

No. Reg. H55022

< T.S

Clas. 001.64404

J37x

UNIVERSIDAD AUTONOMA DE QUERETARO



QUERETARO, QRO. ABRIL DE 1995.



AGRADECIMIENTOS

A mi **Madre**, que en todo momento me aliento y apoyo en esta etapa de mi vida.

A mi **Familia** entera, que comprendió los momentos difíciles por los que pase.

A quienes por diversos motivos no menciono en estas líneas, y que sin embargo le dieron una razón a mi existencia.



MENCION

Una mención y agradecimiento especial a los ISC. Carlos Muñoz Pérez y Francisco Martínez Mejía, quienes generosamente impartieron cátedra y asesoraron para la realización de la presente tesina.

CONTENIDO

CONTENIDO

1. JUSTIFICACION.
2. INTRODUCCION.
3. TOPOLOGIA.
4. DESCRIPCION DE LOS COMPONENTES.
5. DIAGRAMA DE CABLEADO.
6. CAPACIDAD DE EXPANSION.
7. CICLO DE VIDA ESPERADO.
8. AMBIENTE DE SOPORTE DE APLICACIONES.
9. AMBIENTE DE ADMINISTRACION.
10. PROBLEMAS POTENCIALES.
11. FLUJO DE DATOS.
12. PROCEDIMIENTOS DE PRUEBA Y VERIFICACION.
13. IDENTIFICACION DE LOS REQUERIMIENTOS DE LA INSTALACION FISICA.
14. NECESIDADES DE ENTRENAMIENTO Y CAPACITACION.
15. NECESIDADES DE PERSONAL.

- 16. RIESGOS.
- 17. PLANES DE CONTINGENCIA.
- 18. CONCLUSIONES.
- 19. INDICE.
- 20. INDICE DE ILUSTRACIONES.
- 21. BIBLIOGRAFIA.

1. JUSTIFICACION

1. JUSTIFICACION

La presente tesina, ha sido elaborada como un requisito terminal del curso de actualización que sobre "REDES LOCALES" imparte la Escuela de Informática, con la finalidad de que los conocimientos de su alumnado sea renovado y ampliado en el cambiante mundo de la informática.

2. INTRODUCCION

2. INTRODUCCION

Nuestro mundo es hoy, escenario de cambios y transformaciones que en días pretéritos hubiera sido imposible imaginar.

Estos cambios están siendo originados en dos aspectos fundamentales, el humano y el tecnológico. El primero de ellos, está siendo motivado por una exigencia cualitativa y cuantitativa en todos los ámbitos donde la informática no queda exenta. El tecnológico, como respuesta a las necesidades que la modernidad exige, mayor rapidez, capacidad y exactitud.

Por lo anterior, obtener una radiografía de las características de una red, se justifica plenamente dado que éste documento permitirá determinar los requerimientos que le dieron origen, así como las características tecnológicas tanto en Software y Hardware, además del elemento humano que en su concepción, creación y desarrollo participaron.

Dada la volatilidad de nuestra área y la necesidad de documentar todas y cada una de nuestras actividades, la tesina "*Análisis de la Red Institucional de la Facultad de Derecho, UAQ*" aquí presentada, permitirá identificar rápidamente sus componentes lógicos y físicos, con lo cual se podrá conocer, sin necesidad de acceder físicamente a ella, con los beneficios que esto trae consigo.

3. TOPOLOGIA

3. TOPOLOGIA

3.1. LOCALIZACION GEOGRAFICA DE LA RED.

La Facultad de Derecho de la Universidad Autónoma de Querétaro se localiza en la capital del estado de Querétaro, específicamente en el Centro Universitario que se encuentra en el Cerro de las Campanas (Fig. 3.1.).

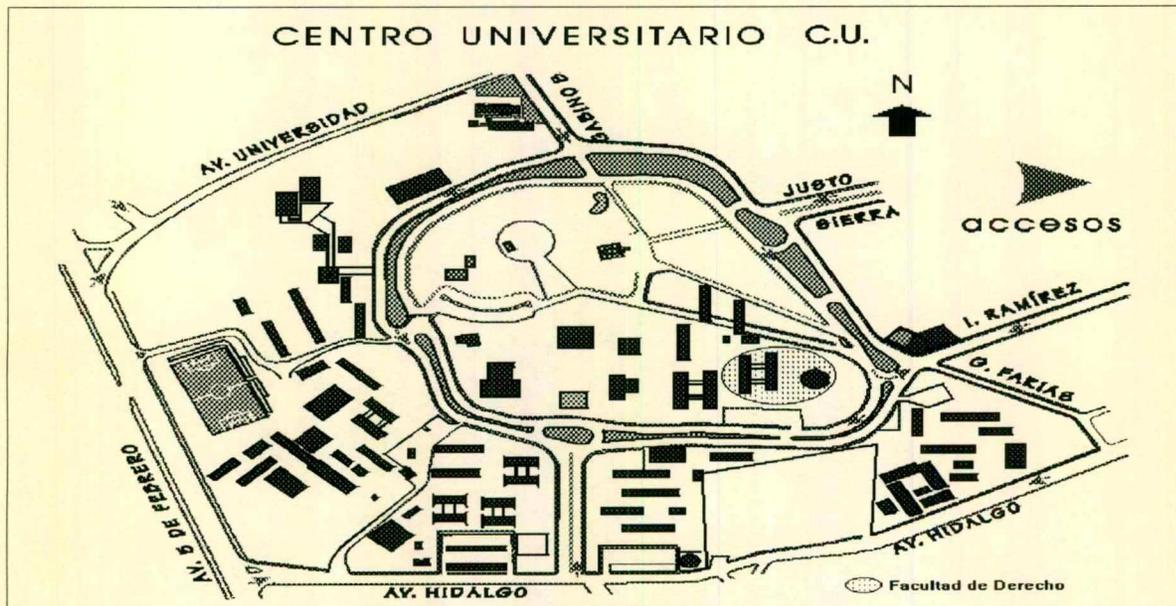


Fig. 3.1. Centro Universitario, UAQ.

3.2. LOCALIZACION FISICA.

La red se localiza en el aula que para tal efecto se adaptó a finales de 1993 en la Facultad, localizándose en la planta baja junto a la dirección de la misma (Fig. 3.2.)

