PROYECTO DE INVESTIGACION
DISEÑO DE LA RED LAN PARA
IL SOLUTION

ANGELA MARIA BARRANCO HORTA
PAULA ANDREA DIAZ LAITON
EDUARD ALEXANDER GONZALEZ
JORGE ALBERTO VALENCIA

Trabajo de Investigación aplicada
Ciclo Preparatorio para Grado

Director
Oscar Ernesto Torres Parra
Ingeniero de Sistemas

CORPORACIÓN UNIVERSITARIA UNITEC
ESCUELA DE INGENIERIA
PROGRAMA DE TECNOLOGÍA EN SISTEMAS
BOGOTA D.C.
IIPL DE 2003

TABLA DE CONTENIDO

ANEXOS

ANEXO 1

Modelo del a Encuesta

ANEXO 1.1

Resultados de la encuesta

ANEXO 2

Plano Lógico

ANEXO 3

Plano Físico

ANEXO 4

Plano de Red

ANEXO 5

Costos

INTRODUCCIÓN

Dado que el manejo de la información de modo eficiente constituye una de las principales inquietudes dentro de cualquier organización, se hace necesario manejarla y emplearla con mucho criterio, siendo que de ello podría depender, en gran medida, el éxito o fracaso de las mismas.

Son muchas las herramientas que, en la actualidad, facilitan al manejo del recurso informativo y el acceso a éste permitiendo utilizar el recurso de la información de manera más eficiente, rápida y confiable.

Una red es un conjunto de computadoras o dispositivos de procesamiento conectados entre sí en forma lógica y física con la finalidad de optimizar sus recursos y emular el proceso de un sistema de cómputo único.

1. OBJETIVO GENERAL

Diseñar una red Lan ("red de área local") en la empresa IL SOLUTIONS para satisfacer las necesidades de los usuarios y brindar eficiencia para el buen funcionamiento de la organización y así mismo mejorar los niveles de seguridad de acceso a la información.

1.1 OBJETIVOS ESPECIFICOS

- Identificar los requisitos generales de la LAN de acuerdo a los distintos usuarios que trabajan en las diferentes áreas por medio de encuestas.
- Efectuar un estudio y diseñar el plano lógico, físico y de red de la organización IL Solution.
- Plantear soluciones alternativas para el desarrollo de la red Lan.
- Identificar la ubicación que deberán tener los dispositivos de interconexión.
- Ubicar en el edificio un sitio estratégico donde funcionará el Centro de Cableado.
- Evaluar herramientas, recursos, costo y viabilidad del proyecto.
- Definir el sistema operativo que se va a utilizar en la red.

1.2 PLANTEAMIENTO DEL PROBLEMA

Debido a que IL SOLUTIONS ha tenido un incremento en el desarrollo de soluciones interactivas, han tomado la decisión de trasladarse a un edificio que cuenta con tres pisos. Se desea diseñar una red Lan para que facilite la comunicación de todas las dependencias que allí funcionarán, y que les permita a todos los usuarios compartir aplicaciones y recursos que sirvan para un óptimo funcionamiento de la organización.

1.3 JUSTIFICACIÓN

El diseño y los ajustes de la nueva red de IL Solutions servirán para dar soluciones importantes de comunicación dentro de la empresa. Además se identificaran vínculos internos y externos que permitirán que la compañía alcance una estrategia adecuada para solucionar inconvenientes que se presentan debido a la falta de una red.

El proyecto diseñado para las nuevas instalaciones de IL Solutions constará de treinta (30) equipos, 7 impresoras, 1 plotter, 1 servidor, 2 switches y 7 puntos adicionales que se distribuirán en las diferentes áreas asignadas por la compañía.

1.4. FACTIBILIDAD

1.4.1 FACTIBILIDAD TECNICA

El "Diseño de la red Lan" desde el punto de vista técnico es viable. Actualmente encontramos en el mercado tecnologías de comunicación que facilitarán soporte a la culminación del diseño de la red.

El hecho de contar con el personal de sistemas en el área donde se ubicará el cuarto de distribución principal (MDF) implica que no es necesaria la contratación de personal externo lo que evitará un gasto adicional para la empresa.

1.14.2 FACTIBILIDAD ECONOMICA

Dado que el proyecto se presenta como tesis de grado, el diseño de la red no generará ningún costo. Ya que de ello depende la realización del proyecto, el diseño elegido responderá a la relación costo-beneficio.

1.14.3 FACTIBILIDAD OPERACIONAL

La instalación de la red en el nuevo edificio de IL SOLUTIONS estará a cargo de personas especializadas quienes podrán atender cualquier inconveniente con respecto a la implantación de la misma.

2. MARCO TEORICO

2.1 NIVELES OSI. ARQUITECTURA POR CAPAS

Arquitectura de conexión interredes de equipos activos, por capas lo cual proporciona las siguientes ventajas:

- Reduce la complejidad: El entendimiento de cómo se realiza la interconexión y operación entre dos computadores se hace mucho más sencillo cuando el modelo se presenta por capas, esta división trae consigo sencillez en el aprendizaje de cada uno de los procesos involucrados en esta comunicación y transferencia de información.

- Estandariza las interfaces: El estándar OSI plantea un modelo en cual un dato pasa de un equipo activo a otro a través de varios niveles o capas, estas se encargan de una parte específica tanto en la parte de codificación como transporte y envió. Bajo este esquema una debe proveer servicios a la capa superior e inferior, para lo cual se debe establecer una interfaz única y estándar entre cada una de las capaz. No importa el trabajo o la tecnología bajo la cual la capa opere, siempre habrá una interfaz estándar para interactuar con las diferentes capas.

- Facilita la ingeniería Modular: Este modelo trae una gran ventaja cada vez más aprovechada, la posibilidad de diseñar equipos de comunicación divididos en módulos, cuya tarea esté orientada a cada una de las funciones de los niveles OSI. Se logra entonces una modularidad que facilita el desarrollo de la tecnología independientemente en cada una de las partes que la componen.

- Asegura la tecnología interoperable: El hecho que las interfaces Sean estándar entre cada una de las capas y la misma modularidad, aprueba que diferentes tecnologías se desarrollen en las capas, sin que se presente incompatibilidad entre éstas. Lo que se logra, es entonces, una alta interoperabilidad entre cada tecnología, permitiendo el desarrollo por diferentes caminos tecnológicos

El modelo se presenta en siete capas, enumeradas desde la inferior (capa No 1 física) hasta la superior (No 7 Aplicación). A continuación la explicación de cada una de ellas:

CAPA DE APLICACIÓN La capa de aplicación provee servicios de red a las aplicaciones de los usuarios. Por Ejemplo, un procesador de palabras es empleada por los servicios de transferencia de archivos en esta capa.

Ejemplos de Aplicaciones:

COMPUTADOR

- Procesador de palabras.
- Presentación gráfica.
- Bases de datos
- Diseño/manufactura
- Planeación de proyectos.

RED

- Correo electrónico.
- Transferencia de archivos.
- Acceso remoto
- Procesos cliente/servidor
- Manejo de red

CAPA DE PRESENTACIÓN

Esta capa provee la representación de datos y el formateo del código. Asegura que los datos que recibe de la red puedan ser utilizados por la aplicación, y asegura que la información enviada por la aplicación pueda ser transmitida en la red.

EJEMPLOS

- Texto, datos: ASCII; EBCDIC:
- Sound, video: Midi. Mpeg, Quick time.
- Gráficas, imágenes: Pitct, Tiff, TPEG, GIF.

CAPA DE SESIÓN

Esta capa establece, mantiene y maneja las sesiones entre las aplicaciones.

Ejemplos de sesiones

- Network File System (NFS): Sistema de archivos distribuidos por Sun Microsystems para permitir el acceso transparente a los recursos basados en redes remotas, usado con TCP/IP y estaciones UNIX.
- Structu red Query Language (SQL): Lenguaje de base de datos desarrollado por IBM para dar a los usuarios formas fáciles para especificar sus necesidades de información en sistemas remotos.

CAPA DE TRANSPORTE

Esta capa segmenta y reensambla los paquetes de datos en un bloque de datos. Se encarga de la interconexión de los equipos. Aquí es donde se negocia el inicio y terminación de una comunicación y la cantidad de paquetes a enviar. Algunas de sus funciones son las siguientes:

- Segmenta las aplicaciones de las capas superiores.
- Establece una conexión extremo- extremo.
- Opcionalmente, asegura la confiabilidad de los datos.
- Se encarga de la Conexión, reconocimiento, Transmisión.

CAPA DE RED

Esta capa determina el mejor camino para mover los datos de un lugar a otro. Maneja el direccionamiento de los dispositivos y supervisa la ubicación de los dispositivos en la red. Los enrutadores operan en esta capa.

CAPA DE ENLACE.

Esta capa provee la transmisión física a través del medio. Maneja el control de errores, la topología de la red, y el control de flujo. Esta capa se encarga de preparar los datos antes de enviarlos a través del medio físico.

Ejemplos de capa de enlace:
LAN: Ethernet, Token ring, FDDI
WAN: Dial Qn demand, SDLC, HDLC, X.25, Frame relay, ISDN, PPP.

CAPA FÍSICA

Esta capa provee las características eléctricas, mecánicas, y funcionales para la activación y mantenimiento del enlace físico entre los sistemas.

Ejémplos:

LAN: Ethernet, Token ring, FDDI.

WAN: EIAITIA-232, G703, V.35, EIA/TIA-449.

La compañía pretende que se realice un diseño de la red Lan, con el fin de que todas las estaciones de trabajo se conecten a la red, cumpliendo con las funciones y compartan con todos aquellos recursos como los dispositivos y los datos entre equipos.

3. CABLEADO ESTRUCTURADO

El cable de par trenzado sin apantallar (UTP) es un conjunto de tres o cuatro pares de cables, en que cada uno de los cables de cada par está trenzado al otro para impedir las interferencias electromagnéticas, el cableado UTP, emplea conectores RJ-45, RJ-11, RS-232 y RS-449. Dado que es mas barato y mas fácil de instalar. Un ejemplo de aplicación UTP, son las redes telefónicas, que utilizan conectores RJ-11, y las redes 10BaseT, que utilizan conectores RJ-45. UTP se presenta en forma de grados de categorías 2, 3, 4, 5, 6 sin embargo ahora se recomienda categoría 5 para cualquier tipo de aplicación de datos.

Los estándares TIA/EIA se refieren a seis elementos del proceso de cableado de LAN. Ellos son:

- Cableado horizontal
- Centro de telecomunicaciones.
- Salas de equipamiento
- Áreas de trabajo
- Facilidades de acceso

NORMA 568-A

Los estándares TIA/EIA-568-A para el cableado horizontal, que definen el cableado horizontal como el cableado tendido entre una toma de telecomunicaciones y una conexión cruzada horizontal. TIA/EIA-568-A incluye los medios para networking que están tendidos a lo largo de una ruta horizontal, la toma o conector de telecomunicaciones, las terminaciones mecánicas del centro de cableado y los cables de conexión o jumpers del centro de cableado. En resumen, el cableado horizontal incluye los medios para networking que se usan en el área que se extiende desde el centro de cableado hasta una estación de trabajo. TIA/EIA-568-A contiene especificaciones que reglamentan el rendimiento de los cables y norma el tendido de dos cables, uno para voz y otro para datos en cada toma. De los dos cables, el cable de voz debe ser UTP de cuatro pares. El estándar TIA/EIA-568-A especifica cinco categorías en las especificaciones. Estas son el cableado Categoría 1 (CAT 1), Categoría 2 (CAT 2), Categoría 3 (CAT 3), Categoría 4 (CAT 4) y Categoría 5 (CAT 5). Entre estos, sólo CAT 3, CAT 4 y CAT 5 son aceptados para uso en las LAN. Entre estas tres categorías, la Categoría 5 es la que actualmente se recomienda e implementa con mayor frecuencia en las instalaciones.

