Plan de actualización informática de las oficinas de la Mutua

Sara Fortea Pinilla
ETIS

Miquel Colobran Huguet

17/06/2004

AGRADECIMIENTOS

Quisiera agradecer a la Mutua, empresa donde trabajo, que haya podido hacer públicos ciertos datos de su organización, para que en un futuro este proyecto pueda ver la luz. De igual forma, muchas de las ideas que han servido para vertebrar estas páginas salieron de numerosas conversaciones sobre las necesidades de la empresa con el Subdirector de Sistemas de Información, Julián Casado Panigua. Y, finalmente, la preparación del conjunto del trabajo contó con el apoyo y el visto bueno de mi tutor, Miquel Colobran, que incidió en los aspectos a desarrollar cuando le presenté la iniciativa.

RESUMEN

La necesidad de actualizar informáticamente la sede central de la Mutua, donde trabajo, ha sido la finalidad de este trabajo, en cuyo desarrollo se ha analizado la situación actual de las instalaciones de la Mutua, con la pertinente evaluación de los elementos de hardware y software vigentes, con los correspondientes servidores de ficheros, estaciones de trabajo, hubs, routers, cableado de los edificios, las aplicaciones utilizadas o los mecanismos de seguridad.

Tras el análisis de la cuestión, se ha realizado una propuesta de modificación de ciertos elementos del edificio, reparando en que la solución fuese viable para la Mutua, tanto a nivel económico como organizativo: prueba de ello es haber descartado soluciones que pudieran ser demasiado atrevidas con respecto a la política de la empresa, como pudiera ser la implantación general de la tecnología Wireless. El patrón sobre el que se ha realizado el proyecto lo ha marcado el déficit actual y la previsión futura.

Tras lanzar la propuesta, se ha realizado una planificación de la migración por fases: en primera instancia, una renovación del sistema operativo de los servidores y, en consecuencia, de las aplicaciones residentes sobre ellos. A continuación se ha planteado una alternativa para el recableado general de los edificios, tanto horizontal como verticalmente. Para una última fase, aunque no menos importante, ha quedado la formación y el reciclaje de los usuarios, que son los principales afectados por unos cambios de tan gran magnitud.

Por último, se han analizado los costes totales de dicha actualización, para lo que se ha tenido en cuenta los elementos de tipo hardware (desde el cableado a las estaciones de trabajo y/o los servidores), y los elementos de tipo software, como la actualización de las aplicaciones.

Página

1. DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

3. PLANNING DE MIGRACIÓN

4. ANALISIS DE COSTES

1. DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

Actualmente las oficinas de la Mutua están formadas por un edificio principal y varios secundarios, formando todos ellos una única estructura. En el edificio principal se encuentran el servidor de ficheros. En lo que a sistemas informáticos se refiere, presentan las siguientes características:

1.1. Servidor de ficheros

1.1.1. Descripción de las características del hardware:

Se dispone de un servidor principal de ficheros:

SERVIDOR NETFINITY 5500 XEON 450 MHz Con 512 Mb RAM, HDX6, 6 discos de 18.6 GB cada uno, un procesador X86 Family 6 Model 5 Stepping 3, AT/AT Compatible, unidades de almacenamiento en discos con controladora RAID 5 basada en hardware.

Gracias a la tecnología RAID (combinación de varios discos duros para formar una única unidad lógica en la que se almacenan los datos de forma redundante y aparentar ser un sólo disco duro lógico para el sistema operativo), tenemos protegidos los datos contra el fallo de una de las seis unidades de discos duros que existen en estos momentos; y si se produce un fallo, nos mantiene el servidor activo y en funcionamiento hasta que se sustituya la unidad defectuosa.

Se escogió RAID 5 ya que ofrece tolerancia a fallos, un alto rendimiento, optimiza la capacidad del sistema, y permite una utilización de hasta un 80% de la capacidad del conjunto de discos. También se dispone de una unidad de backup en cinta.

Además, existen varios servidores secundarios en edificios anexos que se utilizan únicamente como servidores de impresión:

SERVIDOR NETFINITY 3000 PIII 600MHz
Con 128MB 4.6 GB+STREAM y procesadores
X86 Family 6 Model 5, AT/AT Compatible

1.1.2. Descripción de las características del software:

En la organización hay establecido un dominio (un grupo de servidores que comparten bases de datos comunes de directivas de seguridad y cuentas de usuario) con varios equipos con Windows NT Server.

La configuración de la red de área local se caracteriza por tener un servidor principal de ficheros (servidor de dominio; el servidor de nombres de dominios responde ante cualquier petición de los usuarios; están creados todos los usuarios de Windows NT) en el que se almacena todo el software de control de la red así como el software que se comparte con los demás ordenadores de la red, y varios servidores secundarios.

Dentro del dominio, están los servidores secundarios (de equipos con Windows NT Server) que se encargan de autenticar las solicitudes de inicio de sesión: controladores de dominio.

Las principales características que debe proporcionar un servidor de ficheros son las siguientes:

- El almacenamiento de las ordenes, las utilidades y los módulos de programa del sistema operativo
- El almacenamiento de los programas y los datos de usuario.
- La gestión de las funciones del sistema de archivos.
- La gestión de las funciones que se encargan de la seguridad y el acceso de los usuarios.
- La gestión y el control de la red.
- La protección de los datos para garantizar su fiabilidad con funciones tales como la imagen (mirroring) de discos, el control de la fuente de alimentación ininterrumpida y la copia de seguridad de los archivos.

Todos los servidores disponen de un Sistema Operativo Windows NT Server, software para realizar copias de Seguridad (Backup Exec 8.5.), inventario de estaciones y/o captura remota de ellas (Microsoft Systems Management Server), Norton Antivirus, aplicaciones propias tales como Intranet corporativa, software sanitario, de contabilidad ...

Existen dos particiones comunes en todos los servidores, tanto en el servidor principal como en los secundarios: una primera partición (C:/) y una segunda (D:/). En la primera se encuentran instaladas las aplicaciones locales, y en la segunda toda la estructura de datos (directorios personales, directorios públicos, directorios de departamentos, etc ...)

1.2. Plataformas corporativas homogéneas

1.2.1. Descripción de las características del hardware:

Los ordenadores que no son servidores de ficheros reciben el nombre de estaciones de trabajo. Estas suelen ser menos potentes y tienen software personalizado por cada usuario y/o grupo de trabajo. Tal como ocurre con el servidor, el sistema operativo a correr en las estaciones decide el hardware mínimo para ellas.

