de ondas radiales es que personas no autorizadas pueden escuchar la red, posiblemente más allá del confinamiento del edificio donde se ha establecido la red inalámbrica.

Topologías (aunque ya se hablaron de ellas aquí solo se tocaran algunos puntos importantes)

Existen 2 modos fundamentales para el estándar 802.11:

- Ad hoc (también llamada Peer to Peer – punto a punto).- Este método es para que los clientes inalámbricos puedan establecer una comunicación directa entre sí, es decir, los únicos

elementos requeridos son las terminales móviles (computadoras) equipados con los correspondientes adaptadores de red para comunicaciones inalámbricas.

Cada cliente inalámbrico en una red ad hoc debería configurar su adaptador inalámbrico en modo ad hoc y usar los mismos SSID y "número de canal" de la red. Aquí debe notarse que con este tipo de topología las computadoras solo se comunicarían entre ellas, por lo que no se tendría acceso a internet o cualquier otra computadora que no estuviera en la red ad hoc (En caso de querer conectar las computadoras a internet será necesario instalar una pasarela o Gateway especial).

- Infraestructura.- En este tipo de topología ya es necesario contar con uno o varios Access Point. Del mismo modo, como en las redes Ethernet, en las cuales se dispone de un Hub o concentrador para "unir" todos los host, en las conexiones inalámbricas se dispone de los Access Point, los cuales se encargan de comunicar los dispositivos inalámbricos que están dentro de su área de cobertura con la red Ethernet, una red de estas características, es formada con un mínimo de dos equipos, el máximo recomendado varía de acuerdo a las características del Access Point y al ancho de banda disponible, a mayor número de equipos conectados que estén usando la red, menor ancho de banda tendrá cada uno de ellos.

Roaming

Roaming se refiere a la capacidad de cambiar de un área de cobertura a otra sin interrupción en el servicio o pérdida en conectividad. Permite a los usuarios seguir utilizando sus servicios de red inalámbrica cuando viajan fuera de la zona geográfica en la que contrataron el servicio, por ejemplo, permite a los usuarios de teléfonos móviles seguir utilizando su móvil cuando viajan a otro país.

Análisis de requerimientos

Al instalar una red Wireless será necesario tomar en cuenta los siguientes aspectos:

Primeramente contar con el equipo que denominamos "Principales elementos que componen una red Wireless":

- Access Point: Para poder adquirir o conocer mejor el equipo con el que se cuenta se deben tener presentes sus especificaciones (omitiremos el nombre del equipo y dimensiones):
    - Soporta el estándar Wireless IEEE 802.11b, IEEE 802.11g: Como podemos observar soportar las especificaciones 802.11 de Wireless Wi-Fi en sus especificaciones b y n. Esto

es importante tomarlo en cuenta para la frecuencia, área de cobertura, uso tecnología que representa, todos estos puntos están concentrados en la tabla 5.1. Tome nota de que es un Access Point para Wi-Fi y con soporte de estándares b y n ya que las tarjetas Wireless del equipo que se quiera conectar deberá soportar tales estándares.

- Protocolo de gestión remota o administración SNMP, Telnet, HTTP: Lo cual nos indica cuales son las posibles formas de acceder al equipo para configurarlo. Normalmente la configuración se hace vía http.

- Rango de Cobertura: Especifica la cobertura que el servicio puede brindar.

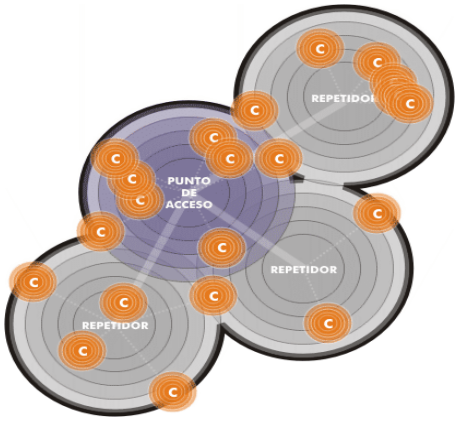


Figura 5.27. Cobertura de un Access Point

- Modos de Operación: Indica cómo puede funcionar. Existen 4 modos de operación:

  - Access Point, se utiliza el modo de conectarse a uno o varios clientes inalámbricos. Los clientes inalámbricos pueden comunicarse sólo a AP en modo punto de acceso.

  - Bridge PtP (puente Point-to-point), permite a los puntos de acceso para comunicarse con otro punto de acceso capaz de punto a punto puente. Sin embargo, ser conscientes de que la mayoría de los fabricantes utilizan los ajustes que permitan reducir al modo

en el punto de acceso. Un típico escenario de esta selección es conectar dos Routers en Mac a través de una conexión inalámbrica.

- Bridge PtMP (puente Punto-a-multi-punto) es la misma que la de punto a punto, sin embargo, este modo le permite utilizar más de dos puntos de acceso.

- AP Cliente (cliente inalámbrico), permite al Punto de Acceso a convertirse efectivamente en un cliente inalámbrico a otro AP. En esencia, la AP se ha convertido en una tarjeta de adaptador inalámbrico. Que se utiliza este modo para que el dispositivo se comunique con un AP. Tarjetas inalámbricas no se comunican con los puntos de acceso en la AP Cliente / Modo cliente inalámbrico.

o Antenas: Debe considerarse si se requiere una omnidireccional o bidireccional de acuerdo al área de cobertura que se requiera.

o Las tarjetas de red para cada unas de las computadoras que sea necesario conectar, considerando como ya se mencionó que manejen el mismo estándar que el Access Point.

o Equipo "especial" para configurar el Access Point, este equipo debe contar con una tarjeta de red.

➢ Tipo de red: Se clasifican de acuerdo al uso que se le dará:

o Empresarial.- Debe dar servicio a una empresa por lo que la seguridad debería ser muy estricta, podría cubrir varios edificios y presentaría servicios muy específicos.

o Hotspot.- Este tipo de red son aquellas que prestan el servicio de internet (ISP - Internet Service Provider – Proveedor de Servicios de Internet). Normalmente implementan DHCP (Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Anfitrión) a fin de que sea más sencillo el acceso para los usuarios. Este tipo de red son las que proveen en los hoteles, restaurantes y lugares públicos.

o Red en una pequeña oficina o una casa.- Una red con estas características no necesitara una gran infraestructura y la seguridad que necesite será básica.

➢ Área de cobertura: Aquí debemos considerar el área que se pretende cubrir tomando en cuenta los obstáculos que se presenten y puedan atenuar la señal, además de las fuentes de

interferencia presenten en el ambiente como pueden ser microondas, pantallas, otras redes cercanas, etc.

Considérese la siguiente tabla para valorar la atenuación de la señal producida por diferentes materiales:

Material del Obstáculo	Atenuación producida
Madera	Baja
Plástico	Baja
Materiales sintéticos	Baja
Cristal	Baja
Cuerpo humano	Media
Ladrillos	Media
Mármol	Media
Agua	Media
Cerámica	Alta
Papel	Alta
Cemento	Alta
Cristal a prueba de balas	Alta
Metales	Muy alta

Tabla 5.2. Atenuación de la señal por distintos materiales.

En caso de tener más de una antena se debe pensar en el Roaming por lo tanto el área de cobertura de las antenas deben traslaparse un poco y así tener acceso sin interrupciones al pasar de la cobertura de una antena a la otra.

Como resultará para estos momentos bastante obvio el área de cobertura también debe considerar las antenas que tendrá el Access Point.

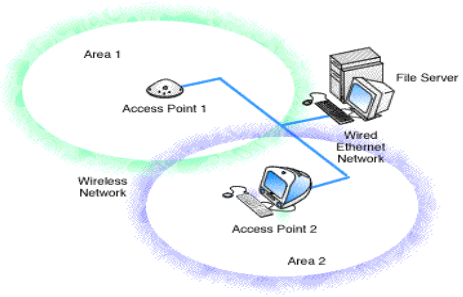


Figura 5.28. Conexión Wireless.

- Tipos de usuarios:
  - Estáticos.- serán aquellos que tendrán las características para conectarse a la red inalámbrica, sin embargo no se moverán, por ejemplo, computadoras de escritorio.
  - Iterantes (Roaming).- Son Aquellos que estarán en movimiento como Laptos, Palms, celulares y todos aquellos que los que se requiera prestar servicio. (Los equipos deberán cubrir requisitos de conexión, como son soportar acceso Wi-Fi).

- Cantidad de usuarios a los que se prestara el servicio.- Es importante considerar cuantos usuarios usaran el servicio, primeramente para adquirir el hardware necesario y con la capacidad suficiente (El equipo tiene un número de usuarios al que puede dar servicio) y en segundo lugar se debe considerar el ancho de banda proporcionado, ya que a mayor cantidad de usuarios, menor ancho de banda tendrá cada uno de ellos.

Bibliografía

douglascomputer.es.tl/Historia_Wifi.htm

http://www.masadelante.com/faq-roaming.htm

http://www.air-stream.org.au/wireless_bridge, modos de operación.

Capítulo 6 - Seguridad informática

La seguridad informática consiste en asegurar que los recursos informáticos de la institución estén disponibles y sean utilizados en los propósitos para los que fueron creados dentro del marco previsto.

Está basada en algunas directrices que de acuerdo a los autores cambian un poco, aquí consideraremos las siguientes:

- Confidencialidad.- La información sea visualizada de forma correcta solo para los usuarios adecuados y sea ininteligible para aquellos individuos que no estén involucrados.
- Integridad.- Garantizar que los datos sean los que se supone que son y que no hayan sido alterados de alguna forma.
- Disponibilidad.- Garantizar que los servicios y/o información esté disponible para los usuarios cuando estos los requieran.
- Autenticación.- asegurar que sólo los individuos autorizados tengan acceso a los recursos. Esto normalmente se hace con contraseñas.

Seguir las directrices anteriores no es sencillo, pues se puede caer en el extremo de querer un sistema 100% seguro, el cual no existe, la seguridad informática no se trata de tener un sistema con estas características, consiste en reducir las vulnerabilidades al mínimo posible.

Pero... ¿Qué debemos proteger?, ¿De quién nos queremos proteger?, ¿Con qué nos protegemos? Con estas preguntas y las directrices anteriores se puede comenzar a plantear y desarrollar una seguridad a la medida de nuestras necesidades.

¿Qué debemos proteger?

Los activos del centro de cómputo. Y por activos se entiende aquellos recursos necesarios para que el centro funcione correctamente y alcance los objetivos propuestos: hardware, software e información. El primero lleva una seguridad física y los restantes a una seguridad lógica (aunque hay sus excepciones, por ejemplo, un firewall es para proteger el software y datos, pero existen firewall de hardware y software). De estos tres el más importante es la información, ya que la pérdida de hardware y software se puede recuperar con dinero y tiempo, pero la información debe considerarse como invaluable.

¿De quién nos queremos proteger?

De aquellas personas o eventos que amenacen (amenaza: evento o individuo que representa un riesgo para el centro y que puede producir daños y/o perdidas) los activos, lo que también podría verse como transgredir alguna de las directrices.

¿Con qué nos protegemos?

Esta pregunta tiene respuestas muy especificas por ejemplo: ¿Con que protejo mis datos que viajan en un formulario?, con un canal seguro como https. Como estas hay millones de preguntas y algunas de ellas se contestarán a lo largo de este capítulo, sin embargo, hay medidas que pueden considerarse como generales, como son tener buenas políticas de seguridad y concienciar a los usuarios acerca de los problemas de seguridad.

¿Cómo protegernos?

La mejor manera de hacerlo es tener un enfoque global del centro de cómputo y la seguridad, tener claro que lo que debemos cuidar son los activos y aun a estos darles prioridades, determinar cuáles son los servicios críticos que pueden influir en el servicio del centro de cómputo.

Políticas

Comenzaremos con las políticas que son acciones generales de un modo bastante abstracto que indica que está y que no está permitido en la operación general del centro de cómputo. Por ejemplo:

"Cambiar contraseñas de los servidores periódicamente"

Es claro que el propósito es proteger la información que se localice en los servidores, sin embargo, no dice como debe cambiarse, es decir, no especifica que debe tener caracteres alfanuméricos y debe tener también números y algún signo como "." (Punto) o "_" (guión) o bien especifica alguna expresión regular, longitud mínima de la contraseña, etc.

Como este tipo de políticas pueden (o mejor aún deben) hacerse también sobre acceso a lugares físicos, horarios, uso de las instalaciones, etc. Todas aquellas que prevean el posible uso que deberá dársele a las instalaciones. (Más información al respecto véase el capitulo 11).

Firewall

Un firewall es un programa (firewall de software) o bien dispositivo especializado (firewall de hardware) que ayuda a proteger el equipo de intrusos típicamente de internet, pero también funciona dentro de una red privada, que podrían intentar eliminar información, hacer que deje de funcionar o hasta robar información personal, como contraseñas ó números de tarjeta de crédito.

Todas las comunicaciones de Internet se realizan mediante el intercambio de paquetes de información, que son la unidad mínima de datos transmitida por la red. Para que cada paquete pueda llegar a su destino, independientemente de donde se encuentren las máquinas que se

comunican, debe llevar anexada la información referente a la dirección IP de cada máquina en comunicación, así como el puerto a través del que se comunican.

Un firewall constituye una especie de barrera delante de nuestro equipo, esta barrera examina todos y cada uno de los paquetes de información que tratan de atravesarlo. En función de reglas previamente establecidas, el firewall decide qué paquetes deben pasar y cuáles deben ser bloqueados. Un firewall puede controlar todas las comunicaciones de un sistema a través de la red. El firewall analiza cada paquete que fluye a través del mismo, puede decidir si lo deja pasar en uno u otro sentido, y puede decidir si las peticiones de conexión a determinados puertos deben responderse o no.

Los firewalls también se caracterizan por su capacidad para mantener un registro detallado de todo el tráfico e intentos de conexión que se producen (lo que se conoce como un log). Estudiando los registros o logs es posible determinar los orígenes de posibles ataques y descubrir patrones de comunicación que identifican ciertos programas maliciosos. Sólo los usuarios con privilegios administrativos pueden acceder a estos registros, pero es una característica que se le puede exigir a estas aplicaciones.

Documentar y proteger

Si alguien intenta atacar los equipos del centro de computo (típicamente los servidores, sin embargo, los equipos de los usuarios no quedan exentos) normalmente intentará saber que aplicaciones están ejecutándose, porqué puerto, que versión, etc. Para esto es importante modificar las configuraciones por defecto de las aplicaciones. A continuación se verán algunos ejemplos de vulnerabilidades y una solución, recuerde que un ataque se hace sobre una vulnerabilidad detectada:

- El comando nmap (comando nativo de sistemas Unix, compatible con sistemas Windows) hace un escaneo de los puertos, los servicios corriendo en el equipo y permite obtener información acerca del sistema operativo que está en ejecución.

  tesis@unam:~$ nmap localhost

  Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2009-08-13 13:21 CDT

  Interesting ports on localhost (127.0.0.1):

  Not shown: 1670 closed ports

  PORT STATE SERVICE

22/tcp open ssh

25/tcp open smtp

80/tcp open http

111/tcp open rpcbind

113/tcp open auth

631/tcp open ipp

657/tcp open unknown

3306/tcp open mysql

5432/tcp open postgres

8080/tcp open http-proxy

Ejemplo de nmap para detectar el sistema operativo

Diagrama 8.1. Resultados al ejecutar de nmap sobre equipo MacOS.

Solución propuesta: dejar abierto los puertos estrictamente necesarios.

- Conocer la versión de apache puede dar pauta a los atacantes para buscar una vulnerabilidad en la versión.

  Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny2 with Suhosin-Patch mod_python/3.3.1 Python/2.5.2 mod_perl/2.0.4 Perl/v5.10.0 Server at localhost Port 80

Solución propuesta:

Al instalar apache puede cambiarse los siguientes archivos:

Httpd-2.0.59/include/app_release.h

#define AP_SERVER_BASEVENDOR “Apache Sofrware Foundation”

#degine AP_SERVER_BASEPRODUCT “Apache”

Podría cambiarse por:

#define AP_SERVER_BASEVENDOR “Microsoft Corp.”

#degine AP_SERVER_BASEPRODUCT “Microsoft-IIS”

Httpd-2.0.59/os/unix/os.h

#define PLATFORM “Unix”

Podría cambiarse por:

#define PLATFORM “Win 32”

Aquí también puede añadirse nunca dejar en un servidor algún archivo con el “phpinfo”[1] ya que provee de mucha información.

- Típicamente el servidor de base de datos Postgresql corre por el puerto 5432 y tiene una base de datos llamada template1. Si no se ponen contraseñas o se permite el acceso estrictamente de algunas direcciones IP cualquier persona puede entrar a consultar la información de la base de datos.

  psql -h localhost -U usuario template1

  template1=#

  Solución propuesta:

  Modificar el archivo postgres/data/pg_htba.conf

[1] El archivo phpinfo es un archivo php que tiene la instrucción phpinfo(); la cual provee de información como: sistema operativo, archivos de configuración, extensiones, etc.

Host base usuario ip/32 métodoDeAutenticación

Donde:

Base: es el nombre de la base de datos a la que se va a conectar

Usuario: es el usuario al que se le permitirá el acceso

Ip: es la dirección Ip de donde se intentara conectar

métodoDeAutenticación:

Los anteriores son solo ejemplos de debilidades en la seguridad, estamos en riesgo ya que estamos dando información a los posibles atacantes.

Algunas técnicas de ataques

Una de las mejores formas de conocer las debilidades de nuestro centro de computo es conocer formas de ataques, de esta manera podremos realizar auto-ataques y/o detectar las vulnerabilidades.

- SQL injection.- En algunos casos (actualmente muchos, el contenido de internet ya no estático, se crea continuamente) los sitios web contiene información que proviene de una base de datos, por lo que la información que se mostrará debe ser solicitada de acuerdo a una o varias variables, que pueden enviarse en la URL:

  Http://sitio/calificaciones?alumno=javier [2]

  Con esta URL es posible armar la consulta a base de datos de la siguiente forma:

  String obtener variable alumno=alumno

  select calificacion from calificaciones where usuario='alumno'

  Fácilmente se podría modificar la URL para que la consulta fuera:

  select calificacion from calificaciones where usuario='alumno' or 1=1

  ¿y que se obtendría?...

  ¡TODAS las calificaciones!

[2] La palabra alumno hace referencia a javier, sin embargo no se puso código para que no estuviera atado a algún lenguaje de programación.

- Exploit.- Es un programa o técnica que aprovecha una vulnerabilidad.

- Negación de servicios (ataque DoS - Denial of Service).- Es un ataque cuyo objetivo es degradar total o parcialmente los servicios prestados a sus usuarios legítimos. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "de negación", pues hace que el servidor no dé abasto a la cantidad de usuarios.

  Una variante de este ataque es el DDoS (de negación de servicio distribuida - Distributed Denial of Service) el cual se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos.

- Programas maliciosos o código malicioso (Malware - Malicious software).- Programa o código de computadora cuya función es dañar o causar un mal funcionamiento de un sistema. (véase capitulo 9, virus y antivirus).

- DNS Poison (Envenenamiento de DNS – Domain Name Service).- Todas las computadoras conectadas se comunican entre ellas por su dirección IP. Cuando se escribe en el navegador www.google.com, nuestra computadora pedirá a nuestro servidor-DNS (el que seguramente nos proporciona el ISP) la dirección IP de www.google.com, éste al no saber cuál es la IP (no almacenan todas las direcciones IP de todos los dominios, sin embargo, si tiene algunas direcciones en su cache), "leerá" la configuración de www.google.com y de allí obtendrá cual es el servidor-DNS responsable de dicho dominio. Contactará a dicho servidor y le preguntará cual es la IP de www.google.com, al recibir respuesta nos conectaremos directamente a la IP.

  Para realizar esto es necesario tener un dominio www.tesis.com configurarlo para que su autoridad sea un DNS que también proporcionará el atacante y tener este DNS configurado como autoridad del dominio (este DNS se denominará DNS-Atacante).

  De este modo cuando la persona realice la consulta de www.tesis.com preguntará a su DNS-victima cual es la IP, si no la sabe, deberá buscar al DNS que la tenga, el cual es el DNS-atacante. Cuando su DNS-victima pregunte al DNS-atacante, este responderá la IP correspondiente de www.tesis.com y cualquier otro dominio que se haya configurado. Debido

a que DNS-atacante es autoridad[3], DNS-victima aceptara TODOS los dominios que responda, por ejemplo podremos responder uno nuevo para yahoo o google. Estos dominios se guardaran en cache para que el acceso sea más rápido.

- Ingeniería social.- En un ataque basado en el engaño hacia los usuarios (el Phishing está basado en ingeniería social), se trata de engañar al usuario para que éste realice ciertas acciones donde el usuario creerá que está haciendo un uso adecuado, pero en realidad está realizando lo que el atacante quiere que haga (normalmente algo indebido) y se generará una vulnerabilidad, casos típicos de Ingeniería Social (aplicado en la informática) son:

  - Enviar correo electrónico pidiendo datos personales y de la misma cuenta de correo haciéndose pasar por una institución de prestigio.

  - Anuncios publicitarios engañosos (típicamente anuncian que "es el visitante X y ha ganado un premio").

  - Mensajes en la computadora (en el fondo de pantalla o ventanas emergentes) de que el equipo se encuentra en riesgo y necesita instalar un antivirus para poder desinfectarlo.

  - Páginas Web fraudulentas - Phishing.- Es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, en general cualquier dato para luego ser usados de forma fraudulenta. Consiste en suplantar la imagen de una empresa o entidad pública, de esta forma hacen "creer" a la posible víctima, que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es. Puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica (estas formas de realizar la estafa quedan fuera del ámbito del documento, por lo que solamente se mencionaran), una web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico.

- MIM (Man in the middle).- Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

[3] Se denomina DNS autoritario a los servidores que tienen "permiso" para resolver directamente (sin preguntarle a otro servidor-dns) determinado dominio. Cuando un DNS, para fines prácticos lo denominaremos DNS1, pregunta a otro DNS, DNS2, alguna dirección IP, DNS2 devolverá la dirección que le pregunto, además de muchos otros dominios del cual él es DNS autoritario, quedando así en la cache del DNS1.

Primeramente debe saberse que cuando se envían mensajes en internet las computadoras tienen tablas que relacionan la dirección IP con la dirección MAC.

Dirección IP	Dirección MAC
192.168.67.10	00-21-63-BF-A2-BB

Diagrama 8.2. Tabla ARP.

Funcionamiento correcto:

Cuando quiere mandarse un mensaje y no se conoce la dirección MAC, el emisor envía un ARP-request y el destinatario responde con su dirección MAC (ARP-replay), generando así la tabla antes mencionada.

Funcionamiento incorrecto:

Un equipo envía ARP-replay (respuesta de IP y dirección MAC) con datos incorrectos. Véase en el diagrama 8.3:

Computadora1		Tabla ARP
IP	192.168.1.1	
MAC	XX:XX:XX:XX:XX:01	

Computadora2		Tabla ARP
IP	192.168.1.2	
MAC	XX:XX:XX:XX:XX:02	

Computadora3		Tabla ARP
IP	192.168.1.3	
MAC	XX:XX:XX:XX:XX:03	

Diagrama 8.3. Tablas ARP (antes del ARP-replay).

La Computadora1 quiere enviar un mensaje a la Computadora3, como no sabe la dirección MAC envía un ARP-request, sin embargo, quien responde es la Computadora2, quedando las tablas como se muestra en el diagrama 8.4:

Computadora1		Tabla ARP
IP	192.168.1.1	IP:192.168.1.1 MAC: XX:XX:XX:XX:XX:02
MAC	XX:XX:XX:XX:XX:01	

Computadora2		Tabla ARP
IP	192.168.1.2	
MAC	XX:XX:XX:XX:XX:02	

Diagrama 8.4. Tablas ARP (después del ARP-replay).

Con este cambio y debido a que los switches normalmente trabajan a nivel MAC, se ha redireccionado el trafico, ahora cuando la computadora1 quiera mandar un mensaje a la computadora3, realmente lo enviara a la computadora2.

Con esto se ha llevado a cabo el ataque, sin embargo, para no levantar sospecha la computadora2 re-direcciona lo que reciba a su destinatario original (computadora3).

- Ataques por fuerza bruta y diccionario.- En el ataque de fuerza bruta se intenta recuperar una clave probando todas las combinaciones posibles hasta encontrar la correcta.

  El ataque por diccionario es similar a la de fuerza bruta, solo que en esta se prueban palabras de un diccionario (Conjunto de palabras típicamente usadas como contraseñas). Este ataque se basa es que los usuarios normalmente usan palabras en su idioma para que sean fáciles de recordar.

Cómo implementar una política de seguridad

Los mecanismos de seguridad pueden causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece, ocasionando que estos mecanismos no sean llevados a cabo o se tienda a hacer “excepciones” lo que acrecentara las vulnerabilidades del centro. Por lo tanto la seguridad informática debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

La implementación, es un proceso Técnico-Administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria. En este sentido, los administradores son los encargados de definir los derechos de acceso a sus superiores.