Los medios para networking reconocidos para estas categorías son:

- Par trenzado blindado
- Par trenzado no blindado
- Cable coaxial

4. PROYECTO EMPRESA IL SOLUTIONS
"DISEÑO DE RED LAN"

IL Solutions es una pequeña empresa que se dedica a crear y diseñar soluciones interactivas, ofreciéndoles a sus clientes ideas dependiendo de sus necesidades.
IL Solutions está ubicado en la Avenida El Dorado al Noroccidente de Bogotá.
Esta empresa ha adquirido un compromiso para crecer cada día como organización, lo cual ha generado grandes posibilidades de construir un sistema de información ágil y ampliar los recursos y las herramientas necesarias para lograr obtener una excelente compañía.
La empresa tiene como meta expandir su sistema de red para comunicarse eficientemente con los demás departamentos.
Este proyecto consiste en brindar una ayuda para el crecimiento de la organización contribuyendo al mejoramiento de los sistemas de red, y de esta manera poder ofrecer a los usuarios una herramienta que les permita desarrollar fácilmente las tareas y procesos correspondientes a cada una de las labores y lograr brindar un mejor servicio al cliente.

4.1. HISTORIA DE LA EMPRESA

IL SOLUTIONS es una empresa dedicada a las soluciones interactivas de negocios, constituida por 30 usuarios encargados del funcionamiento de la empresa.

IL SOLUTIONS comenzó a funcionar en el año 2000, se fortalece como empresa que está en crecimiento, es por eso que IL SOLUTIONS se ve en la necesidad de estar al frente de las nuevas Tecnologías.

Una de las principales funciones que tiene la red es de enviar Imágenes y sonido. Los programas aplicativos que utiliza es Macromedia (Fireworks, Flash, Dreamweaver).

La organización esta conformada por 30 usuarios distribuidos en las diferentes áreas como: Recursos Humanos, área Comercial, Recepción, Sistemas, Diseño grafico, Gerencia general, Gerencia de proyectos y área Administrativa.

QUIENES SON

Son un equipo de profesionales multidisciplinarios que comparten las mismas pasiones por las soluciones de negocios y mercadeo a través de los nuevos medios y los desarrollos interactivos de alto impacto.

La variedad y la combinación de talentos y conocimientos que componen el equipo, permiten aplicar convicciones y visualizar la excelencia hacia los clientes.

QUE HACEN

Ayudan a las compañías o instituciones a implementar soluciones de negocios y mercadeo, a través del Internet, la multimedia, la animación, la edición, el desarrollo y el merchandising, teniendo como valor agregado la calidad, el tiempo y la innovación en sus servicios.

Los tres años de experiencia han permitido brindarle soluciones adecuadas a sus clientes, maximizando sus oportunidades de negocio en el mercado.

4.2 MISIÓN

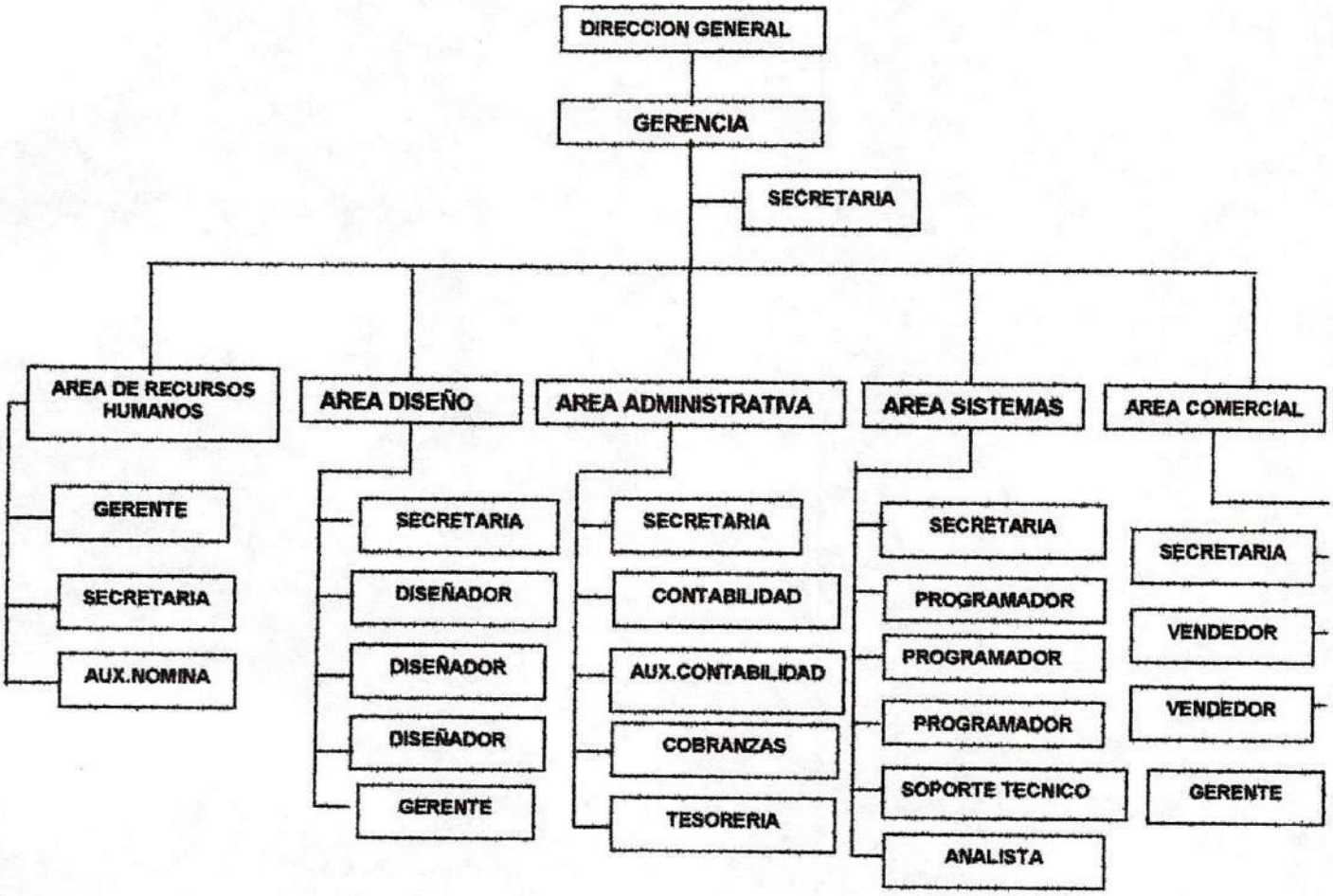
IL SOLUTION es una empresa Colombiana de expresión creativa, que canaliza la energía y los recursos de todas aquellas organizaciones que necesitan los servicios de soluciones interactivas.

4.3 VISIÓN

IL SOLUTIONS será una compañía líder reconocida por su eficiencia, innovación, calidad y servicio en la conceptualización de soluciones de negocios y mercadeo a través de los nuevos medios hacia mercados nacionales y extranjeros.

5. ORGANIGRAMA

IL SOLUTIONS



6. TIPOS DE USUARIOS

Los usuarios que tiene la empresa ILSOLUTIONS esta dividida en ocho áreas las cuales están distribuidas en tres pisos así:

En el primer piso se encuentra:

Recepción:

- 1. Recepcionista

Recursos humanos:

- 1. Auxiliares de nómina.
- 1. Gerente de recursos humanos
- 1. Secretaria.

Área comercial:

- 1. gerente
- 2. vendedores
- 1. secretaria

En el segundo piso se encuentra:

Área de sistemas:

- 1. Gerente
- 3. Programadores
- 1. Analista de sistemas
- 1. Secretaria
- 1. Soporte técnico

Área de diseño grafico:

- 1. Gerente
- 3. Diseñadores
- 1. Secretaria

En el tercer piso se encuentra:

Gerencia de proyectos:

- 1. Gerente de proyectos.
- 1. Auxiliar
- 1. Secretaria

Gerencia general:

- 1. Gerente
- 1. secretaria

Área administrativa:

- 1. Gerente.
- 1. área de contabilidad
- 1. auxiliar contable
- 1. cobranzas
- 1. tesorería
- 1. secretaria

7. METODO DE RECOLECCIÒN

Para la elaboración del proyecto se llevó a cabo una serie de encuestas a algunos de los usuarios de la empresa para saber las expectativas que tienen con relación a la red de la organización, fue necesario realizar varias observaciones en las diferentes áreas que tiene la empresa

Así mismo, se utilizó como medio la encuesta abierta para el personal que labora en la compañía, orientándonos perfectamente en aquella investigación que es requerida para el proyecto en estudio.

Para tipo de encuesta ver anexo 1

8. PASOS PARA EL DISEÑO DE LA RED

Al diseñar la red para IL SOLUTIONS debemos tener en cuenta los siguientes pasos que son de gran importancia.

8.1 ¿PARA QUE ES UNA RED?

La determinación del objetivo de la red nos ayuda a establecer muchos factores, se necesita determinar que personas van a tener acceso a documentos acerca de las políticas de la empresa.

Tal vez se quiera guardar en un lugar común los archivos de datos de varios computadores y tener acceso a ellos. Guardar archivos de datos en un computador con un disco duro relativamente grande permite tener unidades de disco más pequeñas y menos costosas en los demás nodos de la red.

Las redes nos sirven para compartir impresoras. Aun que hay otros dispositivos que no son para red y que permiten también compartir impresoras entre computadores, algunas veces el solo hecho de compartir impresoras justifica suficientemente una red.

La capacidad de que más de una persona use un programa de aplicación común para acceder a los mismos datos es una de las características más poderosas de las redes. Debemos tomar en cuenta si la red manejará aplicaciones multiusuarios.

8.2 ¿CUANTOS NODOS SE NECESITAN?

Una consideración importante cuando se planea la red es determinar cuántos computadores se necesita conectar de inmediato y en el futuro.

El número máximo de nodos conectados en una configuración de red depende de varios factores como la topología física y el tipo de la red.

8.3 ¿CUALES SON LAS NECESIDADES DE RENDIMIENTO?

Los requisitos de rendimiento de la red dependen de varios factores.

Cada sistema operativo de red se comporta diferente, y algunos pueden ser más adecuados para determinados estándares de rendimiento que otros. Afectan el rendimiento, el tipo de adaptador de red, la topología de red que vamos a utilizar y los protocolos.

Si uno de los objetivos principales de la red es compartir impresoras y otros elementos entonces es probable que la configuración de red con menor rendimiento sea más que suficiente. Las impresoras rara vez aceptan datos a una velocidad mayor que la del puerto paralelo de un computador. También, dado que hasta los más lentos adaptadores de red disponibles son más rápidos que un puerto paralelo, la velocidad del adaptador no es, por lo general, un punto a tomar en cuenta.

Si se van a compartir archivos y datos con otros nodos de la red, sin importar el rendimiento, por lo tanto se debe pensar en una red que tenga 10 Mbps, como es el Ethernet que es lo que se va utilizar para el montaje de la red de la empresa IL SOLUTIONS.

Ya que Ethernet es una tecnología de bajo costo y alto rendimiento hace que sea el estándar de red más popular en uso.

Si se tiene en la red muchos nodos con acceso a un servidor común, tal vez valga la pena pensar en un servidor dedicado para proporcionar el rendimiento necesario. En situaciones en las que sólo unos cuantos usuarios acceden con frecuencia a una base de datos común, un servidor dedicado puede proporcionar mejoras significativas de rendimiento.

8.4 ¿QUE NODOS NECESITAN COMPARTIR RECURSOS?

Cuando se determinan las necesidades de la red se deben establecer los nodos que compartan recursos y los que no. Los nodos que comparten sus recursos, como unidades de disco, directorios, e impresoras, se configuran como servidores. El sistema operativo de red que se seleccione deberá soportar varios servidores si es que se necesita compartir los recursos de más de un solo nodo.

9. PUNTOS DE TRABAJO Y USUARIOS LAN

Diseño de la red

Actualmente la compañía cuenta con 30 equipos, el objetivo primordial de IL SOLUTIONS, es trasladarse a un nuevo edificio, la idea de la compañía es tener aparte de sus 30 equipos tener 7 impresoras, 1 ploter, 1 servidor y 2 switches para un total de 41 equipos y actualizar los que funcionan actualmente.