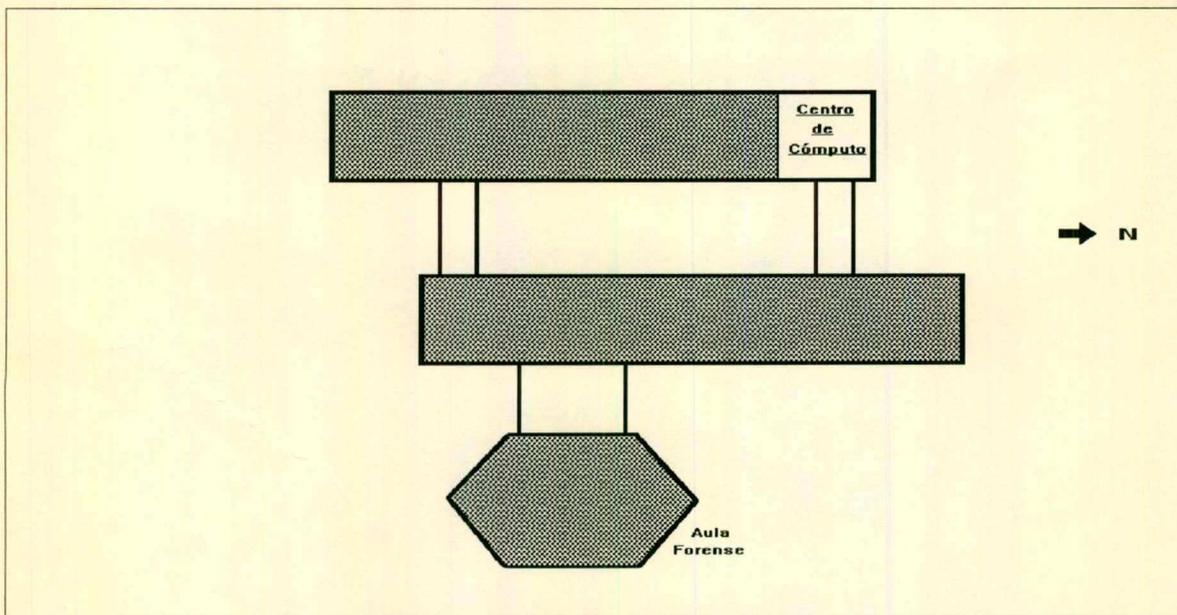


Fig. 3.2. Facultad de Derecho, UAQ

3.3. TOPOLOGIA.

La descripción de la forma en que el cable de transmisión va de un nodo a otro, define cual es su topología. Esta está definida como una estrella distribuida, para lo cual emplea concentradores (Fig. 3.3.)

Para lograr la comunicación entre nodos y concentradores, se emplea cable Twisted Pair, el cual permite una velocidad de transmisión de hasta 10 Mbits por segundo, con una longitud máxima del cable entre nodo y concentrador de 100 mts., y con un número máximo de 1024 nodos, dependiendo por supuesto del número de usuarios soportados por el Sistema Operativo de red.

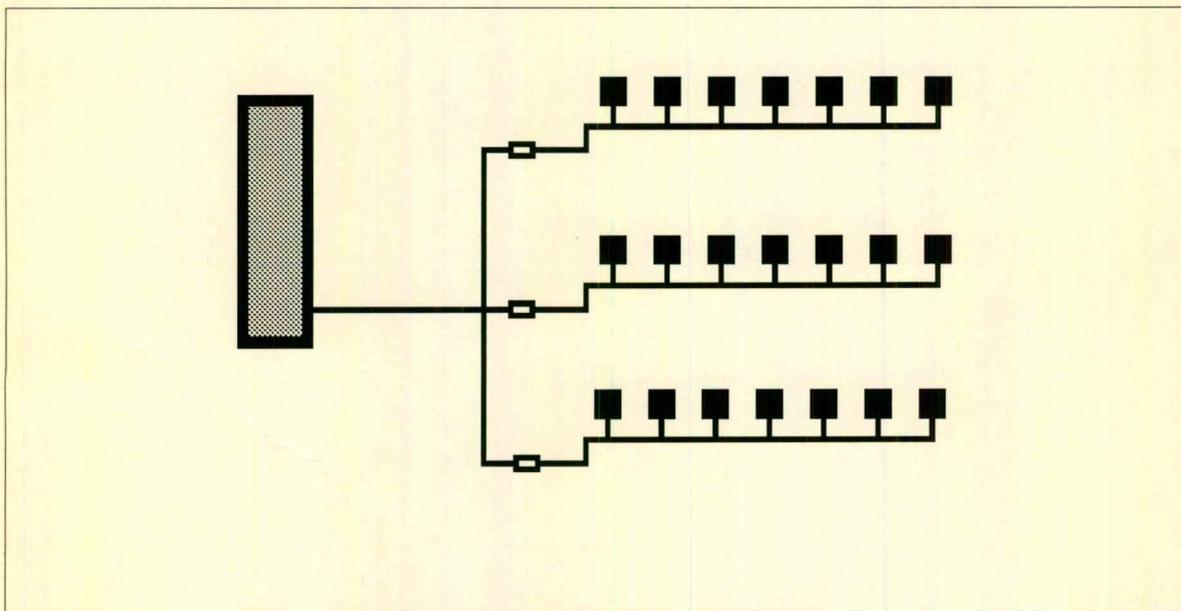


Fig. 3.3. Topología de estrella distribuida.

4. DESCRIPCION DE LOS COMPONENTES

4. DESCRIPCION DE LOS COMPONENTES

Antes de conocer la descripción física de los componentes de la red, observemos su distribución física (Fig. 4.1.):

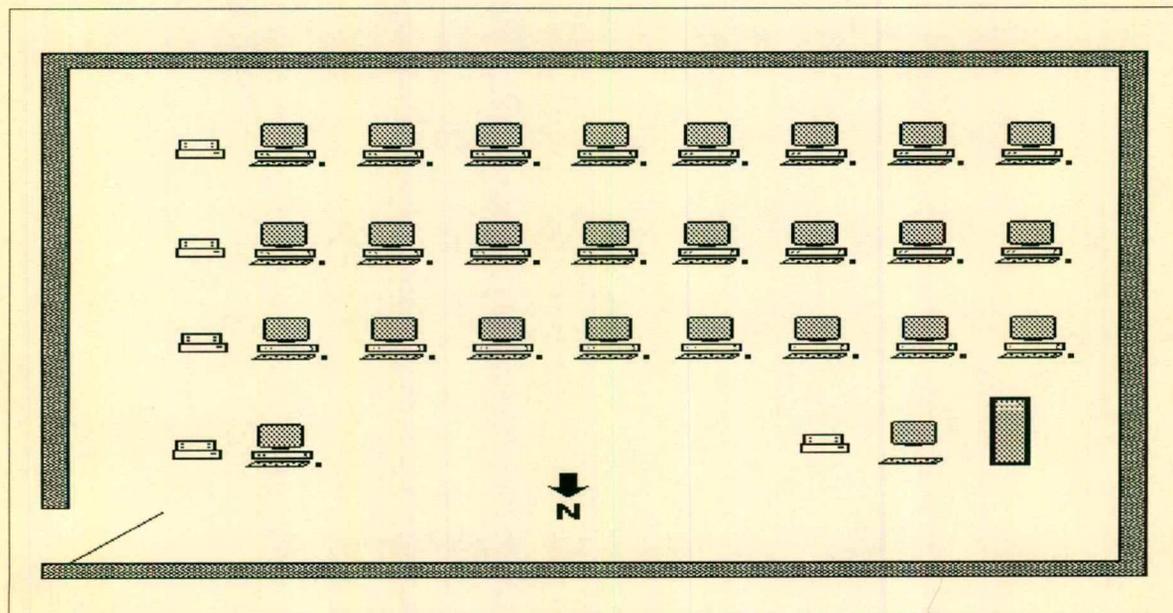


Fig. 4.1. Distribución física.