El documento de las políticas debe ser firmado por la persona que tenga el cargo más alto en la organización. Solamente de esa manera tendrá suficiente autoridad para ser obligatorio para cualquiera (incluyendo a esta persona). Si en algún momento se dan concesiones a un usuario con

cierto rango, lo único que se lograra será tener un hueco en las políticas. Y una vez abierto ese hueco, seguramente habrá más concesiones. Es de suma importancia recordar que todo lo que especifica el documento es obligatorio para todo usuario y eso también cubre al **administrador**. No por ser técnicamente capaz de brincarse el monitoreo o las restricciones significa que tengan autoridad para hacerlo: **Las políticas de la red aplican a cada uno sus usuarios**.

Ahora, no basta con que se elabore dicho documento y lo firme el director, los usuarios de la red tienen que manifestarse enterados con esta normatividad. Solo así se podrán aplicar las sanciones correspondientes a quien no lo respete.

Políticas y procedimientos

Los procedimientos en contraposición a las políticas son documentos bastante largos y detallados que explican a detalle cómo se va a implementar cada uno de los puntos de las políticas.

Los procedimientos deben presentar una estructura similar a la de las políticas, y cada uno de sus puntos debe servir de explicación a su contra parte en las políticas. Al ser un documento derivado, el personal operativo (el administrador normalmente) puede adecuar el documento de procedimientos sin pasar por todo el proceso burocrático que significaría modificar las políticas.

Sistemas de detección de intrusos (IDS - Intrusion Detection System)

Un SDI o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.

Los SDI pueden buscar patrones de ataques también conocidos como basados en firmas o comportamientos sospechoso, como puede ser el escaneo de puertos, etc.

El SDI tiene como función principal alertar al administrador o personal de seguridad para que tome acciones al respecto. Otras implementaciones más complejas son capaces de ir más allá de la notificación de un posible ataque, es decir pueden ejecutar acciones automáticas que impidan el desarrollo de éste.

Tipos de SDI

- HIDS (Host IDS): Estos hacen caso omiso del contenido de los paquetes de red, enfocan su análisis a los datos del sistema: bitácoras, registros de auditorías, estado del sistema, monitoreo del uso de recursos, etc.

  Para realizar la revisión de las bitácoras puede hacerse “a mano” (claro con ayuda de algunas utilerías propias del sistema) o bien con aplicaciones cuya función es esta.

¿Qué puede revisar un HIDS?

- Existencia de archivos con nombres raros, como aquellos que comiencen con "." nombres que son usados para esconder estos archivos.
- Archivos SETUID (con permisos para asumir la identidad de otro usuario).
- Servicios de red inesperados.
- Entradas nuevas en cron/at[4] y verificar que estos archivos no tengan permiso de escritura.
- Nuevas cuentas o sin contraseña.
- Binarios cuyo checksum o MD5 (suma de verificación, medida muy simple para proteger la integridad de datos, verificando que no hayan sido corruptos) no corresponden al del paquete[5].
- Revisión de bitácoras.
- Relaciones de confianza con otros sistemas.
- Entradas de usuarios, especialmente desde host u horas poco comunes.
- Examinar el archivo /etc/passwd, en busca de alteraciones en las cuentas de los usuarios.

A revisar bitácoras

El monitoreo de procesos del sistema lo podemos llevar a cabo con utilerías propias del sistema. Estas herramientas las podemos combinar con scripts personalizados y crones que nos ayuden a automatizar esta labor (claro como se verá posteriormente hay algunas herramientas que pueden hacer esto y no será necesario crear ningún script.)

[4] Cron es un administrador de procesos en segundo plano que ejecuta trabajos a intervalos regulares. Cron se utiliza para automatizar tareas que hay que realizar periódicamente. Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el archivo crontab del usuario que ejecutara los procesos. At es un comando que se encarga de ejecutar tareas a una hora determinada.

[5] Es una función hash muy utilizada en las descargas de archivos de Internet para asegurarse de que el archivo no se ha alterado, ya sea de manera intencionada (virus o troyanos introducidos en el software por un usuario malicioso) o por una descarga incompleta o corrupta. Para calcularse se utiliza el comando md5sum en Linux $ md5sum y obtener una cadena que podremos verificar "manualmente" o bien se usa el comando $md5sum –c archivo, donde archivo es un documento de texto que contiene el nombre de archivo y el m5d para cada archivo.

- NIDS (Net IDS): Un SDI basado en red, detecta ataques a todo el segmento de la red. Protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque. Debido a que el análisis se realiza en tiempo real sobre los paquetes, es posible que reaccione en el momento que se está llevando el ataque, como puede observarse detecta un comportamiento hostil, pero no puede indicar si un ataque fue exitoso o no, solamente nos reporta el hecho de que el ataque ocurrió.

  Nótese que un NIDS resulta inútil cuando el tráfico de red va sobre un canal cifrado.

  Snort es un pequeño sistema de detección de intrusos capaz de realizar el análisis de tráfico en tiempo real y el análisis de los paquetes en redes IP. Puede realizar un análisis del protocolo, realizando búsquedas. Utiliza un flexible lenguaje de reglas para describir el tráfico. Tiene 3 usos principales:

  - Programa Sniffer.
  - Programa de análisis (lleva a cabo el análisis del tráfico de red).
  - Sistema detección de intrusos.

Borrar o suspender una cuenta de un usuario (Para sistemas Linux)

Para eliminar la cuenta de un usuario debe hacerse lo siguiente:

- Comunicar al usuario que se dará de baja la clave. Preguntar al usuario si ya realizo respaldos y en caso contrario, darle un límite de tiempo.
- De acuerdo con las políticas del sitio, respaldar la información del usuario.
- Verificar que el usuario no tenga activado un mecanismo de confianza para acceso remoto: rhosts, shosts, authorized_keys.
- Matar cualquier proceso del usuario.
- Revisar que no haya dejado trabajos calendarizados con at o cron: crontab –l –v login
- Darlo de baja de cualquier otro servicio como mail, impresión, etc.
- Realizar una búsqueda de sus archivos.
- Borrar su directorio HOME (No aplicable para la suspensión de cuenta).

Conclusiones seguridad Lógica

El mayor problema con este tipo de seguridad en un centro de cómputo es el desconocimiento de los usuarios para la toma de medidas de seguridad, esto no hace referencia a una capacitación técnica, si no a hacer entender al usuario como se dan los riesgos de seguridad de informática y cómo prevenirlos. Una solución a lo anterior podría ser pláticas masivas a los usuarios, envió de correos, asesorías, pegando carteles o posters llamativos en la entrada del centro de cómputo, etc., a fin de concientizar a los usuarios.

Debe también enseñársele al usuario buenas prácticas de seguridad que no solo servirán en el centro de cómputo si no que podrán (o deberán) realizar al usar cualquier equipo como son:

- No abrir archivos de extraña procedencia.- Un buen número de malware se propaga a través del correo electrónico como documentos adjuntos, por lo que no es recomendable abrir archivos con extensiones: .exe, .vbs, .bat por mencionar algunos.

- Revisar cualquier archivo en busca de malware.- El malware puede incluirse en prácticamente cualquier archivo (claro pueden ser archivos "disfrazados") por lo que siempre debe analizarse los archivos antes de abrirlos con el antivirus instalado.

- Establecer una contraseña compleja para cualquier servicio.- Debido a que en internet es común encontrar usuarios maliciosos que su objetivo principal es descifrar contraseñas para tener acceso a tu equipo y hacer mal uso de él o causarle problemas es importante contraseñas que cuenten como mínimo ocho caracteres, combinando letras mayúsculas, letras minúsculas, signos de puntuación y números, de esta forma será muy complicado encontrarla por esos usuarios.

Es importante también no revelar ninguna contraseña a otro usuario ya que este puede ser menos precavido que tu o hacer mal uso de ella.

Seguridad Física

La Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware, medios de almacenamiento de datos y a los propios usuarios.

Control de acceso físico

Si una persona no autorizada tiene acceso físico a un equipo de cómputo, éste puede estar en grave riesgo. Para asegurar la integridad y confidencialidad de la información, el acceso físico es un

elemento importante; sin embargo, las herramientas de software no ayudan a prevenir el robo parcial o total de una computadora ni la instalación de hardware no autorizado.

Por lo anterior es conveniente contar con servicio de vigilancia, el cual permitirá o negará el acceso a las personas. Debido a que uno de los propósitos del centro de cómputo es brindar servicios de préstamos de equipo (en general aquí los usuarios tienen acceso a los equipos) dividiremos las áreas en dos secciones:

- Sección para el usuario final: Área de trabajo (espacio físico destinado al usuario final). Aquí podrá tener acceso aquellas personas que requieran el servicio. Es importante tener un registro de las personas que pueden acceder, es decir, aquellas que por alguna razón (estudiantes primordialmente, pero también pueden ser profesores o personal administrativo) pueden hacer uso de las instalaciones.

- Sección para personal autorizado: Área con equipos que prestan un servicio o que son importantes para el funcionamiento del centro, como lo son la acometida, la sala de equipos y el cuarto de telecomunicaciones. (véase capitulo 5 para mayor información de cableado estructurado.)

  A esta sección solo tendrá acceso el personal autorizado (típicamente administradores) y puede estar protegido con algunas cerraduras especiales como lectores de huellas digitales, etc.

Seguridad contra siniestros

Es importante considerar en la seguridad física los siniestros que puedan ocurrir en el centro y hacer especial énfasis en los que se consideren más probables de ocurrir, por ejemplo: si el centro de cómputo se encuentra en un segundo piso, valdría la pena dejar como segunda prioridad inundaciones y acentuar la seguridad ante incendios, por mencionar un siniestro. Lo anterior es para canalizar el presupuesto en las áreas más vulnerables, lo cual no significa que no se tenga un plan de seguridad ante inundaciones (continuando con el ejemplo anterior).

El siniestro que normalmente se prevé (o cuando menos se tienen a la vista extintores) son los *incendios*. Los cuales son causados por un gran número de circunstancias (manejo inadecuado de combustibles, rayos, etc.), debido a que los componentes del centro de cómputo es equipo eléctrico, la principal causa por la que ocurriría un incendio seria instalaciones eléctricas defectuosas.

Existen diferentes tipos de fuego de acuerdo a lo que se esté consumiendo y para cada uno de ellos debe utilizarse diferentes formas de contrarrestarlo.

Clase *	Ocasionado por	Forma adecuada de contrarrestarlo
A	Combustibles sólidos ordinarios	Agua presurizada

	que producen brasas en su combustión, como la madera, papel, textiles, cartón, etc.	Espuma Extinguidores de químico seco de uso múltiple
B	Combustibles líquidos como gasolina, aceites, petróleo, disolventes, derivados del petróleo, etc.	Dióxido de Carbono Químico seco común Extinguidores de uso múltiple de químico seco Halon
C	**Instalaciones y equipos eléctricos cuando están bajo tensión.**	**Dióxido de Carbono** **Químico seco común** **Extinguidores de fuego de halon** **Químico seco de uso múltiple**
D	Fuegos de metales químicamente muy activos (sodio, magnesio, potasio, etcétera), capaces de desplazar el hidrógeno del agua u otros componentes, originando explosiones por la combustión de éste.	Agentes extinguidores de polvo seco Extinguidores de dióxido de Carbono de halon

Tabla 6.1 Tipos de fuego.

* Las clases son: A: de ignición lenta, B: de ignición rápida, C, D: de ignición violenta.

Debemos prestar suma importancia a los fuegos de tipo C que son los que no interesan para nuestro caso.

Los extintores deben tener etiquetas en las que se describen las instrucciones de uso y el tipo de fuego para el que están diseñados, así como la fecha de revisión o de caducidad.

Sugerencias para prevenir o reducir los daños de los incendios:

- Verificar que la instalación eléctrica se encuentre en buenas condiciones y bien instalada (la tierra este conectada de forma correcta).
- Contar con equipo extintores. Existen de varios tipos de acuerdo al tipo de materiales que se puedan incendiar.
- Capacitar al personal en el uso de equipo contra incendios y en la toma de acciones de seguridad ante incendios.
- Contar con una salida de emergencia bien señalizada.

De contarse con los recursos es conveniente seguir las siguientes indicaciones:

- Seleccionar los materiales de construcción e inmobiliario de un material no flamable o bien retardante del fuego.

Otro desastre que pudiera ocurrir son las *inundaciones (o también humedad)* causadas por exceso de precipitación, rotura de presas o desbordamiento de ríos, actividades humanas, falta de drenaje, etc.

Por lo tanto, la ubicación del drenaje en las instalaciones de cómputo y equipo es una decisión importante ya que el daño causado por este desastre es un riesgo seguro cuando el equipo se coloca en algún sótano o sitio donde sea muy viable la acumulación de agua.

Algunas medias de protección son: instalación de detectores de agua o de inundación, bombas de emergencia para resolver inundaciones inesperadas, los pisos falsos también pueden ayudar en este caso o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos (enseguida se mencionara el problema con tener equipos en sitios altos).

Los *terremoto, pequeños sismos o incluso vibraciones* son un desastre que no puede ser evitado, por lo que solo se deben tomar las medidas de seguridad como son: no situar equipos delicados en superficies muy elevadas ya que algún movimiento podría tirar el equipo; puede ser conveniente (y barato) utilizar fijaciones para los elementos más críticos, como las CPUs, los monitores o los routers. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañarían el hardware; también es muy importante no situar equipos cerca de las ventanas, si se produce un temblor pueden caer por ellas, y en ese caso la perdida de datos o hardware pierde importancia frente a los posibles accidentes, incluso mortales, que puede causar una pieza voluminosa a las personas a las que les cae encima. Además, situando los equipos alejados de las ventanas estamos dificultando las acciones de un potencial ladrón que extraiga el equipo.

Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados dañados.

Conclusiones seguridad Física

Cualquiera que sea el desastre es muy común intentar sacar los equipos, sin embargo, debe tenerse siempre en mente que: “Por muy caro que sea el hardware o por muy valiosa que sea la información a proteger, nunca serán magnitudes comparables a lo que supone la pérdida de vidas humanas”.

Bibliografía

http://www.wikilearning.com/tutorial/seguridad_en_unix_y_redes-negaciones_de_servicio/9777-95

http://argentinasec.blogspot.com/2008/08/dns-poison-spoof-by-murder.html

http://seguridad.internautas.org/html/451.html

http://casidiablo.net/man-in-the-middle/

http://www.maestrosdelweb.com/editorial/snort/

http://www.monografias.com/trabajos11/intru/intru.shtml

HUERTA, Antonio Villalón. "Seguridad en Unix y Redes".

Monografias.com

Capítulo 7 - Sistemas de respaldo

Respaldo de Energía: UPS (Uninterruptible Power Supply – Sistema de Alimentación Ininterrumpida).

En ocasiones el suministro de energía eléctrica pone en riesgo los equipos de cómputo, lo cual puede causar pérdida parcial o total de la información, daños en el sistema operativo, corrupción de archivos e incluso daño de hardware.

Los UPS son equipos que se encargan de proveer energía en ausencia del suministro de energía, además de acondicionar la energía para que sea de calidad (aquella energía que carece de interrupciones, sobretensiones (o voltajes pico), deformaciones producidas por armónicas en la red y variaciones de voltaje).

Las sobretensiones o voltajes pico de mayor gravedad pueden ser producidas por:

- Tormentas eléctricas.
- El impacto de un rayo cerca de las líneas de transmisión (se puede inducir hasta millones de voltios de energía).

Para estos casos, no se deben tener conectados equipos a la red eléctrica y es muy recomendable tener instalados sistemas de protección externa, como son los pararrayos que se encargan de desviar la electricidad estática hacia tierra.

Las variaciones de energía puede se causadas por:

- Equipos que de alto consumo de energía para activar motores o compresores (elevadores, refrigeradores, aire acondicionado, etc.).
- Instalaciones defectuosas o improvisadas.
- Problemas con la infraestructura eléctrica del proveedor.

Para anular los voltajes pico se utilizan circuitos supresores de picos los cuales pueden ser:

- Circuitos en paralelo: se encargan de desviar el voltaje en exceso hacia otro circuito (normalmente a tierra).
- Circuitos en serie: contienen el voltaje en exceso sobre la misma línea y sólo permiten el paso de la energía necesaria, esta circuitería está constituida por capacitores y debe ser utilizada

solo en caso de que no se cuente con una tierra física que sirva para drenar la energía en exceso.

La precisión en el funcionamiento de cada UPS varía de acuerdo al modelo, fabricante y costo del equipo.

Hay diversos tipos de topologías de UPS y su elección depende del equipo al que se requiere proteger:

- Off line o Stand by: En esta topología el inversor (el encargado de convertir la corriente directa de las baterías en corriente alterna) se encuentra fuera de la línea del suministro de energía principal (voltaje de entrada).

  Estos UPS están en espera de una interrupción de energía del suministro principal, cuando sucede dicho evento, el interruptor de transferencia cambia para que el suministro de energía este dado por las baterías de respaldo, obviamente, por un tiempo determinado.

  Son equipos de baja potencia y por lo tanto son los más económicos. Son utilizados para equipos de cómputo (PC, servidores, Switch, etc) que no requieren gran potencia.

  El problema que presenta esta topología es que al presentarse un corte de suministro de energía, hay un instante en que el equipo protegido no recibe energía mientras el UPS detecta la falta de suministro y activa el interruptor de transferencia para que se reciba la energía por parte de las baterías.

- On line: a diferencia de los UPS off-line, estos UPS proveen energía constante aunque no haya un fallo de energía. En estos equipos el inversor se encuentra dentro de la línea de suministro de energía principal.

  Estos equipos son más caros pero ofrecen mayor protección para equipos de gran importancia o sensibles ante cualquier fallo en la alimentación de energía (como equipos médicos).

Por cuestiones de características y costo, para equipos de cómputo en un ámbito educativo, es recomendable el uso de UPS off-line, por lo que el resto del capítulo está basado en este tipo de UPS.

Componentes de un UPS off-line.

- Filtro de línea: reduce variaciones de voltaje, los voltajes de alta frecuencia son drenados a tierra y reduce el ruido eléctrico.

- Supresor de picos: recorta los voltajes pico a niveles más seguros.

- Baterías: almacenan la energía suficiente para permitir el funcionamiento de ciertos equipos, las baterías suministran energía solo cuando falla el suministro de energía principal y solo por un tiempo determinado.

- Cargador de baterías: convierte parte de la energía de entrada de corriente alterna (CA) en corriente directa (CD), posteriormente suministrará ésta energía a las baterías.

- Inversor: realiza el proceso inverso que el cargador de baterías, convierte la CD en CA.

- Interruptor de transferencia: este dispositivo sirve para cambiar el suministro de energía para el equipo a proteger, es decir, permite que el equipo reciba energía por el suministro principal o bien por las baterías.

Los UPS son equipos que solo deben ser usados por cuestiones de respaldo y para apagar los equipos de cómputo de forma correcta, al momento de adquirir e instalar UPS debe considerarse:

- No conectar impresoras (las impresoras tienen alto consumo de energía en especial las laser, lo que ocasiona que los UPS gasten de forma exponencial la batería).

- No conectar otros UPS (UPS en cascada).

- Siempre considerar un límite o margen para conectar equipos, y en especial, haber considerado una posible expansión.

- No conectar cargas desconocidas.

- No conectar dispositivos innecesarios (por ejemplo, reproductor de DVD, bocinas, subwoofer, etc.).

- No conectar equipos que requieran mucha energía para funcionar (por ejemplo: taladros, microondas, etc.).

Los UPS tienen un límite de potencia que pueden suministrar a otros equipos, para calcular la potencia requerida (la que deberá proporcionar el UPS) se debe sumar las potencias de los equipos a conectar. Para realizar esta operación la potencia debe estar en Watts y debe considerarse lo siguiente:

- Algunos fabricantes indican la potencia expresada en VA (volts-Ampere), sin embargo, la potencia a calcular debe estar expresada en Watts, si este es el caso, el fabricante también debe otorgar el factor de potencia, de esta forma:

P [W] = S[VA] * Fp

Donde:

P = Potencia activa.

S = Potencia aparente.

Fp = Factor de potencia.

[W] = Unidades de Watt.

[VA] = Unidades Volt-Ampere.

El factor de potencia es la relación entre la P y S y describe la relación entre la potencia de trabajo o real y la potencia total consumida. Es utilizado como indicador del correcto aprovechamiento de la energía eléctrica, el cual puede tomar valores entre 0 y 1, donde 1 representa al valor máximo de Fp y por lo tanto representa al mejor aprovechamiento de la energía.

- En caso de no conocer el valor del Fp, la P debe considerarse como el 60 % de S (considerar el Fp con valor de 0.6).
- No exceder el límite de uso del 90% del UPS.
- Si se considera posible expansión o adición de dispositivos al UPS, usar el 60%, máximo el 70%, de la capacidad del UPS.

Para ejemplificar lo anterior se propone el siguiente ejemplo (el ejemplo es solo para fines demostrativos):

Un centro de cómputo consta de un equipo servidor con dos monitores y 20 equipos PC para el laboratorio de cómputo. El equipo servidor se encuentra ubicado físicamente junto al rack de telecomunicaciones, el cuál contiene un switch que lo mantiene comunicado con los equipos del laboratorio.

El equipo servidor tiene conectada una impresora láser.

Se debe considerar una posible expansión para otro laboratorio de cómputo de 20 equipos (los cuales aún no se han adquirido).

Se pretende adquirir dos equipos UPS, uno destinado al equipo servidor y otro destinado a los equipos del laboratorio. ¿Qué capacidad deben tener los UPS?

A continuación se muestran las especificaciones del consumo de energía de los equipos en cuestión.

Imagen	Equipo	Consumo de energía
	Servidor Power Edge T100 (Dell)	305 W
	Monitor (servidor) LCD L1750 (HP)	30 W
	Switch 4500G 24 puertos (3Com)	370 W
	Impresora laser a color CLP-315 (Samsung)	350 W
	PC (laboratorio) Pavillion Slimline s5120f (HP	220 W
	Monitor (laboratorio) Pavilion 2009m (HP)	56 W

Tabla 7.1 Descripción de equipo.

Solución sugerida:

UPS para el servidor

Como se mencionó anteriormente, en caso de una falla eléctrica los UPS deben ser usados solo para respaldar la información usada en ese momento y apagar los equipos de forma correcta. Es por ello que de los 2 monitores conectados al equipo servidor, solo uno de ellos debería dejarse conectado al UPS.

Las impresoras no deben conectarse a los UPS.

Dado que el servidor está junto al Rack, el switch (switch 1) podría conectarse al mismo UPS.

Al considerar una expansión de un laboratorio de cómputo, se deberá adquirir otro switch capaz de comunicar las computadoras con el servidor, al ser la misma cantidad de computadoras puede considerarse un switch de las mismas características del que ya se tiene (switch 2).

¿Deberían conectarse los switch al UPS? Si el equipo servidor brinda servicios necesarios para el almacenamiento de información ó administración de los clientes, entonces si es necesario conectar los switch a un UPS, en caso contrario, no. Para este ejemplo se considera que si es necesario.

Realizando el cálculo numérico de la potencia total (P total) utilizada por estos 4 dispositivos es:

P total = Potencia servidor + Potencia monitor + P switch 1 + P switch 2

P total = 305 [W] + 30 [W] + 370 [W] + 370 [W]

P total = 1075 [W]

Esta Ptotal debe ser cuando mucho el 90% de la potencia máxima del UPS (P UPS 1), por lo tanto:

P UPS 1 = P total / 0.9

P UPS 1 = 1075 / 0.9

P UPS 1 = 1194.44 [W] ≈ 1200 [W]

Para el UPS del laboratorio se hace el cálculo para un equipo y posteriormente se multiplica por 20 (el CPU y el monitor se adquieren juntos).

P pc = P cpu + P monitor

P pc = 220 [W] + 56 [W]

P pc = 276 [W]

P total = 20 * P pc

P total = 20 * 276 [W]

P total = 5520 [W]

P UPS 2 = P total / 0.9

P UPS 2 = 5520 / 0.9

P UPS 2 = 6133.33 [W] ≈ 6200 [W]

¿Es necesario realizar el análisis del 3er UPS para la expansión planeada? No, ya que cuando se logre hacer la expansión del laboratorio y se adquieran nuevos equipos, estos no necesariamente serán de las mismas características que los ya existentes.

Una alternativa al uso de UPS son las plantas de energía externa, que a diferencia de los UPS, son mayores en costo, dimensiones, consumo de recursos y generadores de ruido.

Respaldo de Datos

El funcionamiento de un centro de cómputo está basado en hardware, software y datos. ¿Cuál de ellos es el más importante? La información albergada en nuestros datos. Ya que el hardware y software son reemplazables, aunque su reemplazo implica dinero y tiempo. Los datos pueden llegar a ser irremplazables y el trabajo de incluso años puede perderse por motivos ajenos al usuario, es por ello que hay que tener especial cuidado con la información.

En ésta sección del capítulo se tratarán 5 puntos para el tratamiento de respaldo y recuperación de datos:

1. Que información debe respaldarse.
2. Cómo se realiza el respaldo de información.
3. Cuando se respalda la información.
4. Donde se guarecerán los respaldos.
5. Herramientas para respaldo y sistemas espejos (mirror).

1. Qué información debe respaldarse.

Los respaldos son pensados para ser usados en caso de un desastre y restaurar los servicios y la información de la forma más rápida posible.

La información del usuario (archivos personales), páginas web, scripts y las bases de datos (los datos) es lo primero que debemos respaldar, ya que sin él debido respaldo, sería muy difícil o hasta imposible recuperar esta información.