Como objetivo final lo que IL SOLUTIONS afirma, es que decisivamente tiene que existir distintos puntos de red, esto quiere decir, que en cualquier momento que se quiera hacer algún cambio en los departamentos, siempre exista un punto de red disponible.

Usuarios: IL SOLUTIONS contará con 30 usuarios que estarán distribuidos en las diferentes áreas que la compañía asigne.

10. ESTRUCTURA DE LA COMPAÑÍA

PISOS	AREA	CANTIDAD EQUIPOS
PRIMER PISO	Recepción	1
	Recursos Humanos:	
	• Secretaria	1
	• Gerente	1
	• Auxiliar Nomina	1
	• Impresora	1
	Comercial:	
	• Gerente	1
	• Vendedor	1
	• Vendedor	1
	• Secretaria	1
	• Impresora	1
TOTAL	EQUIPOS	10
SEGUNDO PISO	Sistemas:	
	• Gerente	1
	• Programador	1
	• Programador	1
	• Programador	1
	• Analista	1
		1

SEGUNDO PISO	• Soporte Técnico	1
	• Secretaria	1
	• Impresora	
	Diseño Grafico:	1
	• Gerente	1
	• Diseñador	1
	• Diseñador	1
	• Diseñador	1
	• Secretaria	1
	• Impresora	1
	• Plotter	
	Centro de Cableado:	1
	• Servidor	2
	• Switches	
TOTAL	EQUIPOS	17
TERCER PISO	Gerencia de Proyecto:	
	• Gerente	1
	• Auxiliar	1
	• Secretaria	1
	• Impresora	1
	Gerencia General:	
	• Gerente	1
		1

TERCER PISO	• Secretaria • Impresora Administrativa: • Gerente • Contador • Auxiliar Contable • Cobranzas • Tesorería • Secretaria • Impresora	1 1 1 1 1 1 1 1
TOTAL	EQUIPOS	14
TOTAL EQUIPOS	DE LA COMPAÑIA	41

11. DISEÑO FISICO DE LA RED

11.1 TOPOLOGIAS

Es el término técnico que describe disposición física en la que está configurada una red; está determinada en parte, por la manera en que los PC'S administran el acceso a la red y en parte a las limitaciones del sistema de señales.

Topología Física: es La forma física en que se encuentran conectadas las computadoras de la red.
Las topologías más comunes son:

11.2 TOPOLOGÍA EN ESTRELLA

Las estaciones se unen a concentradores y las señales se difunden a todas las estaciones o se pasan de unas a otras. Utilizaremos esta configuración puesto que cada conexión no tiene que soportar múltiples PC compitiendo por el acceso, de manera que es posible lograr altas frecuencias de transferencias de datos (aunque la máquina central debe ser bastante rápida.

Para aumentar el número de estaciones de la red o eliminar estaciones no es necesario interrumpir por lo menos parcialmente la actividad, realizándose la operación con bastante sencillez y sin perjudicar al resto de la red.

11.3 TOPOLOGIAS EN BUS

En esta topología todas las estaciones se conectan a un único medio bidireccional lineal o bus con puntos de terminación bien definidos. Cuando una estación transmite, su señal se propaga a ambos lados del emisor, a través del bus, hacia todas las estaciones conectadas al mismo, por este motivo, al bus se le denomina también canal de difusión. La mayor parte de los elementos de las redes en bus tienen la ventaja de ser elementos pasivos, es decir, todos los componentes activos se encuentran en las estaciones por lo que una avería en una estación no afecta más que a ella misma.

11.4 TOPOLOGIA EN ARBOL

Es una variante de la topología en bus, consistente en un bus principal denominado tronco del que parten varios buses secundarios denominados ramas, cada una de las cuales es capaz de admitir varias estaciones. Al igual que en la Topología en bus, las señales se propagan por cada ramal de la red y llegan a todas las estaciones. Además de las ventajas e inconvenientes de las redes en Bus, la red en árbol tiene una mayor adaptabilidad al entorno físico donde se instala la red, con lo que el costo de cableado es aún menor.

11.5 TOPOLOGÍA DE LA EMPRESA

Para el diseño de la red Lan "**IL SOLUTIONS**" se tomará la topología de estrella, puesto a las ventajas que puede suministrar al diseño.
Dado que nos permitirá administrar la red de modo que al aislar una terminal no es necesario cancelar la actividad de la red, cada conexión no tiene que soportar múltiples PC compitiendo por el acceso, de manera que es posible lograr altas frecuencias de transferencias de datos

ADMINISTRACIÓN

La topología en estrella, permite tener un cable independiente para cada estación, y las normativas de instalación y entrega, hacen que el cableado estructurado sea ideal para una óptima administración de cada uno de los recursos y de los servicios que se tiene en la red. La concentración en un punto admite rápidos cambios futuros, adicionar nuevos puntos de red, cambiar de servicio y el tiempo invertido para las labores de mantenimiento.

12. REQUERIMIENTOS DE TRÁFICO DE LA RED

PISOS	AREA	CANTIDAD DE EQUIPOS	ANCHO DE BANDA
PRIMER PISO	Recursos humanos	3	Baja
	Comercial	4	Baja
SEGUNDO PISO	Sistemas	7	Alta
	Diseño Grafico	5	Alta
TERCER PISO	Gerencia de Proyectos	3	Medio
	Gerencia General	2	Medio
	Administrativa	6	Medio

13. SEGURIDAD DE RED

La seguridad implicaría dos componentes principales. El primero consiste en mantener la red a salvo del acceso no autorizado y el segundo consiste en garantizar su capacidad de recuperar los datos tras situaciones catastróficas.

La primera parte de la seguridad implica hacer que la red sea lo más segura posible frente al acceso no autorizado. Esto se podría solucionarse estableciendo normas de seguridad, como la longitud mínima de la contraseña, la edad máxima de la contraseña, las contraseñas únicas (que no permiten que se repita la misma contraseña) y permitir que el usuario inicie sesión en la red únicamente a horas determinadas del día o en días determinados de la semana. Estos parámetros pueden ser controlados directamente por el administrador de red y los exigiría el sistema operativo del a red.

La seguridad también implica la garantía de que los usuarios conozcan las normas de la empresa y que las observen. Un ejemplo de ello podría ser no dejar a los usuarios utilizar nombres de familiares o de mascotas como contraseña.
Otro ejemplo consiste en garantizar que los usuarios estén desconectados de la red o que se active un protector de pantalla protegido por contraseña cada vez que abandonen sus computadores.

14. CENTRO DE CABLEADO (MDF)

El Centro de cableado se situará en el área de sistemas, en el 2ndo piso, tal como se ve en los planos (ver anexos), este cuarto brinda a los equipos de comunicación, seguridad, además, en ese departamento trabajan personas capacitadas para resolver cualquier tipo de problema que pueda presentarse, administrando y controlando toda la red de la compañía.

Las características del centro de cableado son las siguientes:

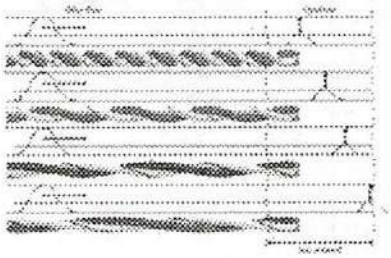
- Se ubicará en un lugar donde no hay humedad, es totalmente seco.

-Los equipos no estarán expuestos al sol, por lo tanto no tendrán problemas de recalentamiento ya que debido a la ventilación del cuarto no generará demasiado calor.

15. TIPOS DE CABLEADO

15.1 CABLES

El Cable es el medio a través del cual fluye la información por la red.



Una red puede utilizar uno o más tipos de cables, aunque el tipo de cable monopolizado siempre estará sujeto a la topología de la red, el tipo de red que utiliza y el tamaño de esta.

Los tipos de cables en redes LAN son:

- Cable de par trenzado sin apantallar (UTP).
- Cable de par trenzado apantallado (STP).
- Cable coaxial
- Cable de fibra óptica.

UTP: (unshielded twisted pair) par trenzado sin apantallar, es el soporte físico más utilizado en las redes de área local, tanto su costo como el costo de instalación es Barato y sencillo. Por él se pueden enviar señales tanto analógicas como digitales Consiste en un mazo de conductores de cobre (protegido cada conductor por un dieléctrico), que están trenzados de dos en dos para evitar al máximo la diafonía.

dieléctrico), que están trenzados de dos en dos para evitar al máximo la diafonía. Un cable de para trenzado para aplicaciones de datos es normal que tenga cuatro pares, como contrapartida su principal inconveniente es su sensibilidad ante interferencias electromagnéticas.

Existen varias categorías:

- Categoría 3: el cable UTP es trenzado por pares y los componentes de la red (conectores, receptores, uniones, etc.) son de un mismo tipo; transmisión hasta 16MHz.

- Categoría 4: al igual que la categoría anterior los componentes de la red pertenecen a esta misma categoría, y poseen un baño de oro de mayor espesor al anterior. El trenzado del cable posee una mayor densidad por pulgada que el de la categoría 3, soporta velocidades de transmisión hasta 20MHZ.

- Categoría 5: Los componentes de la red poseen el mayor espesor de oro en sus contactos con 50 micrones, es una red muy versátil y cómoda para realizar actualizaciones tecnológicas. A su vez, el trenzado del cable posee mayor densidad por pulgada que el de la categoría 4, esta categoría de cable maximiza el traspaso de datos y minimiza las cuatro limitaciones de las comunicaciones de datos (atenuación, crosstalk, capacidad y desajustes de impedancia), de esta forma es capaz de transportar datos a velocidades de hasta 100 Mhz.

- Categoría 6: son categorías de cables que soportan velocidades de transmisión mas elevadas como ser 350 Mhz y 500 Mhz

STP: (shielded twisted pair), una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas; el STP es un cable de par trenzado con protección externa la cual se encarga de proteger de las interferencias a los cables alojados en su interior. Este tipo de cable es usado por lo general en redes de topología Token Ring.

Coaxial: el cable coaxial contiene un conductor de cobre en su interior; este va envuelto en un aislante para separarlo de un apantallado metálico con forma de rejilla que aísla el cable de posibles interferencias externas.

Los tipos de Cable Coaxial son coaxial fino y coaxial grueso. El cable coaxial es muy popular en las redes con topología en BUS, el conector mas usado es el BNC, cuyas siglas son Bayone-Neill-Concelman..

Fibra Optica: consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar, la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes de alta velocidad y para ser usado en Backbone. Uno de los inconvenientes es su interconexión, su alto costo.

Para especificar el sistema de cableado para la empresa IL SOLUTIONS por el cual se regirá el proyecto "diseño de red Lan "se considera las normas que se establece por el sistema de cableado estructurado, Esta lección se concentra en los estándares TIA/EIA-568-A para el cableado horizontal, que se define como el cableado tendido entre una toma de telecomunicaciones y una conexión cruzada horizontal. Se adoptará como medio físico el cable UTP CAT 6, ya que nos permitirá una mayor rapidez en la información, este medio físico tendrá la longitud Máxima de 100 metros como lo establece la norma C.E (cableado estructurado.)

15.2 CABLEADO HORIZONTAL

El cableado horizontal incorpora el sistema de cableado que se extiende desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones.

El cableado horizontal consiste de dos elementos básicos:

Cable horizontal y hardware de conexión: también llamado ("cableado horizontal") proporcionan los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones. Estos componentes son los "contenidos" de las rutas y espacios horizontales.

Rutas y Espacios Horizontales: (también llamado "sistemas de distribución horizontal") Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado horizontal.

El cableado horizontal incluye:

- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Páneles de empate (patch) y cables de empate utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones

El cableado horizontal típicamente:

- Contiene más cable que el cableado del backbone
- Es menos accesible que el cableado del backbone

El cableado horizontal deberá diseñarse para ser capaz de manejar diversas aplicaciones de usuario incluyendo.