Donde es posible identificar:



25 Estaciones de Trabajo (Work Station), con la siguiente configuración cada una de ellas:

- Computadora Personal (PC).
- Procesador: 80386 SX
- Velocidad: 33 Mhz.
- Marca: Acer
- Monitor: SVGA COLOR Y B&N
- Teclado: Español
- Mouse: Instalado.
- RAM: 4 Mb.
- Drive's 3 ½"



Servidor de Archivos e Impresiones, configurada con:

- Computadora Personal (PC).
- Procesador: 80486 SX
- Velocidad: 25 Mhz.
- Marca: Acer
- Monitor: SVGA B&N
- Teclado: Español
- RAM: 8 Mb.
- Disco Duro: 310 Mb.
- Drive's 3 ½"
- CD ROM Instalado



5 Impresoras Start NX-1001.

☐ 4 Concentradores:

SMC

Elite 3608TP

10 BASE-T

* 26 Tarjetas:

SMC

EtherCard PLUS

* 18 Reguladores de voltaje.

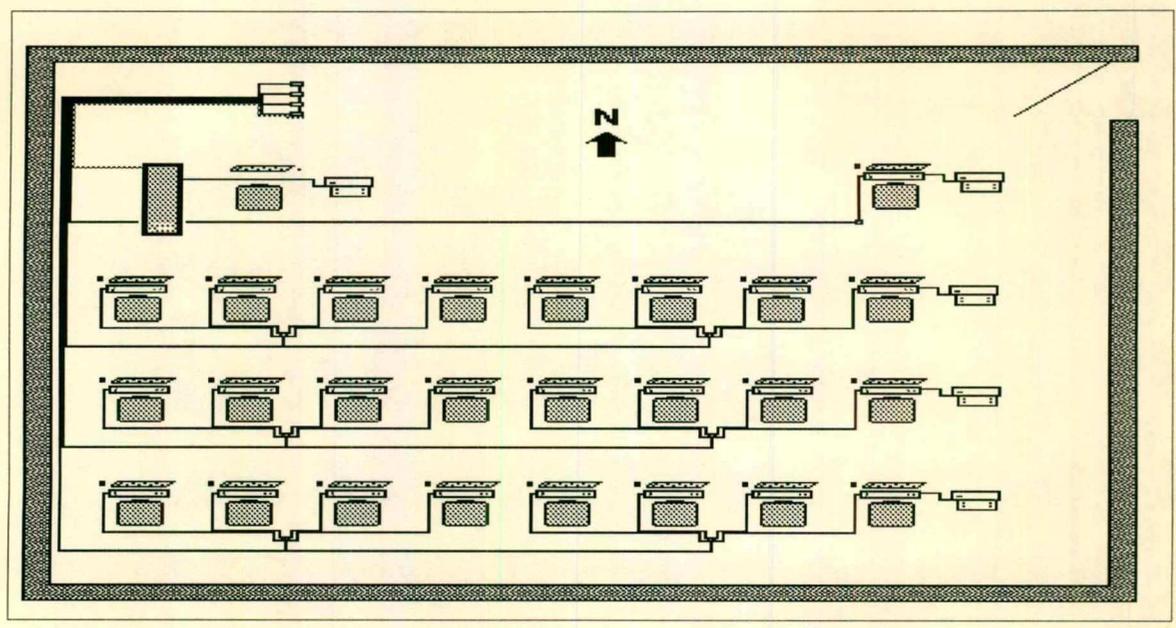
* 1 No-Break para el servidor.

* 4 Eliminadores de corriente para cada uno de los concentradores.

☐ 7 Distribuidores de señal.

5. DIAGRAMA DE CABLEADO

Fig. 5.1. Cableado.



Describir el cableado de la Red Institucional de la Facultad de Derecho, nos permite entender la forma en que los nodos establecen comunicación para poder acceder a la información y al equipo periférico.

En el siguiente diagrama, es posible observar la forma en que dichos nodos se enlazan, empleando cable Twisted Pair.

5. DIAGRAMA DE CABLEADO

6. CAPACIDAD DE EXPANSION

Por expansión física, entendemos la posibilidad de hacer crecer la red en el aula donde ella se encuentra. *Físicamente*, la red ya no podría expandirse en el mismo local, para lograrlo se requeriría ampliar el área o trasladarla a otra más amplia, recordemos que el espacio donde se encuentra es una aula, y no una sala construida especialmente.

6.1. EXPANSION FISICA.

- Físicas.
- Lógicas.
- Conectividad.

características en:

La capacidad de expansión de la red, podemos clasificarla de acuerdo a sus

misma.

Derecho, hace necesaria una evaluación de las capacidades de expansión de la El avance que en materia de cómputo pudiera tener en un futuro la Facultad de

6. CAPACIDAD DE EXPANSION

6.2. EXPANSION LOGICA.

Expansión lógica, comprende la viabilidad de incrementar los nodos que soporta la red. Lógicamente, el Sistema Operativo de red, soporta hasta 50 usuarios por lo que es posible expandirla hasta dicho número de estaciones de trabajo, quedando la posibilidad de agregar 25 estaciones de trabajo.

En cuanto a periféricos y software, la expansión sólo está limitada por el aspecto económico ambas, y el espacio en disco la última. Por ello, se requerirá en su momento, presentar un estudio que permita justificar ante la Dirección de la Facultad, la necesidad de incrementar la calidad y número de los periféricos, así como el software instalado en la red; en cuyo caso seguramente se tendrá que verificar el espacio libre en disco duro (el actual cuenta con 310 Mb) y en su caso adquirir uno con mayor capacidad.

6.3. CONECTIVIDAD.

En cuanto a conectividad, la Universidad Autónoma de Querétaro, pretende congregar en un solo servidor, bases de datos que permitan enriquecer el conocimiento, así como lograr una comunicación con el exterior de la misma, ya sean consultas a bases de datos públicas o comunicación con otros usuarios. En lo que a ello toca, se espera en un futuro poder enlazar la red de la Facultad de Derecho con la red Universitaria coordinada por la Dirección de Informatización para lo cual ya existe un plan detallado.