Algunos factores que pueden causar la perdida de este tipo de información son:

- Errores humanos.
- Invasión al sistema (a nivel usuario).
- Averías lógicas o físicas del medio donde se encontraba la información (partición o disco duro dedicado al almacenamiento de información).

Existe software y empresas dedicadas a la recuperación de información, sin embargo, esto implica pérdida de tiempo y dinero además de que la recuperación de la información no está garantizada.

Los siguientes tipos de archivos a respaldar son los archivos de configuración, los cuales establecen los parámetros y características de los programas para que funcionen de la forma requerida. Ejemplos de estos archivos son: configuración de las interfaces de red (/etc/network/interfaces), dns (/etc/resolv.conf), configuración de las entradas y salidas estándar como lo es el monitor, teclado y mouse (/etc/X11/xorg.conf), impresoras (/etc/cups/cupsd.conf), esquemas y archivos de configuración de bases de datos, etc,

Algunos factores que pueden causar la perdida de este tipo de información son:

- Programas inestables.
- Programas mal instalados.
- Actualizar programas sin verificar la compatibilidad.
- Instalar programas en versión Beta (programas que aún están en fase de pruebas y podrían presentar fallos inesperados).

El último tipo de archivos a respaldar son parte del sistema operativo o inclusive el sistema operativo completo. La avería del sistema operativo no necesariamente implica la pérdida de la información.

Algunos factores que pueden causar la perdida de este tipo de información son:

- Apagado inesperado o incorrecto del sistema.
- Invasión al sistema (nivel administrador).
- Daño al hardware por no utilizar protección eléctrica.
- Sistema operativo inestable (por ejemplo, el volcado de memoria en Windows).
- No dar mantenimiento periódicamente.
- Instalar gran cantidad de programas.
- Instalar programas no confiables.
- Instalar programas que causen conflictos entre sí (por ejemplo, en sistemas operativos Windows, instalar dos programas antivirus).

2. Cómo se realiza el respaldo de información.

Para realizar el respaldo de archivos personales y de configuración puede hacer mediante software especializado (comercial o libre) o de forma manual mediante el uso de scripts y de tareas programadas.

Ejemplos de software especializado son: Time Machine, Mozy, Cobian, Dropbox y Jungle Disk. Cada uno de ellos hace los respaldos de forma distinta, algunos ofrecen respaldo en un servidor externo y otros en el mismo equipo.

Para realizar los scripts para el respaldo de datos, sugerimos el siguiente diagrama de flujo, el cual se elaboró pensando en la eficiencia del equipo, el tiempo para realizar el respaldo y la optimización de su tamaño.

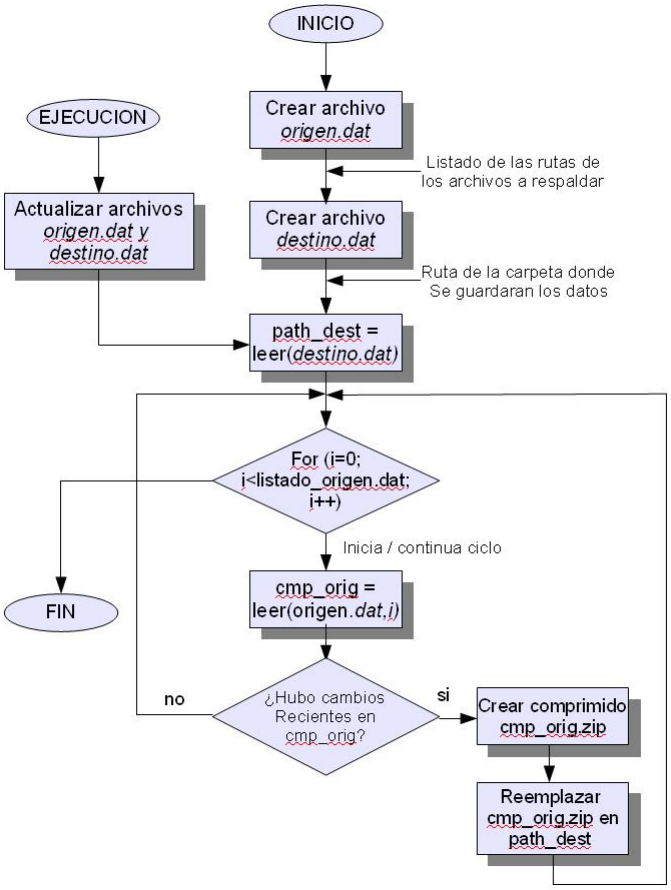


Figura 7.1 Diagrama a bloques de un script para respaldos.

Este es el diagrama de un ejemplo básico y sencillo de cómo hacer un script para realizar respaldo de datos, obviamente podría ser aun más grande y complejo para ajustarse a las necesidades del usuario.

La realización del respaldo del sistema operativo se hace de forma distinta al de los datos, para ello es necesario realizar imágenes del sistema. Se le llama imagen a la copia de toda la partición o del disco duro que contiene al sistema operativo completo, su configuración, los programas instalados y si es el caso, también datos personales.

Para realizar la imagen de un sistema operativo puede utilizarse software comercial (por ejemplo Norton Ghost) o bien herramientas libres (por ejemplo el comando dd – duplícate disk de sistemas operativos Linux).

El mejor camino que recomendamos, por cuestiones de tiempo y de costos, es el uso del comando dd, el cual se usa de una forma muy sencilla y puede ser utilizado tanto para el respaldo de datos y del sistema operativo completo, su desventaja es que no usa compresión de archivos. La sintaxis básica para ellos es la siguiente:

#dd if=origen of=destino

Origen es la carpeta, unidad, partición o disco duro el cual queremos respaldar.

Destino es la carpeta, unidad, partición o disco duro donde queremos crear la imagen del respaldo.

Para respaldar esta partición usamos el comando dd de la siguiente forma:

Ejemplo del uso del comando dd:

dd if=/dev/hda9 of=/dev/hdb5

dd if=/dev/hda9 of=/root/respaldo.iso

dd if=/dev/hda9 of=/media/cdrom0/respaldo.iso

Donde:

- /dev/hdb5 corresponde a la partición 5 de otro disco duro.
- /root/respaldo.iso corresponde a crear una imagen con formato iso dentro del mismo disco duro pero en una ubicación donde solo el administrador tiene acceso.
- /media/cdrom0/respaldo.iso corresponde a crear una imagen con formato iso en un cd.

La restauración del respaldo sería de la siguiente forma:

dd if=/dev/hdb5 of=/dev/hda9

dd if=/root/respaldo.iso of=/dev/hda9

dd if=/media/cdrom0/respaldo.iso of=/dev/hda9

Para respaldar discos duros completos se haría de la forma:

dd if=/dev/hdb of=/dev/hdc

Y para restaurar el respaldo:

dd if=/dev/hdc of=/dev/hdb

Donde:

- /dev/hdb contiene el sistema operativo original.
- /dev/hdc contiene el respaldo del sistema operativo.

Antes de respaldar un sistema operativo completo considere lo siguiente:

- El sistema operativo a respaldar NO debe estar funcionando al hacer el respaldo.
- El sistema operativo se debe respaldar cuando ya está instalado y configurado correctamente.
- El sistema operativo solo debe respaldarse cuando se acaba de instalar y configurar, y en algunos casos, después haber recibido actualizaciones muy grandes (antes de realizar el respaldo es necesario verificar que la actualización no haya causado incompatibilidad con programas y servicios).
- Cada sistema operativo puede cambiar la designación de sus medios, es por ello que se recomienda hacer la verificación de cada medio a utilizar, por ejemplo, algunos sistemas en lugar de utilizar hda como identificador de disco duro, pueden usar sda o uba (u otra que aún no hayamos visto).
- La función restaurar sistema de sistemas operativos Windows XP, Server y NT, solo restauran el registro del sistema, es decir, la información de los programas instalados y la configuración del sistema operativo, NO respalda datos ni programas. Los sistemas operativos Microsoft Windows Vista si tienen el complemento para el respaldo de datos, lamentablemente, es una función muy tardada para realizar el respaldo y restauración de la información, por lo tanto es ineficiente.

3. Cuando se respalda la información.

La frecuencia con la cual se realizará el respaldo para los archivos personales dependerá del tiempo que tardan los usuarios en subir los archivos, si estamos hablando de un servidor de archivos para los alumnos de una dependencia el respaldo tendría que ser diariamente.

Una forma alterna es programando el script del respaldo usando el esquema mostrado en la figura 7.3, dicho script realiza el respaldo solo si hay cambios, el usuario programa la tarea para que se ejecute cada cierto tiempo.

El respaldo para los archivos de configuración no es una tarea que deba programarse, es mejor ejecutarla de forma manual, ya que estos archivos solo cambiarán cuando el usuario realice cambios en algún programa, cosa que no es muy común.

El respaldo para el sistema operativo, es una tarea que normalmente se ejecuta solo una vez, para ello, el sistema operativo no debe estar en funcionamiento y obviamente todos los servicios deben estar detenidos. Es por ello que no se debe planear este tipo de respaldo en más de una ocasión.

Tenga en cuenta que si el respaldo de los datos se hace junto con el respaldo del sistema operativo, el tiempo necesario para realizar los procesos de respaldo y restauración será más prolongado.

4. Donde se guarecerán los respaldos.

Para archivos personales y de configuración el respaldo puede guardarse en:

Ubicación de respaldo con respecto al archivo original	Velocidad	Costo extra	Ventaja	Desventaja	Posibilidad del Siniestro
Misma carpeta	Muy rápido	Ninguno	Fácil de programar y ubicar.	Si sufre algún daño el archivo original, muy probablemente lo sufrirá también el respaldo.	Muy alta
Misma partición	Muy rápido	Ninguno	Fácil de ubicar. El daño al archivo original no afecta al respaldo.	Más complejo para configurar la partición. Si sufre algún daño el disco duro donde está el archivo original, también lo sufrirá el respaldo.	Baja
Mismo disco duro	Muy rápido	Ninguno	En caso de un daño a la partición donde se encuentran los archivos originales, el respaldo está intacto.	Más complejo de configurar, en caso de avería del disco duro donde está el archivo original, también lo sufrirá el respaldo.	Baja
Distinto disco duro (interno)	Muy rápido	Bajo	En caso de un daño al disco duro donde se encuentra el archivo original, el respaldo estará intacto.	En caso de un desastre con el equipo donde se encuentra el archivo original, el respaldo puede resultar dañado.	Baja
Distinto disco	Rápido	Medio	En caso de un daño	Está expuesto a	Baja

duro (externo)			al equipo donde se encuentra el archivo original, el respaldo estará intacto.	pérdida o robo.	
Cinta magnética	Medio	Alto	En caso de un daño al equipo donde se encuentra el archivo original, el respaldo estará intacto.	Expuesto a robo. Debe estar bien guardado y empaquetado, o la unidad podría dañarse y se perdería el respaldo.	Baja
Unidad de CD o DVD	Lento	Bajo	En caso de un daño al equipo donde se encuentra el archivo original, el respaldo estará intacto.	Está expuesto a pérdida o robo. Debe estar bien guardado y empaquetado, o la unidad podría dañarse y se perdería el respaldo.	Media
Servidor remoto	Lento	Alto	En caso de daños al centro de cómputo donde se encuentra el equipo del archivo original, el respaldo está intacto.	Más complejo para configurar, si sufre daños el equipo remoto, el respaldo se verá afectado.	Baja

Tabla 7.2 Tabla comparativa de las diferentes ubicaciones para hacer respaldos.

Tenga en cuenta que la velocidad del respaldo (Muy rápido, rápido, medio y lento) es relativo a las características del equipo y al hardware si es el caso (unidad de cinta, cintas magnéticas para grabar, quemador de CD o DVD, CD o DVD para grabar).

De forma similar, la probabilidad de que suceda el siniestro es relativa a la planeación y cuidados del administrador del equipo servidor y del centro de cómputo.

No es recomendable respaldar información en unidades Flash USB (o mejor conocidas como memorias USB), ya que éstas unidades son más sensibles al daño y no es posible hacer una recuperación de información (a diferencia de los discos duros donde si existe la posibilidad de recuperar la información).

5. Herramientas para respaldo y sistemas espejos (mirror).

Este tipo de sistemas tienen la característica de que se está haciendo una clonación del servidor seleccionado en otro equipo denominado espejo o mirror, la clonación se hace en tiempo real.

Si el servidor seleccionado falla, el mirror lo sustituirá para seguir brindando los mismos servicios con los últimos cambios realizados en el servidor, de esta forma, el usuario seguirá teniendo los servicios mientras el administrador repara el equipo servidor y vuelve a ponerlo en funcionamiento, posteriormente el mirror regresará a su función principal.

Los sistemas mirror se pueden programar mediante software o hardware.

En esta sección se explicarán 3 formas de hacer un sistema mirror: Raid, Rsync y personalizado.

1) Raid: Es el acrónimo de "Redundant Array of Independent Disks - matriz redundante de discos independientes", es un método mediante el cual se combinan dos o más discos duros para aumentar la velocidad y/o tener un sistema confiable ante una caída del sistema y pérdida de los datos.

   Un sistema Raid hace que el sistema operativo vea a todo el conjunto de discos duros como si fueran un solo disco duro lógico.

   Ventajas de un sistema Raid:

   - Aumenta el tiempo de funcionamiento y la disponibilidad de la Red.
   - Protege contra la pérdida de datos y proporciona recuperación de los mismos en tiempo real.
   - Permite manejar dos o más unidades en paralelo para aumentar el rendimiento del sistema.

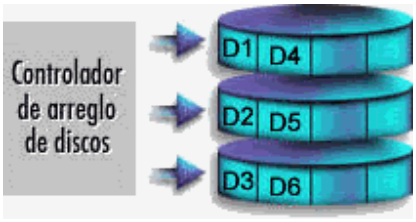
   Desventajas:

   - Costo.
   - Tiempo para su configuración.

   El Raid Advisory Board o "RAB" (organización fundada en 1992 orientada al desarrollo educativo, estandarización y clasificación de los sistemas de almacenamiento Raid) define 7 niveles de Raid (del Raid 0 al 7) y la combinación entre ellos, cada nivel realiza sus tareas de forma distinta, sin embargo, los niveles Raid más comerciales son el 0, 1, 5 y 10 (se puede hacer la combinación de ellos para obtener distintos resultados, la combinación más común es la del Raid 1 con el Raid 0, por eso se le llama Raid 10), es por ello que solo se mencionarán estos niveles dentro el capítulo.

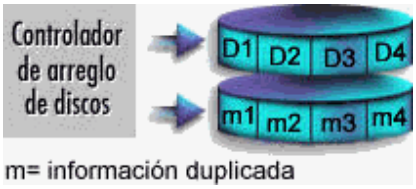
   - Raid 0: Mejor conocido como Striping ó Fraccionamiento, este Raid está compuesto por dos o más discos duros conectados en paralelo, y se encarga de dividir los datos de entrada en distintos bloques que serán almacenados en los distintos discos duros, esto aumenta la velocidad y el rendimiento del sistema.

     Es el más rápido debido a que el almacenamiento sobre un disco duro, se realiza en forma secuencial, es decir, se introduce un bloque de información y no se puede almacenar más hasta que la unidad esté lista para recibir el siguiente bloque. En el almacenamiento en paralelo, se almacenan los bloques en distintos discos duros al mismo tiempo.



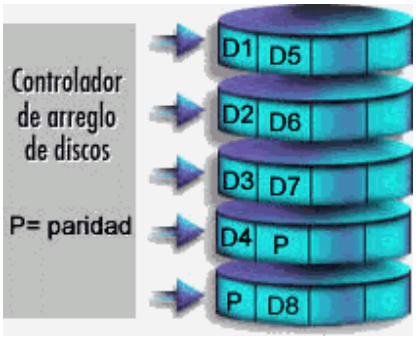
Este tipo de Raid no ofrece protección contra fallos, por lo que es recomendado usarlo cuando se requiere alta velocidad en lectura y escritura de información pero sin tolerancia a fallos.

- Raid 1: Conocido como mirroring o espejo, como su nombre lo dice, se hace una replicación exacta de la información, para este tipo de raid es necesario tener un disco duro adicional por cada disco de almacenamiento primario de la información.
  Cada vez que se realiza un cambio en algún disco duro, dicho cambio también se realiza en el disco mirror.
  Su punto favorable es ofrecer gran seguridad ante un fallo, si un disco duro deja de funcionar la información es obtenida desde el otro disco duro de forma inmediata.
  Las desventajas de este tipo de Raid son el costo y el procesamiento de los datos es más lento.
  Es utilizado cuando se requiere tener alta disponibilidad de la información y cuando solo se cuenta con 2 unidades de disco duro, por ejemplo, servidores de archivos pequeños.



- Raid 5: Ofrece acceso independiente a los datos con paridad distribuida. Divide los datos en X número de bloques igual al número de discos duros disponibles, los bloques son almacenados en los discos duros junto con información de paridad, mediante ésta paridad se asegura la integridad de los datos. Cuando se daña alguno de los bloques de datos, haciendo uso de la paridad y del resto de los bloques de datos, se reconstruye el bloque dañado en tiempo real.
  Al tener la paridad de la información distribuida en distintos discos duros, se evita el problema de cuello de botella, éste problema se da cuando la paridad se almacena exclusivamente en un disco duro (como lo es en el caso de Raid 3 y 4).

Este nivel de Raid es el más utilizado y requiere de 3 discos duros para operar.

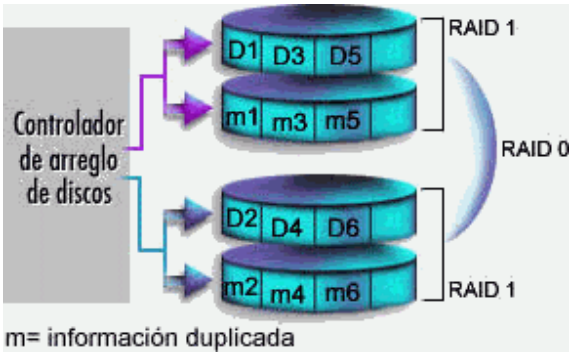


- Raid 10: Además de los raid definidos por RAB, se puede hacer la combinación de ellos para obtener distintos resultados, la combinación más común es la del Raid 1 con el Raid 0, por eso se le llama Raid 10.

  Combina la optimización del sistema para el almacenamiento de la información (Raid 0) y realiza un espejo de la información que se va utilizando (Raid 1), después del Raid 5, es el nivel Raid más utilizado.

  Ofrece mejor protección y disponibilidad de los datos que el Raid 5.

  Su desventaja es que el costo para implementarlo es grande (mayor al Raid 5), requiere de al menos 4 discos duros, si se desea incrementar la capacidad de almacenamiento, ésta debe hacerse en número par (6, 8, 10… discos duros).



Además de los niveles de Raid, también están los tipos de Raid, los cuales pueden ser implementados por Hardware o Software.

Un Raid por software tiene las siguientes características:

- Bajo costo monetario.
- Es gestionado por el procesador del sistema.

- Consume recursos que afectan al resto de las aplicaciones.
- No ofrece protección para el sistema operativo.
- Soporta Hot spare[1] (Repuesto en caliente).
- No soporta Hot swap[2] (Intercambio en caliente).

Un Raid implementado por hardware tiene las siguientes características:

- Alto costo monetario.
- Independencia del sistema operativo.
- Alto rendimiento.
- Protección contra datos y sistema operativo.
- Soporta Hot swap y Hot spare.

2) Rsync: Es una herramienta de Linux que nos permitirá estar realizando respaldos remotos de una forma dinámica y eficiente.

   Una característica muy importante de Rsync es que al realizar el primer respaldo de información se hace completo, es decir se lleva a cabo en TODOS los archivos y en ocasiones posteriores, cuando se necesite hacer un nuevo respaldo SOLO se llevará a cabo en los archivos que hayan sido modificados, por lo que el respaldo será hecho con mayor rapidez.

   Para realizar los respaldos (tanto remotos como locales), Rsync primero compara el archivo a respaldar con el que encuentra en la carpeta del servidor mirror, para ello pueden ocurrir tres cosas:

   - El archivo original no existe en el respaldo: para este caso, se crea el nuevo archivo.
   - El archivo original es distinto al del respaldo: se sobrescribe el archivo de respaldo.
   - El archivo original es igual al del respaldo: no se realiza ninguna acción.

   Al copiar solo las modificaciones realizadas se optimiza la transferencia de los archivos y por lo tanto se consume menos recursos en los equipos y se tiene menor tráfico de red.

   No se explicará como configurar esta herramienta de Linux, ya que existe una gran cantidad de manuales en Internet que explican cómo hacerlo, para mayor información se puede consultar la página del autor de Rsync.

[1] Es la capacidad de que cuando un disco duro falla, el disco destinado al respaldo entra en funcionamiento de forma inmediata y sin la intervención del usuario, también se le conoce como repuesto automático o desasistido.

[2] Es la capacidad de poder cambiar un disco duro defectuoso estando el sistema operativo bajo funcionamiento, esto evita interrupciones de trabajo.

3) Personalizado: Se puede realizar un script entre 2 equipos para realizar el efecto espejo, a continuación se explica cómo funcionaría dicho script sobre sistemas Linux, no se detallará el código del script realizado.

Funcionamiento Principal

Para éste caso, ambos servidores están en condiciones iguales con 3 interfaces de red cada uno.

Se mantiene una comunicación constante entre ambos servidores, si dicha comunicación se establece de forma correcta se considerará que el estado Funcionamiento Principal. Si la comunicación es interrumpida se considerará el estado Funcionamiento Mirror.

La 1er interfaz de red (eth0) de cada servidor está conectada a Internet.

El servidor principal está conectado a Internet mediante una IP pública.

El servidor mirror está físicamente conectado a Internet, tiene configurada la misma IP pública que el otro servidor pero su interfaz de red esta desactivada mediante el comando ifdown.

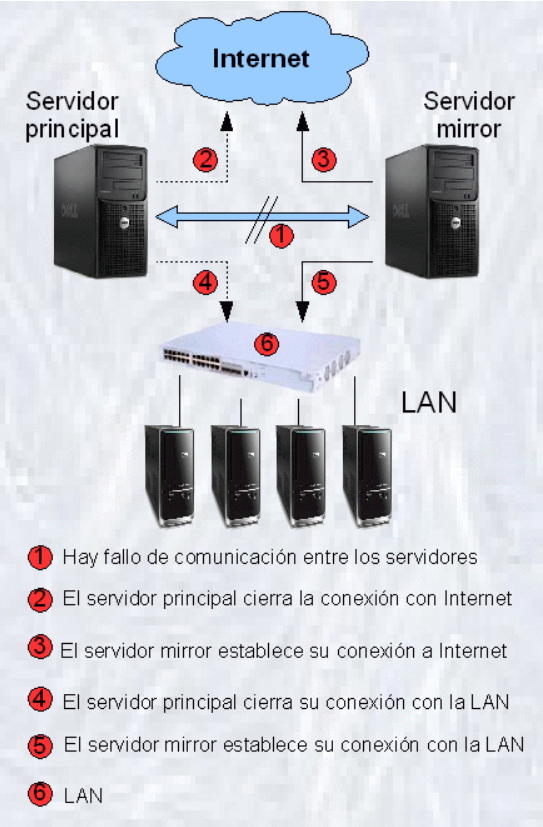
#ifdown eth0

Haciendo uso de 2da interfaz de red (eth1) de cada servidor, éstos mantienen la comunicación constante en la cual el servidor principal le informa al servidor mirror si está activo o no.

Cada equipo tiene configurada una IP privada distinta pero que pertenezcan al mismo segmento, por ejemplo, podrían tener las IP 192.168.13.5 y 192.168.13.21.

Este paso es muy importante, ya que la comunicación puede hacerse tan compleja como el usuario lo desee, una forma sencilla es haciendo uso del comando ping, el cual nos sirve para saber si otro equipo de la red está respondiendo ante nuestras peticiones (siempre y cuando el firewall lo permita).

#ping 192.168.13.5



Una forma más segura y completa de saber el estado del servidor principal, es mediante el uso de software de desarrollo con comunicaciones TCP/IP, por ejemplo, el desarrollo de un programa elaborado con java ó combinando el uso de Shell scripting y openSSH.

En esta comunicación también se estará realizando el paso de archivos del servidor principal al servidor mirror. El administrador de los equipos es el que decidirá si este proceso se deberá hacer en tiempo real o cada cierto periodo de tiempo.

El servidor principal está conectado a una LAN a la cuál le puede brindar distintos tipos de servicios, esta comunicación se realiza mediante la 3ra interfaz de red (eth2) y una IP privada perteneciente a un segmento distinto al de la 2da interfaz, por ejemplo puede tener la IP 192.168.8.32.

El servidor mirror está físicamente conectado a la LAN, tiene configurada la misma IP que el servidor principal pero su tercer interfaz de red está desactivada.

#ifdown eth2

Funcionamiento Mirror

Existe algún fallo de comunicación entre los servidores.

El servidor principal cierra la comunicación con Internet, esto lo hace desactivando su 1er interfaz de red.

#ifdown eth0

El servidor mirror activa su 1er interfaz de red y establece conexión con Internet.

#ifup eth0

El servidor principal cierra la comunicación con la LAN, esto lo hace desactivando su 3er interfaz de red.