Las estaciones de trabajo no han de ser tan potentes como el servidor, simplemente necesitan una tarjeta de red, el cableado pertinente y el software necesario para comunicarse con el servidor. Las modelos de estaciones de los que dispone actualmente la Mutua son los siguientes:

IBM Netfinity con 128/256 Mb de Ram, 20 Gb de HD, CD-ROM / DVD
Portátiles Thinkpad R31,
Portátiles Toshiba Satelite Pro 4600

Dentro de la estructura organizativa, las plataformas se clasifican en dos grandes grupos según la característica del puesto:

1. Equipos conectados al servidor principal de dominio; llevan incorporada la tarjeta de red (mayoritariamente Ethernet e integrada en la placa, aunque existen algunos todavía con Token Ring).
Existe un subgrupo que, por características del puesto, posee un doble arranque; por un

lado un arranque corporativo para conectarse al servidor y poder trabajar en las oficinas, y por otro lado un arranque autónomo.

2. Equipos autónomos sin conexión en red.

1.2.2. Descripción de las características del software:

Todas las estaciones de la Mutua presentan la misma configuración: son estaciones dotadas con Windows 2000 Professional o NT WorkStation, y Aplicaciones Internas necesarias para el desarrollo de las actividades de la empresa. En general, "Aplicaciones Internas" son aquellas soluciones que corren dentro de la red corporativa y que permiten al personal contar con información actualizada de productos, servicios, objetivos, cursos, etc.

Si son estaciones conectadas en red, arrancan con restricciones del sistema operativo, para que los usuarios no puedan modificar opciones tales como: acceder al Panel de Control, al disco duro ni a la disquetera, etc. Además, se mapean dos unidades de red: una personal y otra del departamento y/o perfil al que pertenezca dicho usuario, donde guardarán sus datos.
Si son estaciones autónomas, no tienen ninguna restricción, son abiertas totalmente pero con un cliente antivirus instalado.

1.3. Cableado del edificio principal y edificios colindantes

1.3.1. Cableado actual de los edificios:

Los edificios presentan una columna vertical que corre desde el sótano y/o planta baja hasta la última planta, conectándose a él cables horizontales en cada piso mediante amplificadores especiales (hubs).

Como he indicado anteriormente, disponemos de una Red de Area Local Corporativa, con topología en estrella (todas las estaciones están conectadas mediante enlaces bidireccionales a un nodo central que controla la red y que asume las funciones de gestión y control de las comunicaciones), de PC’s con Sistema Operativo Microsoft Windows NT Server y estaciones Windows 2000.
La topología en estrella nos proporciona una flexibilidad en cuanto a la configuración y

reconfiguración, así como la localización y control de fallos que se producen. Aunque, cuando falla el servidor, queda fuera de servicio toda la red de la organización.
Se tiene implantado un Sistema de Cableado Estructurado de Datos Categoría 5 (datos a 100 Mbps, Fast Ethernet; además permiten la migración de tecnología 10Mbp a 100Mb) en prácticamente todo el edificio corporativo principal y colindantes, un armario de datos conteniendo panel RJ45 Categoría 5 y un Switch Alcatel (Omni Switch/Router) con tres módulos: uno para fibra óptica, otro para Token Ring y otro para Ethernet.

Todo el cableado se recoge de forma ordenada en el rack que está instalado al lado del servidor; también están metidos en unas canaletas para evitar la rotura de los mismos.

Junto a este rack se dispone de un armario de Colt Telecom que contiene las conexiones de fibra óptica (existe un anillo de fibra con dos centros, con un ancho de banda de 1 Gb)

Los cables están etiquetados e identificados. La conexión entre el concentrador, así como entre las rosetas (que también se encuentran etiquetadas) y las estaciones corporativas, es a través de latiguillos RJ45.

1.3.2. Velocidad de transmisión existente:

Con los edificios colindantes existe un enlace punto a punto con el edificio principal con una velocidad de 100 y 1 Gb, dependiendo del caso.

De esta forma se extiende la red local hasta centros y/o edificios distantes de las oficinas centrales, por medio del uso de enlaces de fibra óptica de altas prestaciones. Así, los usuarios perciben que están trabajando en una única LAN, independientemente del sitio físico donde se encuentren.

Existe también un router ADSL para un grupo de equipos de trabajo autónomos, con una velocidad contratada de 2 Gb.

1.3.3. Descripción de las conexiones de la planta principal y del resto de plantas:

En cada una de las plantas del edificio/s existe un rack con uno o dos hubs Ethernet 3COM SuperStack3 de 12 o 24 puertos, según las necesidades y/o maus RJ45 para el servicio Token

Ring, que conectan todo el piso del edificio (con un medio de transmisión denominado vertical, principal o backbone) que también puede ser fibra óptica.
Del rack principal donde se encuentra el switch salen dos o cuatro líneas de servicio que van a cada una de las plantas donde existe un rack.

1.4. Impresoras y colas de impresión

1.4.1. Modelos de impresoras:

Las impresoras de las que dispone la Mutua son Hewlett Packard, a excepción de un grupo reducido, que son Canon.
Se clasifican en tres grandes grupos:

- Impresoras laser: modelos HP LaserJet 4, LaserJet 4000, LaserJet 4200
- Impresoras inyección tinta: modelos HP Deskjet 895Cxi, Deskjet 2000C, Deskjet 2200C
- Impresoras multifunción: modelos Canon IR 2200, IR 3300.

1.4.2. Configuración de las colas de red:

Las colas de impresión del edificio principal se encuentran configuradas en el servidor de dominio Primario. Y las colas de impresión que pertenecen a los otros edificios se encuentran configuradas en los respectivos servidores.

Actualmente existen unas 60 colas de impresión que se distribuyen por plantas, departamentos y edificios.

La filosofía que se sigue para conectar las impresoras en red en la Mutua consiste en conectar varias a través de una JetDirect externa Ethernet o Token Ring (HP JetDirect 500X, ya que nos permiten conectar impresoras y otros dispositivos directamente a una red, adaptando el puerto paralelo de la impresora al puerto de red, siendo posible conectar hasta tres impresoras) y asignándole una dirección IP fija.

El nombre que se asigna al recurso compartido del servidor es una breve descripción orientativa de la ubicación de dicha impresora.

1.5. Mecanismo de seguridad físico:SAI

Como medida de seguridad pasiva son básicos los mecanismos de tolerancia a fallos, que hacen posible que el sistema siga funcionando. Por ejemplo, un sistema de alimentación ininterrumpida para cuando falla el suministro eléctrico (SAI).

En estos momentos se dispone de un SAI conectado al servidor de archivos, que, en el caso de que se produzca una interrupción en el suministro de energía, mantiene el servidor en funcionamiento. Además, este sistema corrige todas las deficiencias de la corriente eléctrica.