7. CICLO DE VIDA ESPERADO

Así mismo, se recomienda considerar la memoria RAM de las estaciones de trabajo (4 Mb), antes de la instalación de Software, ya que en la actualidad el mínimo requerido por la mayoría de los programas son 4 Mb, no dudando que en un futuro este mínimo se incrementa a 8 Mb como ya esta sucediendo con algunos programas.

Del mismo modo, la adquisición de nuevos periféricos se verá originado por las necesidades de los usuarios y de la disposición de la Dirección de la Facultad para adquirirlos.

En cuanto hace al equipo es de reciente adquisición, de procesadores 386 para las estaciones de trabajo y 486 para el servidor de archivos, su ciclo de vida está determinado en gran medida por el Software que en él se instale, calculándose una vida activa de tres años, después de lo cual se requerirá una revisión y posible actualización de los equipos. Es importante señalar, que dicha revisión deberá tomar en cuenta el comportamiento del servidor con algunos programas, recordemos que tiene un procesador 486 SX, a sólo 25 Mhz. de velocidad, siendo probable entonces, que dicha revisión se tenga que dar antes del tiempo considerado.

7.1. HARDWARE.

7. CICLO DE VIDA ESPERADO

7.2. SOFTWARE.

El Software instalado en la red requerirá para mantenerlo actual, una revisión y actualización de versiones anualmente. La instalación de nuevos paquetes y programas está determinado por los requerimientos de los usuarios y los lineamientos de la Dirección. En la adquisición de los mismos, es indispensable considerar que estén orientados a red, pues como viene sucediendo con el Software instalado, al no estar orientado a red se tienen problemas diversos durante su ejecución por más de un usuario, lo que origina pérdidas de información e incomformidad por parte de los usuarios.

**8. AMBIENTE DE SOPORTE DE
APLICACIONES**

8. AMBIENTE DE SOPORTE DE APLICACIONES

Los programas y paquetes instalados en la red, así como sus características, se describen a continuación:

Paquete	Versión	licencia	Descripción
Microsoft Word for Windows ®	6.0	03631-072-0302907	Procesador de textos.
Microsoft Works for Windows	2.0	34-070-0200-511015	Procesador de textos, hoja de cálculo, base de datos.
Microsoft Excel	4.0	00-065-04000-02208210	Hoja de cálculo.
Microsoft Power Point	3.0	0-079-0300-72225347	Preparación de presentaciones.
Microsoft Windows	3.1		Ambiente Operativo.
Novell Netware ®	3.11	06349707	Sistema Operativo de red (50 usuarios).

Ninguno de los paquetes está orientado a red, por lo que técnicamente sólo debieran emplearse en una sola estación, lo que al no hacerse, origina problemas corregibles al instalar programas orientados a red.

9. AMBIENTE DE ADMINISTRACION

9. AMBIENTE DE ADMINISTRACION

Las características y políticas de administración de la red las podemos clasificar como:

- Sistema Operativo.
- Herramientas.
- Conectividad.
- Grupos, usuarios y privilegios.
- Supervisor.
- Seguridad.

9.1. Sistema Operativo.

El Sistema Operativo Novell Netware 3.11 soporta 50 usuarios como máximo de los cuales 25 se encuentran ya enlazados, quedando igual número de estaciones disponibles.

9.2. Herramientas.

Las herramientas disponibles para la administración de la red son las que provee el Sistema Operativo Novell Netware 3.11 mediante el empleo de comandos, además de aquellas que mediante menús es posible ejecutar y que son descritos a continuación:

Herramienta	Descripción
Fconsole	Permite realizar actividades propias de la consola, pero en una estación de trabajo.
Filer	Administración de archivos y directorios.
Install	Modificación de configuraciones, volúmenes, etc.
Monitor	Manejo de usuarios, conexiones, apertura de archivos, monitoreo de actividades, etc.
Pconsole	Manipulación de tareas que ya se encuentren en la cola de impresión.
Printcon	Configuración de las tareas de las colas de impresión.
Printdef	Definición de dispositivos de impresión y secuencias de escape.
Session	Permite manipular el mapeo de los discos, observar usuarios y envío de mensajes.
Syscon	Manejo de la seguridad , derechos, usuarios, grupos, etc.
Volinfo	Monitoreo de espacio libre de los volúmenes activos del servidor.
Vrepair	Permite la corrección de volúmenes de la red.

9.3. Conectividad.

La topología de la red permite en caso de la caída de una estación de trabajo por una desconexión accidental o deliberada, no se caiga toda, así si una estación se desconecta no se eliminará la señal en toda la red con lo cual se asegura que las estaciones podrán laborar a pesar de un imprevisto como este.

Las impresoras están ruteadas de acuerdo a la fila de las estaciones de trabajo, así la impresora de la fila 1 (Q_star_F1), atenderá las impresiones de dicha fila, a menos que se cambie la configuración (Fig. 9.1.), pudiendo además, emplear la impresora definida para el maestro (Q_star_maestro) y la definida para el servidor (Q_star_s), todas controladas por el Servidor de Impresión (PS_Derecho) de la red.

La Red Institucional de la Facultad de Derecho se encuentra dentro de los planes de expansión de la Red Institucional de la UAQ, al ocurrir esto, se podrá acceder a los bancos de información en ella disponible así como conectarse con otras Instituciones. De acuerdo con dicho plan, la integración sería mediante fibra óptica que ya se encuentra tendida en algunos tramos del Centro Universitario.

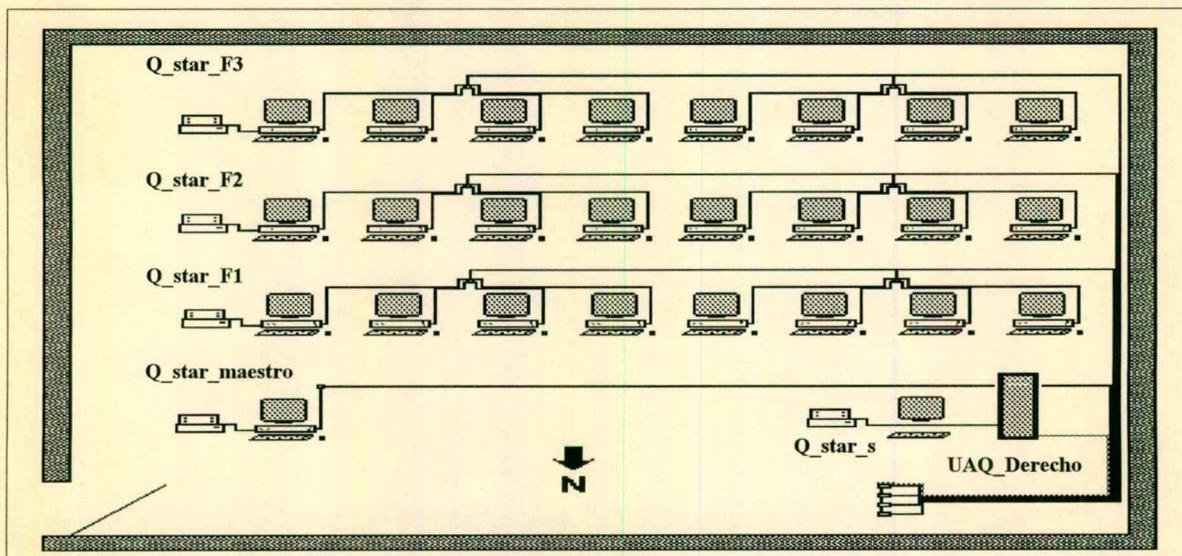


Fig. 9.1. Definición del servidor y colas de impresión.