- Comunicaciones de voz (teléfono)
- Comunicaciones de datos
- Redes de área local

TOPOLOGIA: El cableado horizontal se debe implementar en una **topología de estrella**. Cada salida de del área trabajo de telecomunicaciones debe estar conectada directamente al cuarto de telecomunicaciones.

15.3 DISTANCIA DEL CABLE: La distancia horizontal máxima es de 90 metros independiente del cable utilizado para IL SOLUTION siendo de 81 metros. Esta es la distancia desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones. Al establecer la distancia máxima se hace la previsión de 10 metros adicionales para la distancia combinada de cables de empate (3 metros) y cables utilizados para conectar equipo en el área de trabajo de telecomunicaciones y el cuarto de telecomunicaciones.

SALIDAS DE AREA DE TRABAJO: Los ductos a las salidas de área de trabajo debemos preveer la capacidad de manejar tres cables Las salidas de área de trabajo deben contar con un mínimo de dos conectores. Uno de los conectores debe ser del tipo RJ-45 bajo el código de colores de cableado T568A (recomendado) o T568B.

MANEJO DEL CABLE: El destrenzado de pares individuales en los conectores y paneles de empate debe ser menor a 1.25. cm para cables UTP categoría 6

EVITADO DE INTERFERENCIA ELECTROMAGNETICA: A la hora de establecer la ruta del cableado de los closet de alambrado a los nodos es una consideración primordial evitar el paso del cable por los siguientes dispositivos.

- Motores eléctricos grandes o transformadores (mínimo de 1.2 metros).
- Cables de corriente alterna.
- Luces fluorescentes y balastros (mínimo 12 centímetros). El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos
- Intercomunicadores (mínimo 12 cms.)
- Equipo de soldadura.
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros)
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

16. CANALETAS

Para el diseño de la red se utilizarán canaletas plásticas por que facilitan y resuelve todos los problemas de conducción y distribución de cables. Se utilizarán para la fijación a paredes, chasis y paneles, vertical y horizontal.
Los canales en toda su longitud están provistos de líneas de prerruptura dispuestas en la base para facilitar el corte de un segmento de la pared, para su acoplamiento con otras canales formando T, L salida de cables.

La canaleta deberá instalarse con los accesorios y acopladores requeridos, tales como ángulos rectos, externos e internos, coples, piezas tipo T con los radios de curvatura que correspondan a la categoría 6 del cableado estructurado.

17. TOPOLOGÍA LÓGICA

La **topología lógica** de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast (Ethernet) y transmisión de tokens (Token Ring).

La topología de broadcast significa que cada host envía sus datos hacia todos los demás hosts del medio de red. Las estaciones no siguen ningún orden para utilizar la red, el orden es el primero que entra, el primero que se sirve.

La transmisión de tokens controla el acceso a la red al transmitir un token eléctrico de forma secuencial a cada host. Cuando un host recibe el token, eso significa que el host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token hacia el siguiente host y el proceso se vuelve a repetir.
La topología lógica que se utilizara en la red será Broadcast.

18. FAST ETHERNET

Full-Duplex

La comunicación Full-Duplex para 100BaseTX y 100BaseFX es llevada a cabo desactivando la detección de las colisiones y las funciones de loopback, esto es necesario para asegurar una comunicación fiable en la red. Sólo los switches pueden ofrecer Full-Duplex cuando están directamente conectados a estaciones o a servidores. Los hubs compartidos en 100BaseT deben operar a Half-Duplex para detectar colisiones entre las estaciones de los extremos. Por consiguiente utilizaremos la tecnología Fast Ethernet por que nos brinda las siguientes ventajas:

- Los datos pueden moverse entre Ethernet y Fast Ethernet sin traducción protocolar.
- Fast Ethernet también usa las mismas aplicaciones y los mismos drivers usados por Ethernet tradicional.
- Fast Ethernet está basado en un esquema de cableado en estrella, ésta topología es más fiable y en ella es más fácil de detectar los problemas que en 10Base2 con topología de bus.
- En muchos casos, las instalaciones pueden actualizarse a 100BaseT sin reemplazar el cableado ya existente.
- Fast Ethernet sólo necesita 2 pares de UTP categoría 5.

Fast Ethernet ofrece tres opciones de medio de transmisión:

Nombre	Sistema de Comunicacion	Tipo Cable/Categoria
100Base-T4	half-duplex. Debido a que utiliza 3 pares para transmitir y recibir.	4 pares de UTP Categoria 3,4,5 . Los datos son transmitidos en 3 pares (cada uno a 33 Mbps) utilizando codificacion 8B/6T, la cual permite frecuencias menores y decrementa las emisiones electromagneticas. y el cuarto par es para detectar colisiones.
100Base-TX	half o full-duplex	Dos pares de UTP categoria 5 o STP Tipo I half duplex. Un par para transmisiones (con una frecuencia de operacion de 125 MHz a 80% de eficiencia para permitir codificacion 4B5B). Y el otro par para detectar collisiones y recibir. Utiliza un esquema de codificacion MLT-3, tambien utilizado en ATM.
100Base-FX	half o full-duplex	Fibra optica de 62.5(core)/125 (cladding) -micron multimodo. Capaz de sostener un throughput de 100 Mbits/s en distancias mayores a 100m. Utiliza un fibra para transmisiones y la otra para deteccion de colisiones y para recibir.

Utilizaremos la tecnología Fast Ethernet debido a que el diseño de red es una topología en estrella.

19. SEGMENTACIÓN DE COLISIONES

La compañía ha decidido ampliar sus instalaciones, proponemos 37 dominios de colisión debido a que hay un dominio por cada puerto de los switches.

20. EQUIPO DE CAPA 2

20.1 SWITCH

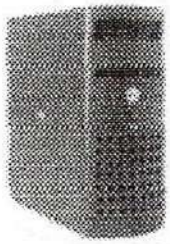
Son dispositivos utilizados para entregar todo el ancho de banda a un segmento de red en una fracción de tiempo. Permite utilizar toda la velocidad inter.-red. Un switch en su presentación es muy parecido al hub, sólo difiere en su función lógica y en la adición de unos puertos para funciones adicionales. El switch realiza transferencia de tráfico de broadcast y de multicast, pero disminuye el dominio de colisión al mínimo.

Algunas **características** especiales de los switch son las siguientes. Número de puertos. Se consiguen de 12,24, 48 puertos. Además de los puertos nominales (12 o 24), tienen otros puertos adicionales que sirven para conectar un equipo a una velocidad mayor o para unirlo a otro switch, También se le pueden conectar opcionalmente, módulos para interconexión de fibra óptica.

20.2 EQUIPOS DE TRABAJO

Se dará a la empresa tres opciones de servidores.

PowerEdge 400SC



US $399

Pequeñas empresas buscando una forma económica de migrar a redes punto a punto basadas en servidor Pequeñas empresas buscando un servidor de entrada al mejor precio

.

Bajo Costo de Implementación: El servidor PowerEdge™ 400SC es un servidor muy accesible en precio, especialmente diseñado para facilitar su instalación, puesta en marcha, funcionamiento y solución de problemas. El servidor PowerEdge 400SC es perfecto para empresas pequeñas y oficinas en casa que requieren un servidor local

Integración Fácil: El servidor PowerEdge 400SC fue diseñado para reducir al mínimo el costo de propiedad al cliente mediante el uso de tecnologías comprobadas. El servidor PowerEdge 400SC se entrega con un CD de Soporte del Sistema, totalmente gratis, para facilitar su instalación.

Desempeño: Al ofrecer tecnología actual a un precio bajo, el servidor PowerEdge 400SC proporciona gran valor a las empresas pequeñas que se encuentran reemplazando las redes de Punto a Punto, o que simplemente necesitan su primer servidor local. Con la posibilidad de elegir entre los procesadores Intel Pentium® 4 con bus frontal a 800 MHz, o el procesador económico Intel Celeron, el cliente elige la potencia que mejor se ajusta a su bolsillo. (Los procesadores Celeron soportan bus frontal de 400 MHz. El procesador Pentium 4 3.20 GHz con bus frontal de 800 MHz soporta tecnología Hyper-threading.)

ESPECIFICACIONES

Procesadores

- Un solo procesador Intel® Pentium® 4 a 2.26, 2.40, 2.80 y 3.20 GHz o un solo procesador Intel Celeron® a 2.0 y 2.30 GHz
- *Procesadores Celeron: bus frontal de 400 MHz*
- Procesadores Pentium 4: bus frontal de 800 MHz

Bus frontal

- De 800 MHz para procesadores Pentium 4
- De 400 MHz para procesadores Celeron

Caché

- Pentium 4: Caché Nivel 2 de 512 KB
- Celeron: Caché Nivel 2 de 128 KB

Chipset

- Intel 875P

Memoria

- 128 MB to 4 GB ECC DDR-266 registered SDRAM

Ranuras de Entrada y Salida I/O

- 3 ranuras de 32 bits a 33 MHz (soporta tarjetas 5v, tres disponibles, una para video)

Controladores de Unidades de Disco

- 2 IDE
- Controlador SCSI Ultra320 SCSI opcional

Controlador RAID

- CERC IDE RAID 1

Bahías para Disco

- 2 de 1.0" sin capacidad "Hot Swap" para discos duros
- 2 de 5.25" con acceso frontal, donde se puede colocar una unidad CD/DVD y una TBU
- 1 de 3.5" para disco Floppy estándar

Elija Entre Unidades SCSI o IDE:

- Unidades de disco duro IDE de 40 GB, 80 GB o 120 GB (o)
- Unidades de disco duro SCSI 36 GB o 73 GB

Capacidad Máxima de Almacenamiento Interno

- IDE: de hasta 240 GB
- SCSI: de hasta 146 GB

Opciones de Respaldo en Cinta

- Internal, PowerVault™ 100T, IDE Travan40, 20/40 GB

Comunicaciones

- NIC Gigabit integrado (Intel)

Dispositivos de Captura

- Teclado PS2
- Mouse PS2

Puertos

- 6 puertos USB 2.0, 1 paralelo, 2 serial y 2 PS/2

Abastecimiento de Energía

- Abastecimiento de energía con interruptor manual (250W)

Sistema de Enfriamiento

- Un ventilador

Chasis

- Altura: 42.7 cm. (16.8 pulgadas)
- Ancho: 19.0 cm. (7.5 pulgadas)
- Profundidad: 44.9 cm. (17.7 pulgadas)
- Peso: 35 libras

Gráficos

- Tarjeta de gráficos PCI ATI Rage XL económica (sin soporte AGP)

GARANTIA

- **Estándar:** 3 años de partes y mano de obra en sitio, el siguiente día hábil.
- **Opcional:** 1 año de partes y mano de obra en sitio el siguiente día hábil y segundo y tercer año el siguiente día hábil en servicio de partes solamente.

PowerEdge 1600SC

US $923

- Compartir Impresion/Archivos hasta con 50 usuarios.
- Capacidad de E-mail server hasta con 50 usuarios.
- Organizaciones de todos los tamaños que necesitan un servidor poderoso y a la vez económico con características de última.
- technología como procesadores Xeon™ dobles, Discos Duros "Hot Plugs", Fuentes de poder redundantes y "Hot Plug", tecnología U320 y NIC Gigabit integrado.

Desempeño - El servidor de primer nivel PowerEdge™ 1600SC cuenta con procesador doble Xeon™ y ofrece a pequeñas empresas y clientes remotos un desempeño sólido a un precio accesible. Power Edge 1600SC proporciona poder para la red a un precio accesible para su presupuesto.

Disponibilidad - El servidor Power Edge 1600SC cuenta con abastecimiento de energía redundante con capacidad hot-plug como una opción para ayudar a

incrementar la disponibilidad del sistema. Junto con el soporte SCSI o IDE RAID, el Power Edge 1600SC tiene características que se combinan para ayudarle a aumentar al máximo el tiempo de funcionamiento del sistema y la disponibilidad de la información.discos duros con capacidad hot-plug opcionales y sistema de administración remota opcional (DRACIII/XT).