1.6. Copias de seguridad y Disaster Recovery

Ante todo, debemos recordar una de las leyes de mayor validez en la informática, la "Ley de Murphy":

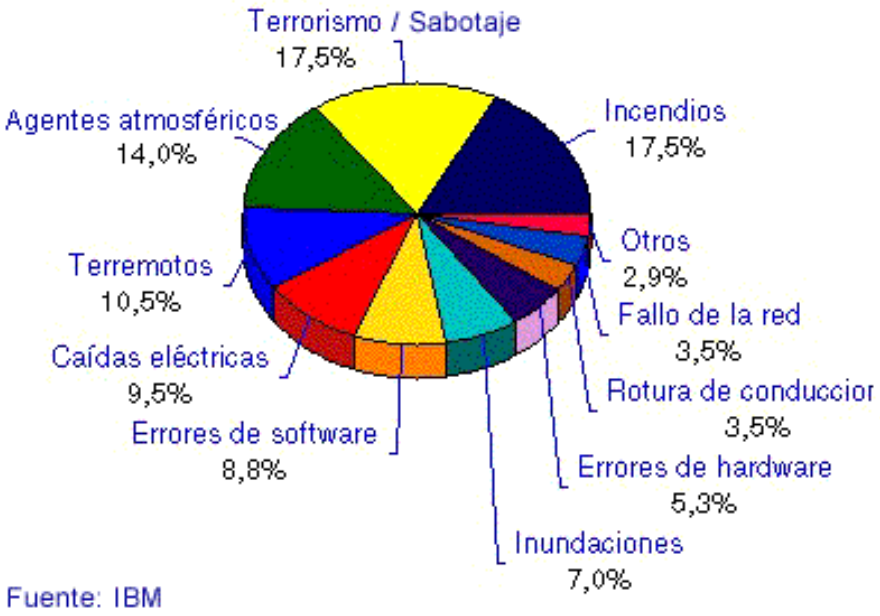
- Si un archivo puede borrarse, se borrará
- Si dos archivos pueden borrarse, se borrará el más importante
- Si tenemos una copia de seguridad, no estará lo suficientemente actualizada

Por tanto, es fundamental contar con una política correcta de copias de seguridad adecuada a las características de la entidad y sus recursos.

Existen normas básicas sobre la filosofía de los Backups:

1. Hacer copias de seguridad de todos los datos importantes
2. Hacer copias de seguridad de los discos de instalación de los programas
3. Actualizar las copias de seguridad lo más frecuentemente posible
4. Revisar el estado de las copias de seguridad de vez en cuando
5. Copiar los directorios de archivos de datos
6. No confíar en los disquetes como dispositivo de backup ya que su fiabilidad es ínfima
7. Si se utilizan cintas magnéticas, tener varios juegos de copias, intercambiarlos de forma rotatoria y renovándolos de vez en cuando
8. Guardar las copias en lugar seguro

Razones de las caídas de los sistemas informáticos



1.6.1. Política de copias de seguridad:

El volumen de información que se respalda en la organización es solamente datos. Actualmente, dado el volumen de los datos almacenados en el servidor de la Mutua, característica de los mismos y su permanente actualización y modificación, se combina la copia completa con la copia incremental. Se respaldan los directorios de trabajo de los usuarios y los perfiles de los escritorios que se cargan cuando arranca una estación.

La frecuencia de realización de las copias de seguridad es diaria, de lunes a viernes; Se utiliza una secuencia de Respaldo GFS (Grandfather-Father-Son): una copia incremental cada día, y una copia completa semanal, (con rotación de cintas) y cada mes se sobreescriben.

Las copias se inician de forma automática: están planificadas para que se realicen diariamente a partir de las 23:00 horas, asegurándonos así de que no hay usuarios que puedan estar accediendo o modificando datos susceptibles de ser respaldados.
Cada mañana se revisa que el backup haya sido satisfactorio, y cambia la cinta.

Se utilizan cintas HP DLT-IV con una capacidad de compresión 40/80 Gb, ya que al tener un tiempo de vida superior a 30 años, no es necesario preocuparse de su mantenimiento. Éstas se van rotando: cada día se utiliza una cinta diferente; así durante cuatro semanas, disponiendo así de copias de seguridad de un mes completo.

Gracias además al duplicado de Información en Línea (RAID5), es posible mantener copias en linea ("Redundancy") el sistema es capaz de recuperar información sin intervención de un Administrador.
Con el uso de "Hot-Swappable Drives" es posible sustituir y recuperar la Información de un disco Dañado y sin la necesidad de configurar o reiniciar el sistema.

1.6.2. Software y dispositivos utilitzados:

Para realizar los Sistemas de Backup se utiliza el software **Veritas Backup Exec 8.5** y la unidad de backup en cinta del servidor principal.

En el Veritas se tienen programadas dos tareas de respaldo: la incremental y la completa, tal y como se ha mencionado anteriormente.

1.6.3. Disaster Recovery

Gracias a toda la política de copias de seguridad explicada anteriormente (copias de seguridad y sistema RAID 5), se puede llegar a recuperar el estado inicial del sistema en caso de que se produzca una caída del mismo.

1.6.4. Archiving

Periódicamente, aquellos ficheros que no han sido accedidos y/o modificados durante una periodo largo de tiempo se archivan en CD-ROM/ DVD; se guardan en un armario de seguridad y se borran del servidor (previo aviso y consentimiento de los propietarios).

1.7. Aplicaciones

1.7.1. Descripción de las aplicaciones:

Las aplicaciones corporativas que se utilizan en la Mutua se pueden englogar en dos grandes grupos:

- Aplicaciones comunes a todos los usuarios: Microsoft Office 97, Cliente Norton Antivirus Corporate Edition 7.01, Compresores, Cliente Lotus Notes v5, Intranet corporativa (internet privado, aplicaciones de uso interno de la Mutua), Digitalizar (para escanear documentos a una resolución que acota directamente el programa y no el usuario), Adobe Acrobat Reader 5.0, Internet Explorer 5.0.

- Aplicaciones propias de cada perfil de usuarios: software propio adecuado al perfil de trabajo (perfil sanitario, perfil administrativo, perfil técnico ...)

Todas las aplicaciones se encuentran instaladas en el servidor de ficheros de la organización; en las estaciones se realiza una instalación local, no completa, que permite el acceso a la aplicación que reside en el servidor.

1.7.2. Restricciones de uso:

No hay restricciones de uso sobre las aplicaciones comunes a todos los usuarios: todo empleado de la Mutua que esté dado de alta en el domino puede acceder a ellas.

Únicamente el Lotus Notes no permite tener arrancadas dos sesiones distintas; un usuario puede estar validado en dos equipos diferentes, pero no puede tener arrancada la aplicación en ambos.

Sin embargo, las aplicaciones asociadas al perfil del usuario solamente pueden acceder aquellos usuarios que pertenecen a dicho perfil.

1.7.3. Requerimientos técnicos:

Las estaciones de las que dispone la organización presentan las suficientes características técnicas como para soportar el software comentado anteriormente: el disco duro no se utiliza para

almacenar datos sino únicamente para realizar la instalación local de las aplicaciones; y la memoria (mínimo 128 Mb) y el procesador son suficientes.