9.4. Grupos, usuarios y privilegios.

9.4.1. Grupos.

Los grupos facilitan la asignación de derechos en los directorios y archivos, haciendo más sencillo el añadir usuarios a la red. Al crear usuarios, pueden ser asignados a determinados grupos de trabajo, heredando todos sus derechos.

Los grupos definidos en la red son:

- Administración.

Grupo definido para los usuarios de la Red Institucional de la Facultad de Derecho: alumnos, maestros, etc.

- Bellas_artes.

Grupo huésped definido para los alumnos de la Escuela de Bellas Artes, que asisten a solicitud de la Dirección de la misma.

- Everyone.

Grupo por default del Novell Netware.

Aun cuando el manejo de grupos de trabajo no está siendo aplicado al máximo, se recomienda hacerlo ya que de ese modo la creación de usuarios sería más sencilla,

rápida y fácil de controlar sus derechos, al controlar solamente los derechos del grupo y no de manera individual como se viene realizando.

9.4.2. Usuarios.

Para poder acceder a la red es indispensable contar con: un nombre de usuario registrado por el administrador, así como de un disquete de arranque de la misma, que en su caso es proporcionado por el administrador de la red.

Los usuarios registrado en la red, así como los derechos que cada uno de ellos tiene sobre los directorios del servidor son:

Grupo	Usuario	Directorio(s)	Derechos
	Sistemas	Mail/17000001	RWCEMF
		Usr/Sistemas	RWCEMFA
	Supervisor	Mail/1	RWCEMF
		System/16000001	SRWCEMFA
	Ramos	Aplic	SRWCEMFA
		Mail/18000002	RWCEMF
		Usr/Alumno	SRWCEMFA
		Usr/Ramos	RWCEMFA
Administración	Alumno	Aplic/Windows	R C F
		Aplic/Winword	R C F
		Mail/0000001	RWCEMF
		Usr/Alumno	R F
	Asesor	Mail/1400001	RWCEMF

Grupo	Usuario	Directorio(s)	Derechos
		Usr/Asesor	RWCEMF
	Cdrom	Aplic/Windows	R F
		Mail/19000001	RWCEMF
		Usr/Cdrom	R F
Bellas_artes	Belia	Usr/Bella	R F

Los derechos arriba indicados, corresponden de acuerdo a la inicial, en:

Derecho	Significado	Descripción
S	Supervisor	Supone todos los derechos sobre el directorio, sus archivos y sus subdirectorios.
R	Read	Permite abrir o leer un archivo.
w	Write	Proporciona la posibilidad de abrir o escribir sobre un archivo. Los derechos Create, Erase y Modify trabajan conjuntamente con este derecho.
c	Create	Crear directorios, modificar, abrir nuevos archivos y cerrarlos.
E	Erase	Facilita el borrar directorios, subdirectorios y archivos.
M	Modify	Ofrece el modificar archivos, directorios y subdirectorios.
F	File Scan	Derecho mediante el cual es posible buscar archivos.
A	Access Control	Permite modificar las listas de acceso.

Los directorios que se encuentran en el servidor de archivos a los cuales tienen o pueden tener acceso los usuarios de la red son:

Directorio	Descripción
Mail	Directorio de correo donde se almacenan los subdirectorios de cada uno de los usuarios.
Usr	Usuarios, conteniendo los subdirectorios de cada uno de los usuarios de la red.
System	Sistema Operativo Novell Netware 3.11.
Aplic	Aplicaciones tales como Windows, Winword, etc.

9.5. Supervisor.

El supervisor es el que tiene la responsabilidad sobre la administración de los recursos de la red, creación o eliminación de usuarios, derechos, colisiones, cambios de colas de impresión, control de acceso a la sala, etc.

Los usuarios Sistemas y Ramos tienen derechos similares al supervisor, empleados para dar mantenimiento o verificar problemas (Sistemas), y poder registrar o modificar características de los usuarios (Ramos).

9.6. Seguridad.

La estructura de la seguridad de la red esta definida por:

- 1) Seguridad de las instalaciones.

- 2) Acceso a la sala.
- 3) Acceso a la red.
- 4) Derechos.
- 5) Restricciones.

- 1) Seguridad de las instalaciones.

Recién instalada, la sala del centro de cómputo carecía de una protección adecuada, factor que fue corregido al poner en puertas y ventanas herrería como protección, sin embargo es necesario incrementar dicha seguridad en las ventanas pues a pesar de la protección, es posible lanzar un proyectil en cuyo caso dicha protección puede ser burlada; la puerta al ser de aglomerado, puede también ser objeto de agresión con relativa facilidad. A pesar de esto, hacen falta señalamientos como el de evitar comer, fumar o beber dentro de las instalaciones. Así mismo, hacen falta extinguidores y detectores de humo para evitar posibles incendios.

- 2) Acceso a la sala.

El acceso a la sala es perfectamente respetado y supervisado por el administrador de la red, al permitir el acceso, únicamente a los alumnos que tiene derecho a él en un horario definido previamente.

- 3) Acceso a la red.

Para lograr tener acceso a la red se requiere una vez librado el acceso a la sala, de un disquete así como del nombre del usuario que permita ingresar a la red.

Es aquí donde existe un problema potencial, en el caso de que el disquete de arranque puede ser copiado sin ningún problema por el usuario, en cuyo caso el acceso podría darse sin tener que solicitar tal disquete al administrador.

Lo anterior no tendría mayor importancia si todos los usuarios fueran controlados y registrados en la red, cosa que actualmente no se está realizando al emplear un solo usuario para todos los alumnos de Derecho y otro para los usuarios de Bellas Artes, Con ello, se tienen problemas de información y configuración de programas y paquetes al entrar todos los usuarios con un sólo nombre.

4) Derechos.

Los derechos que los usuarios tienen, están dados de acuerdo a su actividad, sin embargo, convendría (como se señaló en el punto anterior) crear un usuario por alumno para evitar problemas con la información que cada uno de ellos genera y la configuración personal de los paquetes que ellos emplean.

Se requiere también, reconsiderar el hecho que tres usuarios cuenten con derechos similares al supervisor, ya que en un momento determinado cualquiera de ellos puede cambiar la configuración de la red, cuya responsabilidad total es del administrador de la misma.