Capacidad de Escalación Aún cuando la cantidad de empleados en su empresa se mantenga sin cambio, la información de su organización aumentará, por lo que hemos diseñado este sistema con una capacidad de expansión de hasta 4 GB de memoria ECC DDR SDRAM y soporte hasta para cuatro unidades IDE cableadas de 1", o seis discos duros con capacidad hot-plug SCSI de hasta con 438GB de almacenamiento SCSI interno.

Protección de la Información Sabemos que respaldar la información es esencial para la salud de su negocio. Además de las diversas opciones RAID, el servidor Power Edge 1600SC soporta soluciones de respaldo en cinta de alta capacidad con las unidades internas de respaldo en cinta SCSI como el PowerVault™ 100TDDS4 o el PowerVault 110T DLT VS80, o la unidad interna de respaldo en cinta PowerVault 100T TR40.

ESPECIFICACIONES

Procesadores

- Hasta 2 procesadores Intel® Xeon™ 1.80 GHz, 2.0 GHz, 2.40 GHz, 2.80 GHz, 3.06 GHz

Bus Frontal

- Bus frontal de 533 MHz para el procesador de 2.0, 2.40, 2.80 y 3.06 GHz
- Bus frontal de 400 MHz para el procesador de 1.80 GHz

Caché

- Caché 512KB L2 para todas las velocidades de procesadores

Conjunto de Chips

- Conjunto de Chips ServerWorks® GC-SL

Memoria

- SDRAM ESS DDR-200 de 128 MB hasta 4 GB

Ranuras de Entrada y Salida I/O

- 44 sockets DIMM para soportar memoria DDR de hasta 4 GB
- Memoria DDR (Double Data Rate) para mejor desempeño
- Memoria con soporte de Revisión y Corrección de Errores (ECC, por sus siglas *en inglés) para mayor disponibilidad*

Controladores de Unidades de Disco

- Controlador SCSI LSI Logic 53C1020 de Canal Sencillo LVD Ultra320 SCSI
- Controlador Opcional SCSI 39160 para respaldo opcional en cinta

Controlador RAID

- PERC3/SC (controlador PCI RAID de canal sencillo con 32MB de caché)
- CERC-ATA 100 IDE (controlador ATA RAID de cuatro canales)

Bahías para Disco

- Bahías de Unidades de Disco Duro: Hasta 6 bahías para discos duros en configuración hot-plug (opcional) o hasta 4 bahías para discos duros en *configuraciones cableadas.*
- Bahías para accesorios periféricos: 1 bahía para unidades floppy y 1 bahía para unidad óptica con opción CD-ROM estándar o DVD-ROM opcional o una unidad combinada CD-RW/DVD-ROM y 1 bahía adicional para una unidad óptica opcional o una unidad SCSI o IDE para respaldo en cinta.

Unidades de Discos Duros

Elija entre:

- Un máximo de 6 discos duros SCSI de 1.0" U320 10K o 15K en configuraciones hot-plug
- Un máximo de 4 discos duros SCSI de 1.0" U320 10K o 15K en configuraciones cableadas SCSI
- Un máximo de 4 discos duros IDE ATA100 en configuraciones cableadas

Capacidad Máxima de Almacenamiento Interno

- Un máximo de 876 GB de almacenamiento interno SCSI o un máximo de 480 GB de almacenamiento interno IDE

Opciones de Respaldo en Cinta

- PowerVault 100T TR40
- PowerVault 100T DDS 4
- *PowerVault 110T DLT VS80*

Comunicaciones

- NIC Intel Gigabit estándar sencillo integrado
- NIC opcional adicional: Intel 10/100/1000, Intel 10/100, o Broadcom 10/100/1000
- Módem Opcional: Módem interno Broadcom ModemXtreme PCI V.92 de 56Kbits

Dispositivos de Captura

- Mouse y teclados

Puertos USB

- Puertos Duales Universales Seriales (USB)

Abastecimiento de Energía

- Abastecimiento estándar de 450W no redundante
- Opción de abastecedores de energía redundante con características hot-plug (2 *de 450W), para mayor disponibilidad y para ayudar a mantener el servidor* funcionando y corriendo las aplicaciones correctamente.

Sistema de Enfriamiento

- 2 ventiladores (no redundantes)

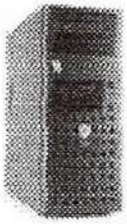
Chasis

- Chasis de Torre
- *Las dimensiones aproximadas son 17.61" altura x 8.57" ancho x 22.53"* profundidad (44.73cm x 21.77cm x 57.23cm)
- *Peso 73 lb. (totalmente equipada)*

Gráficos

- Controlador de gráficos ATI-Rage XL integrado con 8MB de memoria SDRAM (no

POWER EDGE600 SC



US $599

Para pequeñas empresas que corren aplicaciones simples en las que comparten funciones de archivo e impresión y que necesitan precios verdaderamente bajos.

Costo de Implementación Bajo - El modelo PowerEdge 600SC es un para su fácil instalación, excelente funcionamiento, corrección de problemas y capacidad de expansión servidor accesible diseñado. El servidor PowerEdge 600SC es la plataforma perfecta para las empresas pequeñas o para los servidores con aplicaciones de grupo de trabajo que requieren de poco soporte de sistemas.

Capacidad de Escalación - Aún cuando la cantidad de empleados se mantenga igual, la información de su empresa aumentará. Por lo tanto, hemos diseñado este sistema de tal manera que tiene la capacidad de escalar a un máximo de 4 GB de memoria ECC DDR SDRAM y soportar hasta 4 unidades de disco IDE o SCSI de 1" con un total de 480 GB de almacenamiento interno.

Protección de Datos - Sabemos que el respaldo de datos es una actividad esencial para que las empresas funcionen correctamente El servidor 600SC soporta soluciones de respaldo en cinta de alta capacidad ya sea con unidades de respaldo en cinta internas IDE (PowerVault™ 100T IDE) o SCSI (PowerVault 100T DDS-4 o PowerVault 110T DLTVS80.

Mayor Tiempo en Funcionamiento - Ordene su sistema con un controlador RAID y establezca redundancia de datos en una solución eficiente para la administración del almacenamiento interior. El mantenimiento del servidor se simplifica con el chasis PowerEdge 600SC al que se le puede dar servicio sencillamente. Entre otras características de disponibilidad se encuentran la memoria ECC y el fácil acceso a componentes internos.

ESPECIFICACIONES

Procesadores

- Un solo procesador Intel® Pentium® 4 de 2.40, 2.8 y 3.06 GHz
- Un solo procesador Intel® Celeron™ de 1.80 y 2.0 GHz

Bus Frontal

- Bus Frontal de 533 Mhz para Pentium 4 y 400 Mhz para Celeron

Caché

- Pentium 4: Caché L2 de 512 KB
- Celeron: Caché L2 de 128 KB

Conjunto de Chips

- ServerWorks® Grand Champion™ SL

Memoria

- SDRAM ESS DDR-200 de 128 MB hasta 4 GB

Ranuras de Entrada y Salida I/O

- 5 Ranuras PCI en total
- 4 de 64 bits y 33 MHz (Soporta tarjetas 3.3V)
- 1 de 32 bits y 33 MHz (Soporta tarjetas 3.3V)

Controladores de Unidades de Disco

- Tres canales integrados IDE para un máximo de seis dispositivos IDE
- Controlador 39160 Ultra3 SCSI opcional

Controlador RAID

- Controlador RAID IDE CERC ATA-100 opcional (Nivel RAID 0, 1, 5)
- Controlador RAID PERC 3/SC opcional (Nivel RAID 0, 1, 5)

Bahías para Disco

- 4 bahías de 1" sin capacidad hot-swap
- 2 bahías frontales de 5.25" que pueden alojar un CD y/o un DVD-ROM y un TBU
- 1 bahía estándar de 3.5" para disco floppy
- *Estándar: 48X EIDE CDROM*
- *Opcional:* 16X DVD ROM

Elija entre Unidades SCSI o IDE:

- Unidades de Disco IDE 7,200 RPM: 20 GB, 40 GB, 80 GB, 120 GB
- Unidades de Disco SCSI 10,000 RPM: 18 GB, 36 GB, 73 GB

Capacidad Máxima de Almacenamiento Interno

- Un máximo de 480 GB de almacenamiento interno (IDE)

Opciones de Respaldo en Cinta

- PowerVault 100T, IDE, TR5, 10 GB
- PowerVault 100T, IDE, Travan40, 20/40 GB
- PowerVault 100T, SCSI, DDS4, 20/40 GB
- PowerVault 110T, SCSI, DLTVS80, 40/80 GB

Comunicaciones

- NIC Gigabit Intel integrado
- Intel Pro1000XT opcional
- Intel Pro 100S opcional
- Broadcom 5703 opcional
- Módems internos y externos 56K V.90 *opcionales*

Dispositivos de Captura

- Mouse Logitech y Microsoft
- Teclados Chicony USB y NMB Rubberdome PS/2

Puertos

- 2 USB 1.1, 1 paralelo, 1 serial, 1 de video, 1 NIC, 1 mouse PS/2, 1 teclado PS/

Abastecimiento de Energía

- Abastecimiento de energía única de 250W
- Auto-interruptor de 110/220 Voltios

Sistema de Enfriamiento

- Tecnología de enfriamiento activa con tres ventiladores para distribuir la carga enfriadora equitativamente

Chasis

- Chasis de torre - 17" (43.1 cm) altura X 8" (20.3 cm) ancho X 19.5" (49.5 cm)

profundidad
Peso aproximado: 37 lb. (16.8 kg)

Gráficos

Controlador integrado ATI-Rage XL con 8 MB de memoria SDRAM (no tiene capacidad de crecimiento)

Administración

Los dispositivos de administración de sistemas integrados (LM-81 y MAX1617) detectan eventos en el sistema como fallas en ventiladores o problemas de *temperatura o voltaje.*

El software de administración supervisa los Ventiladores (Ventilador Posterior del Sistema, Ventilador Frontal del Sistema), Voltajes (al centro del CPU, +1.5, +2.5, +3.3, +12 y +5 voltios), Temperaturas (temperatura del CPU) y estado de la memoria.

El software de administración puede leer los registros de incidentes y mostrarlos en la página de Registro de Hardware dentro del software de administración. El *usuario también puede definir Acciones de Alerta cuando los censores rebasen* los umbrales establecidos.

La opción de recuperación automática permite al sistema reiniciarse o apagarse cuando se quede estático. La opción de apagado térmico, en caso de estar habilitada, puede activar el apagado del sistema operativo o apagado del sistema cuando la temperatura del CPU rebase el umbral establecido. El software funcionará únicamente si la temperatura del CPU es mayor a los límites establecidos durante una cantidad específica de tiempo.

SERVICIO

GARANTIA

- **Estándar:** 3 años de partes y mano de obra en sitio el siguiente día hábil.
- **Opcional:** 1 año de partes y mano de obra en sitio el siguiente día hábil y segundo y tercer año el siguiente día hábil en servicio de partes solamente.

20.3 EQUIPO CUARTO DE COMUNICACIONES

POWERCONNECT 3348

US $200

Switch de Ethernet Rápida Administrada de 48 Puertos con capacidad de Apilamiento y Enlaces Gigabit.

Switch de Ethernet Rápida Administrada de 48 Puertos con Enlaces Gigabit, Características Empresariales y Opciones de Apilamiento.

Soporta los estándares de la industria incluyendo calidad de servicio (reconoce L2, L3/L4), soporte multitransmisión, agregación de enlaces, configuraciones de VLAN dinámicas y □empe spanning tree.

Proporciona capacidades de seguridad robustas a través de ACLs basadas en flujo, seguridad MAC basada en puerto, autenticación remota RADIUS, encriptamiento SSL/SSH, y filtro de acceso administrativo basado en IP.

Se puede administrar de manera remota mediante un CLI estándar de la industria, un servidor web incorporado o una aplicación administrativa basada en SNMP.

Se puede administrar de manera remota mediante un CLI estándar de la industria, un servidor web incorporado o una aplicación administrativa basada en SNMP.