1.8. Administración de datos y usuarios.

1.8.1. Datos: Ubicación, seguridad y utilización de los mismos

Los datos se encuentran almacenados en el servidor principal, adonde acceden todos los usuarios. El servidor se encuentra permanentemente bloqueado: para desbloquearlo y poder acceder es necesario validarse con la clave de administrador.

En principio, la utilización de los datos es estrictamente laboral y confidencial, existiendo una cláusula de privacidad sobre ellos (para todos los empleados de la Mutua) que detalla la imposibilidad de difundir dichos datos en cualquier actividad que no sea la estrictamente laboral que se desempeña.

1.8.2. Usuarios: Permisos, perfiles y grupos:

Las políticas de seguridad que hay establecidas determinan a qué aplicaciones puede acceder cada usuario.

Existen un conjunto extenso de perfiles, y dentro de cada perfil, una serie de grupos de usuarios. Está establecido así porque dentro de un mismo perfil existen características muy distintas entre diferentes puestos de trabajo (p.e., dentro del perfil sanitario, no es lo mismo un administrativo, que un ATS, que un médico)

También se tiene un usuario genérico que tiene acceso únicamente a las aplicaciones comunes y a la intranet de la Mutua. Dicha cuenta se utiliza para usuarios de nueva incorporación a los que todavía no se les ha asignado un perfil concreto, usuarios en prácticas, etc.

Los administradores del dominio no tienen restricciones: tienen acceso a perfiles, cuentas y datos. Además, a través de esta cuenta se administran y configuran los dispositivos y periféricos.

1.9. Política de seguridad

En una red organizativa debemos proveernos de mecanismos de seguridad apropiados. Se ha intentado controlar los siguientes puntos:

- La identificación y autentificación del usuario: clave de acceso y contraseña correspondiente.
- La autorización de acceso a los recursos, es decir, sólo personal autorizado por la Mutua.
- La confidencialidad; para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento.

Por tanto, la seguridad comprende, básicamente, lo siguiente:

a) *Identificación:* (ID) saber en todo momento quién es el usuario que solicita hacer uso del servicio.
b) *Autentificación:* la posibilidad de probar que el usuario es quien dice ser; prueba de identidad. En nuestro caso, por ejemplo un *contraseña* secreto que solo el usuario debe conocer.
c) *Control de Acceso:* cuando ya se sabe y se puede probar que un usuario es quien es, el sistema decide lo que le permite hacer.
d) *Confidencialidad:* protección de la información para que no pueda ser vista ni entendida por personal no autorizado.
e) *Integridad*: es la cualidad que asegura que el mensaje es seguro, que no ha sido alterado. La integridad provee la detección del uso no autorizado de la información y de la red.
f) *No repudiación:* prevención de la negación de que un mensaje ha sido enviado o recibido y asegura que el enviador del mensaje no pueda negar que lo envió o que el receptor niegue haberlo recibido.

La RFC 1244 lista los siguientes recursos de red que usted debe considerar al calcular las amenazas a la seguridad general

1. HARDWARE: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, routers.
2. SOFTWARE: programas fuente, programas objeto, programas de diagnostico, sistemas operativos, programas de comunicaciones.

3. DATOS: durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoria, bases de datos, en tránsito a través de medios de comunicación.
4. PERSONAS: usuarios, personas necesarias para operar los sistemas.
5. DOCUMENTACION:sobre programas, hardware, sistemas, procedimientos administrativos locales.
6. SUMINISTROS: papel, formularios, cintas, medios magnéticos.

1.9.1. A nivel de usuario:

Las cuentas sin contraseña son peligrosas. Si éstas no están establecidas correctamente, puede comprometerse la seguridad del sistema. Asimismo, si un usuario privilegiado abandona la organización, se debe cambiar la contraseña de las cuentas privilegiadas.
Además deben cambiarse las cuentas de usuario de quienes salgan de la compañía.

Todo usuario al identificarse con su clave, arranca su propio perfil, el cual determina a qué aplicaciones y datos va a tener acceso. Es decir, sólo podrán utilizar aquello que venga determinado por políticas de seguridad.

Un usuario nunca podrá acceder a datos del directorio de trabajo y/o aplicaciones de otro usuario que no pertenezca a su grupo de trabajo. Además, aquellos datos que el usuario guarde en su directorio personal, solamente él y los administradores de red tendrán acceso a ellos.

1.9.2. A nivel de administración

Todos los recursos importantes de la red, hosts, servidores... deben estar ubicados en una red físicamente segura. Físicamente seguro quiere decir que el servidor esté guardado en una habitación o colocado de tal modo que se restrinja el acceso físico a él.

1.9.2.1. Seguridad física:

No es fácil asegurar físicamente las máquinas. Se ha limitado el acceso desde máquinas no seguras hacia las más seguras.

Y a pesar de que la máquina y/o servidor esté seguro físicamente, debemos tener cuidado sobre qué personas tiene acceso a ella.

En todas las estaciones de la Mutua (a excepción de los equipos autónomos), se ha eliminado el principal medio de entrada/salida: las disqueteras. Éstas se encuentran deshabilitadas por Bios (la Bios tiene contraseña) para evitar posibles infecciones de virus del exterior, extracción de información confidencial ...

El servidor de ficheros (ya sea el principal o los secundarios) se encuentra aislado del resto de equipos.

Los racks existentes están cerrados con llave.

Las cintas de backup se encuentran en un lugar independiente del servidor de ficheros y etiquetadas por números.

1.9.2.2. Seguridad de acceso:

A nivel de estaciones, no se tiene acceso al disco duro ni a la disquetera, y sólo se puede acceder a la red de area local a través de la cuenta de un usuario dado de alta en el dominio (cuya cuenta no esté bloqueada o deshabilitada) y su contraseña correspondiente.

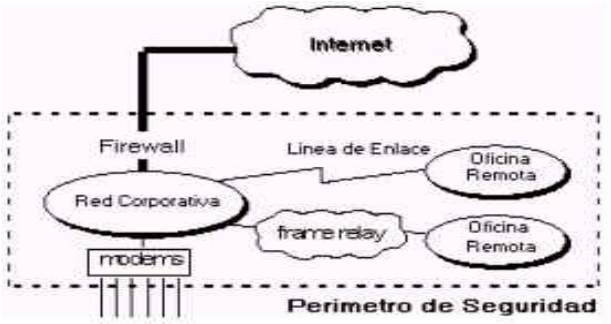
Con esto se consigue evitar el uso ilegal de software, evitar el ingreso de virus, evitar el robo de información, etc.

A nivel de servidor/res, es necesario validarse con la contraseña de administrador para poderlos utilizar.

Es posible recibir ataques externos, de Internet. Por eso es conveniente usar un dispositivo firewall para ofrecer un punto de resistencia a la entrada de intrusos en la red. Controla todas las comunicaciones que pasan de una red a otra y en función de lo que sean, permite o deniega su paso (examina el tipo de servicio al que corresponde, ya sea web, correo, IRC..., y decide si lo permite o no). Además mira si la comunicación es entrante o saliente.