#ifdown eth2

El servidor mirror activa su 3er interfaz de red y establece comunicación con LAN.

#ifup eth2

Cuando se entra al estado Funcionamiento Mirror, se da el mantenimiento al servidor principal, una vez que el servidor principal está reparado, se vuelve a conectar a red y el mismo programa debe realizar los siguientes pasos para poder regresar al estado Funcionamiento Principal.

- Verificar cambios en los archivos del servidor mirror, si hubo cambios, se actualizan en el servidor principal.
- Se reanuda la comunicación entre los servidores, si la comunicación es exitosa o no se notifica al administrador para saber si el servidor principal se deja o se vuelve a retirar para verificar el fallo.
- Si la comunicación fue establecida correctamente, el servidor mirror cierra conexión con Internet y LAN.
- El servidor principal establece conexión con Internet y LAN.
- Se entra al estado Funcionamiento Principal.

Este esquema es solo una propuesta, ya que puede haber variaciones que permitan ajustarse a las necesidades propias de cada situación, puede mejorarse el sistema para tener mayores funciones, ampliar el esquema para que un servidor monitoree múltiples servidores estableciendo jerarquía entre ellos, cambiar la forma de administrar el funcionamiento mirror (por ejemplo, mediante reglas de firewall), etc.

Para el servidor mirror, una opción de mantener el rendimiento de su hardware (usar los mínimos recursos mientras está en estado de espera) es que los servicios brindados (como Web, Nat, correo, etc.) no estén activos si no hasta que se entre en el estado Funcionamiento Mirror.

Bibliografía

http://www.enterate.unam.mx/Articulos/2004/Abril/energia.htm

http://www.samba.org/rsync/

http://www.conae.gob.mx/wb/CONAE/CONA_419_el_factor_de_potenc

http://elec.itmorelia.edu.mx/armonico/Capitulo%20I.htm

http://www.c-mos.com/pdfsproductos/manual_de_ventas_UPS_reducido.pdf

http://www.unicrom.com/Tut_TopologiasUPS1.asp

http://www.hard-h2o.com/vertema/72408/como-seleccionar-un-sai-para-pc.html

http://www.chw.net/foro/otro-hardware-f27/113873-q-necesito-saber-para-comprar-una-ups-p2.html

http://www.pcmag.com/encyclopedia_term/0,2542,t=RAID+Advisory+Board&i=50153,00.asp

http://www.pctelecos.com/documents/raid.pdf

http://www.sindominio.net/~apm/articulos/raid

http://www.smdata.com/queesraid.htm

http://www.informatica-hoy.com.ar/hardware-pc-desktop/Tipos-de-RAID.php

Capítulo 8 - Selección de equipos.

Al adquirir nuevos equipos hay que tener presente cuál será la utilización y el alcance de los equipos, para que la inversión realizada sea aprovechada en lo mayor posible. Durante este capítulo se consideran solo los equipos que, de cierta forma, son usados de forma directa por y para los usuarios.

Al hacer la adquisición de los equipos se pueden dar los siguientes casos:

- Adquirir un equipo de grandes características de tal forma que sus recursos no sean aprovechados, esto ocasiona perdida de inversión en equipo de alto costo.

- Adquirir un equipo de bajos recursos que no sea capaz de cumplir las necesidades para las cuales fue adquirido, perdida de inversión ya que el equipo no puede ser usado para las necesidades planteadas y será necesario invertir en otro equipo.

- Adquirir un equipo con los recursos suficientes (casi exactos) que cumplan nuestras necesidades. A corto plazo es una buena inversión, sin embargo, en un futuro se puede dar el caso de que las necesidades aumenten y el equipo con sus características actuales no pueda realizar las nuevas tareas a menos que se le instale, de forma adicional, los recursos necesarios. En este caso sería mejor inversión adquirir un equipo nuevo con mayores características y reutilizar el equipo reemplazado en otras actividades.

- Adquirir un equipo con los recursos sobrados de tal forma que cumplan las necesidades requeridas (sin utilizar todos sus recursos) y planeando el cumplimiento de nuevas necesidades a largo plazo, esta es la mejor inversión, se planea un crecimiento a mediano y largo plazo.

En una buena planeación debe considerarse la adquisición de equipos adicionales que puedan ser usados para reemplazar a otro equipo en caso de que sufra algún daño (stock).

Los principales equipos a utilizar en un centro de cómputo, para “uso directo” de los usuarios son las impresoras, PCs y equipos servidores (se usa el término de “uso directo” en los equipos servidores a pesar de que el alumno no hace uso directamente de él, si no que hace uso de sus servicios).

PCs (Personal Computers - Computadoras Personales).

En este apartado se tratará la elección de una PC basada en su funcionamiento y en sus características de hardware.

En un centro educativo, las características físicas de mayor interés en una PC son: procesador, memoria RAM, tarjeta de red, capacidad de disco duro y unidad de CD/DVD. Existen otros dispositivos de hardware, sin embargo, para la finalidad de un centro educativo, se consideró que los dispositivos mencionados anteriormente son los de vital importancia a analizar.

Procesador.

Es el cerebro de la computadora y su tarea es administrar la comunicación de las diferentes partes de la computadora y mantiene la sincronía entre el hardware y el software.

El procesador utiliza las instrucciones almacenadas en la memoria RAM para realizar tareas específicas. Utiliza tiempo compartido para la ejecución de dichas instrucciones, es decir, el procesador dedica cierto tiempo en ejecutar una instrucción, si la instrucción no termino de ejecutar su tarea asignada en el tiempo reservado, la instrucción queda suspendida y el próximo periodo de tiempo de uso del procesador es empleado para otra instrucción.

Hoy en día (marzo de 2010), existen procesadores de doble y cuádruple núcleo, esto es, que un solo procesador puede ejecutar 2 o 4 tareas de forma simultánea, respectivamente, lo cual reduce el uso de tiempo compartido y hace que se puedan ejecutar mayor cantidad de instrucciones.

Memoria RAM (Random Access Memory – Memoria de acceso aleatorio).

La memoria RAM es el dispositivo que nos permitirá ejecutar múltiples aplicaciones al mismo tiempo y es también aquella que definirá la velocidad en la que trabajarán las aplicaciones.

Cada vez que se abre alguna aplicación, las instrucciones (o comandos) y datos temporales que maneja dicha aplicación son cargadas en la memoria RAM para que el procesador pueda hacer uso de ellas, cuando la aplicación o programa se cierra, las instrucciones guardadas en la RAM referentes a esta aplicación son borradas y la RAM esta lista para almacenar mas información de otras aplicaciones.

De esta forma, se puede deducir que entre mayor sea la memoria RAM se podrá almacenar mayor cantidad de información que permitirá manejar más programas de forma simultánea y con mayor velocidad.

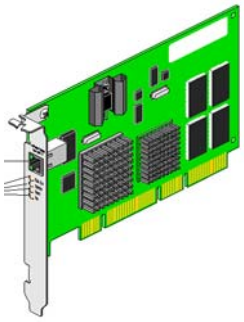
La memoria RAM es de tipo volátil, es decir, al apagar el equipo se borrarán todos los datos de ella.

Cabe resaltar que las capacidades de un procesador y de la memoria RAM están muy ligadas y deben estar casi igualadas para un óptimo aprovechamiento de ambos recursos, esto es:

- Un procesador de grandes capacidades con una memoria RAM muy pequeña no es bien aprovechado, ya que la capacidad del procesador está limitada a la cantidad de instrucciones que se pueden almacenar en la RAM.

- Un procesador de bajas capacidades con una memoria RAM muy grande, se está desperdiciando la RAM, ya que, a pesar de que pueda almacenar gran cantidad de información, el procesador no podrá leerlas todas y solo utilizará una pequeña parte de la RAM.

Tarjeta de red



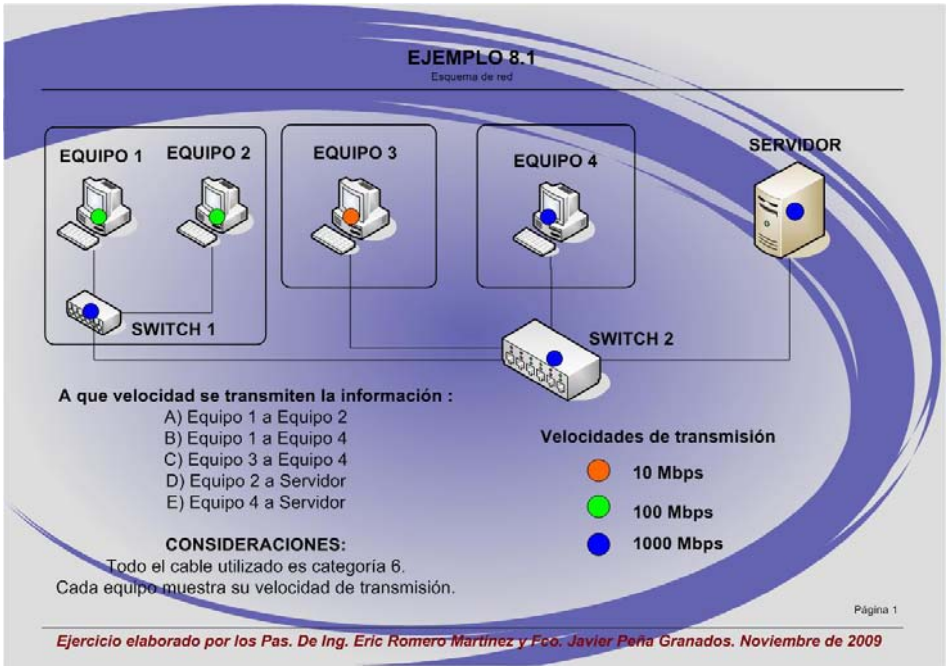
Internet es una gigantesca fuente de información y un recurso muy utilizado en el ámbito educativo, es por ello que este recurso debería estar disponible en cualquier institución educativa.

La tarjeta de red (alámbrica o inalámbrica) es el dispositivo más común mediante el cual una PC se conecta a Internet.

La velocidad de transmisión (es la capacidad con la cual se transfiere la información por unidad de tiempo) es medida en bps (bits por segundo) y en derivados de 1024 unidades, como Kbps (Kilo bits por segundo), Mbps (Mega bits por segundo), Gbps (Giga bits por segundo).

Cabe mencionar que la velocidad de transmisión no solo depende de la tarjeta de red, también depende del medio utilizado, lo dispositivos de interconexión utilizados (switch, hub, router, etc.), del proveedor de servicios de Internet (ISP) y de una correcta estructura de red.

Ejemplo:



Ejemplo 8.1. Velocidad de transmisión de datos

Cuando dos dispositivos de red de diferentes velocidades de transmisión están conectados entre sí, la velocidad en la que se transmiten los datos es igual al del dispositivo de menor velocidad, ya que por sus características de fabrica, no puede transmitir información a mayor velocidad a pesar de que el Ancho de Banda del medio no se ocupe en su totalidad.

El cable de par trenzado de categoría 6 permite velocidad de hasta 1000 Mbps, ya que transmiten en Full dúplex[1].

Continuación ejemplo 8.1:

- Los equipos de menor velocidad son los equipos 1 y 2, que transmiten a 100 Mbps, por lo que la velocidad en que se transmiten los datos será de 100 Mbps.

- El equipo de menor velocidad de transmisión es el equipo 1, por lo que la velocidad de transmisión entre los equipos será de 100 Mbps.

- El equipo de menor velocidad de transmisión es el equipo 3, por lo que la velocidad de transmisión entre los equipos será de 10 Mbps.

[1] La transmisión full dúplex es en forma bidireccional y de forma simultánea, es decir, ambos extremos del canal de comunicación pueden enviar y recibir información al mismo tiempo (como el cable de teléfono), para redes de computadoras, el cable UTP categoría 6 utiliza los 4 pares de hilos para esta finalidad.

- El equipo con menor velocidad de transmisión es el equipo 2, por lo que la velocidad de transmisión entre los equipos será de 100 Mbps.
- El equipo 4, el Switch 2 y el Servidor tienen velocidad de transmisión de 1000 Mbps, por lo que la velocidad de transmisión entre los equipos será de 1000 Mbps.

Suponga que el cableado horizontal entre el switch 2 y el equipo 4 es remplazado por cable categoría 5E, ¿La velocidad de transmisión del inciso e) sigue siendo de 1000 Mbps?

La respuesta es… NO, a pesar de que los 3 dispositivos en cuestión tengan la capacidad de transmitir a 1000 Mbps, el cable categoría 5e transmite en Half dúplex[2], el cuál puede transmitir máximo a 100 Mbps. Con esta nueva modificación, la respuesta a este último inciso es 100 Mbps.

Disco Duro

Es el dispositivo que nos permitirá almacenar información que pueda ser utilizada posteriormente, como lo son programas, documentos, análisis electrónicos, etc.

Un equipo PC, normalmente, puede tener instalado desde 1 hasta 4 discos duros (dependiendo del modelo de la tarjeta madre). Los discos duros pueden ser de distinta capacidad.

Para una institución educativa, el tener un solo disco por PC es suficiente, ya que la cantidad de información, aparte del sistema operativo y de los programas, que se requiere almacenar utiliza poco espacio, por ejemplo, el sistema operativo y los programas utilizarán aproximadamente un espacio de 15 GB, y para los usuarios se puede destinar al menos 15 GB, por lo que el disco duro a utilizar sería de 40 GB (no existen discos duros de 30 GB).

Existen archivos que por su formato pueden tener un peso en disco duro muy grande, como lo son los videos, juegos, películas, música. El uso excesivo de estos tipos de archivos puede llegar a saturar al disco duro. Sin embargo, para fines educativos y de administración, estos archivos no tienen por qué estar almacenados en los equipos y se considera que este no es argumento válido para invertir en discos duros extras para una PC.

Algunos administradores pueden argumentar que se requiere al menos un disco duro adicional por cada PC para que funcione como respaldo del sistema operativo y los programas, para que en caso de avería, se active el respaldo y el equipo siga en funcionamiento de forma inmediata (no hay tiempo de espera para la reparación ante este desastre).

[2] La transmisión half dúplex es en forma bidireccional pero no es en forma simultánea, es decir, ambos extremos del canal de comunicación pueden enviar información en un tiempo y recibir información en otro tiempo (como el walky talky), para redes de computadoras, el cable UTP categoría 5e utiliza 2 pares de hilos para esta finalidad.

Una solución alterna, es que se fragmente el disco duro y en una partición oculta se ponga una imagen ó respaldo del sistema operativo y de los programas, en caso de avería (si la avería es directamente con el disco duro y no con el sistema operativo, el reemplazo del mismo es obligatorio y la partición oculta no servirá de nada) del sistema operativo (causado por un mal cierre del sistema, mal uso del usuario o malware), se puede restaurar el sistema y los programas utilizando la partición oculta. La ventaja es que se ahorra mucho dinero en la compra de los discos duros adicionales por cada PC, la desventaja es que si hay un tiempo de espera cada vez que se avería algún equipo.

Unidad de CD/DVD

La unidad lectora de disco compacto la podemos encontrar en las siguientes clasificaciones:

- CD-R, solo lectura de CD.
- CD-W, lectura y escritura de CD.
- CD-R/DVD-R, lectura de CD y DVD.
- CD-W/DVD-R, lectura de CD y DVD, escritura en CD.
- CD-W/DVD-W, lectura y escritura en CD y DVD.

Para equipos destinados a laboratorio de alumnos, se recomienda unidades CD-R/DVD-R, para que los alumnos puedan ver información provenientes de ambos tipos de discos compactos. No se recomienda dejar unidades grabadoras de discos de acceso libre a los alumnos, por que podrían abusar de ello y utilizar las unidades con fines ajenos al desarrollo académico.

Si el equipo será usado por personal que asesore o apoye a los alumnos en situaciones especiales, se podría instalar unidades CD-W/DVD-R, de tal forma que si los alumnos desean grabar un proyecto o trabajo en unidad de CD, puedan dirigirse con el personal de apoyo y pedir que pasen su información a CD. No se recomienda usar unidad CD-W/DVD-W, ya que es muy difícil que un proyecto académico supere la capacidad de un CD y sea necesario usar DVD.

Si el equipo es usado para apoyo especial, por ejemplo, para edición de videos, se podría instalar una unidad CD-W/DVD-W, para poder grabar proyectos de gran espacio en disco DVD. Dichos equipos deben ser usados por personal responsable.

La elección de la unidad de CD no debe ser aleatoria, ya que, hay que tener en cuenta que tanto los alumnos como el personal podrían abusar del uso de estas unidades, por ejemplo: ver

películas en un lugar no permitido, crear discos de música, clonar o crear películas, etc. (actos ilegales en una institución educativa). Por ello, al elegir las unidades a instalar también se deben establecer políticas de uso.

Servidores

Los equipos servidores (o simplemente "servidores") son equipos de cómputo de grandes capacidades que tienen la finalidad de brindar servicios a varios usuarios también llamados "clientes" (los usuarios pueden ser personas o equipos de cómputo).

A diferencia de los equipos PC, la elección de un equipo servidor dependerá del tipo de servicio que brindará.

Si el tipo de servicio tiene que ver con el almacenamiento de información, hay que pensar, en primera instancia, tener una fuerte capacidad de almacenamiento (servidor de base de datos, servidor de archivos, servidor de correo, servidor de respaldos, espejos).

Si el tipo de servicio está dedicado al procesamiento de instrucciones se debe contar con uno o varios procesadores y suficiente memoria RAM (servidor de aplicaciones, servidor web basado en php o Tomcat donde las tareas se ejecutan en el servidor).

Si el tipo de servicio está basado en el funcionamiento de red, hay que cuidar que el recurso de red (tarjetas ethernet) y de procesamiento sean los adecuados para llevar a cabo dichas tareas (servidor IRC, servidor NAT).

Habrá servidores que debido a su función requerirán tener grandes recursos, por ejemplo un servidor de Audio/Video, donde los videos almacenados utilizan un gran espacio en disco, se requiere muy buena memoria RAM y procesador(es) para procesar un video a un formato determinado (cuando es necesario) y un buen ancho de banda para mantener un flujo continuo del audio/video cuando éste sea consultado por Internet (streaming).

Impresoras

Existen diversos tipos de impresoras, como son plotters, de matriz de punto, inyección de tinta, lásers, etc. Para esta tesis solo se está tomando en cuenta las impresoras más comunes en las instituciones educativas, que son las de inyección de tinta y láser.

¿Cuáles son las características que mas infieren en la elección de una impresora?

- Resolución: Capacidad para la calidad de las impresiones, la cual está dada por el número de puntos (pixeles) que la impresora puede dibujar sobre unidad de superficie, esta medida está dada en puntos por pulgada (ppp).

  Dado que los trabajos son de uso académico, no se requiere de gran calidad en la resolución de las impresiones, por ello, no se recomienda que el costo de la impresora dependa de esta característica, independientemente si la impresora será de uso personal o masivo.

- Velocidad de impresión: Es la capacidad que tiene la impresora de imprimir páginas por minuto (ppm) o caracteres pos segundo (cps).

  Para impresoras de uso personal, no se recomienda que el costo de la impresora dependa de esta característica, ya que las impresiones realizadas son en pequeñas cantidad y normalmente, no son continuas. Para las impresoras de uso masivo, donde la cantidad de impresiones realizadas es muy grande y en todo instante, de ésta característica puede depender el hecho de evitar o generar colas de espera.

- Laser o inyección de tinta: Es la forma o método con el cual se realizan las impresiones.

  Anteriormente, una diferencia importante entre estos tipos de impresoras era la velocidad de impresión, donde las impresiones laser eran muy superiores a las de inyección de tinta. Hoy en día, hay impresoras de inyección de tinta con una velocidad muy semejante a las impresoras laser. La característica que sigue marcando la diferencia es la cantidad de hojas que se pueden imprimir, los cartuchos de inyección de tinta pueden imprimir en un promedio de 300 a 500 hojas, mientras que los tóner de las impresoras laser pueden imprimir en un promedio de 1000 a 2000 hojas. La capacidad de impresiones realizadas depende del tamaño del cartucho/tóner y de la configuración de la impresora (una de las modificaciones que se puede hacer a la configuración de las impresoras es la calidad de la impresión, el reducir dicha calidad permitirá mayor cantidad de impresiones).

  Un par de puntos que no hay que olvidar, es que los cartuchos de tinta son más económicos que los tóners y que las impresoras láser requieren mayor consumo de energía que las impresoras de inyección de tinta.

Tanto los cartuchos de tinta como los tóners pueden ser rellenados para volver a ser usados, lo cual reduciría costos, pero el usar consumibles (se entiende por consumible a todo aquel material que es usado una sola vez, para el caso de las impresoras, se entiende por consumible a los cartuchos de tinta y tóners) rellenados puede traer complicaciones y causar daños a la impresora (como derramamiento de tinta o daños al chip de seguridad) y se tendría una pérdida de tiempo (y posiblemente de dinero) para reparar la impresora. Además de que algunas empresas lo consideran un acto ilícito y han tratado de evitar esto mediante el uso de chips de seguridad.

Dentro de esta misma característica, podemos tratar el hecho de adquirir una impresora a color o monocromo. ¿Cómo hacer la elección correcta?. Para ello se debe hacer un análisis del tipo de archivos que se imprimirán, el análisis aquí expuesto está basado en uso general.

Es muy importante saber el posible aprovechamiento que tendría una impresora a color (inyección de tinta o láser), ya que esta es la característica que marcará mas la diferencia en el costo de una impresora u otra.

Para las impresoras de uso personal, se acostumbra imprimir documentos para tramites académicos, los cuales no es necesario imprimir a color, a menos que la impresora tenga como segundo uso la impresión de carteles o avisos del departamento que tengan que ser impresos a color para que cumplan con su objetivo, que es llamar la atención del público.

Para las impresoras de uso masivo se suele imprimir trabajos académicos (tareas, artículos, cuestionarios, etc.) los cuales no requieren ser impresos a color, a menos que se trate de una institución u organización donde se desarrollen trabajos a color y sea necesario imprimirlo así (como una organización de diseño gráfico), aunque si se tiene planeado realizar impresiones a color de forma masiva, hay que considerar que el costo para mantener este servicio será muy elevado.

- Buffer de memoria: Es una zona de almacenamiento de las impresoras donde se tiene la información que se desea imprimir.

  La PC trabaja más rápido que una impresora, sin el buffer de memoria, cuando la PC envía un archivo a imprimir tendría que esperar a que termine dicha impresión antes de imprimir otro documento. De forma similar, cuando el buffer de memoria se llena, la PC no puede enviar más documentos hasta que se libere espacio en dicho buffer.

Para impresoras de uso personal, el buffer de memoria puede ser lo más pequeño posible, ya que los documentos impresos (Como historiales académicos, tiras de materias, comprobantes de inscripción, etc.) son documentos que constan de una o dos hojas aproximadamente.

Para las impresoras de uso masivo se recomienda altamente tener un buen buffer de memoria, ya que esto permitiría atender más rápidamente a los usuarios y reducir las colas de espera.

- Interfaz de conexión: es el medio mediante el cual se hace la comunicación entre la PC y la impresora.

Si la impresora será manipulada por un solo equipo de cómputo, lo más común es utilizar puerto paralelo, serie ó USB. La velocidad de transferencia de datos para estos tres puertos es distinta, la menor de ellas es la del puerto serie, le sigue el puerto paralelo, y finalmente, el puerto USB es el que tiene mayor velocidad y actualmente es el más utilizado de los 3 (modelos antiguos de impresoras no cuentan con este último puerto).

Hay impresoras que son compartidas o bien que están conectadas a una red para ser usadas por múltiples usuarios, si la impresora está siendo compartida a través de otro equipo, la conexión recomendada es que sea por puerto paralelo o USB (por cuestiones de costos).

Si la impresora está conectada en red, puede realizarse mediante puerto Ethernet o enlaces inalámbricos como infrarrojos, Bluetooth o Wi-Fi.

El puerto infrarrojo no es muy utilizado, esta tecnología fue desplazada por Bluetooth, ambas tecnologías son de conexión a corta distancia y con velocidades de transferencia bajas, pero el infrarrojo tiende a ser incómodo por que se debe tener siempre alineados los dispositivos a conectar, y un pequeño movimiento puede causar la interrupción de la comunicación.

Wi-Fi ó Bluetooth.

Las ventajas que tiene Wi-Fi sobre Bluetooth son: el radio abarcado por la señal de Wi-Fi es mayor, conexiones y transferencia de datos más rápidas y utiliza más y mejores protocolos de seguridad.

Ventaja que tienen Bluetooth sobre Wi-Fi, el costo es menor.

La elección de la interfaz a utilizar esta vez no depende si la impresora será de uso masivo o personal, si no que dependerá del entorno en el cuál será utilizado.

Para la adquisición de una impresora hay que saber en primera instancia si será de uso personal o masivo.

Se considera impresora de uso personal aquella que es usada por una persona o por un pequeño grupo de personas, por ejemplo, por personal administrativo que se encarga de imprimir oficios de eventos realizados por los alumnos (por ejemplo constancias, tiras de materias, etc.). La cantidad de impresiones realizadas es relativamente pequeña.