5) Restricciones.

En cuanto hace a las restricciones, estas no se están dando completamente ya que al existir un solo usuario para todos los alumnos de Derecho y otro para todos los alumnos de Bellas Artes, no se le está dando importancia para el control de acceso: el Password, cambio periódico del mismo, número de conexiones, espacio disponible en

disco, restricciones de horario, acceso y derechos a determinados directorios, etc., todo ello con la finalidad de tener buen control sobre los usuarios de la red y proporcionar un óptimo servicio a los mismos.

10. PROBLEMAS POTENCIALES

10. PROBLEMAS POTENCIALES

Los problemas potenciales que la red podría presentar durante su desempeño pueden ser:

- Caídas
- Respaldos
- Seguridad de la Información.
- Control de Usuarios y grupos.

10.1. Caídas.

Dada la topología y el empleo de concentradores y distribuidores, una caída por desconexiones es remota, aún así, se requiere que el cableado esté más oculto e identificados cada uno de los cables, el concentrador al que pertenecen y la línea o distribuidor que conectan.

El empleo del No-Break, permite cerrar todas las aplicaciones que estuvieran abiertas al momento de ocurrir una ausencia de electricidad, con lo cual la pérdida de energía redundaría en la pérdida de tiempo e información que no se hubiera almacenado por los alumnos, aún cuando los paquetes no tendrían mayor problema.

Así, en caso de una caída prolongada o ausencia indefinida de corriente eléctrica es indispensable definir planes de contingencia que permitan continuar prestando el servicio de cómputo a la comunidad estudiantil de la Facultad de Derecho. Con ello, no habría que detener o modificar los planes de estudio definidos.

10.2. Respaldos.

En la actualidad, no se realizan respaldos de información en la red, esto a la larga podría provocar efectos negativos como la pérdida de la configuración, usuarios, derechos, etc.

Si bien la información manejada en la red no es de la magnitud que sería en una red administrativa, esto no evita que deban realizarse respaldos (mínimo de la configuración), ya que en casos extremos podrían reinstalarse los paquetes o programas afectados.

También, se requiere establecer políticas y normas que señalen a los usuarios su responsabilidad en cuanto a su información, capacitarles a este respecto sin dejar de tener el administrador, la responsabilidad de la red.

10.3. Seguridad de la información.

Una de las principales características que se deben de buscar en la información es su seguridad, entendiendo por esta el hecho de mantenerla íntegra, pudiendo verse afectada al modificarla o eliminarla.

Al momento de realizar este material, no existe una adecuada seguridad de la información al contarse con un solo usuario para todos y cada uno de los alumnos que ingresan a la red. De esa forma, no es posible contar con una seguridad plena de información para los cual se requiere otorgar una clave de usuario para cada uno de ellos, definiendo su espacio en disco y comprobando que los derechos que cada uno de los usuarios tenga, se refieran única y exclusivamente a su información y no a la de otros usuarios de la red.

Del mismo modo, se requiere tomar medidas respecto a evitar la proliferación y contagio de virus que pueden dañar la información. Actualmente los discos de arranque cuentan con un antivirus residentes en memoria, sin embargo éste ha perdido vigencia al no ser la última de las versiones del antivirus y por lo tanto puede no incluir algunos de los virus actualmente existentes, al respecto es indispensable adquirir e instalar un antivirus que demuestre su eficacia y actualización constante como los son los antivirus de la empresa McAfee.

10.4. Control de usuarios y grupos.

En cuanto a usuarios, la red cuenta con dos que son de uso común por los estudiantes de la Facultad de Derecho y de la Escuela de Bellas Artes respectivamente:

- Alumno
- Bella

Al ser de uso común, se tienen problemas en cuanto a configuraciones y derechos sobre la información, por eso, es indispensable delinear a cada uno de los

usuarios (creando uno para cada uno de los alumnos) y los grupos a los cuales pertenecen para evitar problemas de este tipo.

Al tener un control más estricto respecto a los usuarios, es posible evitar la posibilidad de sabotajes por parte de un alumno, al negarle derechos sobre la información que no le concierne. Del mismo modo, es indispensable controlar el acceso de disquetes por parte de los usuarios que pudieran contener virus que un momento determinado causaran daño en la información y proliferación entre los usuarios de la red, si bien es prácticamente imposible verificar uno a uno todos los disquetes de cada uno de los usuarios que ingresen a la red, si es posible cargar en memoria programas antivirus que eviten emplear disquetes que pudieran estar contaminados.

11. FLUJO DE DATOS

12. PROCEDIMIENTOS DE PRUEBA Y VERIFICACION

12. PROCEDIMIENTOS DE PRUEBA Y VERIFICACION

Al trabajar en la red, el administrador de la misma debe tomar en cuenta diversos aspectos que en un momento dado le permitan evitar problemas substanciales en ella, y así, brindar un óptimo servicio a los usuarios.

La red no tiene en realidad una carga enorme en cuanto a horario, con lo cual se podría dar de baja en caso de necesitarlo para una óptima administración de la misma.

En la actualidad no se realizan acciones en cuanto a procedimientos de prueba y verificación, a excepción de las acciones correctivas necesarias cuando no se puede ingresar a la red o cuando termina la sesión sin explicación alguna; sin embargo es indispensable considerar dichas acciones preventivas.

Algunos aspectos que deben ser tomados en consideración con la finalidad de evitar posibles problemas en la red, son:

- Desbordamiento de paquetes.
- Paquetes enviados VS colisiones.
- Porcentaje de ocupación de los buffers.
- Porcentaje de tiempo de ocupación del procesador.

Desbordamiento de paquetes:

El módulo LAN INFORMATION ofrece una opción muy útil, RECEIVE PACKET OVERFLOW COUNT, mediante el cual es posible obtener el número de paquetes de información que no están funcionando correctamente en la red y actuar en consecuencia.

Paquetes enviados VS colisiones:

Existen momentos en el desempeño de la red en que se vuelve lenta, disminuyendo el tiempo de respuesta. Cuando esto ocurre, se recomienda verificar los paquetes que han sido enviados y la proporción que existen entre las colisiones y los errores detectados y corregir los problemas en cuestión. Para lograr tal información, elegir la opción LAN INFORMATION del módulo MONITOR).

Porcentaje de ocupación de los buffers:

Las áreas de memoria intermedia existente en la red, deben estar libres en su mayoría para poder proporcionar un servicio óptimo. Para evitar que se saturen, se debe observar el porcentaje de saturamiento el cual debe ser menor o igual al 20% para evitar problemas. De existir tales problemas, será necesario verificar el número de buffers disponibles, así como su tamaño, para lograr lo anterior, es necesario ejecutar el módulo MONITOR.