También permite algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local (es el caso de conexiones Teletrabajo de ciertos puestos directivos de la Mutua para trabajar desde casa o de viaje).

La seguridad, a nivel de red corporativa nos la proporciona y gestiona una empresa externa que tiene contratada . Disponen de cortafuegos, proxy, antivirus ...



1.10. Atención a los usuarios.Gestión de las incidencias.

Existe un soporte informático local que se encarga de la gestión de las incidencias que se producen en las oficinas centrales de la Mutua; esto engloba tanto el edificio principal como los edificios secundarios que se encuentran cercanos.

Los usuarios dirigen sus problemas, ya sean de tipo hardware o software, al departamento de Sistemas de Información. Y desde allí, según el carácter de la incidencia, se resuelve localmente o se reporta, a través de una BBDD de Incidencias, a una empresa externa para su posterior resolución.

En el caso de que el problema sea de tipo harware y requiera la sustitución y/o reparación de material informático, como monitores, cambio de placa base, discos duros, etc... se solicitará la intervención de un soporte técnico que tiene contratado anualmente . Dicho soporte atiende el parte de avería en un plazo aproximado de 24 horas desde la recepción del aviso.

Los usuarios en todo momento saben el estado de su incidencia, ya que en el momento de la recepción del problema los técnicos informáticos abren una incidencia que contiene toda la descripción y características, llegándole al usuario un correo con la notificación de la misma. Lo mismo ocurre durante el seguimiento y cierre.

2. PROPUESTA DE LA SITUACIÓN FINAL

2.1. Recableado del edificio

A finales de los años 80, las típicas Redes de Área Local contaban con menos de cinco usuarios, todos ellos en una pequeña área de oficina; eran redes con requerimientos sencillos de cableado. Conforme la red ha ido creciendo, los requerimientos de componentes e inversión han sido mayores. De esta forma, la planeación de actividades y administración de tiempos se han vuelto conceptos básicos para la ejecución de proyectos de cableado, puesto que las LAN pueden usar diferentes componentes, software y aplicaciones sobre el mismo cable.

Un edificio ya no puede ser sólo un elemento pasivo para una organización. En la actualidad, los criterios que se utilizan para definir un cableado no son los mismos que se usaban hace unos años; los edificios de hoy tienen que contemplar factores como: el cableado para equipos, su organización y el desempeño, así como el tipo de cable que debe instalarse para cumplir con los requerimientos de las demandas de redes de alta velocidad.

En comparación con otras inversiones de equipo de cómputo, la que se hace en el cableado de una LAN debe durar un periodo mucho mayor que la inversión en software (que, en promedio, es de dos a tres años) y en hardware (que es de aproximadamente cinco años). Con respecto al cableado, éste debe representar una inversión que dure, por lo menos, 20 ó 25 años, ya que pagará dividendos por mucho tiempo: de esa inversión depende la selección de todos los componentes del cableado y la supervisión de la red.

2.1.1. Categoría 6 vs.tecnología Wireless

Categoría 6

Las categorías de los cables UTP especifican unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia.

Por ejemplo, el actual cable de categoría 5 que se tiene en estos momentos en edificio es un estándar dentro de las comunicaciones en redes LAN. Es capaz de soportar comunicaciones de hasta 100 Mbps con un ancho de banda de hasta 100 Mhz. Este tipo de cable es de 8 hilos, es decir, cuatro pares trenzados. Está diseñada para manejar cualquier aplicación actual basada en cable de cobre para datos, voz o imagen –desde voz analógica hasta Fast Ethernet.

La atenuación del cable de esta categoría viene dada por esta tabla referida a una distancia estándar de 100 metros:

Velocidad de transmisión de datos	Nivel de atenuación
4 Mbps	13 dB
10 Mbps	20 dB
16 Mbps	25 dB
100 Mbps	67 dB

Actualmente la categoría 5 es el medio más popular para aplicaciones de datos de alta velocidad, debido a su facilidad y bajo costo de instalación, y a su bajo consumo de espacio.

Sin embargo, ya existen cables UTP categoría 6 (y ya se utilizan; estándar ANSI/TIA/EIA-568-B.2-1 que fue ratificado por la TIA/EIA en Junio del año 2002) que pueden alcanzar una velocidad de transmisión de 1Gbps con un ancho de banda de 250 Mhz para Ethernet. Provee un mayor rendimiento que CAT5, y sus especificaciones y características son mas exigentes en cuanto a problemas de crosstalk y system noise (ruido).

Soporta no sólo las aplicaciones actuales sino también aquellas que están a punto de aparecer.

El conector para el UTP de categoría 6 sigue siendo el RJ45 (mientras que el conector para categoría 7 aún no se conoce, ya que se trata de un cable blindado incompatible con lo que se tiene instalado actualmente).

La calidad de la transmisión de datos depende del rendimiento de los componentes del canal. Por lo tanto, para transmitir de acuerdo a las especificaciones CAT6, los conectores, cables, cableados y demás dispositivos relacionados en conectividad deben cumplir el estándar CAT6.

El estándar intenta lograr un rendimiento máximo y completo aun con medios genéricos, siempre que cumplan con la categoría, lo que permite que componentes de cualquier marca puedan ser combinados en el canal.

Comparación de Especificaciones Cableado UTP			
	Categoría 5	**Categoría 5e**	**Categoría 6**
Frecuencia	100 MHz	100 MHz	250 MHz
Atenuación (Min. a 100 MHz)	22 dB	22 dB	19.8 dB
Impedancia Característica	100 ohms ± 15%	100 ohms ± 15%	100 ohms ± 15%
NEXT (Min. a 100 MHz)	32.3 dB	35.3 dB	44.3 dB
PS-NEXT (Min. a 100 MHz)	Sin Especificaciones	32.3 dB	42.3 dB
ELFEXT (Min. a 100 MHz)	Sin Especificaciones	23.8 dB	27.8 dB
PS-ELFEXT (Min. a 100 MHz)	Sin Especificaciones	20.8 dB	24.8 dB
Return Loss (Min. a 100 MHz)	16.0 dB	20.1 dB	20.1 dB
Delay Skew (Max. por 100 m)	Sin Especificaciones	45 ns	45 ns

Ventajas de la Categoría 6:

- Soporta todas las aplicaciones actuales y las que se prevén a medio plazo
- Fácil y rápida de instalar.
- Ancho de banda de hasta **250** MHz.
- Se convertirá en la categoría de cableado por defecto.
- Misma distancia de transmisión y métodos de instalación que la Categoría 5 y 5e.
- Compatible física y eléctricamente con las categorías inferiores.