ESPECIFICACIONES

Atributos de los Puertos

- 24 puertos de switcheo auto sensores de Ethernet Rápida 10/100BASE-T
- 2 puertos de switcheo auto sensores de Ethernet Gigabit 10/100/1000BASE-T
- *2 ranuras SFP para soporte de medios de fibra (Nota: las ranuras SFP se utilizan* en lugar de los puertos 10/100/1000BaseT ya incluidos) o 1 ranura SFP con soporte de apilamiento en la segunda ranura SFP
- Las capacidades de apilamiento pueden soportar hasta un máximo de 192 puertos de Ethernet Rápida o hasta un máximo de seis switches por pila
- Sistema de Apilamiento Intercambiable con el equipo PowerConnect 3348
- Auto negociación para velocidad, modo duplex y control de flujo
- Auto MDI/MDIX
- Espejeo de puertos (muchos a uno)
- *Control de tormenta de transmisiones con función de activación y desactivación* por separado para transmisiones sencillas desconocidas, transmisiones múltiples desconocidas y tráfico de transmisiones

Desempeño

- Capacidad del switch de 8.8 Gb/s
- Velocidad de envío 6.5 Mpps
- Hasta un máximo de 8,000 direcciones MAC
- Modo de re-envío almacenamiento y re-envío

Disponibilidad

- Spanning Tree (IEEE 802.1D) y □empe Spanning Tree (IEEE 802.1w) con soporte para Enlace Rápido
- Soporte para energía redundante externa a través del PowerConnect RPS-600 (se vende por separado)
- *Tres ventiladores de enfriamiento para lograr redundancia*

VLAN

- Soporte VLAN para etiquetado y basado en puerto en concordancia con IEEE 802.1Q
- Hasta un máximo de 256 VLANs soportadas
- VLAN dinámica con soporte GVRP

Calidad de Servicio

- Etiquetado IEEE 802.1p
- Asignación de prioridad basada en puerto
- Cuatro señales de prioridad por puerto
- Asignación de prioridad que reconoce L2/L3/L4

.WRR ajustable y programación estricta de fila de espera

Multitransmisión

.IGMP de snooping Soporte de Multitransmisión IP
.Multitransmisión IP estática

Seguridad

.Filtro de dirección de IP para □empera administración vía Telnet, HTTP, HTTPS/SSL, SSH y SNMP
.*Preferencias y ajustes que puede definir el usuario para activar o desactivar el* acceso administrativo a Web, SSH, Telnet, SSL
.*Alerta de domicilio MAC basado en Puerto y seguro*
.Soporte RADIUS para acceso a administración de switches
.Soporte para Listas de Control de Acceso (ACLs); hasta un máximo de 248 *Entradas de Control de Acceso (ACEs) por ACL de Ethernet Rápida y hasta un* máximo de 120 ACEs por ACL de Ethernet Gigabit; hasta un máximo de 2,000 *ACE's totales por switch*
.Las ACLs pueden identificar flujos basándose en el Protocolo (Puerto TCP/UDP), Dirección IP Origen/Destino, Puerto Origen/Destino, Valores DSCP, Valores de *Precedencia IP, Direcciones MAC Origen/Destino, e Identificación de VLAN*
.Las ACLs pueden se pueden asignar a puertos, grupos de agregación de enlaces y VLANs

Otro Sistema de Switcheo

.Agregación de Enlaces con soporte para un máximo de seis enlaces agregados por switch y hasta un máximo de ocho puertos por enlace agregado (IEEE 802.3ad)
.Soporte LACP

Administración

.Internase de administración basado en Web
.CLI estándar de la industria accesible vía Telnet o consola
.*Soporte para SNMPv1 y SNMP v2c*
.4 grupos RMON soportados (historia, estadísticas, alarmas y eventos)
.Transferencias TFTP de firmware
.*Soporte para imágenes firmware duales*
.Soporte para carga y descarga de configuración de archivos
.Estadísticas para el monitoreo de errores y optimización del desempeño incluyendo las tablas de información sobre los puertos
.Soporte para administración de direcciones IP □empe/DHCP
.*Capacidad de conexión remota al sistema Syslog*

Chasis

MIB Support

- MIB-II
- Bridge MIB
- Interfaces Evolution MIB
- RMON MIB
- RADIUS MIB
- Etherlike MIB
- Entity MIB
- Extended Bridge MIB
- Dell3300.MIB

Soporte para Standares

- IEEE 802.1D
- IEEE 802.1Q
- IEEE 802.1p
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3z
- IEEE 802.3ab
- IEEE 802.3ac
- IEEE 802.3ad

Accesorios Periféricos (se venden por separado)

- Abastecedor de energía redundante RPS-600
- Transceivers SFP de Dell (SX y LX)

Ambiental

- Temperatura de Operación: 0C – 50C
- Temperatura de Almacenamiento: -40C to 70C
- Operación bajo Humedad Relativa: 10% - 90%
- Humedad Relativa de Almacenamiento: 5% - 90%
- 100-240VAC, 50-60Hz

POWERCONNECT 5224

US $500

El Sistema Powerconnect™ 5224 Ofrece Conectividad Gigabit Confiable A Un Costo Muy Bajo.

El sistema incluye 24 puertos con velocidad wire-speed, Ethernet Gigabit con características avanzadas de administración para cumplir con todas las necesidades de la medianas y grandes organizaciones.

Soporta estándares abiertos de la industria incluyendo calidad de servicio (L3), soporta multi-cast, agregación de ligas y configuraciones dinámicas VLAN.

Se puede administrar de manera remota vía CLI, estándar de la industria, utilizando un servidor de red integrado, o bien, empleando aplicaciones administrativas basadas en SNMP.

Provee una mejor administración de la configuración a través de sus capacidad de configurar archivos al cargarlos o descargarlos.

Ofrece un diseño flexible al utilizar capacidades Ethernet Gigabit tanto de cobre como de fibra.

21. DIRECCIONAMIENTO IP

Las Direcciones IP son cadenas de 32 bits organizadas como una secuencia de cuatro bytes. Estas cadenas tienen una representación como cuatro números enteros separados por puntos y en notación decimal. Las direcciones representan la interfase de conexión de un host con la red. La dirección de red se compone de una parte de red y una de host, la parte de red la utiliza el router en la nube de redes. Para ver si el destino está en la misma red física se extrae la parte de red de la dirección IP de destino, y se compara con la dirección de red de origen.
Cuando un paquete atraviesa una red, las direcciones IP de origen y destino no cambian nunca. Una dirección IP es calculada por el protocolo de enrutamiento IP y el software, y se conoce como dirección de próximo salto.

La parte de red de la dirección se emplea para realizar direcciones selecciones de ruta. La función de conmutación permite a un router aceptar un paquete por una interfaz y reenviarlo a una segunda interfaz. La función de determinación de ruta permite al router seleccionar la interfaz mas adecuada.

21.1 SERVICIOS DE RED

Los servicios que la red prestará a la compañía serán los siguientes:

1. 1 impresora en Recursos Humanos.
2. 1 impresora en el área Comercial.
3. 1 impresora, 1 Servidor y 2 switches en el área de Sistemas.
4. 1 impresora en el área de Diseño Gráfico.
5. 1 impresora en el área de Gerencia de proyectos.
6. 1 impresora en el área de Gerencia General.
7. 1 impresora en el área de Administración.

En el área de Diseño Gráfico se Comparten los archivos intercambiando la información entre aquellos equipos que conforman la red de ese departamento, comenzando desde el servidor hasta los puntos de trabajo en donde se guardan los archivos mencionados.

21.2 TIPO DE ACCESO AL NODO

El MDF se encuentra en el segundo piso y se conectan con el 1er piso y el 3er piso por medio de cable Utp cat 6, este a su vez se distribuye a los sitios de trabajo del 2ndo piso por medio del mismo par trenzado Utp cat 6.

21.3 DISTRIBUCION DE DIRECCIONES IP

ITEM	DIRECCION IP	MASCARA DE SUBRED	MAC	TRAFICO	UBICACION
1	192.129.0.5	255.255.255.0	00-07-2B-73-86-BA		GERENCIA GENERAL
2	192.129.0.10	255.255.255.0	00-09-6B-F2-3E-CA		SECRETARIA GENERAL
3	192.129.0.11	255.255.255.0	00-03-09-2D-64-2C		PROGRAMADOR
4	192.129.0.14	255.255.255.0	00-D0-B7-E5-5F-2F		GERENCIA DE R.H.
5	192.129.0.15	255.255.255.0	00-09-6B-F2-E5-56		SECRETARIA DE R.H.
6	192.129.0.16	255.255.255.0	00-05-04-3F-2B-46		TESORERIA
7	192.129.0.19	255.255.255.0	00-09-6B-F2-6B-CB		GERENCIA DE SISTEMAS
8	192.129.0.20	255.255.255.0	00-E2-08-3C-CB-2F		SOPORTE TECNICO
9	192.129.0.21	255.255.255.0	00-07-2B-73-8C-63		ANALISTA
10	192.129.0.23	255.255.255.0	00-03-09-2D-82-5B		
11	192.129.0.27	255.255.255.0	00-E2-08-3C-80-38		DISEÑADOR UNO
12	192.129.0.28	255.255.255.0	00-05-04-3F-7B-69		DISEÑADOR TRES
13	192.129.0.29	255.255.255.0	00-09-6B-F2-1B-68		DISEÑADOR DOS
14	192.129.0.30	255.255.255.0	00-09-6B-F2-8B-47		GERENCIA DISEÑO GRAFICO
15	192.129.0.37	255.255.255.0	00-09-6B-F2-5C-82		VENDEDOR DOS
16	192.129.0.38	255.255.255.0	00-05-04-3F-4E-BF		VENDEDOR UNO
17	192.129.0.39	255.255.255.0	00-07-2B-73-4F-44		SECRETARIA SISTEMAS
18	192.129.0.43	255.255.255.0	00-08-02-31-88-E2		AUXILIAR CONTABLE
19	192.129.0.45	255.255.255.0	00-09-6B-F2-BA-80		AUXILIAR R.H
20	192.129.0.49	255.255.255.0	00-08-02-31-8C-42		COBRANZAS
21	192.129.0.54	255.255.255.0	00-09-6B-F2-87-70		GERENCIA ADMINISTRATIVA
22	192.129.0.58	255.255.255.0	00-D0-B7-E5-CA-4 A		SECRETARIA ADMINISTRATIVA
23	192.129.0.61	255.255.255.0	00-05-04-3F-4D-98		SECRETARIA DE G.PROYECTOS
24	192.129.0.72	255.255.255.0	00-08-02-31-3D-20		SECRETARIA DE PROYECTOS
25	192.129.0.73	255.255.255.0	00-05-04-6B-5F-BC		PROGRAMADOR UNO
26	192.129.0.77	255.255.255.0	00-03-09-2D-3B-1C		GERENCIA COMERCIAL
27	192.129.0.82	255.255.255.0	00-08-02-31-1C-73		CONTABILIDAD
28	192.129.0.86	255.255.255.0	00-D0-B7-E5-47-71		AUXILIAR NOMINA
29	192.129.0.91	255.255.255.0	00-05-04-3F-2C-31		GERENCIA DE PROYECTOS
30	192.129.0.98	255.255.255.0	00-05-04-3F-6F-49		IMPRESORA LACER
31	192.129.0.99	255.255.255.0	00-05-04-3F-CF-43		IMPRESORA LACER
32	192.129.0.105	255.255.255.0	00-E2-08-3C-51-BD		PROGRAMADOR TRES
33	192.129.0.118	255.255.255.0	00-09-6B-F2-3C-48		SERVIDOR
34	192.129.0.134	255.255.255.0	00-09-6B-F2-7E-59		IMPRESORA AREA SISTEMAS
35	192.129.0.100	255.255.255.0	00-05-04-3F-6F-50		IMPRESORA LACER
36	192.129.0.101	255.255.255.0	00-05-04-3F-6F-51		IMPRESORA LACER
37	192.129.0.102	255.255.255.0	00-05-04-3F-6F-52		IMPRESORA LACER

22. SISTEMAS OPERATIVOS

El Sistema operativo que se utilizará para el servidor es Windows NT 2000 Server., ya que soporta el protocolo TCP/IP (el cuál se requiere para poder establecer conexiones a Internet) y proporciona una interfaz amigable al Administrador de la red.