Se considera impresora de uso masivo aquella que su función principal es imprimir todo aquel documento que el usuario necesita, como son impresiones de trabajos, presentaciones, avances de tesis, reportes de servicio social, etc. Este tipo de impresoras estarán trabajando la mayor parte del día.

Existen impresoras compartidas que son utilizadas por toda un área, al ser usada por más de una persona se podría denominar como impresora masiva, sin embargo, el termino personal o masivo lo estamos orientando a la cantidad de impresiones que se realiza y no a la cantidad de usuarios que la utilizan, es por ello, que este tipo de impresoras las consideraremos como personales.

Las licitaciones

Es un proceso de concurso entre proveedores, para adjudicarse la adquisición o contratación de un bien o servicio. Para ello, se deben fijar las bases del bien o servicio requerido y los proveedores deben realizar sus ofertas basadas en los requisitos establecidos.

Existen dos tipos de licitaciones:

1) Públicas: son aquellas donde se publican las bases del bien o servicio a adquirir y cualquier persona u organismo puede participar en el concurso establecido.
2) Privadas: son aquellas donde se envía una invitación y las bases solo a las personas u organismos a los que se les permitirá participar en el concurso.

Las etapas para llevar a cabo una licitación son:

- Definición de requerimientos: En las secciones anteriores de este mismo capítulo se hizo mención de las características más importantes de los equipos a adquirir, con base en ello, se podrá establecer las características o los requisitos mínimos.

- Selección de la licitación como mecanismo de compra: Si se trata de una entidad gubernamental o del sector público, tendrá que realizarse una licitación pública, si es una entidad privada se puede optar por una licitación privada.

- Elaboración de las bases: Son los documentos aprobados por la autoridad de la entidad en cuestión, en dichos documentos se establecen, de manera general y/o particular, los aspectos administrativos, técnicos y económicos del bien a adquirir.

- Llamado, periodo de consultas y recepción de ofertas: Periodo establecido en el que los proveedores podrán exponer sus productos, entregar documentos relacionados y realizar sus ofertas, es decir, es el periodo de tiempo en el cuál los proveedores deben convencer al cliente que su producto es el más conveniente.

- Evaluación de ofertas: una vez presentadas y entregadas todas las ofertas de los oferentes, se debe realizar el análisis y evaluación de cada una de ellas y verificar que cumplan con las especificaciones administrativas, técnicas y económicas. Cabe mencionar que las evaluaciones deben ser realizadas basándose en los criterios establecidos en las bases.

  Para el proceso de evaluación debe tomarse en cuenta aspectos importantes como:

  - Precio.
  - Plazo de entrega.
  - Duración de garantía.
  - Tiempo de respuesta en caso de falla.
  - Promociones.

  No necesariamente deben ser estos 5 puntos para realizar una evaluación, cada entidad define sus propios criterios de evaluación, pero estos criterios son los que recomendamos ampliamente.

- Adjudicación: Se efectuará a la oferta más conveniente y por medio de un acto administrativo debidamente notificado al adjudicatario y a los demás ofertantes.

No se pueden adjudicar ofertas cuando:

- No cumplen con todos los requisitos establecidos en las bases.
- El ofertantes está inhabilitado para establecer contratos con la entidad en cuestión.
- Proviene de una persona que no tiene el poder suficiente para efectuarla.

- Pasos posteriores: firma y entrega de documentos, entrega de bienes, verificación del equipo, etc. Cabe entidad puede definir los procedimientos a realizar en este último paso.

En México, las compras gubernamentales o del sector público, se regulan por las disposiciones de la Ley del artículo 134 Constitucional de los Estados Unidos Mexicanos:

"Los recursos económicos de que dispongan el Gobierno Federal y el Gobierno del Distrito Federal, así como sus respectivas administraciones públicas paraestatales, se administrarán con eficiencia, eficacia y honradez para satisfacer los objetivos a los que estén destinados.

Las adquisiciones, arrendamientos y enajenaciones de todo tipo de bienes, prestación de servicios de cualquier naturaleza y la contratación de obra que realicen, se adjudicarán o llevarán a cabo a través de licitaciones públicas mediante convocatoria pública para que libremente se presenten proposiciones solventes en sobre cerrado, que será abierto públicamente, a fin de asegurar al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes.

Cuando las licitaciones a que hace referencia el párrafo anterior no sean idóneas para asegurar dichas condiciones, las leyes establecerán las bases, procedimientos, reglas, requisitos y demás elementos para acreditar la economía, eficacia, eficiencia, imparcialidad y honradez que aseguren las mejores condiciones para el Estado.

El manejo de recursos económicos federales se sujetará a las bases de este artículo.

Los servidores públicos serán responsables del cumplimiento de estas bases en los términos del Título Cuarto de esta Constitución."

Bibliografía

http://www.impresoras-hp.com/caracteristicas-impresoras-laser.htm

http://es.wikipedia.org/wiki/Bluetooth

http://www.peco.com.ve/-para-que-sirve-la-memoria-ram-.php

http://es.wikipedia.org/wiki/Ethernet

http://www.masadelante.com/faqs/tipos-de-servidores

http://redesinformaticas.wikispaces.com/Tipos+de+servidores

http://www.funcionpublica.gob.mx/unaopspf/comunes/art134.htm

http://www.juridicas.unam.mx/publica/librev/rev/revdpriv/cont/9/dtr/dtr2.pdf

http://www.chilecompra.cl/secciones/formacion/documentos/guias-practicas-html/pdf/guia%208.pdf

Capítulo 9 - Malware y antivirus

Primeramente comencemos con las dos definiciones que le dan nombre a este capítulo.

Definición: Malware (**Mal**icious soft**ware** – Código malicioso)

Programa o código de computadora cuya función es dañar o causar un mal funcionamiento de un sistema.

Definición: Antivirus

Programa diseñado específicamente para detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominados malware).

¿Qué software entra en la categoría de malware?

Existen varias clasificaciones de código malicioso entre las que se encuentran:

- Virus.- Programas creados para infectar sistemas y a otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente y así interferir en el funcionamiento general del equipo, registrar, dañar o eliminar datos, perjudicar el sistema operativo o bien propagarse por otros equipos y a través de Internet.

  Su acción comienza al abrir un archivo infectado, el código que conforma al virus se guarda en memoria y se añade a los programas que se ejecuten ya que toma el control del sistema operativo. Dependiendo de la programación del virus es el daño que causa en el equipo infectado.

  Los virus de script son una subcategoría un de una variedad de lenguajes script (VBS, BAT, PHP, etc.). Una de las principales habilidades de los virus en script consiste en ser capaces de

enviarse con gran facilidad a través de programas de correo electrónico como Outlook o cliente IRC.

Las formas más comunes de infección son:

- El intercambio de dispositivos de almacenamiento como son las memorias USB, discos compactos, etc. provenientes de fuentes sospechosas o desconocidas.
- Al abrir un archivo adjunto (ya sean documentos, hojas de cálculo, archivos ejecutables, imágenes, etc.) contenido en un correo electrónico (algunos correos tienen documentos adjuntos con extensión vbs, que ya se menciono que pueden ser virus).
- Redes Peer-to-Peer que son aquellas utilizadas para distribuir software, música, videos, etc.

- Caballos de Troya (troyanos).- Un troyano o caballo de Troya es aquel programa que se hace pasar por un programa válido siendo en realidad un programa malicioso. Su objetivo es pasar inadvertido al usuario e instalarse en el sistema cuando este ejecuta el archivo "huésped". El troyano actúa sin el conocimiento ni consentimiento del usuario. Su nombre viene por la semejanza con el caballo que los griegos utilizaron para disfrazar su identidad y ganar la guerra contra la ciudad de Troya.

  Las formas más comunes de infección son:

  - Instalar algún programa que proviene de un sitio no confiable, software no oficial o que no cuentan con algún mecanismo de autenticidad (los proveedores de algunos programas incluyen en md5 para verificar la autenticidad).
  - Adquirir uno de estos códigos maliciosos mediante correo electrónico dentro de un archivo adjunto.

  Los caballos de Troya realizan múltiples acciones, llevando a cabo acciones destructivas, espiar, robar información (como contraseñas), inclusive descargar e instalar programas espía.

- Puertas traseras (Backdoors).- Abren un canal de comunicación en la computadora infectada que permite la conexión de otra computadora que realiza acciones maliciosas sin que el usuario víctima se dé cuenta.

- Gusanos de Internet (Worms).- Son programas desarrollados que buscan propagarse lo más rápido posible tratando de infectar al mayor número de equipos. No dependen de archivos portadores para contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema.

- Las formas más comunes de infección son:

    - Cualquier usuario que navega por internet puede ser infectado.

  Cuando un gusano infecta un equipo, éste ocupa un ancho de banda considerable así como espacio en memoria, ocasionando que los equipos se vuelvan excesivamente lentos en las respuestas a cualquier petición que el usuario haga al equipo. Sin embargo algunas versiones no afectan el rendimiento del equipo para evitar ser detectados por el usuario y de esta forma lograr garantizar su permanencia en el equipo.

  Existen gusanos que están programados para realizar acciones tales como detener algún servicio y de esta forma ocasionar que el equipo se reinicie sin autorización del usuario (un ejemplo de esto es el caso del gusano Blaster). También pueden incorporar otro tipo de malware como “puertas traseras”.

  Pueden duplicarse tal velocidad que pueden colapsar y tirar las redes en las que se infiltran.

- Bots.- Para nuestros fines Bots hace referencia a una computadora que ha sido comprometida y que ejecuta las instrucciones que el intruso ordena (en la literatura también puede encontrarse que hace referencia al diminutivo de robot).

  Los Bots son propagados a través de Internet utilizando a un gusano como transporte, envíos masivos de ellos a través de correo electrónico o aprovechando vulnerabilidades en navegadores. Los equipos infectados suelen formar redes de equipos “zombis”, que pueden ser utilizados por sus autores para lanzar ataques de denegación de servicios en forma distribuida, enviar correo electrónico no solicitado, etc.

- Software espía (Spyware).- Son programas “espía” que se instalan en las computadoras sin el conocimiento del usuario, recompilan información del usuario o de las computadora infectada, enviándola remotamente a otra persona. El spyware se puede dividir en dos categorías:

    - Software de vigilancia.- Encargado de monitorear todo el sistema mediante el uso de transcriptores de teclado y captura de pantallas. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas. Normalmente, este software envía información a sus servidores, en función a los hábitos de navegación del usuario.
    - Software publicitario.- También llamado adware (se hablara a continuación).

- Adware.- Cualquier programa que automáticamente se ejecuta, muestra o baja publicidad Web al equipo después de instalado el programa o mientras se está utilizando la aplicación. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en inglés.

- Exploit.- Software que ataca una vulnerabilidad particular de un sistema operativo.

Recomendaciones

Mucho del malware que infecta los equipos se instala sin nuestro consentimiento y muchas veces nadie se entera de ello, por lo que es conveniente:

- Mantener actualizado su sistema operativo (haciendo especial énfasis en Windows), ya que un sistema no actualizado puede estar propenso a distintos ataques de malware.

- Los navegadores es importante mantenerlos actualizados ya que puede ocasionar infecciones de spyware. Estos problemas surgen debido a huecos de seguridad existentes en los navegadores que utilizan ActiveX, que pueden permitir ejecutar código que instale este tipo de aplicaciones maliciosas. Otro tipo de trampas o engaños son las de crear sitios Web con código malicioso para que cuando un usuario que se encuentre utilizando ActiveX se acceda a esa página y se instale software malicioso en su equipo.

- Es importante mantener los mensajeros instantáneos actualizados (MSN Messenger, AOL, ICQ, Yahoo Messenger, etc.). Estos programas tienen características como: personalizar los contactos con los que se desea entablar comunicación, avisar sobre el arribo de nuevos correos electrónicos, transferir archivos, entablar comunicación por audio y/o video, entablar varias conversaciones a la vez, jugar en línea, entre otras y debido a ello se han vuelto una herramienta de la vida diaria tanto para el trabajo como para el hogar poniéndose en la mira de virus, caballos de Troya y gusanos.

- Recuerde que unos de los principales medio de infección es el correo electrónico, por lo que tenga control sobre las personas e instituciones a las que se les proporciona su cuenta de correo. Esta información es parte de su información personal y no debe ser difundida indiscriminadamente, así como revisar las políticas de privacidad que maneja cada institución (esto al registrarse en algún sitio) y saber que hará con nuestros datos antes de proporcionarlos.

- No abrir, responder, ni dar clic en enlaces o descarga de archivos adjuntos, que recibamos en correos electrónicos no solicitados de los cuales se desconozca el remitente.

- Ignorar correos cadena. Lo único que provoca esto es la acumulación de direcciones de correo que pueden ser usada para spammers[1].

- No contestar correo basura.

[1] Spam.- son mensajes no solicitados (basura), típicamente de tipo publicitarios, que son enviados masivamente. Se puede hacer por distintas vías por ejemplo wikis, foros, blogs, etc, sin embargo el más utilizado es el correo electrónico.

- Debido a que el uso de los equipos será compartido, recordar cerrar la sesión de correo al finalizar su uso.

- Instalar software antivirus (de esto hablaremos enseguida) y mantenerlo actualizado.

- No dar clic en ligas de dudosa procedencia como: videos de algún personaje público, dinero al instante, etc.

Antivirus

> *Definición: Programa diseñado específicamente para detectar y eliminar virus informáticos y otros programas maliciosos (malware). El software antivirus puede identificar y bloquear una gran cantidad de virus antes de que infecten un equipo de cómputo. Una vez que se instala es importante mantenerlo actualizado.*

El software antivirus analiza archivos en busca de ciertos patrones que puedan indicar una infección por malware, aunque los detalles varían entre los distintos paquetes. Los patrones que busca se basan en firmas o definiciones de virus conocidos. Los creadores de virus constantemente crean nuevos virus o actualizan los ya existentes, por tal motivo es importante instalar las últimas definiciones de virus en tu equipo.

La mayoría del software antivirus permite realizar dos tipos de escaneos en tu equipo de cómputo:

- Escaneos automáticos: Dependiendo del software que se haya elegido, es posible configurarlo de forma que automáticamente analice archivos o carpetas específicas o programarlo para que ejecute un análisis completo del equipo en ciertos intervalos de tiempo.

- Escaneos manuales: También, es una buena recomendación escanear archivos que se reciben de fuentes externas antes de abrirlos, especialmente correos electrónicos y memorias USB.

Cuando un antivirus encuentra algún tipo de malware (en escaneo automático o manual) la mayoría de ocasiones produce una ventana de alerta notificando que ha encontrado un malware (esto puede variar del antivirus y más específicamente de la configuración del mismo) y pregunta si se desea "limpiar" el archivo (remover el malware). Es recomendable verificar que el malware fue eliminado completamente, primero esperando la retroalimentación de software confirmando la eliminación exitosa o bien el fallo, ya que no es inusual que el antivirus no pueda eliminar completamente el malware. Eliminado el malware se debe también hacerse un segundo escaneo manual para buscar otro malware o bien tener una segunda confirmación de la eliminación. En caso de que el malware no pueda ser eliminado por el antivirus o bien si desea cerciorarse si tu equipo

está infectado existen varias herramientas gratuitas (escaneos en línea o antivirus libres) que pueden ayudar, como son:

Compañía	Página Web
	http://www.eset.com
	http://housecall.trendmicro.com
	http://www.pandasoftware.es
	http://www.bitdefender-es.com
	http://security.symantec.com
	http://www.kaspersky.com
	http://us.mcafee.com

Tabla 9.1. Compañías de antivirus

Los daños que puede provocar el malware en este punto ya son fáciles de observar y se mencionaran los siguientes:

a) Consumir recursos del equipo ocasionando la baja de la productividad.

b) Robo de información.- Como ya se menciono puede ser robada cualquier tipo de información desde contraseñas hasta archivos completos que pueden ser sensibles para los usuarios.

c) Mal funcionamiento del equipo.

d) Que el equipo sirva como atacante a otros equipo, esto en el caso de que sea controlado por alguna persona con estas intensiones.

Como puede verse los daños que puede causar el malware son graves y por ello debe tenerse algún software que proteja los equipos, sin embargo, esto tiene un costo (así es $ dinero) y para seleccionar el que se adecue a nuestros requerimientos y necesidades debe analizarse varios candidatos. Para ello existen varios análisis que pueden ayudarnos a ello, por ejemplo la empresa

"Av Comparatives[2]" publica un análisis con sus resultados a las pruebas que los someten. Aquí un ejemplo

Niveles de certificación	Mejor producto
AVIRA	1. Symantec
Kingsoft	2. Kaspersky
F-Secure	3. ESET
Sophos	
Kaspersky	
Microsoft	
Avast	
Symantec	
ESET	
McAfee	

Tabla 9.2. Resultados del 2009.

Teniendo el estudio como preámbulo para seleccionarse el más adecuado debe hacerse un estudio propio de beneficio-costo-rendimiento tomarse en cuenta los equipos con los que se dispone, ya que típicamente los antivirus consumen muchos recursos ya que el análisis de los archivos es costoso (en recursos computacionales).

No sugerimos necesariamente un estudio que requiera muchos recursos económicos, lo cual es la típica limitante, bastara documentarse en sitios especializados o de divulgación y si es posible probar algunos antivirus en los equipos. La mayoría de ellos cuentan con versiones de prueba (trial) que pueden descargase de sus sitios oficiales y tienen opción a actualizarse.

[2] La empresa Av Comparatives es una empresa Austriaca sin fines de lucro que proporciona pruebas de antivirus al público.

Programas de reinicie y restaure

Existen programas que restauran el sistema operativo a un mismo estado (también llamado estado original, definido por el administrador) sin importar los cambios que se le hagan, a este tipo de software se le clasifica como de tipo “reinicie y restaure”, es decir, al momento de reiniciar el equipo, se volverá a tener su estado original.

Bibliografía

http://seguridad.unam.mx

http://www.eset.com

http://housecall.trendmicro.com

http://www.pandasoftware.es

http://www.bitdefender-es.com

http://security.symantec.com

http://www.kaspersky.com

http://us.mcafee.com

Capítulo 10 - Instalación de un equipo servidor

Este capítulo va dirigido a programadores, administradores y toda aquella persona que tengas las nociones básicas de redes de computadoras, programación en Shell y manejo básico-intermedio de Sistemas Operativos Linux.

El objetivo no es dar al usuario un manual o un curso de cómo utilizar Linux, su objetivo es mostrar una metodología que sirva como guía al usuario en la toma de decisiones para instalar y configurar un Servidor de acuerdo a sus necesidades, para fines prácticos y evitar la expansión de este capítulo, no se hará mención de conceptos ni comandos básicos, tampoco se hará mención de la configuración de la red para Sistemas Operativos Linux. Los temas aquí tratados son sólo una sugerencia personal que hemos seguido durante nuestra experiencia en el tema, es responsabilidad del usuario el seguir, parcial o totalmente, ésta metodología.

Un equipo servidor ("Servidor" de ahora en adelante) es aquel equipo capaz de brindar algún(os) servicio(s) para algún(os) cliente(s). Un cliente puede ser una persona, un equipo de cómputo u otro dispositivo.

Consideraciones iniciales:

- De ser posible, un servidor debe brindar un único servicio, es decir, tener equipos o servidores dedicados.
- Si un servicio tiene una demanda muy fuerte, habrá que pensar en distribuir la carga generada en diversos servidores, esto para evitar la saturación y "caída" del servicio.
- Cada equipo servidor debe estar acompañado por su unidad de respaldo de energía (UPS), dado que son equipos que brindan servicios de vital importancia se debe asegurar en lo mayor posible la disponibilidad de dichos servicios.
- Dedicar un espacio físico suficiente para tener el servidor, el cual deberá tener un ambiente adecuado (luminosidad, temperatura, humedad, etc.).

Planeando la instalación de un servidor

Los pasos a seguir para la instalación, configuración y puesta en macha de los servicios a brindar en un Servidor con Sistema Operativo Linux son:

- Elección del sistema operativo.
- Planear la estructura de los directorios.
- Establecer contraseñas.
- Conexiones remotas.
- Firewall.
- Instalación y configuración de servicios.
- Instalación y configuración del sistema de respaldo.
- Instalación y configuración de scripts personales.
- Configuración de tareas automatizadas.
- Instalación de herramientas de seguridad.
- Mantenimiento al servidor.

Elección del sistema operativo [1]

Se ha elegido instalar la distribución Debian, que es una distribución de Linux orientada a servidores y no al usuario final, otras distribuciones orientadas a servidores son Red Hat Enterprise y Suse Enterprise (no son los únicos).

Debian es gratuito y está en constante actualización por una comunidad a nivel global, lo cual permite encontrar los errores existentes y corregirlos de la mejor forma posible.

La primera recomendación es instalar solo el sistema base (se lleva a cabo mediante una instalación con netinstall), y posteriormente solo instalar los paquetes necesarios para evitar el

[1] "Podría ganar dinero programando software propietario, y posiblemente me divertiría escribiendo código. Pero yo se que al final de mi carrera, vería hacia atrás y me daría cuenta que invertí muchísimos años construyendo murallas para dividir a la gente, en lugar de hacer algo por unirla" – Richard Stallman

consumo innecesario de recursos que disminuyan la eficiencia del equipo, inclusive, recomendamos no instalar el entorno gráfico[2].

Debian está estructurado por un conjunto de directorios, cada uno de ellos tiene un propósito distinto y pueden ser usados por ciertos usuarios, por el administrador del equipo (también llamado superusuario ó "root") o por el propio sistema operativo (solo se hará mención de alguno de ellos para fines prácticos). Los directorios más importantes son:

/ (raíz) – De aquí parten todos los directorios del sistema operativo.

/home – Llamado "home directory" y es el lugar donde, por default, se almacenan los directorios de los usuarios normales (recordando que Unix es un sistema operativo multiusuario).

/usr – contiene librerías, documentos y programas que los usuarios normales pueden ejecutar.

/sbin – Contiene los programas que el root puede ejecutar.

/etc – Contiene archivos de configuración del sistema.

/lib – Contiene las librerías compartidas para la mayoría de las operaciones del sistema.

/var – Contiene las bitácoras del sistema, archivos de correo de los usuarios, archivos enviados a imprimir, entre otros.

/root – "Home directory" del root.

/dev – Contiene las referencias a los dispositivos detectados por el sistema operativo.

Swap – Memoria de intercambio, este espacio reservado es utilizado para evitar la saturación de la memoria RAM física del equipo, ésta debe ser al menos el doble de la memoria RAM, para servidores con memoria RAM mayor a 1GB no es necesario instalar la swap.

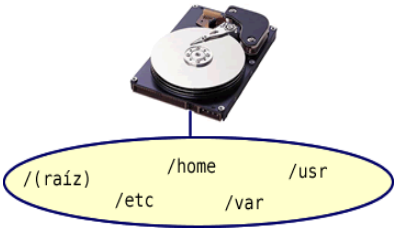
Planear la estructura de los directorios.

Antes de comenzar la instalación del sistema operativo (S.O.) se debe tener en mente cual es la función del servidor con el fin de planear la distribución óptima del espacio en disco duro de los directorios más importantes.

Los directorios pueden estar repartidos en una sola partición, en distintas particiones de un solo disco duro e incluso en múltiples discos duros. La mayor prioridad para decidir la distribución de los directorios es el hardware disponible.

- Instalación en una sola partición en un solo disco duro: Esta instalación presenta las siguientes características:

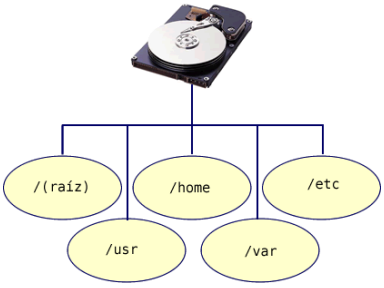
[2] Más información consulte el sitio oficial http://www.debian.org



Ventaja.- Sencillo de instalar, utilizar y darle mantenimiento.

Desventaja.- En caso de avería del sistema operativo, si no se cuenta con el respaldo o espejo correspondiente, habrá que instalar y configurar nuevamente todo el sistema operativo y las aplicaciones requeridas.

- Instalación en diversas particiones en un solo disco duro: Esta es la configuración es la más recomendable por cuestiones de eficiencia y costo. Tiene las siguientes características:

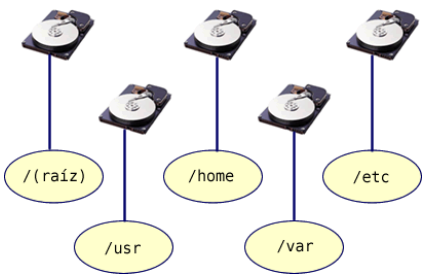


Ventaja: Cada partición mantiene su información por separado.

Desventaja: Se debe tener planeada la estructura de los directorios y dar un estimado de cuanto espacio debe utilizar cada directorio para evitar la saturación de espacio de una partición lo que ocasionaría que algunos servicios dejaran de funcionar.

Por ejemplo, se crean dos particiones, una para /usr y otra para /usr/local, si /usr está al 30% de su capacidad y /usr/local está al 100%, no se podrá almacenar más información en /usr/local aunque sea un subdirectorio de /usr, ya que están en particiones distintas y no pueden actuar como una sola para compartir el espacio disponible.

- Instalación en diversas particiones y distintos discos duros: Es la configuración más complicada, cara y más segura.