Inconvenientes de la Categoría 6:

- Requiere un cierto cuidado en la instalación.
- El precio evidentemente es algo mayor que el de Categoría 5 y 5e.
- Actualmente, no hay posibilidad de Categoría 6 en exteriores.

Tecnologia inalámbrica

Las redes inalámbricas locales (Wireless LANs WLANs, Wi-Fi) conforman una de las tecnologías electrónicas de crecimiento más rápido en toda la historia.

Estándares:

- 802.11: Primer estándar WLAN, velocidad de transmisión hasta 2 Mbps, alcance hasta 100 metros y banda de radio frecuencia 2.4 GHz
- 802.11 a: Aprovado en Julio de 2003, gana velocidad pero pierde interoperabilidad con otras normas. Velocidad de transmisión hasta 54 Mbps, alcance hasta 50 metros y banda de radio frecuencia 2.4 GHz
- 802.11 b estándar más extendido en la actualidad, velocidad de transmisión hasta 11 Mbps, alcance hasta 100 metros y banda de radio frecuencia 2.4 GHz, compatible con 802.11 g
- 802.11 g: Compatible con 802.11 b, es el estándar más rápido disponible actualmente, velocidad de transmisión hasta 54 Mbps, alcance hasta 100 metros y banda de radio frecuencia 2.4 GHz.

Ventajas de la Tecnología Wireless:

Los sistemas inalámbricos o Wireless se utilizan en redes de área local por la comodidad y flexibilidad que presentan:

- No son necesarios los sistemas de cableado para conectar los equipos al servidor
- Fácil redistribución de la red: los puestos se pueden desplazar sin grandes problemas, (gran movilidad), añadir un equipo, etc.
- Permite aumentar el número de usuarios sin necesidad de infraestructura adicional
- Mayor versatilidad (portátiles)
- Descenso de los costos: la reducción de costes de la implantación de una red Wireless puede suponer un ahorro de hasta un 95% frente al despliegue tradicional
- Rapidez de implantación

- Estética: en una instalación Wireless desaparecen los cables de las estaciones, las rosetas y se reducen al mínimo las canalizaciones visibles

Inconvenientes de la Tecnología Wireless

- Menor robustez: las redes con cableado estructurado son por lo general más robustas frente a interferencias y condiciones adversas que las inalámbricas, expuestas a obstáculos y demás
- Menor velocidad: en Fast Ethernet estamos obteniendo unos límites máximos de 100 Mbps, frente a los 54 Mbps en una WLAN (802.11g). Mucha más lentitud a la hora de transmisión de datos
- Exige una planificación de las zonas de cobertura y sus frecuencias
- Necesidad de mantenimiento
- Menor alcance, limitado por el componente Wireless a unas determinadas distancias
- Seguridad: es uno de los puntos clave de las desventajas de esta tecnología

Además, padecen de fuertes imposiciones administrativas en las asignaciones de frecuencia que pueden utilizar: son sistemas cuyos parámetros de transmisión están legislados por las Administraciones Públicas. En algunos casos, se requieren permisos especiales, dependiendo de la banda de frecuencia que utilicen.

Cuadro comparativo:

Especificaciones comunes	
Velocidad	2/11 Mbps
Alcance	500 – 150 m
Plug&Play	Sí
Tipo de Red	WLAN
Hub o concentrador	No

Particularidades	
Seguridad	64-128 bit WEP
Frecuencia	2.4-2.472 Ghz
Potencia	10 dBm

Especificaciones comunes	
Velocidad	10/100 Mbps
Alcance	100 m aprox
Plug&Play	Si
Tipo de Red	LAN
Hub o concentrador	Sí (usual)

Particularidades	
Conector	RJ-45
Cables	Category 5/6
Repetidores	Más de tres

CONCLUSIONES:

En el caso de la organización, se debe optar por una solución híbrida: Categoría 6 para la conexión de los equipos fijos de la Mutua, y tecnología Wireless para los equipos portátiles.
Con esto se conseguiría dotar de movilidad a los puestos que, por necesidades del trabajo que desempeñan, la necesitan, que son portátiles.

Como el número de portátiles en la Mutua significa una proporción pequeña del total de los equipos que se tienen, prevalece la ventaja de la movilidad a la pérdida de velocidad de transmisión de datos, ya que al dividirse la velocidad de transmisión entre un número reducido de estaciones, la disminución de la misma apenas se acusará.

En las salas de formación que existen en la Mutua (en todos los edificios) también la tecnología inalámbrica es más idónea.

2.1.2. Categoría 6 vs Fibra Optica

Fibra óptica

La creciente demanda de velocidad de transmisión de datos dentro de las redes corporativas ha hecho que la industria de la fibra óptica reexamine el tipo de fibra multimodo recomendada para realizar sistemas de cableado en redes corporativas (a velocidades de transmisión de datos de 155Mbps).

Enlace entre edificios: Opción Preferente

- *Más de 90 metros:* Categoría 5, teniendo en cuenta que quedamos limitados a voz y datos de baja velocidad; las aplicaciones de alta velocidad deberían soportarse mediante fibra óptica.

- *Menos de 90 metros*: Categoría 6 si el camino está mecánicamente protegido.
  En ambos casos se recomienda tender también **fibra óptica OM3**.

Enlace entre repartidores: Opción Preferente

A partir de la instalación actual de los edificios, y planteando la posibilidad del recableado general del edificio principal y secundarios, no tiene sentido implementar la red de cableado si no ofrece las mayores posibilidades; por esto es recomendable la **Categoría 6 para el cobre** (que soportará

todas las aplicaciones) y también **fibra óptica OM3**, para enlazar los equipos de electrónica.

Cableado hasta la toma de usuario : Opción Preferente

¿Cobre o Fibra hasta el puesto de trabajo?

Uno de los parámetros a tener más en cuenta en el coste del sistema es el medio de transmisión Elegido. Teniendo en cuenta el coste y el rendimiento del sistema, se plantean las siguientes opciones:

1ª OPCIÓN: Cobre hasta el puesto

Ventajas:

- Conocido, intuitivo.
- Medio aceptado por el mercado.
- Fácil de instalar.
- Coste moderado.
- Capacidad de transmisión hasta 1 Gbps (para la Categoría 6).

Inconvenientes:

- Capacidad alta pero limitada.

2ª OPCIÓN: Fibra óptica hasta el puesto

Ventajas:

- Capacidad de transmisión muy por encima de las necesidades actuales
- Máxima seguridad. Señales casi imposibles de interceptar
- Soporta distancias de canal de hasta 300 m
- Mayor facilidad para arquitecturas centralizadas, sin repartidores de planta
- Inmune a todas las interferencias electromagnéticas

Inconvenientes:

- Diferentes métodos y útiles de instalación
- Coste aún elevado

CONCLUSIONES:

Teniendo en cuenta que la capacidad del cableado de cobre, aunque no tan alta como la de la fibra óptica, se ha incrementado considerablemente con la aparición en el mercado de la Categoría 6, y considerando la relación entre estas capacidades y el coste de las dos alternativas, en principio en el caso real de la Mutua habría que decantarse por la instalación de cableado de Categoría 6 en el subsistema horizontal.