Por otra parte, es importante destacar que el sistema operativo Windows NT 2000 Server puede manejar un máximo de 250 estaciones, lo cual no genera inconvenientes dado que el número de estaciones a conectar en la red es de 30 equipos, lo cual es considerablemente inferior a esa cantidad. De acuerdo a lo especificado anteriormente, se puede apreciar que Windows NT 2000 Server posee las características apropiadas para cumplir con los requerimientos de la red propuesta.

22.1 VENTAJAS OFRECIDAS AL UTILIZAR WINDOWS NT

- Controla el acceso en el sistema de archivos.
- Optimiza los procesos de segundo plano, como transporte de paquetes en red y entrega de correo electrónico.
- Facilita la recuperación de datos borrados de disco por error
- Es seguro y confiable.
- Permite el acceso a Internet.
- Alcanza un mayor rendimiento en la compartición de Archivos.

22.2 PRINCIPALES CARACTERÍSTICAS DE WINDOWS NT.

- Permite el uso de múltiples procesadores.
- Permite compartir archivos del sistema propio con otros usuarios de la red y la conexión con directorios compartidos de otros sistemas.
- Proporciona un gran desempeño en la administración de memoria, ya que protege la memoria al asegurarse que múltiples programas se ejecuten en su propio espacio de memoria y no corrompan la memoria usada por otras aplicaciones.
- Soporta múltiples protocolos tales como: TCP/IP, Netbui y otros.
- Facilita el acceso a Internet con los exploradores más modernos.
- Soporta grandes dispositivos y periféricos de hardware.
- Ofrece seguridad local, exige identificación de usuario y contraseña para acceder al sistema.

Para las estaciones de trabajos se empleará el sistema operativo Windows 2000 Professional, debido a que, además de presentar una interfaz de fácil manejo a los usuarios, proporciona a éstos el soporte para ejecutar el conjunto de aplicaciones que cumplen con los requerimientos de información y trabajos que se manejan en las diferentes áreas de la compañía.

22.3 SEGURIDAD DE WINDOWS 2000 SERVER NT

A medida que evolucionan los sistemas de TI, también lo hacen las amenazas a la seguridad que estos pueden sufrir. Para proteger su entorno de forma eficaz contra los ataques, necesita conocer con detalle los peligros con los que puede encontrarse.

Al identificar las amenazas a la seguridad, debe tener en cuenta dos factores principales: 1) Los tipos de ataques que seguramente sufrirá y 2) los lugares donde pueden tener lugar. Muchas organizaciones no tienen en cuenta el segundo factor, pues asumen que un ataque grave sólo puede venir del exterior (normalmente, a través de su conexión a Internet). En CSI/FBI Computer Crime and Security Survey (encuesta sobre delitos y seguridad informáticos de CSI/FBI), el 31% de los encuestados citaron sus sistemas internos como un punto de ataque frecuente. Sin embargo, muchas empresas pueden no estar al corriente de que se están dando ataques internos, básicamente porque no comprueban si existen.

Administración de riesgos

No existe un entorno de TI totalmente seguro y al mismo tiempo útil. Al examinar su entorno, deberá evaluar los riesgos que sufre actualmente, determinar un nivel de riesgo aceptable y mantener el riesgo a ese nivel o por debajo del mismo. Los riesgos se reducen aumentando la seguridad de su entorno.

Como norma general, cuanto más alto sea el nivel de seguridad de una organización, más costosa resultará su implementación y más posibilidades habrá de que se reduzca su funcionalidad. Tras evaluar los posibles riesgos, quizá tenga que reducir el nivel de seguridad para conseguir aumentar la funcionalidad y reducir el costo.

Para entender los principios de la administración de riesgos, es necesario entender algunos términos básicos utilizados en el proceso de administración de riesgos. Estos incluyen recursos, amenazas, vulnerabilidades, explotaciones y contramedidas.

Recursos

Un recurso es cualquier elemento de su entorno que intente proteger. Puede tratarse de datos, aplicaciones, servidores, enrutadores e incluso personas. El objetivo de la seguridad es evitar que sus recursos sufran ataques.

Una parte importante de la administración de riesgos consiste en determinar el valor de sus recursos. No utilizaría cerraduras normales y un sistema de alarma doméstico para guardar las Joyas de la Corona. De forma similar, el valor de sus recursos determinará, por lo general, el nivel de seguridad apropiado para protegerlos.

Amenazas

Una amenaza es una persona, un lugar o un elemento que puede tener acceso a los recursos y dañarlos. En esta tabla se muestran distintos tipos de amenazas con ejemplos.

Tabla 2.1: Amenazas a entornos informáticos

Tipo de amenaza	Ejemplos
Natural y física	Fuego, agua, viento, terremoto Corte eléctrico
No intencionada	Empleados no informados Clientes no informados
Intencionada	Atacantes Terroristas Espías industriales Gobiernos Código malicioso

Vulnerabilidades

Una vulnerabilidad es un punto en el que un recurso es susceptible de ser atacado. Se puede interpretar como un punto débil. Las vulnerabilidades se dividen a menudo en las categorías que se muestran en la siguiente tabla.

Tabla 2.2: Vulnerabilidades en entornos informáticos

Tipo de vulnerabilidad	Ejemplos
Física	Puertas sin cerrar
Natural	Sistema antiincendios averiado
De hardware y software	Software antivirus no actualizado
De medios	Interferencia eléctrica
De comunicación	Protocolos no cifrados
Humana	Procedimientos no seguros de asistencia técnica

Explotación

Una amenaza que se aprovecha de una vulnerabilidad de su entorno puede tener acceso a un recurso. Este tipo de ataque se denomina explotación. La explotación de recursos se puede realizar de varias maneras. En la siguiente tabla se incluyen algunas de las más comunes.

Tabla 2.3: Explotaciones en entornos informáticos

Tipo de explotación	Ejemplo
Explotación de vulnerabilidad técnica	Ataques a fuerza bruta Desbordamiento del búfer Problemas de configuración Ataques repetidos Secuestro de sesión
Obtención de información	Identificación de dirección Identificación de sistema operativo Exploración de puertos Búsqueda de servicios y aplicaciones Exploración de vulnerabilidades Análisis de respuestas Enumeración de usuarios Destrucción de documentos Fuga de dispositivos inalámbricos Ingeniería social

Denegación de servicio	Daño físico Eliminación de recursos Modificación de recursos Saturación de recursos

Cuando una amenaza utiliza una vulnerabilidad para atacar un recurso, las consecuencias pueden ser graves. En esta tabla se muestran algunos de los resultados de explotaciones que pueden producirse en su entorno y algunos ejemplos.

Tabla 2.4: Resultados de explotaciones

Resultados de una explotación	**Ejemplos**
Pérdida de confidencialidad	Acceso no autorizado Reasignación de privilegios Personificación o robo de identidad
Pérdida de integridad	Daños en datos Desinformación
Pérdida de disponibilidad	Denegación de servicio

Relación entre amenazas, vulnerabilidades y riesgo

Las amenazas y vulnerabilidades identificadas en su organización se deben calificar y clasificar mediante un estándar; por ejemplo: baja, media o alta. La clasificación variará entre las organizaciones y a veces incluso dentro de una misma organización. Por ejemplo, la amenaza de terremotos es sustancialmente más elevada para las oficinas cercanas a una falla que para las que se encuentran en otros lugares. De manera similar, la vulnerabilidad de daños físicos a equipos sería muy alta para una organización de productos electrónicos altamente delicados y frágiles, mientras que una empresa de construcción puede tener un nivel de vulnerabilidad más bajo.

Contramedidas

Las contramedidas se aplican para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo en su entorno. Por ejemplo, una organización de productos electrónicos frágiles puede aplicar contramedidas de seguridad física como fijar la maquinaria a los cimientos del edificio o agregar mecanismos de amortiguación. Estas contramedidas reducen la posibilidad de que un terremoto pueda causar daños físicos a sus bienes. Una vez aplicadas todas las contramedidas para reducir las amenazas y vulnerabilidades, sólo quedan riesgos residuales.

Defensa en profundidad

Para reducir el riesgo en su entorno, debe usar una estrategia de defensa en profundidad para proteger los recursos de amenazas externas e internas. El término defensa en profundidad (en ocasiones denominada seguridad en profundidad o seguridad multicapa) procede de un término militar utilizado para describir la aplicación de contramedidas de seguridad con el fin de formar un entorno de seguridad cohesivo sin un solo punto de error. Las capas de seguridad

que forman la estrategia de defensa en profundidad incluyen el despliegue de medidas de protección desde los enrutadores externos hasta la ubicación de los recursos, pasando por todos los puntos intermedios.

Con el despliegue de varias capas de seguridad, ayuda a garantizar que, si se pone en peligro una capa, las otras ofrecerán la seguridad necesaria para proteger sus recursos. Por ejemplo, que el servidor de seguridad de una organización esté en peligro, no debe significar que un atacante pueda tener acceso sin trabas a los datos más confidenciales de la organización. En el caso ideal, cada capa debe proporcionar diferentes formas de contramedidas para evitar que se utilice el mismo método de explotación en varias capas.

Es importante recordar que sus recursos no son sólo datos, sino que cualquier elemento de su entorno es susceptible de ser atacado. Como parte de su estrategia de administración de riesgos, debe examinar los recursos que protege y determinar si dispone de protección suficiente para todos. Por supuesto, la cantidad de medidas de seguridad que pueda aplicar dependerá de la evaluación de riesgos y el análisis de costos y beneficios de la aplicación de contramedidas. Sin embargo, el objetivo consiste en garantizar que un atacante necesitará unos conocimientos, tiempo y recursos significativos para superar todas las contramedidas y tener acceso a sus recursos.

Defensa de datos

Para muchas empresas, uno de los recursos más valiosos son los datos. Si estos datos cayeran en manos de la competencia o sufrieran daños, tendrían problemas importantes.

A nivel de cliente, los datos almacenados localmente son especialmente vulnerables. Si se roba un equipo portátil, es posible realizar copias de seguridad,

restaurar y leer los datos en otro equipo, aunque el delincuente no pueda conectarse al sistema.

Los datos se pueden proteger de varias formas, incluido el cifrado de datos mediante EFS (Encrypting File Service) o sistemas de cifrado de otros fabricantes y la modificación de las listas de control de acceso discrecional en los archivos.

Defensa de aplicaciones

Como una capa de defensa más, el refuerzo de las aplicaciones es una parte esencial de cualquier modelo de seguridad. Muchas aplicaciones utilizan el subsistema de seguridad de Windows 2000 para proporcionar seguridad. No obstante, es responsabilidad del programador incorporar la seguridad en la aplicación para proporcionar una protección adicional a las áreas de la arquitectura a las que la aplicación puede tener acceso. Una aplicación existe en el contexto del sistema, de modo que siempre se debe tener en cuenta la seguridad de todo el entorno al considerar la seguridad de una aplicación.

Se debe probar en profundidad el cumplimiento de la seguridad de cada aplicación de la organización en un entorno de prueba antes de permitir que se ejecute en una configuración de producción.

Defensa de hosts

Debe evaluar cada host del entorno y crear directivas que limiten cada servidor sólo a las tareas que tenga que realizar. De este modo, se crea otra barrera de seguridad que un atacante deberá superar antes de poder provocar algún daño. El capítulo 4, "Asegurar servidores basándose en su función", incluye directivas que aumentan la seguridad para cinco funciones de servidor de Windows 2000 comunes.

Un modo de hacerlo consiste en crear directivas individuales en función de la clasificación y el tipo de datos que contiene cada servidor. Por ejemplo, las directivas de una organización pueden estipular que todos los servidores Web son de uso público y, por lo tanto, sólo pueden contener información pública. Sus servidores de bases de datos están designados como confidenciales de la empresa, lo que significa que la información debe protegerse a cualquier precio. De ahí las clasificaciones que se muestran en la siguiente tabla.