Porcentaje de tiempo de ocupación del procesador:

La ocupación del procesador puede en un momento dado, ocuparse en su mayoría con lo cual los procesos puede volverse lentos. Por eso, se recomienda observar el porcentaje de ocupación del procesador debiendo tomar las medidas pertinentes en su momento, como sería el modificar la configuración del servidor, aumentar el tamaño y número de bloques o buffers, o bien, evitar la ejecución de procesos que requieran una gran atención por parte del procesador.

13. IDENTIFICACION DE LOS REQUERIMIENTOS DE LA INSTALACION FISICA

13. IDENTIFICACION DE LOS REQUERIMIENTOS DE LA INSTALACION FISICA

La sala donde se ubica la Red Institucional de la Facultad de Derecho, si bien no fue construida exprofeso ha sido adaptada para poder albergarla.

Dicha adaptación fue eléctrica y física, agregándole tierra física y protecciones en las ventanas y puerta.

A pesar de lo anterior, existen características que no han sido consideradas completamente en cuanto a la instalación física de la red.

La instalación no cuenta con detectores de humo ni extinguidores que permitan evitar un daño mayor en el momento en que origine un incendio, así mismo el área donde se encuentra el servidor es una área desprotegida completamente, pudiendo cualquier persona acceder a dicho lugar y apagarlo en su caso. Se requiere además, proteger los vidrios de las ventanas y la puerta, ya que pese a contar con protecciones, estas no protegerían contra proyectiles. Por otro lado las hojas de las impresoras se encuentran en el pasillo donde invariablemente son pisadas además cualquier usuario puede apagarla.

Por otra parte se requiere si en un futuro se va a conectar a la Red Institucional de la UAQ, las adecuaciones físicas de la instalación y del servidor necesarias para lograr dicha conexión.

**14. NECESIDADES DE ENTRENAMIENTO Y
CAPACITACION**

14. NECESIDADES DE ENTRENAMIENTO Y CAPACITACION

En la actualidad, la red es atendida por una persona encargada de su administración y orientación para los usuarios que lleguen a trabajar a la misma.

Dicha persona es responsable de la administración, instalación de programas y paquetes.

Para lograr que dicha persona cumpla cabalmente con sus atribuciones, se requiere una capacitación constante y permanente para evitar y corregir problemas. Dicha capacitación debe incluir acciones preventivas y correctivas en cuanto a caídas de la red y mejoras del desempeño.

Su capacitación debe incluir entre otros, los siguientes temas:

- Actualidades de Hardware,
- Actualidades de Software,
- Prevención y rehabilitación de caídas de red,
- Uso de herramientas preventivas y correctivas,
- Configuración física y lógica de la red, entre otros.
- Virus, prevención y corrección.

Para lograr una capacitación plena, se recomienda que el administrador asista a los siguientes cursos:

- Administración Netware 3.1X.¹
- Administración Avanzada Netware 3.1X. ¹
- Instalación y configuración Netware 3.1X. ¹
- Tecnología de redes. ¹
- Soporte técnico en redes. ²
- Administración de redes. ²
- Virús. ²
- Introducción a la Internet. ²
- Servicios de Internet. ²
- TCP/IP. ²

¹ Impartidos en un CNE de Novell.

² Coordinados por la Dirección de Informatización.

15. NECESIDADES DE PERSONAL

15. NECESIDADES DE PERSONAL

A pesar de que ya existe una persona responsable de la Red Institucional de la Facultad de Derecho (por las mañanas), se recomienda su constante capacitación y en caso de pretender aprovechar al máximo el Centro de Cómputo, contratar otra persona que se responsabilice del Centro por las tardes y en ausencia del titular.

El responsable del Centro de Cómputo, depende directamente del Director de la Facultad, así, el establecimiento de un plan de capacitación, contratación de personal, expansión de la red, etc., necesariamente deberá ser aprobado por él.

16. RIESGOS

16. RIESGOS

Los riesgos con que se enfrenta la Facultad de Derecho de no tener una red eficiente son:

- Errónea visión de la computación por parte de los alumnos de la Facultad.
- Inconformidad de los alumnos por el mal o deficiente funcionamiento de la red.
- Desconfianza de los maestros del área en cuanto explicar temas que no son posibles de ejercitar en la computadora por deficiencias en la red.
- Gasto improductivo, al no lograr un uso adecuado y eficiente de la red.
- Fallas frecuentes por no contar con Software adecuado y manuales de referencia.

17. PLANES DE CONTINGENCIA

17. PLANES DE CONTINGENCIA

En la actualidad no existe ningún plan de contingencia que permita en un momento dado, recurrir a él en caso de algún imprevisto, y así aminorar su impacto con los usuarios.

Por lo anterior se recomienda elaborar planes de contingencia que observen entre otras cosas:

- Qué hacer en caso de descompostura de una o más computadoras cuya presencia sea indispensable para la atención de los usuarios o capacitación.
- Acciones a tomar en el momento que la red se caiga y por alguna circunstancia no sea posible su rehabilitación total.
- Reinstalación de programas que se hayan visto dañados.
- Suplencia del maestro, administrador o ponente en caso de ausencia o enfermedad.

- Recepción en calidad de préstamo de impresoras en caso de descompostura y/o falla de alguna de ellas (en caso de no poder solventar las necesidades con sus propias impresoras).

A manera de sugerencia, a continuación se detalla un plan general de contingencia, en él, se describen situaciones y acciones contingentes que permitan superarlas.

a) Descompostura de equipo:

- Localizar y aislar completamente el problema.
- Informar a los usuarios y docentes respecto al desperfecto, evitando el empleo del equipo descompuesto.
- En caso de tratarse de una estación de trabajo, monitor, impresora o regulador, y siempre que el administrador no pueda solucionar el desperfecto, solicitar servicio a la Dirección de Sistemas de la UAQ y de requerirse, gestionar el préstamo del equipo que permita continuar prestando servicio en el centro de cómputo.
- Si la descompostura atañe al servidor, y en caso de ser corregible por el administrador, se debe proceder a su reparación. En el caso de que el desperfecto no sea corregible por el administrador, solicitar a la Dirección de Sistemas proceda a su reparación. En esta circunstancia, se requiere haber establecido con otra institución (se sugiere la Escuela de Enfermería), un convenio donde se establezcan las obligaciones y derechos que tienen cada uno de los firmantes. En dicho documento, se deben detallar los motivos, horarios y condiciones para poder

acceder al empleo de su Centro de Cómputo, informando de esto a los alumnos y docentes, para dirigirse a trabajar al Centro de Cómputo de la Institución convenida.

b) Caída de la red:

- Localizar y aislar el problema.
- Informar del problema a los usuarios y docentes.
- Proceder a su reparación, ya sea originado por Hardware o Software. Si el problema rebasa la capacidad del administrador, se deberá solicitar apoyo a la Dirección de Sistemas de la UAQ, cabiendo la posibilidad de considerar el solicitar se facilite el Centro de Cómputo de la Escuela con la cual se ha establecido el convenio de apoyo.

c) Programas dañados o daños en la información:

- Localizar y aislar el daño del programa o información.
- Comunicar a los usuarios y docentes para evitar el uso o aplicación del programa o información en cuestión.
- Determinar la causa del daño y en su caso proceder aplicando antivirus, o corrigiendo los derechos que los

usuarios pudieran tener y que les permitan modificar características de los programas o información, o bien, verificar la superficie del disco duro que pudiera ser también el origen de los problemas.