En caso de que algún disco duro sufra algún daño, no se verá afectado ningún otro disco duro, por lo que la información estaría intacta (esta configuración es muy efectiva para sistemas RAID1 y RAID10, para mayor información puede consultar el capítulo 7).

En caso de que el servidor sufra alguna intrusión, al invasor le será más difícil poder acceder a otros discos duros que a otras particiones.

Establecer contraseñas

Es muy importante:

- Siempre tener una contraseña para cada usuario y para cada servicio que así lo requiera.
- Utilizar contraseñas con longitud mínima.
- Utilizar la combinación de letras mayúsculas, minúsculas y símbolos especiales.
- Crear la contraseña basada en una frase o palabras que ayuden al usuario a recordarla.
- Cambiar las contraseñas periódicamente, establecido en las políticas por cuestiones de seguridad.
- NO utilizar palabras comunes o fechas, ya que se pueden corromper muy fácilmente por un ataque de diccionario.

Las contraseñas en Linux.

Las contraseñas para los usuarios son almacenadas dentro del archivo configuración shadow, típicamente se localiza en /etc/shadow.

```
tesis@unam# cat /etc/shadow | grep portafolio09
portafolio09:$1$i7ctx0J0$lz6gsrQ4LWe.UaTxxqiWB.:14522:0:99999:7:::
tesis@unam#
```

El archivo shadow, entre otras cosas, contiene el nombre del usuario y su correspondiente contraseña encriptada. Cada elemento de este archivo está separado por el símbolo de dos puntos (:), en la imagen anterior, el usuario es portafolio09 y la contraseña encriptada es 1i7ctx0J0$lz6gsrQ4LWe.UaTxxqiWB. (Incluyendo el punto final).

Para modificar alguna contraseña se usa el comando passwd (man passwd).

Conexiones remotas

Todo servidor debe ser administrable de forma remota, ya que en caso de que falle alguno de sus servicios, éste debe ser arreglado lo más pronto posible (disponibilidad).

Primeramente se debe verificar que esté instalado solo un programa de conexión remota, el más recomendado es Open Secure Shell (OpenSSH[3]), ya que maneja conexiones seguras mediante el puerto estándar destinado para ello (puerto 22) y maneja la encriptación de información para que en caso de que exista un ataque de MIM (Man In the Midle), éste solo verá la información

[3] Más información acerca del uso de Open SSH consulte el sitio oficial http://www.openssh.org.

encriptada y no le servirá de nada (recuerde que el proteger el servidor no quiere decir que el medio de comunicación esté protegido).

OpenSSH contiene, entro otras cosas, dos módulos de gran importancia:

- SSH – Client: sirve para poder conectarse a otro equipo.
- SSh – Server: permite que otros equipos se puedan conectar al servidor.

Una vez instalado OpenSSH (client y server), se debe verificar al menos tres aspectos importantes en cuestión de seguridad. Esto se verifica en el archivo de configuración de OpenSSH, el cual típicamente se encuentra en /etc/ssh/sshd_config.

- No permita la conexión directa del usuario root: característica PermitRootLogin.
- No permita contraseñas en blanco: característica PermitEmptyPasswords.
- Solo permita la conexión de usuarios establecidos: características AllowUsers, DenyUsers, AllowGroups y DenyGroups.

Cada vez que se cambia el archivo de configuración de una aplicación, no es necesario reiniciar todo el equipo, solo el (los) servicio(s) relacionados. Y es importante verificar que los cambios sean los efectivos.

Para reiniciar el servicio de OpenSSH use el comando:

```
#/etc/init.d/ssh restart
```

En el directorio /etc/init.d se encuentran los procesos en ejecución y pueden detenerse, reiniciarse o iniciarse mediante los parámetros “stop”, “restart” y “start” respectivamente.

Cancelar otros servicios de conexión remota

Se deben cancelar otros servicios que tienen la misma finalidad, ya que el no hacerlo, es una vulnerabilidad que pondría en riesgo al servidor, estos servicios son “telnet” y “ftp”.

Para cancelar estos servicios basta con comentar las líneas respectivas en el archivo de configuración “services”, éste archivo es una lista de los servicios de red de Internet, ubicado en /etc/services.

Para que los cambios tengan efecto, se debe reiniciar los servicios que fueron modificados, en caso que se hayan realizado muchos cambios se puede optar por reiniciar el “run level” o bien todo el equipo.

Firewall

El firewall (“cortafuegos” en español) de sistemas Linux se configura de forma manual mediante la herramienta iptables (kernel 2.4 o superior), aunque también se ofrecen herramientas gráficas que permiten hacer la configuración.

Se mencionará la forma de planear un firewall de alta seguridad mediante el uso de iptables. Durante el desarrollo no se mencionara la parte gráfica debido a dos principales razones:

1) El configurar un entorno gráfico del sistema operativo y la herramienta gráfica para dicha labor, reduce el desempeño del servidor.
2) Es mejor una instalación manual, ya que así se comprende que es lo que el firewall está haciendo y es más rápido y eficiente darle mantenimiento.

El firewall de Linux consta de un conjunto de reglas en las cuales se especifica al sistema que está permitido y que negado, entre más detalladas sean las reglas, mejor será nuestra protección.

Por ejemplo, observe las siguientes reglas:

- Permitir el acceso al protocolo TCP.
- Permitir el acceso al protocolo TCP por el puerto 22.
- Permitir el acceso al protocolo TCP por el puerto 22 a mi LAN.
- Permitir el acceso al protocolo TCP por el puerto 22 a mi LAN que entra por la interfaz 1.
- Permitir el acceso al protocolo TCP por el puerto 22 a mi LAN que entra por la interfaz 1, que no tengan cierta dirección MAC.

Observe que, en forma ascendente, cada una de las reglas es más restrictiva que las anteriores, la última regla es la más robusta por lo que ofrece un mayor nivel seguridad.

Para que el firewall permita conexiones, se debe conocer los puertos a los que se les permitirá el acceso, por ejemplo:

- Servidor Web: se permite el puerto 80.
- Servidor Web seguro (https): se permite el puerto 8080.
- Servidor de base de Datos con Postgresql: se permite el puerto 5432.
- Servidor de archivos con ftp: se permiten los puertos 20 y 21.

Estos puertos son los utilizados por defecto y pueden cambiarse en los archivos de configuración de cada aplicación.

Políticas del firewall.

DROP niega todo y sólo permite lo que se establezca en las regla, es más segura pero más complicada de configurar.

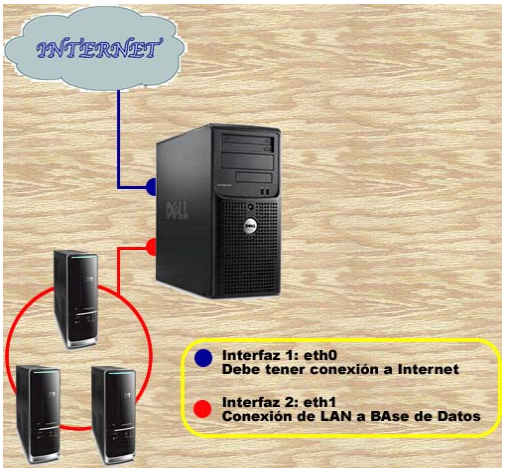
ACCEPT permite todo a excepción lo que se establezca en las reglas, es más insegura pero sencilla de configurar.

Para servidores, la mejor política es DROP, ya que con la política ACCEPT es más probable que queden huecos de seguridad (vulnerabilidades).

Forwarding

Otro aspecto que es tratado en el firewall es la comunicación entre interfaces, es decir, permitir o negar el paso de paquetes entre interfaces.

Ejemplo: suponga que se tiene un servidor Web y de Bases de Datos (mostrado en la figura siguiente), el cual tiene 2 interfaces de red, la primera (eth0) es para tener conexión a Internet y la otra (eth1) es para permitir a una red LAN el acceso a las bases de datos. Además, se quiere permitir la conexión remota a través de OpenSSH (puerto 22).



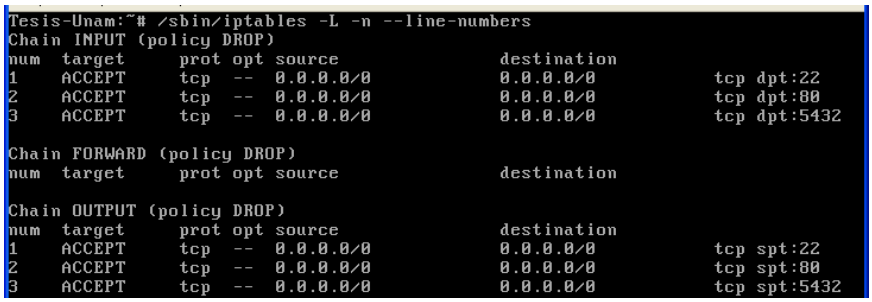
Solución:

```
Tesis-Unam:~# cat firewall.sh
#Paso 0: Limpiar el firewall de las reglas que se tengan
/sbin/iptables -F       #Se limpian todas las reglas
/sbin/iptables -X       #Se eliminan todas las reglas
/sbin/iptables -Z       #Se escribe zeros en las reglas

#Paso 1: Establecer la política DROP
/sbin/iptables -P INPUT DROP    #Se niega todo lo que quiera entrar
/sbin/iptables -P OUTPUT DROP   #Se niega todo lo que quiera salir
/sbin/iptables -P FORWARD DROP  #Se niega la comunicación entre interfaces

#Paso 2: Permitir la conexión remota
/sbin/iptables -A INPUT -p tcp --dport 22 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

#Paso 3: Permitir la conexión con Web
/sbin/iptables -A INPUT -p tcp --dport 80 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

#Paso 4: Permitir la conexión a la base de datos con Postgresql
/sbin/iptables -A INPUT -p tcp --dport 5432 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --sport 5432 -j ACCEPT
```

Con esta configuración solo se dejan abiertos los puertos requeridos y se tiene bloqueada la comunicación entre interfaces.

Verificación de las reglas

Para comprobar que las reglas estén funcionando correctamente puede hacer pruebas con los puertos en cuestión y/o revisar las reglas activas establecidas en iptables.



Nótese que en cada cadena de INPUT, OUTPUT y FORWARD se muestra la política establecida y el orden numérico en el que se establecieron las reglas, cabe mencionar que el orden de las reglas es muy importante, ya que este orden también es el que establece la prioridad, la primer regla es la que tiene mayor prioridad sobre las otras (0.0.0.0/0 es el equivalente a “Cualquier lado”).

Con esta configuración se asegura que no se podrán utilizar otros puertos además de los establecidos, pero se puede ser más específico en las reglas para tener mayor seguridad, en la interfaz eth0 debe tener conexión a Web, pero no a base de datos, se puede especificar que el puerto 80 y 22 sean de uso exclusivo para eth0 y el puerto 5432 sea de uso exclusivo para la interfaz eth1.

Instalación y configuración de servicios

La instalación de paquetes puede realizarse de 2 maneras: con la herramienta apt o manual.

Instalación con apt (solo para distribuciones Debian y Ubuntu)

La ventaja de usar apt es que automáticamente se descargará, desempaquetará y se instalarán paquetes los necesarios y se instalará la aplicación solicitada. La desventaja es que puede ser posible que no se obtenga la versión más reciente.

Si se utilizará la herramienta apt, antes de instalar cualquier paquete es recomendable ejecutar la herramienta apt-get update para que obtenga la lista de los paquetes más actuales que se encuentran en los repositorios (servidores encargados de distribuir los paquetes del sistema

operativo) configurados desde la instalación (para modificar la lista de repositorios, puede editarse el archivo de configuración de apt /etc/apt/sources.list).

Lo anterior NO garantiza que se obtendrán los paquetes y aplicaciones más actuales, solo obtendrá lo más nuevo que se encuentra en los repositorios. Para obtener los paquetes y aplicaciones más actuales deben ser descargados desde el sitio oficial de cada uno de ellos.

Comando APT[4]	
Parámetros	**Acción**
Apt-get update	Actualiza la lista de paquetes disponibles
Apt-cache search paquete	Busca paquetes relacionados con paquete
Apt-cache policy paquete	Muestra el estatus de paquete
Apt-get install paquete	Instala paquete
Apt-get remove paquete	Desinstala paquete

Tabla 10.1. Herramienta APT y algunos de sus parámetros

Instalación manual

La ventaja de una instalación manual es que se puede personalizar la instalación y se puede obtener la versión más reciente, esto se hace visitando el sitio oficial de la aplicación del servicio que se quiere brindar, por nombrar a algunos están:

- Servidores Web (apache): http://www.apache.org
- Servidor Proxy (apache): http://www.apache.org
- Servidor de Base de Datos (postgresql): http://www.postgresql.org
- Servidor NAT (Firestarter): http://www.fs-security.com

Para instalar estas u otras aplicaciones necesita:

- Descargar la aplicación.
- Comprobar la integridad del paquete descargado. En el sitio oficial de cada aplicación se puede descargar algún medio para verificar la integridad del paquete, por ejemplo el MD5 del paquete.
- Descomprimir y/o desempaquetar la aplicación.
- Verificar los requisitos para instalar la aplicación.
- Configurar el archivo necesario para la instalación (make file) e instalar la aplicación.

[4] Más información acerca del uso de apt, consulte su manual (man apt).

- Configurar la aplicación: Una vez instalada, se debe configurar su funcionamiento y características en el archivo de configuración correspondiente.
- Reiniciar o comenzar la aplicación.

Instalación y configuración del sistema de respaldo

Para crear un sistema de respaldo puede hacerlo mediante herramientas dedicadas a esta tarea (como lo es rsync) o bien con un script personal.

Independientemente si el respaldo es elaborado con una herramienta o un script personal, se debe programar esta tarea para que se ejecute cada cierto tiempo, esta tarea será mencionada posteriormente en este mismo capítulo.

Para mayor información acerca de este tema puede consultar el apartado “Datos” del capítulo 7: “Sistemas de respaldo”.

Instalación y configuración de script personales.

El administrador puede crear scripts que ejecuten ciertas tareas, de acuerdo a las necesidades que se tengan, para que los script puedan ser ejecutados deben tener los permisos de ejecución, ya sea para el propietario del script, al grupo o cualquier persona, todo depende del objetivo del mismo script.

Ejecutar un script

El primer paso para ejecutar un script es brindar los permisos de ejecución del script mediante el comando chmod (man chmod).

Para ejecutar un script existen 3 formas distintas:

1) Utilizar la ruta absoluta o relativa donde se encuentra el script.
2) Definir en el PATH la ruta donde se encuentra el script,
3) Crear un enlace suave del script en una ruta que este definida dentro del PATH, como lo es /usr/local/bin.

Los scripts contienen instrucciones que se pueden ejecutar como si estuviera trabajando en la terminal, además de que puede combinar la programación en Shell con otros lenguajes de programación (ansi-c, java, perl, awk, etc.), para obtener otro tipo de resultados.

En algunas distribuciones Linux, cuando se va a crear un script, la primera línea debe ser:

#!/bin/bash

Con esto, el Shell de Linux reconoce al archivo como una secuencia de instrucciones, si no se tiene esta primera línea, no se podrá ejecutar el script.

Configuración de tareas automatizadas.

La automatización de tareas las catalogamos de acuerdo al momento en que se requiere que actúen:

- Por tiempo.
- Por runlevel.
- Por horario.

Por tiempo.

En esta catalogación, se utiliza la herramienta "sleep", la cual hace un delay o retardo en el sistema especificado en segundos (man sleep).

Por runlevel (nivel de ejecución).

En sistemas operativos Unix, se utiliza el término runlevel para especificar el modo de operación del sistema operativo, o mejor dicho, las aplicaciones que se ejecutarán automáticamente y en un cierto orden en el equipo.

Los runlevel estándar están definidos del 0 al 6 de la siguiente forma (puede haber variantes en cada una de las distribuciones Linux):

0. Apagado del equipo.
1. Sistema monousuario (un solo usuario).
2. Multiusuario sin soporte de red.
3. Multiusuario con soporte de red.
4. No usado.
5. Multiusuario con soporte de red y entorno gráfico.
6. Reinicio del equipo.

Al iniciar el equipo, se consulta el archivo de configuración /etc/inittab para saber que runlevel ejecutar, para saber que runlevel está activo, se puede usar el comando "runlevel" o "who –r".

¿Cómo se puede saber que se ejecuta en cada runlevel?. Dentro del directorio /etc existen los directorios rc1.d, rc2.d… rec6.d, cada directorio corresponde a un runlevel y contiene los script que se ejecutan al momento de entrar al runlevel correspondiente.

En cada directorio rc se encuentran los scripts y/o enlaces suaves a ejecutar, cada elemento debe comenzar con la letra S mayúscula o K mayúscula seguida de un número y de una palabra, la letra S indica de que el script está habilitado, la K indica que está deshabilitado, el número indica el orden ascendente en que se ejecutarán los scripts, y finalmente la palabra es solo indicador para el usuario.

Para iniciar un runlevel se utiliza el comando /sbin/init seguido del número del runlevel al que se quiere acceder, solo el usuario root puede hacer esta acción.

¿Cómo programar una tarea en un runlevel?, simplemente se hace un enlace suave (man ln) dentro del directorio del runlevel donde se quiere que se ejecute la tarea.

Por horario

Se puede programar la tarea para que se ejecute de acuerdo a un horario establecido, para ello se utiliza la herramienta llamada “crontab”, con esta herramienta, las tareas se pueden programar de acuerdo a los siguientes parámetros:

- La hora: (0 a 23 hrs).
- Los minutos: (0 a 59 minutos).
- El día del mes: (de 1 a 31 día).
- El día de la semana: (0 - 7, el 0 7 el 7 representan el día domingo).
- El mes: (1-12 meses).

Se debe editar la tabla del crontab utilizando el parámetro –e (crontab -e), cada línea de ésta tabla representa una tarea, la sintaxis para crear tareas es:

[minutos][hora][dia][mes][dia_de_la_semana][comando]

Puede utilizar el comodín (*) dentro de las tareas programadas.

Cada usuario tiene su propia tabla de tareas programadas, sin embargo, los privilegios para ciertas acciones se siguen manteniendo (un usuario normal no podría utilizar comandos que solo el root puede usar, por ejemplo, la herramienta iptables).

Para editar las tareas programadas se utiliza el comando “crontab –e”, para consultar las tareas programadas, se utiliza el comando “crontab –l”, para borrar todas las tareas programadas del usuario se usa el comando “crontab –r.

Instalación de herramientas de seguridad

Se pueden instalar herramientas para la elaboración de pruebas de seguridad y/o para mayor protección del servidor, a continuación se describe en forma breve algunas de ellas.

- Ethereal: Programa para elaborar escaneos de los paquetes de red (sniffer).
- Nmap: Escaneo de puertos.
- Jhon the Ripper: Realizar ataques de diccionario.
- Hydra: Realizar ataques por fuerza bruta.
- Jail: Crea espacios llamado “jaulas”, las cuales pueden aislarse del resto del espacio del disco duro, usado normalmente para conexiones remotas, para evitar que los clientes puedan salir de esa “jaula” y estar navegando por todo el servidor.
- Ecryptfs: Cifra sistemas de archivos en Linux.
- Sleuth kit: Conjunto de herramientas para análisis forense.
- Snort: Herramienta para la detección de intrusos en la red.
- Netcat: Es conocida como la navaja suiza del protocolo TCP/IP, en breve, sirve para leer y escribir datos a través de conexiones de red utilizando el protocolo TCP o UDP.

Mantenimiento del servidor.

Es muy importante darle mantenimiento continuo al servidor para asegurarnos de que no tendrá fallas posteriores y evitar la interrupción de algunos de sus servicios.

Para un correcto mantenimiento de un servidor, se debe monitorear constantemente:

- La cantidad de memoria utilizada mediante el uso del comando “free –tom” para evitar la saturación, una mala instalación de algún paquete o el uso inadecuado del servidor pueden ser causa de esto. El saturar la memoria hace que el servidor este más lento de lo normal e incluso que se quede “congelado” y todo deje de funcionar.

- El espacio utilizado en las particiones del disco duro para evitar su saturación, la falta de espacio puede ocasionar que algunos servicios no se puedan ejecutar, en especial, debe tener cuidado con el directorio /var, si este llega a estar saturado, no se podrán almacenar mas bitácoras, las aplicaciones en Linux no se pueden ejecutar si no se tiene de escritura a su bitácora correspondiente. El monitoreo se puede hacer mediante el uso de la herramienta "df".

- Los últimos accesos que se han tenido al sistema mediante el uso del comando "last".

- Que los usuarios conectados sean usuarios autorizados, esto mediante el comando "who".

- El estatus de la red mediante el uso de la herramienta "netstat –a".

- La no existencia de procesos extraños mediante el uso del comando "ps –fea".

- La no existencia de nuevas cuentas de usuario (de personas o de aplicaciones) sin previa autorización, esto mediante la verificación del archivo /etc/passwd.

- El estatus del firewall mediante la herramientas "iptables –L –n".

- Revisar las bitácoras del sistema y de las aplicaciones, que por default son encontradas en el directorio /var/logs, con más detalle se puede hacer un análisis forense (no se entrará en detalle con este punto, porque su extensión es demasiado grande para ser considerada en este capítulo).

Algunas veces será necesario darle mantenimiento al sistemas y/o a sus aplicaciones, en cuyo caso, tendrá que acceder al runlevel 1, en el cuál se carga la menor cantidad de aplicaciones, no se tendrá funcionamiento de la red (el mantenimiento tiene que hacerse "in situ ") y los clientes conectados no podrán utilizar el servidor durante este periodo de tiempo.

Bibliografía

Manual page de cada uno de los comandos utilizados.

http://www.dgsca.unam.mx/software-de-interes-para-la-comunidad-unam/#ohsi

http://www.debian.org

http://fs-security.com

http://www.apache.org

http://www.postgresql.org

www.google.com/linux

http://www.sleuthkit.org/

http://www.snort.org/

http://netcat.sourceforge.net/

http://www.antoniomtz.org/2009/06/hackeando-passwords-fuerza-bruta-brute-force-con-hydra/

http://freeworld.thc.org/

http://www.scribd.com/doc/6963842/NetCat-para-Ignorantes

http://www.openwall.com/john/

http://www.oreillynet.com/cs/user/view/cs_msg/23694

Capítulo 11 - Políticas de un centro de cómputo

Primeramente se debe dejar claro que la intención del presente capítulo no pretende proponer un documento que deba ser seguido "al pie de la letra", ni por el usuario o por la institución. El objetivo es proponer lineamientos generales y ejemplos para lograr la creación de este documento.

El documento de políticas de uso es fundamental sin el cual el rol del administrador solo se complica innecesariamente, increíblemente este un documento que rara vez se encuentra o está mal elaborado.

Para evitar problemas de jerarquía este documento debe ser firmado preferentemente por la persona que tenga el cargo más alto de la institución (de no ser posible, la firma de la persona encargada de la unidad informática bastara), de esta manera el documento tendrá suficiente autoridad para ser obligatorio para cualquier persona, esto incluye claro al administrador del centro de cómputo.

Tener el documento firmado por la máxima autoridad dentro de la institución no es suficiente, los usuarios del centro (o en caso de prestarme algunos servicios extras como NAT) deben manifestarse de enterados y estar de acuerdo con el documento.

Definiremos política como:

> "Las acciones generales de un modo bastante abstracto que indica que está y que no está permitido en la operación general del centro de cómputo."

Ahora de acuerdo a la definición debemos dejar claro que está permitido y que no en el centro de cómputo, cada caso puede tener particularidades, por ejemplo, no permitirse el uso de mensajeros instantáneos, sin embargo, dejando a un lado el principal uso de este software, conversaciones entre conocidos sin mucha relevancia en el centro, el mensajero puede servir como un medio de comunicación muy efectivo entre personas, lo más evidente seria pensar que existen otros métodos y eso es claro y es por ello que las políticas deben diseñarse "a la medida" para así recoger las características propias de cada centro.

Las políticas deben tener las siguientes características:

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.

- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Las políticas cuyo principal objetivo es permitir un uso adecuado no tienen una solución definitiva, sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables.

Separación de políticas y procedimientos

El documento de políticas es un documento típicamente de un par de páginas, en contraposición de los procedimientos que son documentos bastante largos y detallados, donde se explican a detalle cómo se van a implementar las políticas.

Al ser el documento de procedimientos un documento derivado, el personal operativo puede adecuar el documento de procedimientos sin necesidad de pasar por todo el proceso burocrático que significaría modificar las políticas.

Esta separación se hace debido a que políticas adecuadas para el momento en que son elaboradas con el paso del tiempo se vuelven obsoletas, inclusive tratando de seguir las recomendaciones anteriores.

Ejemplos de políticas

Uso del equipo:

El usuario deberá utilizar el equipo asignado en actividades relacionadas con el ámbito académico.

Queda prohibido guardar archivos que contengan música, fotografías o cualquier otro tipo de archivo que no se relacione con el ámbito de la institución.

El usuario tiene la responsabilidad de avisar oportunamente sobre cualquier anomalía detectada en los diferentes sistemas.

Queda prohibida la instalación de cualquier hardware adicional a los equipos. El usuario podrá solicitar al responsable, la instalación de software específico el cual requiera permisos de administrador.

Las solicitudes de soporte técnico, asesoría y capacitación deberán presentarse de manera oportuna al responsable, para que éste evalúe y lleve a cabo la prestación del servicio.