El cableado horizontal es el que requiere más tiempo de instalación (50% del total) y el que más perturbaciones crea cuando, por infravaloración de las necesidades, hay que recablear.
Por tanto, es muy recomendable elegir una alternativa segura y capaz para este subsistema, que nos garantice su utilidad durante el mayor tiempo posible. Con estos requisitos, sólo hay una respuesta: **Categoría 6.**

Y, el cableado entre repartidores de planta, tal y como se ha comentado anteriormente, ambas opciones son idóneas, tanto **Categoría 6** como **Fibra Óptica**.

2.1.3. La nueva tecnología: Wimax

Es el nuevo complemento de la la tecnología inalámbrica Wi-Fi.
Es un nuevo estándar, también llamado 802.16, compuesto por el 802.11a, 802.11b y 802.11g que tiene un alcance de unos 50 kms y ofrece un mayor ancho de banda, con velocidades de transmisión de 70 Mbps.
Aunque Wimax se creó en el año 2003, no han salido productos que lo integraran hasta la última feria de Hannover. Su uso no se autorizará hasta finales del 2004, pero supone un gran avance en cuanto a velocidad de transmisión se refiere.

2.2. Migración servidores

2.2.1. Instalación S.O. Windows 2003 Server

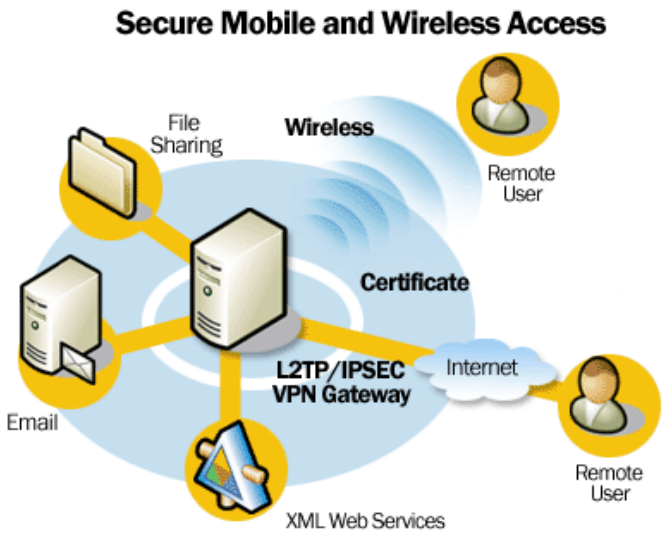
Windows Server 2003 es un sistema operativo de servidor que supone una evolución notable en la fiabilidad, disponibilidad, escalabilidad, productividad, y facilita el manejo de discos y volúmenes y la recuperación de datos.
Microsoft Windows Server 2003 ofrece muchos beneficios cuando se utiliza en el dominio de Windows NT 4.0, ya sea como servidor de archivos, servidor de impresión, servidor de aplicaciones Web, servidor de acceso remoto, ...

Debido a que Windows Server 2003 es muy superior en rendimiento, fiabilidad y seguridad, es una solución ideal para la consolidación de hardware, con importantes ahorros en costes asociados a la infraestructura.
Microsoft proporciona un conjunto limitado de herramientas para gestionar entornos NT 4.0. Sin embargo, en el caso Windows Server 2003 este conjunto es mucho más amplio, orientado a gestionar de forma centralizada su entorno de servidores.

Las más importantes características y mejoras de la migración desde Windows NT Server 4.0 son las siguientes:

1. Active Directory
2. Políticas de Grupo: consola de Gestión de Políticas de Grupo
3. Rendimiento del Servidor
4. Recuperación de copias instantáneas de Volumen
5. Internet Information Services 6.0 y Microsoft .NET Framework
6. Servicios de Terminal
7. Soporte de Cluster de hasta 8 nodos
8. Soporte integrado de PKI mediante Kerberos versión 5
9. Herramienta de línea de comandos Windows Management Instrumentation (WMIC)
10. Servicios inteligentes de ficheros: EFS, DFS y FRS

Además, Windows 2003 Server es más seguro que Windows NT 4.0. Windows 2003 Server incluye un importante acceso remoto y funciones inalámbricas LAN que no se encuentran disponibles en Windows NT 4.0, como tecnologías de autentificación y cifrado fuertes.



2.2.2. Actualización de las aplicaciones de los servidores

Una vez se haya completado la migración a Windows 2003 Server, se procederá a actualizar las aplicaciones que residen en los servidores: las que lo necesitan por requerimientos del nuevo sistema operativo y el resto para actualizar la versión.

2.2.3. Establecer cuotas máximas del volumen de datos de los usuarios

Windows 2003 Server supone un cambio fundamental si se compara con Windows NT 4.0, gracias a un conjunto de nuevas funcionalidades, entre las que destaca el Directorio Activo (o Active Directory), que sustituye al administrador de cuentas de seguridad (SAM) de Microsoft Windows NT versión 4.0.

El nuevo Modo de Aplicación de Directorio Activo (ADAM) permite ejecutar Directorio Activ como una aplicación en los dominios de Windows Server 2003. Esto proporciona una parte de la funcionalidad de Directorio Activo a las aplicaciones y servicios.

El servicio del Directorio Activo de Microsoft simplifica la administración de complejos directorios de redes.

La Consola de Gestión de Directivas de Grupo (Group Policy Management Console o GPMC), que está disponible como componente adicional de Windows Server 2003, proporciona un nuevo marco de trabajo para la administración de estas directivas.

Con la migración a Windows 2003 Server se abre la posibilidad (ante el aumento del volumen de datos que los usuarios tienen en sus directorios personales y de trabajo) de establecer cuotas máximas del volumen de los mismos.

Para proceder a esto es necesario establecer, a priori, unas directrices para determinar las necesidades de cada usuario y así determinar el volumen máximo de datos que se le asignará en función las actividades que desarrolla dentro de la organización, nivel jerárquico, etc.

2.2.4. Monitorización del tráfico de la red

La monitorización de red permite solucionar y prevenir muchos de los problemas que se presentan: cuellos de botella, sobrecarga de usuarios, intrusiones, etc..
Network Monitor es el componente de monitorización que viene incluido Microsoft Systems Management Server

Instalación de un equipo conectado en red para la monitorización del trafico, con el sotware Microsoft Systems Management

Los analizadores de red son mecanismos, hardware o software, que permiten la monitorización del tráfico que se transmite por un segmento de red.

La monitorización del tráfico de la red requiere herramientas especializadas como *software* de supervisión de red dedicado (como Microsoft System Management Server) o un rastreador de paquetes.