- Recuperar el programa o información de los respaldos realizados o proceder a la reinstalación completa de los programas de sus discos originales.

d) Conatos de incendio:

- Localizar el origen de la conflagración.
- Informar a los usuarios y docentes del peligro, evitando causar pánico o alarma innecesaria.
- Dar de baja el servidor y apagar los interruptores de corriente eléctrica, de ser posible.
- Aplicar el extinguidor al origen del incendio, dicho extinguidor deberá ser especialmente adquirido para un medio donde se localicen computadoras y dispositivos de almacenamiento magnético. Pudiera ser necesario solicitar la presencia del cuerpo de bomberos, aún cuando sólo sea para evaluar los orígenes y condiciones de la conflagración.
- Evaluar los daños y orígenes del incendio, corregir tales orígenes y solicitar a la Dirección de Sistemas de la UAQ, una revisión al equipo dañado.

18. CONCLUSIONES

18. CONCLUSIONES

El deseo que antaño se tenía respecto a dejar de tener aisladas las computadoras y compartir recursos y programas, es hoy una realidad con las redes de computadoras.

El tener una red, no se limita en interconectar las computadoras de una área u organización, para que una red sea realmente eficiente se requiere de una correcta administración para lograr compartir todos y cada uno de los recursos de la misma.

La Red Institucional de la Facultad de Derecho es incipiente al contar con alrededor de dos años de instalada, sin embargo se sugiere para un mejor funcionamiento:

- Revisar y establecer claramente, políticas para el registro de usuarios y grupos, ya que hasta el momento sólo se cuenta con un usuario (en cada uno de los dos grupos) para acceder a la red, con los consiguientes problemas de cambios de configuración, pérdidas de información, etc. Al registrarlos, se deben establecer posibles horarios de trabajo, directorios, fechas válidas de acceso, etc.
- Obtener e instalar lo más rápido posible, software original y orientado a red, ya que el software que actualmente se tiene instalado no otorga una confiabilidad al funcionar deficientemente debido a este factor.
- Establecer convenios y planes de contingencia detallados, que permitan emplear otro centro de cómputo en caso de falla grave en el

de la Facultad, recibir en calidad de préstamo computadoras o impresoras para suplir algunas con descomposturas, etc.

- Planificar y delinear lo más rápido posible, el acceso a la Red Institucional de la UAQ, donde es posible consultar bancos de información jurídicos, que permitirían un mejor aprovechamiento de la red por parte de los usuarios.
- Adquirir e instalar equipo de prevención y sofocación de incendios así como capacitar al responsable de la red en cuanto a su empleo y mantenimiento.
- Establecer junto con la Dirección de Sistemas de la UAQ, periodos de mantenimiento preventivo del equipo instalado en la red.
- Considerar la posibilidad de adicionar como usuarios a la red, al personal administrativo y docente de la misma, siempre que se observen adecuadamente las medidas de seguridad necesarias.
- Considerar y tomar las medidas necesarias para prevenir y contrarrestar en su caso, la presencia de virus en la red.

Todos los puntos aquí indicados, no dejan de ser sugerencias, la utilidad que de ellas se obtenga dependerá de la Dirección de la Facultad de Derecho y del administrador de la red.

19. INDICE

19. INDICE

	<u>Pág.</u>
CONTENIDO	1
1. JUSTIFICACION	3
2. INTRODUCCION	4
3. TOPOLOGIA	5
3.1. LOCALIZACION GEOGRAFICA DE LA RED.....	5
3.2. LOCALIZACION FISICA.....	6
3.3. TOPOLOGIA.....	6
4. DESCRIPCION DE LOS COMPONENTES	8
5. DIAGRAMA DE CABLEADO	11
6. CAPACIDAD DE EXPANSION	12
6.1. EXPANSION FISICA.....	12
6.2. EXPANSION LOGICA.....	13
6.3. CONECTIVIDAD.....	13
7. CICLO DE VIDA ESPERADO	14
7.1. HARDWARE.....	14
7.2. SOFTWARE.....	15
8. AMBIENTE DE SOPORTE DE APLICACIONES	16
9. AMBIENTE DE ADMINISTRACION	17
9.1. SISTEMA OPERATIVO.....	17
9.2. HERRAMIENTAS.....	18
9.3. CONECTIVIDAD.....	19
9.4. GRUPOS, USUARIOS Y PRIVILEGIOS.....	20
9.4.1. GRUPOS.....	20
9.4.2. USUARIOS.....	21
9.5. SUPERVISOR.....	23
9.6. SEGURIDAD.....	23
10. PROBLEMAS POTENCIALES	27
10.1. CAIDAS.....	27

	<u>Pág.</u>
10.2. RESPALDOS.....	28
10.3. SEGURIDAD DE INFORMACION.....	28
10.4. CONTROL DE USUARIOS Y GRUPOS.....	29
11. FLUJO DE DATOS.....	31
12. PROCEDIMIENTOS DE PRUEBA Y VERIFICACION.....	32
13. IDENTIFICACION DE LOS REQUERIMIENTOS DE LA INSTALACION FISICA.....	35
14. NECESIDADES DE ENTRENAMIENTO Y CAPACITACION.....	36
15. NECESIDADES DE PERSONAL.....	38
16. RIESGOS.....	39
17. PLANES DE CONTINGENCIA.....	40
18. CONCLUSIONES.....	44
19. INDICE.....	46
20. INDICE DE ILUSTRACIONES.....	48
21. BIBLIOGRAFIA.....	49

20. INDICE DE ILUSTRACIONES

20. INDICE DE ILUSTRACIONES

	<u>Pág.</u>
Fig. 3.1. Centro Universitario, UAQ.....	5
Fig. 3.2. Facultad de Derecho, UAQ.....	6
Fig. 3.3. Topología de estrella distribuida.....	7
Fig. 4.1. Distribución Física.....	8
Fig. 5.1. Cableado.....	11
Fig. 9.1. Definición del servidor y colas de impresión.....	19

21. BIBLIOGRAFIA

21. BIBLIOGRAFIA

- * Novell Netware
Manual de referencia
Tom Sheldon
Mc Graw Hill

- * Redes de Ordenadores
Andrew S. Tanenbaum
Prentice Hall