Seguridad:

Las cuentas y contraseñas que les sean proporcionadas son intransferibles, por lo que es responsabilidad de cada usuario conservarlos en un lugar seguro.

Es importante cambiar con frecuencia la contraseña y no compartirla.

Generales:

Queda estrictamente prohibido a los usuarios fumar frente a su Equipo de Cómputo o consumir bebidas o alimentos.

Cómo concluir el documento

En las políticas es importante dejar claro que estas incluyen a TODO el personal que usara los equipos, es decir, también el administrador y para darle autoridad al documento es conveniente escribir por quien fue aprobado, normalmente alguien con un alto grado en la institución típicamente el director, algún jefe de la unidad de computo o bien comité o junta:

> *"El presente documento fue aprobado por Nombre y entrará en vigor al día siguiente de su aprobación."*
>
> *Como ya se menciono las políticas deben irse adaptando a las nuevas tecnologías y es por ellos que es conveniente considerarse esto en el documento:*
>
> *"Cualquier punto no contemplado en estas políticas será estudiado y resuelto, por "Nombre del o de los responsables."*

Capítulo 12 - Sistema Administrativo de Recursos y Estadísticas (SIARE)

El propósito de este capítulo es presentar nuestra propuesta para la elaboración de un sistema que ayude al administrador a monitorizar y organizar los servicios más comunes que pueden ser brindados en el centro de cómputo y de ninguna manera pretende ser una guía para la programación de tales sistemas (ya que existen algunos en el mercado).

El capítulo NO contendrá todo el código fuente, solo se añade el código que pueda presentar problemas para ser implementando, además de algunos anexos a consideración de los autores.

Introducción

Un buen administrador es aquella persona que sabe administrar sus recursos disponibles para obtener el mejor resultado posible y el administrador de un centro de cómputo no es la excepción.

Identificación de los recursos

El administrador del centro de cómputo cuenta con dos tipos de recursos que dependen de él: el recurso humano (su grupo o equipo de trabajo) y el equipo de cómputo (tecnología utilizada en el centro), en capítulos anteriores se menciono como administrar de forma adecuada algunos de los equipos del centro de cómputo (PCs, impresoras, instalaciones, etc.) y al equipo de trabajo (mediante las políticas del centro), este capítulo tratará de la administración del "funcionamiento y aprovechamiento" de estos recursos.

En general, el recurso humano puede componerse de:

- Administrador del centro.
- Personal de mantenimiento preventivo y correctivo (Taller).
- Atención a alumnos.
- Atención a profesores.

Cada grupo de personas tienen labores diferentes e interactúan con distinto tipo de población, de acuerdo a las necesidades que se tenga.

En general, el recurso tecnológico puede componerse de:

- Equipos PC.
- Equipos Servidores.
- Impresoras y consumibles.

El sistema propuesto (SIARE) tiene la finalidad de permitir la interacción entre ambos tipos de recursos para que las tareas a realizar se hagan de la forma más rápida y eficiente posible y que pueda ser monitorizada por el administrador.

Identificación de las actividades.

Las tareas más comunes de un centro de cómputo son:

A. El personal de Atención a alumnos debe realizarles el préstamo de equipo PC a los alumnos.

B. El personal de Atención a alumnos debe imprimir los trabajos de los alumnos.

C. El personal de Atención a profesores debe reservar un laboratorio de cómputo (parcial o total) a los profesores que así lo soliciten.

D. El personal de Atención a profesores debe notificar al personal de Atención a alumnos las fechas y horarios en las que no se puede usar el laboratorio de cómputo.

E. El personal de Atención a alumnos debe reportar al personal de Mantenimiento preventivo/correctivo los equipos dañados del laboratorio de cómputo.

F. El personal de Mantenimiento preventivo / correctivo debe arreglar los equipos del centro de cómputo que sufran algún daño.

G. El personal de Mantenimiento preventivo / correctivo debe notificar al personal de Atención a alumnos los equipos que han sido reparados y que están listos para ser usados.

H. El personal de Atención a profesores debe notificar al personal de Mantenimiento preventivo / correctivo cuando se requiera la instalación de programas adicionales en algún laboratorio.

I. El personal de Mantenimiento preventivo / correctivo debe instalar programas adicionales a los equipo de cómputo para los profesores que así lo soliciten.

J. El Administrador debe revisar continuamente que estas tareas (entre otras) se estén realizando de forma correcta y eficiente.

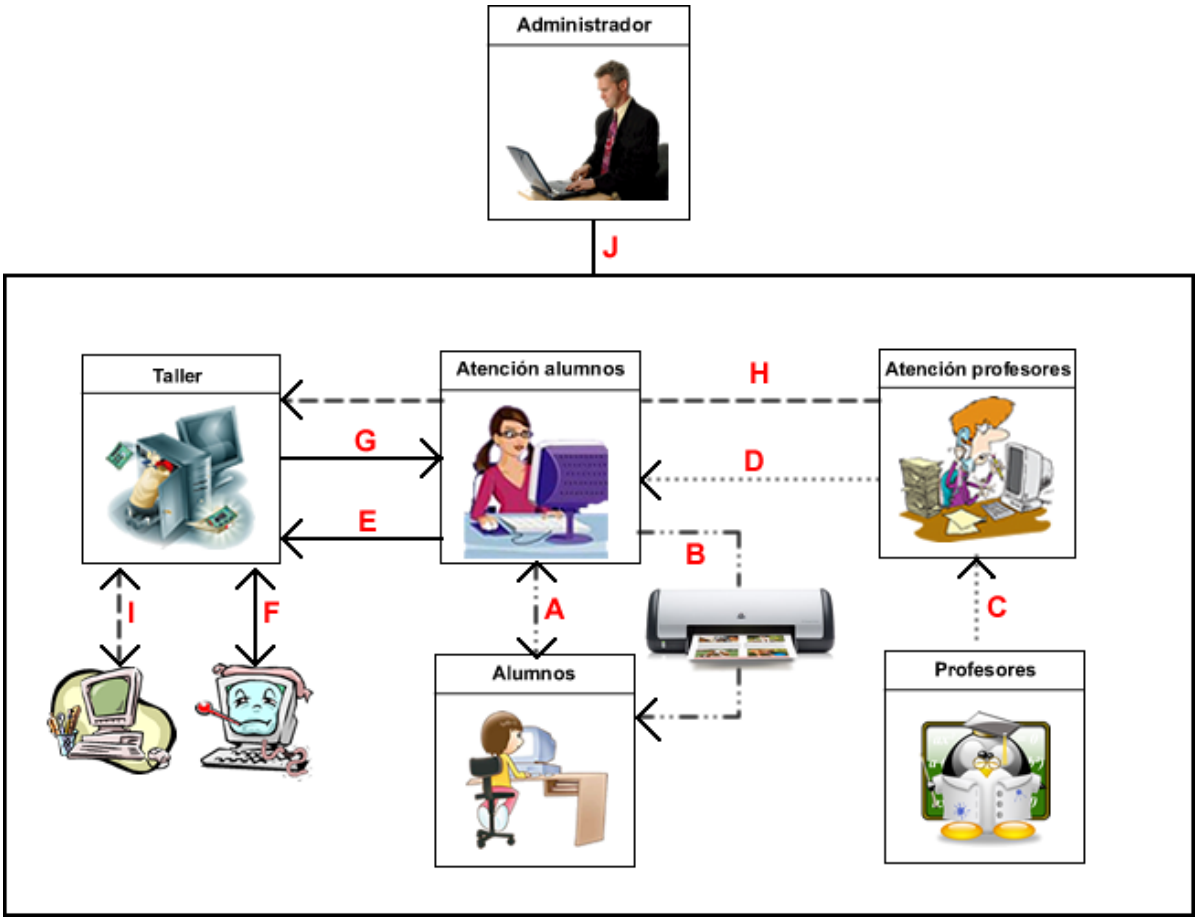


Figura 12.1. Esquema de las actividades del centro

Objetivo del SIARE.

El sistema SIARE permitirá:

- Mantener una comunicación directa entre el personal para reportar la solicitud/solución de una labor.

- Utilizar el recurso de una forma más eficiente y equitativa.
- Crear una base de datos que registrará todo suceso realizado manteniendo la información del suceso (descripción, solicitante, responsable, hora de solicitud y atención) de tal forma que toda esta información pueda ser utilizada para cuestiones estadísticas de los servicios brindados.
- La conexión remota entre equipos para cuestiones de mantenimiento preventivo/correctivo.
- Monitorizar las actividades realizadas y pendientes que han sido solicitadas en el departamento.

Para un mejor desempeño del sistema SIARE, debe utilizarse una red LAN para la comunicación entre equipos.

Composición del SIARE

El SIARE está compuesto por 6 módulos, cada módulo tiene distintos procesos para realizar tareas específicas, los módulos son:

1. Préstamo a alumnos: Permite reservar equipos de cómputo para que puedan ser usados por los alumnos, la sistematización de este módulo obliga al usuario a utilizar un equipo en específico solo durante el tiempo asignado, esto para tener un mejor control de acceso al laboratorio de cómputo, uso de recursos y evitar molestias entre los usuarios para respetar el tiempo prestado de los equipos.
2. Impresión: Permite administrar el recurso de impresión estableciendo un límite de hojas para el alumno por día, de manera que el recurso pueda ser utilizado por la mayor cantidad de usuarios posible.
3. Reservación de curso: Permite reservar todo un laboratorio de cómputo para un evento en específico.
4. Reporte al taller: Permite mantener la comunicación con el personal de mantenimiento preventivo / correctivo para notificar alguna falla o actualización que se requiera en algún equipo o laboratorio de cómputo.
5. Uso de equipo: Permite al alumno hacer uso de un equipo de cómputo siempre y cuando se esté respetando la relación usuario – equipo – horario, dicha relación es elaborada desde el módulo Préstamo a alumnos. Este módulo tiene la peculiaridad de que no trabaja en el mismo

entorno que el resto de los módulos, por cuestión de seguridad, éste modulo se trabaja independiente de los anteriores (evita que el alumnos tenga acceso al sistema reservado para personal del laboratorio).

Permisos para uso del SIARE.

Al iniciar el sistema se deberá identificar y autenticar al usuario, cada tipo de usuario podrá usar solo los módulos correspondientes a sus labores, los permisos para usar los módulos se describen la tabla 12.1.

Modulo/Usuario	Administrador	Atención alumno	Atención profesores	Taller	Alumnos
Préstamo a alumnos	Sí	Sí	No	No	No
Impresión	Sí	Sí	No	No	No
Reservación de cursos	Sí	No	Sí	No	No
Reporte al taller	Sí	Sí	Sí	Sí	No
Uso de equipos	No	No	No	No	Sí

Tabla 12.1. Roles del SIARE

Código Interesante

En esta sección se mostrará fragmentos de código que podrían resultar de gran interés debido a que su propósito no es muy general y por lo tanto no es muy conocido. Con el fin de hacerlo más didáctico se dividirá en:

- Código común: Es aquel que puede ser usado indistintamente en ambas aplicaciones cliente y servidor.
- Código de servidor: Aquel que se instalará en el equipo que administrara el sistema.
- Código de cliente: Código instalado en las computadoras que serán usadas por los usuarios y las cuales administrará el sistema.

Código común

Primeramente hablaremos del proceso de instalación, este consiste en copiar a la computadora deseada los archivos del sistema y crear accesos intuitivos para los usuarios.

Este proceso puede realizarse de diferentes formas, por ejemplo, existen aplicaciones cuyo fin es, precisamente, crear instaladores e instalar el sistema, sin embargo, para el SIARE proponemos usar comandos y variables de entorno de Windows para realizar este proceso, por lo tanto mencionaremos algunos.

- Comandos: Son los encargados de realizar alguna acción.

  - mkdir.- Crea una carpeta en la dirección indicada.

    mkdir "c:\WINDOWS/carpeta"

  - copy.- Copia un archivos de una posición a otra.

    copy C: \Administrador\archivo C:\Documents and Settings\Administrador\destino\

  - shorcut.- Crea un icono de acceso directo.

  - del.- Elimina uno o más archivos.

    del /f /s /q “C: \Administrador\archivo”

    Los parámetros significan lo siguiente:

    - /f Fuerza la eliminación de los archivos de solo lectura.
    - /s Elimina los archivos especificados en todos los subdirectorios.
    - /q Modo silencioso. No pide confirmación con comodín global.

  - attrib.- Muestra o cambia los atributos de un archivo.

    attrib +s +h +r “C: \Administrador\archivo”

    - +s Establece atributo de archivo del sistema.
    - +h Lo convierte en archivo oculto.
    - +r Hace al archivo de solo lectura.

  - logoff .- Cierra la sesión del usuario

  - reg.- Herramienta de registro de consola para Windows.

  - rmdir.- Elimina un directorio

    rmdir “C: \Administrador\carpeta”

- Variables de entorno: En cada versión de sistemas Windows o bien dependiendo del nombre del usuario, algunas carpetas pueden variar de ubicación, por ejemplo “C:\Documents and Settings\Tesis>” en esa ruta podemos apreciar que el usuario es “Tesis” y para cada usuario eso será variable. Sin embargo Windows tiene variables que mantienen esas referencias sin cambio, es decir, sin importar que usuario o el idioma del sistema operativo se puede tener una referencia a la carpeta de mis documentos (por mencionar un ejemplo).

  - %programfiles% .- C:\Archivos de Programa
  - %systemroot% o %windir% .- C:\WINDOWS
  - %homedrive% .- C:
  - %userprofile% .- C:\Documents and Settings\Usuario

Cuando se realizan programas con java (solamente con java) la interacción entre diferentes clases se lleva acabo de la forma tradicional, datos que regresan las funciones y manipulación de objetos. Sin embargo, para hacer que java interactué con otro programas por ejemplo vbs (posteriormente veremos que las aplicaciones java que se proponen deben interactuar con este tipo de archivos) pueden hacerlo mediante el estado de terminación de la maquina virtual, es decir, notificar al archivo que ejecuto al programa en java como termino, esto en código se escribe así:

System.exit(n)

Donde n es el estado que finalización.

A fin de comprender lo anterior se propondrá un ejemplo: Imagine que un programa en java verifica que autenticidad de un usuario mediante clave y contraseña, ambas guardadas en alguna base de datos. Este programa en java será ejecutado por un archivo vbs[1]. ¿Cómo se llevaría a cabo el proceso?

Necesitaríamos un archivo vbs que contenga algo similar a lo siguiente:

```
1. retorno=WshShell.Run("java -jar C:\acceso.jar",0,true)
2. if retorno = 123 then
    3. 'msgbox "acceso permitido"
4. end if
```

y por otro lado el jar debe tener verificar y tener un retorno similar a esto:

```
1. if datos correctos
```

[1] Los archivos vbs (visual basic script) son archivos capaces de ejecutar instrucciones propias el sistema operativo Windows.

2. System.exit(123)
3. else
4. System.exit(999)

El proceso se inicia al dar clic en el archivo vbs el cual ejecuta acceso.jar (línea 1).

Al ejecutar acceso.jar se verfican los datos (líneas 1 y 2). Si los datos con correctos o incorrectos se regresará 123 o 999 respectivamente (líneas 2 y 4), ambos números son por convención del programador.

Si los datos fueron correctos el programa java retorna 123 y se verifica en el archivo vbs (línea 3) y se manda un mensaje de acceso permitido, de lo contrario no pasa nada.

Nota: los archivos vbs (visual basic script) son archivos capaces de ejecutar instrucciones propias el sistema operativo windows.

Finalmente mencionaremos el comodín "*" (asterisco) que significa todo o cualquier. Algunos ejemplos son los siguientes:

```
del %homedrive%\angelica\matutino\*.*
```

Que significa borra todos los archivos con cualquier nombre y cualquier extensión de la carpeta "matutino".

Código Servidor

Para instalar el cliente se ejecutara el siguiente archivo bat.

```
mkdir "%programfiles%\angelica"
mkdir "%systemroot%\angelica%"
mkdir "%programfiles%\angelica\lib"
mkdir "%homedrive%\angelica"
mkdir "%homedrive%\angelica\matutino"
mkdir "%homedrive%\angelica\vespertino"

copy *.jar "%programfiles%\angelica"
copy *.gif "%systemroot%\angelica"
copy psi.ico "%programfiles%\angelica"
copy postgresql-8.0-311.jdbc3.jar "%programfiles%\angelica\lib"
copy Shortcut.exe "%systemroot%"

shortcut /F:"%userprofile%\Escritorio\Reportes.LNK" /A:C /T:"%homedrive%\angelica"
/I:"%programfiles%\angelica\psi.ico"
```

shortcut /F:"%userprofile%\Escritorio\Turno Matutino.LNK" /A:C /T:"%programfiles%\angelica\sistemaMat.jar" /I:"%programfiles%\angelica\psi.ico" /P:"%systemroot%\angelica %homedrive%\angelica\matutino"

shortcut /F:"%userprofile%\Escritorio\Turno Vespertino.LNK" /A:C /T:"%programfiles%\angelica\sistemaVes.jar" /I:"%programfiles%\angelica\psi.ico" /P:"%systemroot%\angelica %homedrive%\angelica\vespertino"

Tareas realizadas:

- Crea en el sistema operativo las carpetas que contendrán los archivos necesarios.
- Copia los archivos a las carpetas creadas.
- Crea los iconos en el escritorio para el acceso rápido.

Código Cliente

Debido a que el objetivo es crear el sistema con java, deben surgir algunas preguntas: ¿Cómo monitoreamos el tiempo que el usuario ha usado el equipo?, ¿Cómo forzamos a reiniciar el equipo?, etc.

Java no puede realizar estas tareas (sería posible ejecutar comandos nativos de Windows y similar el comportamiento, sin embargo se propone otra solución) por lo que se recurre a pequeños scripts que realicen estas tareas con ayuda de los programas en java. Por lo tanto el funcionamiento (propuesto) es el siguiente:

Crea un archivo instalador intalar.bat que contiene lo siguiente:

```
install.jar
copy monitor.vbs %windir%
copy shutdown.exe %windir%
mkdir "%programfiles%\siare"
mkdir "%programfiles%\siare\lib"
copy *.jar "%programfiles%\siare"
copy postgresql-8.0-311.jdbc3.jar "%programfiles%\siare\lib"
reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v siare /d
monitor.vbs /f
reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Policies\System /v
DisableTaskMgr /d 1 /f
```

```
attrib +s +h +r "%windir%\monitor.vbs"
attrib +s +h +r "%programfiles%\siare\lib\*.*"
attrib +s +h +r "%programfiles%\siare\*.*"
attrib +s +h +r "%programfiles%\siare\lib" /s /d
attrib +s +h +r "%programfiles%\siare" /s /d

logoff
```

El archivo realiza las siguientes tareas:

- Ejecuta el archivo install.jar.- este programa genera el archivo monitor con los parámetros correctos (Aula y Maquina). Note que es un archivo vbs (visual basic script).
- Copia algunos archivos.
- Crea las carpetas en el sistema operativo, las cuales contendrás los archivos jar restantes.
- Añade al registro el archivo monitor.
- Modifica las propiedades de los archivos copiados.

El archivo monitor (propuesto) es el siguiente y realiza las siguientes tareas:

```
Set WshShell = WScript.CreateObject("WScript.Shell")
' ********** Definición de las variables **********
dim salida1, salida2, tiempo, extra
salida1=81082
' ********** Ciclo para controlar "acceso" **********
do while salida1 = 81082
      salida1=WshShell.Run("java -jar C:\archiv~1\angelica\acceso.jar 2 3",0,true)
      if salida1 = 81082 then
            tiempo=WshShell.Run("java -jar C:\archiv~1\angelica\minutos.jar",0,true)
            'msgbox "acceso permitido"
            'msgbox tiempo
            WScript.Sleep(tiempo)
' ********** Ciclo para controlar "analisis" **********
            salida2=81082
            do while salida2 = 81082
```

```
                    salida2=WshShell.Run("java -jar C:\archiv~1\angelica\analisis.jar 2
3",0,true)
                    if salida2 = 81082 then
                        extra=WshShell.Run("java -jar C:\archiv~1\angelica\message.jar
1",0,true)
                        WScript.Sleep(1800000)
                    end if
                loop
                extra=WshShell.Run("java -jar C:\archiv~1\angelica\bye.jar",0,true)
                WScript.Sleep(270000)
        end if
    loop
    WshShell.Run("shutdown -l")
```

Tareas realizadas:

- Ejecuta acceso.jar con los parámetros 2 3 los cuales son aula y maquina (ambos parámetros correctos gracias a install.jar)
- Si el acceso es permitido, se ejecuta minutos.jar para obtener el tiempo que se tiene por sesión. Se manda un mensaje de acceso permitido y el programa “duerme” el tiempo que se obtuvo.
- El siguiente ciclo es para verificar si el tiempo de uso permitido ha terminado.

Cuando su tiempo de uso ha terminado bye.jar mandara un mensaje, esperara unos segundos y reiniciara el equipo.

Conclusiones.

Nuestra visión mientras estuvimos desarrollando este trabajo es el de visualizarlo como una herramienta de gran ayuda para todas aquellas personas que se dediquen a la administración para la creación o mejoramiento de un centro de cómputo educativo, para lograrlo tuvimos que compartir, analizar, criticar y expandir nuestros conocimientos y experiencias laborales en esta rama.

Intentamos realizar un trabajo que no sea un informe técnico ni mucho menos una guía a seguir paso a paso, si no que es una expresión de nuestras sugerencias personales que nos han dado (las que ya aplicamos en el mundo laboral) y que podrían dar (no se han aplicado) un excelente resultado en esta pesada labor llamada “Administración”.

Cada uno de los capítulos de este trabajo lo desarrollamos de tal forma que se plantee un panorama general de la situación actual, se observe cuales son las necesidades actuales y/o futuras que se pueden presentar, se analicen las distintas soluciones posibles a las necesidades planteadas y se decida cuál es la mejor opción basándose en el esquema costo-beneficio (tomar la mejor decisión dentro del alcance de capital).

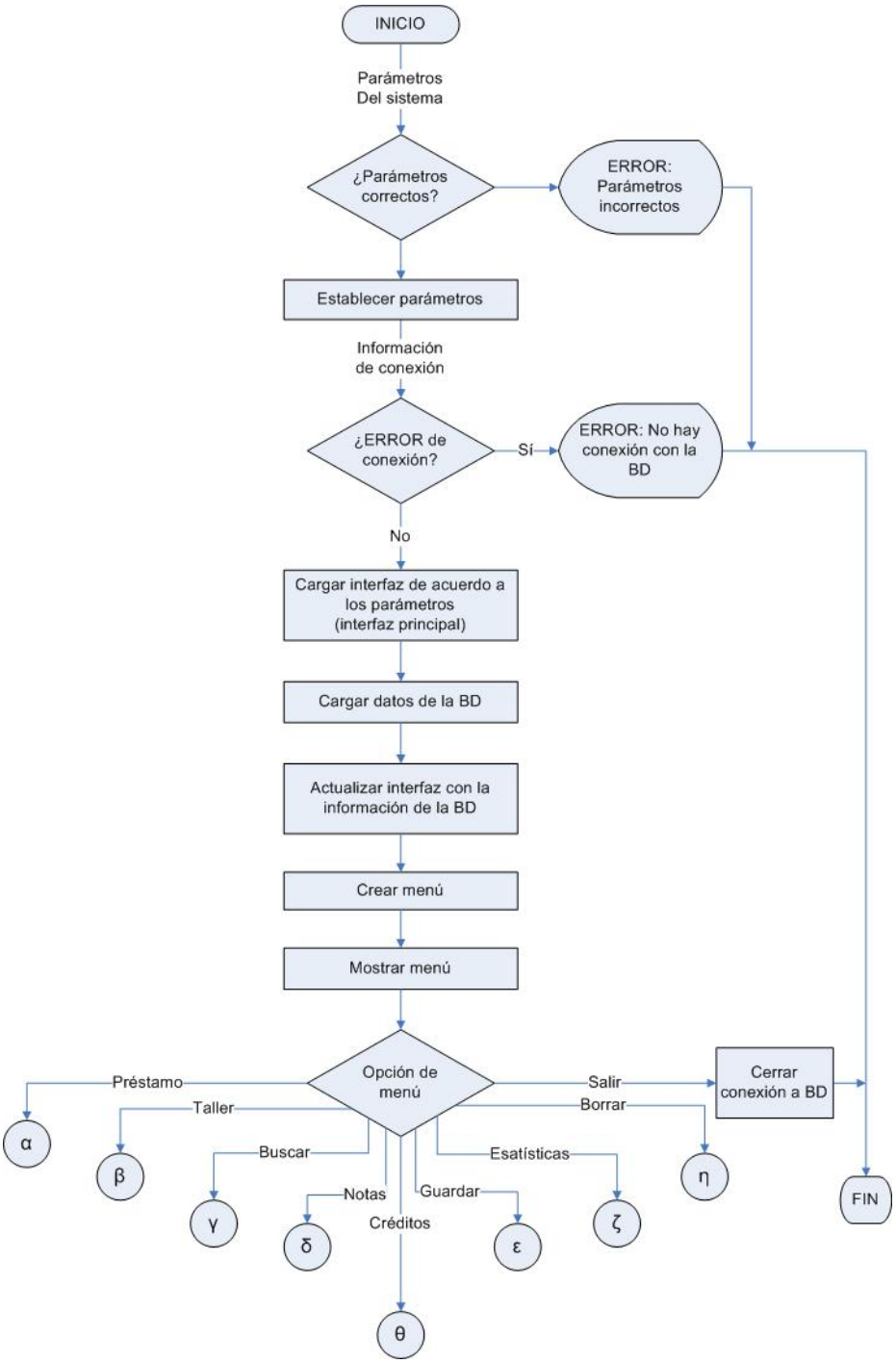
A nuestro criterio, abarcamos los aspectos más relevantes para un centro de cómputo educativo, tratando siempre de tener en cuenta a quien va dirigido el servicio prestado, cuál es su perfil general, necesidades y capacidades (estudiantes, maestros y personal que interactúa con ellos).