Tabla 2.5: Clasificación de servidores

Valor	Definición
De uso público	La distribución de este material no está limitada. Incluye información de marketing, materiales de venta e información seleccionada para uso público. Los datos incluidos en servidores de Internet públicos deben ser de uso público.
Sólo para uso interno	La revelación de esta información es segura para la distribución interna, pero puede provocar daños considerables a la organización si se hace pública. Debe colocarse por lo menos un servidor de seguridad entre esta información e Internet.
Confidencial de la empresa	La revelación de esta información puede provocar daños graves a la organización en conjunto. Esta información es del tipo más confidencial y sólo se expone si es absolutamente necesario. Deben colocarse por lo menos dos servidores de seguridad entre esta información e Internet.

Defensa de redes

Si dispone de una serie de redes en la organización, debe evaluarlas individualmente para asegurarse de que se ha establecido una seguridad apropiada. Si un enrutador sufre un ataque eficaz, puede denegar el servicio a partes enteras de la red.

Debe examinar el tráfico admisible en sus redes y bloquear el que no sea necesario. También puede considerar el uso de IPSec para cifrar los paquetes en sus redes internas y SSL para las comunicaciones externas. Asimismo, debe supervisar la existencia de detectores de paquetes en la red, que sólo deben usarse bajo controles estrictos.

Defensa de perímetros

La protección del perímetro de su red es el aspecto más importante para detener los ataques externos. Si su perímetro permanece seguro, la red interna estará protegida de ataques externos. La organización debe disponer de algún tipo de dispositivo de seguridad para proteger cada punto de acceso a la red. Es necesario evaluar cada dispositivo, decidir qué tipos de tráfico se permiten y desarrollar un modelo de seguridad para bloquear el resto del tráfico.

Los servidores de seguridad son una parte importante de la defensa del perímetro. Necesitará uno o más servidores de seguridad para asegurarse de minimizar los ataques externos, junto con la auditoria y la detección de intrusiones para estar seguro de detectar los ataques en caso de que se produzcan. Para obtener más información sobre la auditoria y la detección de intrusiones.

23. SEGURIDAD FÍSICA

Todo entorno en el que usuarios no autorizados puedan obtener acceso físico a equipos es inherentemente inseguro. Un ataque de denegación de servicio muy eficaz puede ser simplemente quitar el sistema de alimentación de un servidor o las unidades de disco. El robo de datos (y la denegación de servicio) puede producirse si alguien roba un servidor o incluso un equipo portátil.

Debe considerar la seguridad física como un elemento fundamental para su estrategia de seguridad global. Una prioridad principal será la de establecer una seguridad física para las ubicaciones de los servidores. Puede tratarse de salas de servidores del edificio o de centros de datos enteros.

También debe tener en cuenta los accesos a los edificios de la organización. Si alguien puede tener acceso a un edificio, puede tener oportunidades para llevar a cabo un ataque aunque ni siquiera pueda conectarse a la red. Estos ataques pueden incluir:

- La denegación de servicio (por ejemplo, conectar un equipo portátil a la red como servidor DHCP o desconectar la alimentación de un servidor)
- El robo de datos (por ejemplo, robar un equipo portátil o detectar paquetes en la red interna)
- La ejecución de código malicioso (por ejemplo, activar un gusano desde el interior de la organización)
- El robo de información de seguridad crítica (por ejemplo, cintas de copia de seguridad, manuales de funcionamiento y diagramas de red)

Como parte de la estrategia de administración de riesgos, debe determinar el nivel de seguridad física apropiado para su entorno. A continuación se enumeran algunas de las posibles medidas de seguridad física.

- Establecer seguridad física para todas las áreas del edificio (esto puede incluir tarjetas de acceso, dispositivos biométricos y guardias de seguridad)
- Requerir a los visitantes que vayan acompañados en todo momento
- Requerir a los visitantes que firmen un registro de entrada de todos los dispositivos informáticos
- Requerir a todos los empleados que registren cualquier dispositivo portátil de su propiedad
- Fijar físicamente todos los equipos de sobremesa y portátiles a las mesas

Directivas y procedimientos

Casi todas las medidas descritas hasta ahora están destinadas a evitar el acceso no autorizado a los sistemas. No obstante, está claro que habrá personas de su entorno que necesiten acceso de alto nivel a los sistemas. Toda estrategia de seguridad será imperfecta a menos que pueda garantizar que estas personas no van a hacer un uso indebido de los derechos que se les han concedido.

Antes de contratar a nuevos empleados para la organización, debe asegurarse de que se someten a un proceso de investigación de seguridad, con una investigación más rigurosa para aquellos que vayan a tener un mayor acceso a los sistemas.

Respecto a los empleados existentes, resulta esencial que sean conscientes de las directivas de seguridad y de lo que está permitido y prohibido (y, preferiblemente, también por qué). Esto es importante por dos razones. En primer lugar, si los empleados no son conscientes de lo que está prohibido, pueden llevar a cabo acciones que inconscientemente pongan en peligro la seguridad del entorno. En segundo lugar, si un empleado ataca adrede su entorno de TI y no se

ha prohibido explícitamente en las directivas de la empresa, puede resultar muy difícil entablar demanda contra esta persona.

En un entorno basado en Windows 2000, puede controlar de forma muy precisa los derechos administrativos de los usuarios. Debe asegurarse de definir detalladamente el alcance de los derechos administrativos que debe tener cada empleado de TI. Ningún empleado debe tener más acceso administrativo del que sea estrictamente necesario para realizar su trabajo.

Puede notificar a sus usuarios acerca de la seguridad mediante un programa de orientación seguido de recordatorios a intervalos regulares y actualizaciones visiblemente expuestas de los procedimientos de seguridad. Resulta esencial que los empleados se den cuenta de que cada uno de ellos desempeña un papel en el mantenimiento de la seguridad.

23.1 Métodos de ataque comunes y medidas preventivas

Como parte de la estrategia de defensa en profundidad, debe comprender los métodos empleados por los atacantes y defenderse contra los ataques más comunes. En este apartado se estudia una serie de tipos de ataques y se sugieren medidas para proteger su entorno contra los mismos.

Obtención de información

Los atacantes siempre intentan conseguir información sobre su entorno. A veces la información resulta útil por sí misma y en otras ocasiones es un medio para conseguir otras informaciones y otros recursos.

La clave para evitar la obtención de información es restringir el acceso no autorizado a los recursos desde el exterior. Los métodos para conseguirlo incluyen:

• Asegurarse de que sólo dispositivos específicos e identificados de la red permiten la conectividad mediante acceso remoto. Una utilidad de búsqueda de módems debe comprobar todos los prefijos de empresas para buscar dispositivos no autorizados. Los dispositivos de acceso remoto también se pueden detectar activando la detección de exploración en el sistema telefónico cuando esté disponible.

• Deshabilitar NetBIOS sobre TCP/IP, incluidos los puertos 135, 137, 139 y 445 en los equipos directamente conectados a Internet a través del servidor de seguridad externo. Esto hace más difícil para las personas externas la utilización de redes estándar para conectarse a servidores.

• Habilitar sólo los puertos 80 y 443 tanto en los adaptadores de red orientados a Internet y el servidor de seguridad para el tráfico destinado a un conjunto de servidores Web. De este modo se elimina la mayor parte de las técnicas de reconocimiento basadas en puertos.

• Revisar la información del sitio Web público para asegurarse de que:

  • Las direcciones de correo electrónico utilizadas en el sitio no son cuentas de administrador.

  • No se ha especificado la tecnología de la red.

  • La información general de la empresa publicada en el sitio es apropiada y no se puede utilizar para descubrir o deducir características del sistema de seguridad. Este tipo de información incluye sucesos actuales y recientes. Por ejemplo, si en el sitio Web se anuncia que su empresa acaba de adquirir otra firma, los atacantes pueden elegir a la nueva adquisición como objetivo pensando que su red se ha conectado precipitadamente a la nueva red corporativa y que, por lo tanto, es menos segura.

• Revisar las publicaciones de los empleados en grupos Usenet para evaluar el tipo de información que exponen.

• Administrar el tipo de contenido que contiene el código fuente del sitio Web para evitar que un atacante revise este código (una técnica en ocasiones denominada criba de código fuente) para obtener información valiosa. Algunos de los elementos que el equipo de seguridad debe buscar en el código fuente son los comentarios incorrectos, las contraseñas incrustadas y las etiquetas ocultas.

• Revisar la información proporcionada al público en general para su dirección IP y los registros de nombre de dominio.

Limitar la capacidad de explorar y obtener información valiosa

Tanto el Protocolo de control de transporte (TCP) como el Protocolo de datagrama de usuario (UDP) utilizan puertos para comunicarse. Utilizando la exploración de puertos, los atacantes pueden descubrir los servidores de su entorno que están escuchando y luego usar esta información para descubrir vulnerabilidades.

Existe una serie de exploraciones que resultan útiles para los atacantes. Se pueden utilizar para obtener información sobre puertos que están escuchando, protocolos presentes o incluso el sistema operativo (SO) del host y el estado de la versión. La identificación de los puertos, protocolos y SO de un host ayudarán a descubrir muchas vulnerabilidades que quizás no se descubrirían si no se explorara el dispositivo.

RECOMENDACIONES

- Para el manejo de los distintos equipos de comunicación es necesario la capacitación al personal que va ha estar a cargo de estos.

- Preparar al personal que trabaja en las dependencias de la compañía en el uso y manejo de los distintos sistemas operativos(en aquellos casos en que sea necesario) Los cuartos de equipo y el Cuarto de Telecomunicaciones deben estar a cargo de un personal capacitado para ello (podría ser el personal que trabaja en soporte técnico.)

- Sustituir las máquinas obsoletas que se encuentran en el edificio por otras que se adapten a los requerimientos propios de una red.
- realizar mantenimiento a los equipos y a los dispositivos que operan en la red.
- No permitir el consumo de comidas, bebidas y cigarrillos, en las áreas de trabajo donde se encuentren los computadores o las terminales de red.
- Conservar la seguridad en la red examinando la temperatura, la humedad y la irradiación.
- Realizar controles continuos a fin de conservar la inspección en los niveles de corriente, efectuando el mantenimiento necesario a los polos a tierra y así evitando peligros a los trabajadores.
- Realizar actualizaciones periódicas a las copias de seguridad, y colocarlas en un lugar seguro.
- Establecer quien va a ser la persona encargada del manejo, direccionamiento, configuración y seguridad de la red.

CONCLUSIONES

El diseño del proyecto de red planteado, para la empresa IL SOLUTIONS, evitará, en gran medida, a que se presenten problemas en el nuevo edificio permitiéndole a quienes allí laboran poder acceder a ésta, de manera más rápida, eficiente y confiable. En el edificio se pudo determinar la necesidad de interconectar todas las dependencias que funcionan en la compañía, por lo que hemos considerado conveniente diseñar una red de comunicación que permita manejar con mayor eficiencia y rapidez los procesos que se llevan a cabo en la mencionada edificación.

Es necesario manejar una tecnología que cumpla con las necesidades de la compañía, tomando en cuenta, los procesos que se requieren, y así lograr el beneficio y el bienestar de todo el personal que trabajan en la red.

BIBLIOGRAFIA

- Información proporcionada por la compañía IL SOLUTIONS.
- Catálogos de Dell computers
- Academia de networking de cysco Systems, guía del segundo año

ANEXO 1
MODELO DE LA ENCUESTA

1. ¿Existe información de carácter privado?

   SI___ NO___

2. ¿Utilizaría la red de la empresa?

   SI___ NO___

3. ¿Qué desventajas podría encontrar en la red?

_____

_____

4. ¿Utiliza Internet?

   SI___ NO___

5. ¿Qué tipo de información trabajan?

   _____

   _____

6. ¿Cuántos usuarios utilizaría la red?

   _____

7. ¿La organización tiene recursos diseñados al proyecto de red?

   SI___ NO___