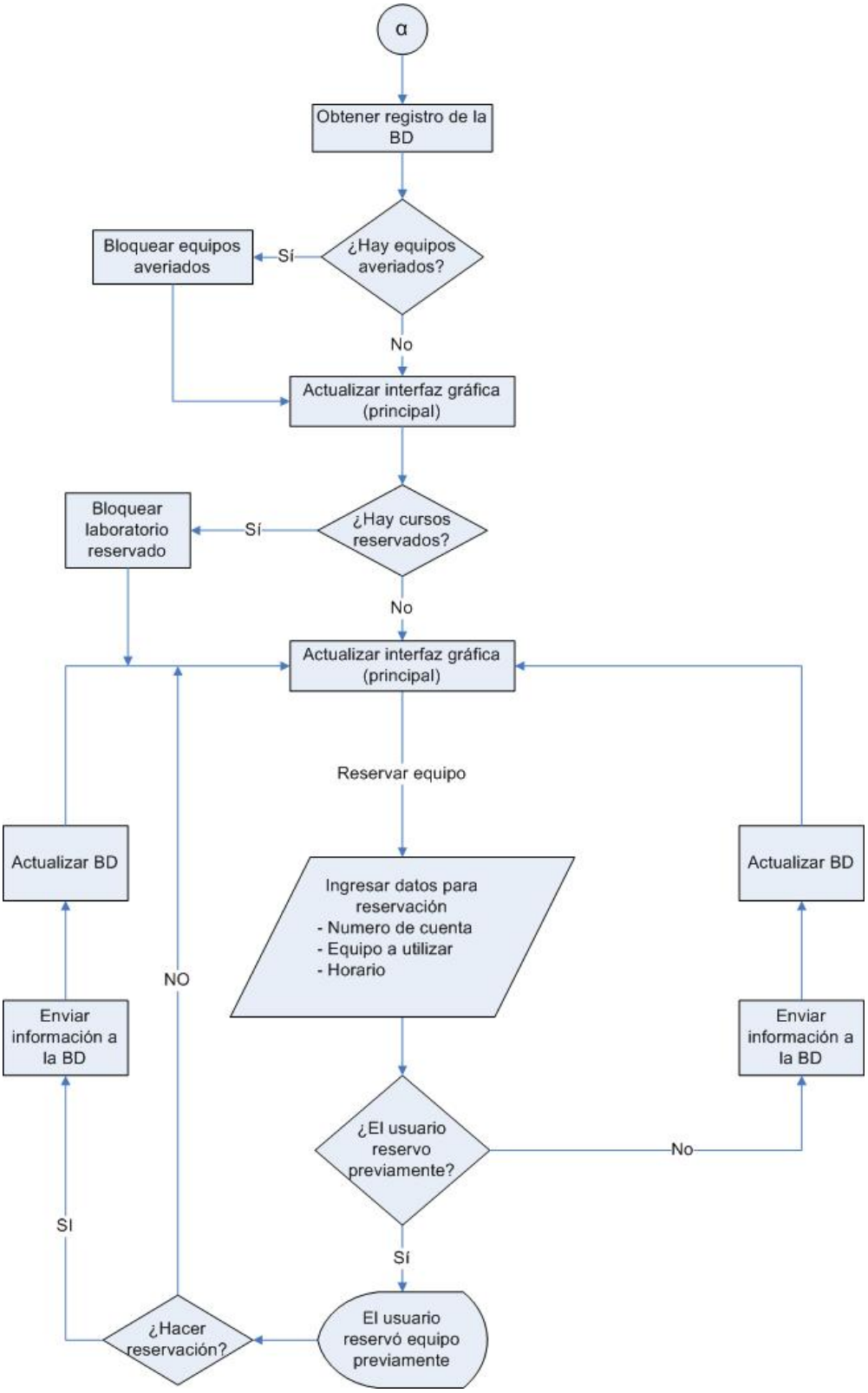
Propusimos el planteamiento para el desarrollo de un sistema para la administración de un centro de cómputo educativo y desarrollamos algunos de los módulos que lo componen, esto con la idea de que en el futuro, las personas que lean nuestra tesis tengan ideas más claras de cómo pueden aprovechar la tecnología para realizar mejor su labor, ya sea individual o en equipo, que se den cuenta de que la principal limitante es el desempeño y la creatividad personal, y que la falta de recursos no tienen porqué ser un obstáculo para el mejoramiento del ambiente laboral, en cualquiera de los sentidos y en la rama que sea.

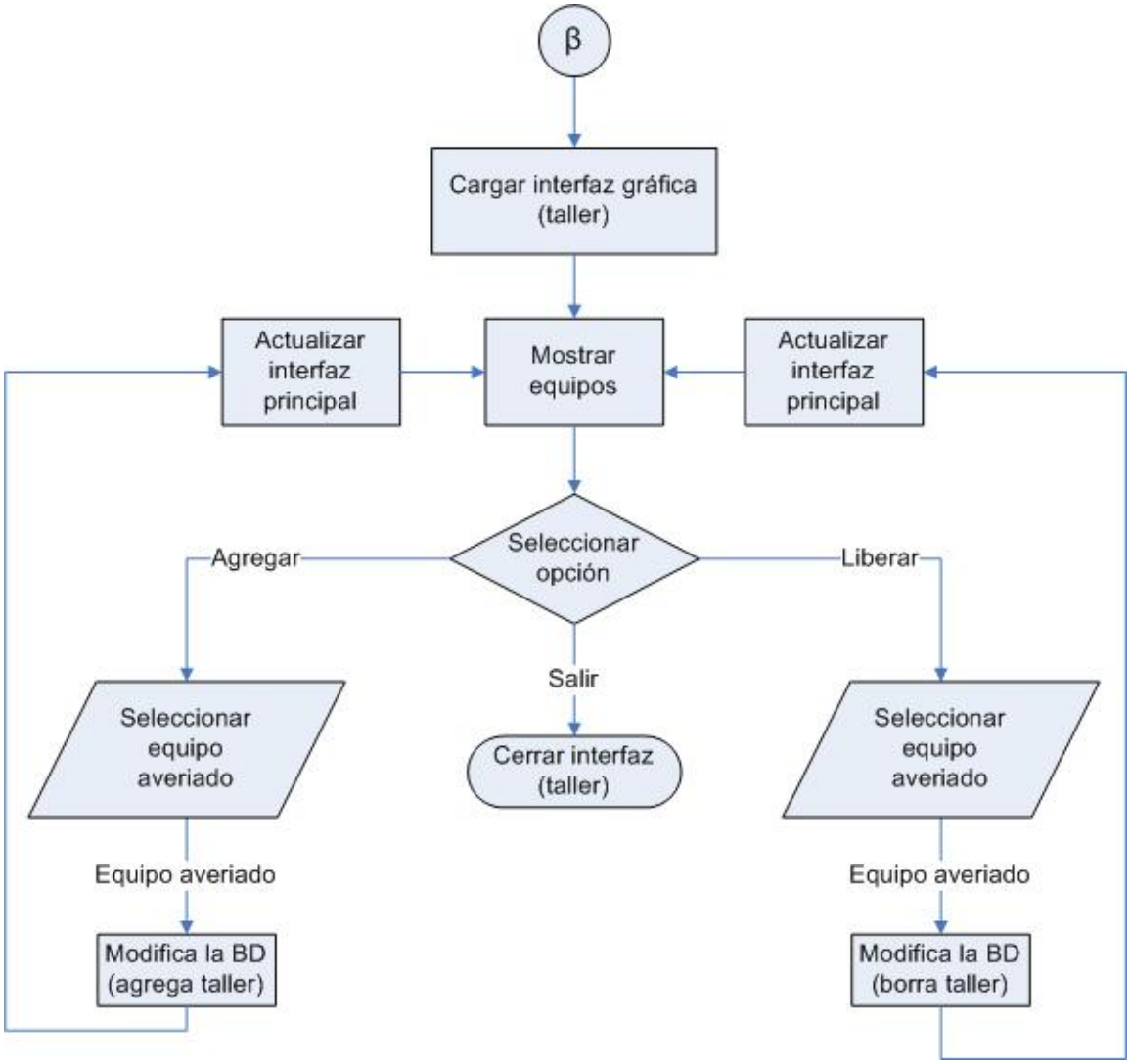
Y nuestra última visualización con este trabajo, es que no sea solo eso, queremos que este trabajo sea solo el principio para el desarrollo de un proyecto que pueda mejorar la calidad de vida de las personas, que se ponga en alto el nombre de la Universidad Nacional Autónoma de México y que se cambie la ideología de las personas para hacerlas mejores, con mas valores humanos, habilidades y responsables, para que México pueda cambiar para bien y sea un mejor país que destaque por la capacidad y valores de su gente, y con la educación, se puede lograr.

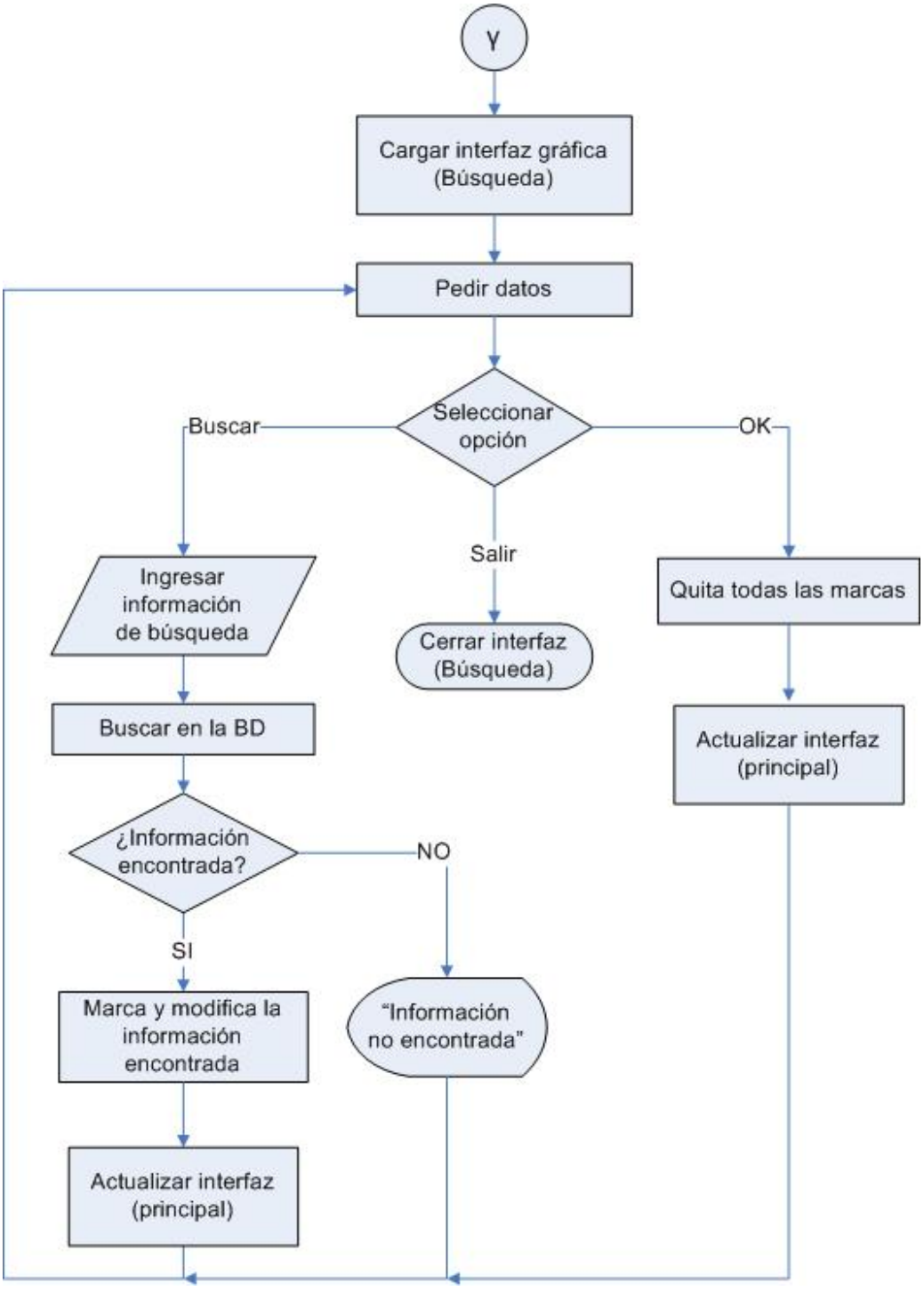
Apéndice

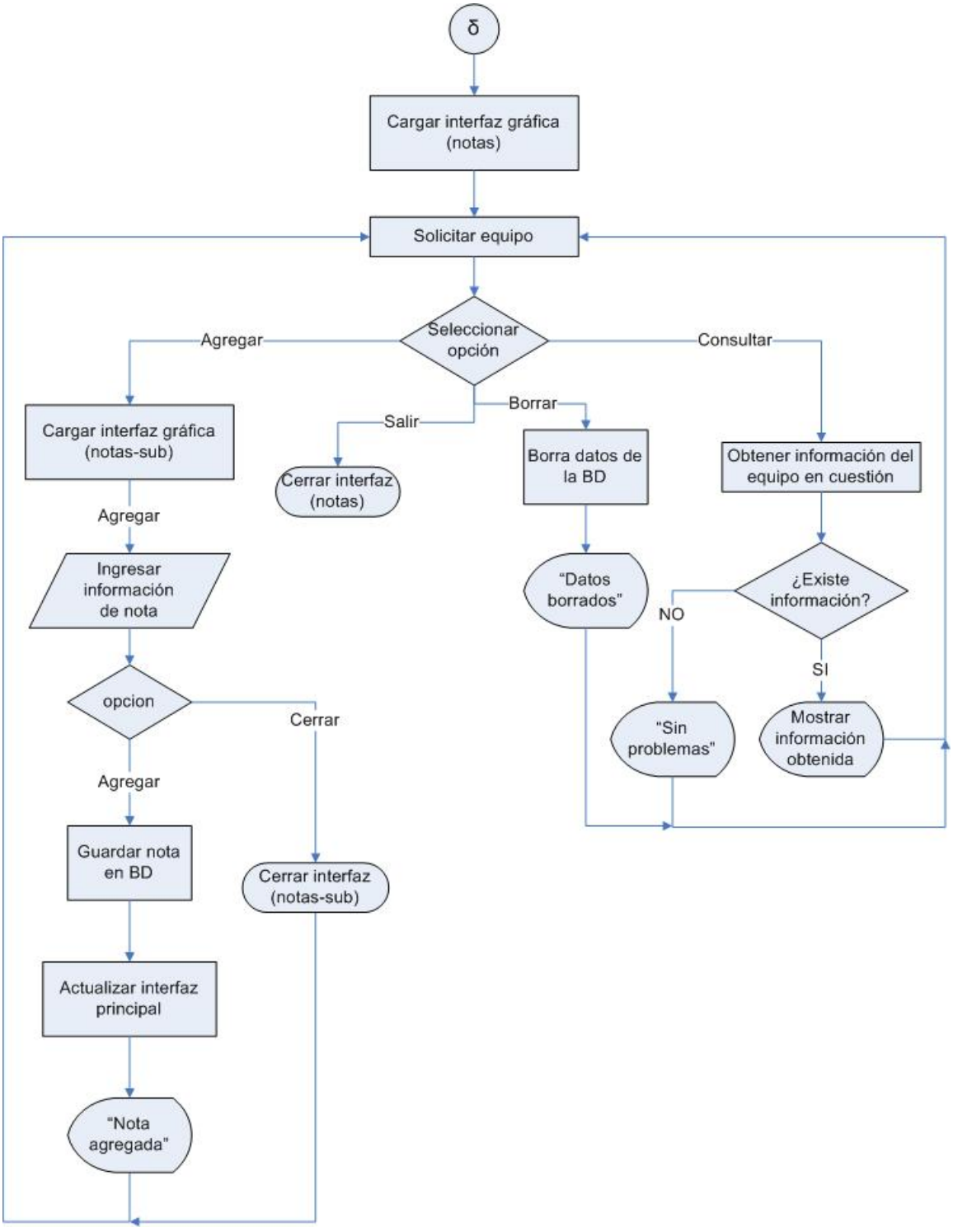
Diagramas de flujo para el demo de SIARE.

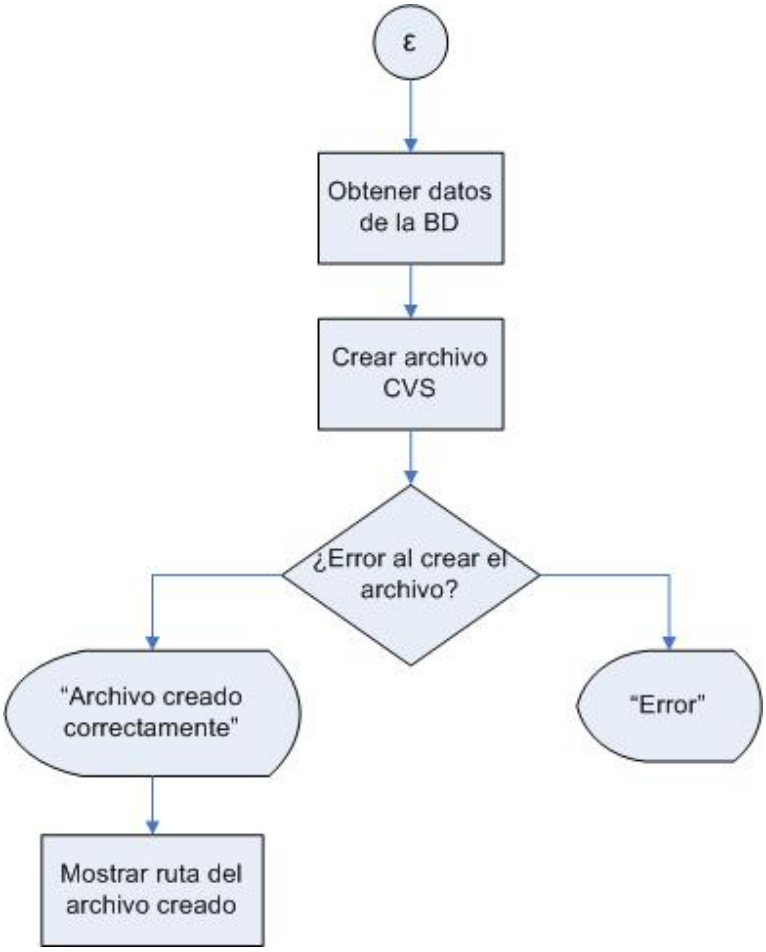



α
Obtener registro de la BD
¿Hay equipos averiados?
Sí
Bloquear equipos averiados
No
Actualizar interfaz gráfica (principal)
¿Hay cursos reservados?
Sí
Bloquear laboratorio reservado
No
Actualizar interfaz gráfica (principal)
Reservar equipo
Ingresar datos para reservación
- Numero de cuenta
- Equipo a utilizar
- Horario
¿El usuario reservo previamente?
No
Sí
El usuario reservó equipo previamente
¿Hacer reservación?
SI
NO
Enviar información a la BD
Actualizar BD
Enviar información a la BD
Actualizar BD

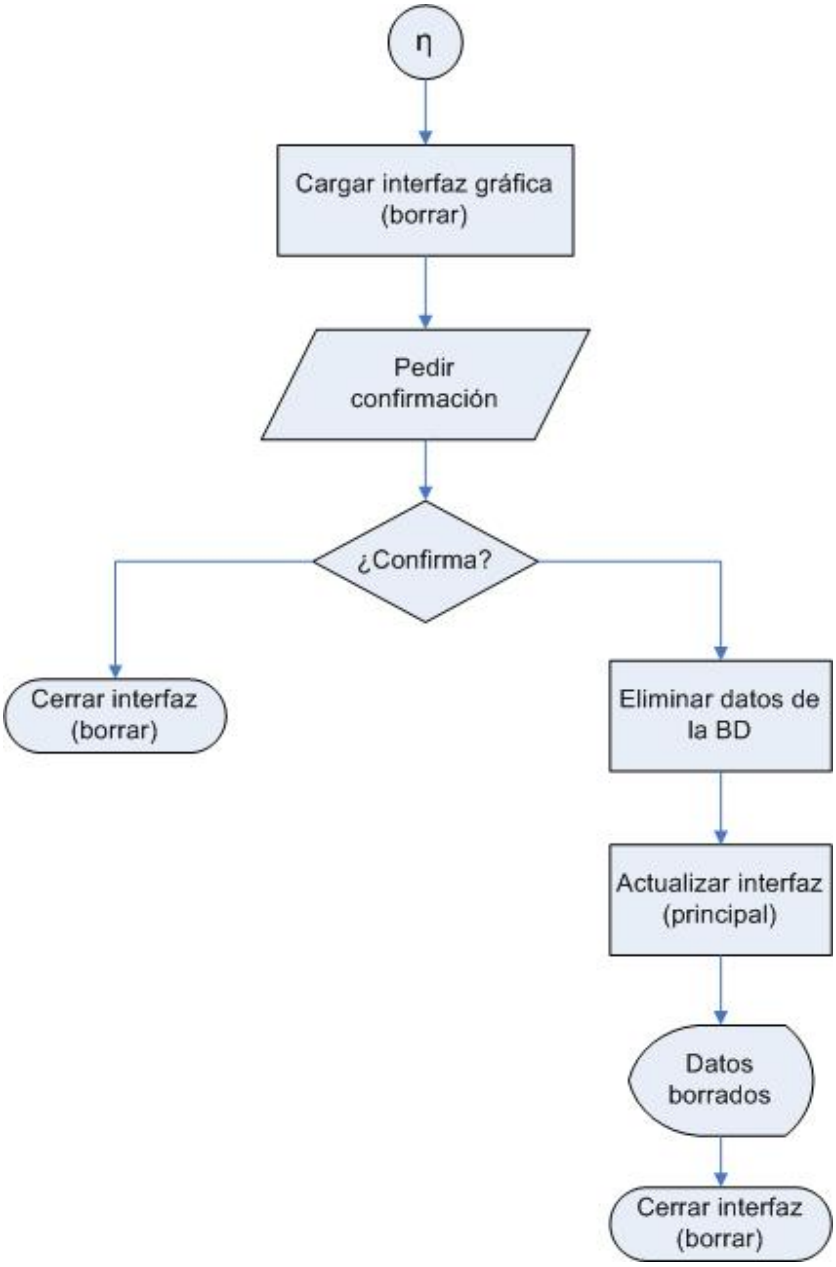

β
Cargar interfaz gráfica (taller)
Actualizar interfaz principal
Mostrar equipos
Actualizar interfaz principal
Seleccionar opción
Agregar
Liberar
Salir
Seleccionar equipo averiado
Cerrar interfaz (taller)
Seleccionar equipo averiado
Equipo averiado
Equipo averiado
Modifica la BD (agrega taller)
Modifica la BD (borra taller)


Y
Cargar interfaz gráfica (Búsqueda)
Pedir datos
Seleccionar opción
Buscar
OK
Salir
Ingresar información de búsqueda
Cerrar interfaz (Búsqueda)
Quita todas las marcas
Buscar en la BD
Actualizar interfaz (principal)
¿Información encontrada?
NO
SI
Marca y modifica la información encontrada
"Información no encontrada"
Actualizar interfaz (principal)


δ
Cargar interfaz gráfica (notas)
Solicitar equipo
Seleccionar opción
Agregar
Consultar
Salir
Borrar
Cargar interfaz gráfica (notas-sub)
Cerrar interfaz (notas)
Borra datos de la BD
Obtener información del equipo en cuestión
Agregar
Ingresar información de nota
"Datos borrados"
¿Existe información?
NO
SI
opcion
Cerrar
"Sin problemas"
Mostrar información obtenida
Agregar
Guardar nota en BD
Cerrar interfaz (notas-sub)
Actualizar interfaz principal
"Nota agregada"


ε
Obtener datos de la BD
Crear archivo CVS
¿Error al crear el archivo?
"Archivo creado correctamente"
"Error"
Mostrar ruta del archivo creado


ζ
Obtener información de la BD
Hacer análisis requerido
Dar formato a la información
Mostrar resultado del análisis


η
Cargar interfaz gráfica (borrar)
Pedir confirmación
¿Confirma?
Cerrar interfaz (borrar)
Eliminar datos de la BD
Actualizar interfaz (principal)
Datos borrados
Cerrar interfaz (borrar)


θ
Cargar interfaz gráfica (creditos)
Mostrar créditos
Cerrar interfaz (créditos)