Lo más usual es instalar en un equipo un software que analice la red, poniendo su tarjeta de red en modo promiscuo. Actualmente existen analizadores de red en modo texto (por ejemplo Tcpdump) y gráficos (por ejemplo Ethereal).

2.3. Subdivisión de la red organizativa en dos subredes: una para la Mutua y otra para el Servicio de Prevención

En los últimos tiempos el Servicio de Prevención de la Mutua ha sufrido un notable crecimiento. Esto repercute en el rendimiento de los servicios.

El principal problema que acusa la organización ante este aumento es el volumen de datos que ha de albergar el servidor de dominio: en estos momentos los datos pertenecientes al Servicio de Prevención suponen una cuarta parte del volumen total de datos.

Además, las copias de seguridad tienen una duración extremadamente larga: a pesar de realizarse durante la noche, el día de la semana que se realiza una copia completa a la mañana siguiente se debe

poner una segunda cinta para que contínue el respaldo (ya que son necesarias dos cintas) y ralentiza todo el servicio durante esa mañana.

La solución pasa por traspasar todos los ficheros de datos del servidor principal de dominio a uno de los servidores secundarios, concretamente el que existe en el Servicio de Prevención, que en estos momentos se está utilizando únicamente como servidor de impresión.

De esta forma se consigue descargar el servidor principal, además de minimizar el tiempo de respaldo de las copias de seguridad.

Con esto se conseguirá también que las copias de seguridad se realicen únicamente durante la noche. En el servidor secundario hará falta una cinta de backup en cinta, la instalación del software necesario para la realización de las copias y la compra de cintas DLT para hacer el respaldo.

2.4. Políticas de backup

2.4.1. Redefinición copias de seguridad

El volumen de datos de la organización estará dividido en dos: los datos residentes en el servidor de dominio (únicamente los propios de la Mutua) y los datos residentes en el servidor secundario del Servicio de Prevención.

Por tanto, se ha de hacer una redefinición de las copias de seguridad del servidor principal, y una definición nueva para las que se realizarán, a partir de ahora, en el servidor del Servicio de Prevención. Es decir, se realizarán diariamente dos copias de seguridad simultáneas pero en servidores diferentes: una en el servidor principal, que respaldará los ficheros de dicho servidor, y otra en el servidor del Servicio de Prevención, que respaldará los datos que, como se ha comentado en el anteriormente, se han traspasado.

La planificación de las copias se mantendrá con la misma política: una copia incremental cada día, y una copia completa semanal, con rotación de cintas, y cada mes se sobreescriben.

2.4.2. Realización copias de seguridad

Las copias de seguridad de ambos servidores se harán por la noche. Cada servidor respaldará los datos que residan en su servidor.

Con esto se consigue que solamente se necesite una cinta para cada respaldo, sin tener que prolongar la copia durante la mañana, con la consiguiente ralentización del servicio.

En el caso del respaldo en el servidor de dominio, se seguirá utilizando las cintas HP DLT-IV (ya que por su capacidad son idóneas), sin embargo, en el caso del respaldo del Servicio de

Prevención se comprarán cintas de menor capacidad, ya que el volumen a respaldar es mucho menor, aproximadamente de una cuarta parte.

2.5. Conexión de portátiles autónomos

Con la instalación de Windows Server 2003 las redes inalámbricas són más sencillas y seguras. Windows Server 2003 soporta el estándar IEEE 802.1x, el cual utiliza una autenticación de red basada en certificados y un modelo de autorización.

Windows Server 2003 también incluye soporte para el Protocolo de Autenticación Extensible -Seguridad de Nivel de Transpor te (EAP-TLS, *Extensible Authentication Protocol - Transport Level Security*). Este protocolo permite un acceso seguro.

2.5.1. Tecnología Wireless

La oportunidad de poder conectar los portátiles, y ciertos equipos (creando una WLAN, Red de Área Local Inalámbrica) con el servidor es una de las mayores ventajas de la tecnología Wireless, ya que proporcionarán la portabilidad para aquellos puestos que la necesitan y que en estos momentos están “atados” al cableado estructural.
Además, se facilita también la movilidad de los portátiles entre los edificios colindantes.

2.5.2. Copias de seguridad y archiving

Se dispondrá de un equipo portátil con grabadora DVD y disquetera habilitada, con conexión Wireless, para que los usuarios hagan copias de seguridad, en cd roms o disquets, de sus ficheros. La movilidad que proporcionará la conexión inalámbrica, facilitará que dicho puesto de "autoservicio" se instale y/o mueva según requerimientos del servicio.

3. PLANNING DE MIGRACIÓN

3.1. 1ªfase: Migración de Windows NT Server a Windows 2003 Server

¿Por qué actualizar de Windows NT 4.0 a Windows Server 2003?

Microsoft Windows Server 2003 proporciona muchas herramientas nuevas, servicios y características que son un factor decisivo para la actualización desde Windows NT Server 4.0.

Además, beneficios inmediatos al actualizar sin instalar el servicio de Active Directory, significativos beneficios de administración, reducción de gastos que proporciona Active Directory, avances en la inclusión de funciones cruciales de los servidores, archivo, impresión y conectividad segura en red de cable e inalámbrica, administración de identidades de Active Directory, servicios de administración y servidores Web seguros y fiables (Internet Information Services 6.0).

Las 10 características principales para actualizar desde Windows NT Server 4.0 a Windows 2003 Server

Windows Server 2003 integra un potente entorno de aplicación para desarrollar soluciones empresariales y servicios Web XML innovadores, que mejoran enormemente la eficacia del proceso. Las principales funciones y mejoras nuevas son:

1. **Active Directory**

   El servicio Microsoft Active Directory simplifica la administración de directorios de red complejos y facilita que los usuarios localicen recursos incluso en las redes de mayor tamaño. Este servicio de directorio de nivel corporativo es escalable, basado en tecnologías estándar de Internet y está plenamente integrado, a nivel de sistema operativo, en Windows Server 2003 Standard, Windows Server 2003 Enterprise y Windows Server 2003 Datacenter.

   Windows Server 2003 proporciona numerosas mejoras fáciles de usar en Active Directory y nuevas funciones, incluyendo las relaciones de confianza entre bosques, la posibilidad de cambiar el nombre de los dominios y la posibilidad de desactivar atributos y clases en el esquema para que se puedan modificar sus definiciones.

2. **Directiva de grupo: Consola de administración de directivas de grupo**
Se puede usar la Directiva de grupo para definir la configuración y las acciones permitidas para los usuarios y equipos. A diferencia de las directivas locales, la Directiva de grupo se puede utilizar para establecer directivas que se aplicarán a un sitio, dominio o unidad organizativa determinados en Active Directory. La administración basada en directivas simplifica tareas como el funcionamiento de actualizaciones del sistema, la instalación de aplicaciones, la creación de perfiles de usuario y el bloqueo de sistemas de escritorio.

La Consola de administración de directivas de grupo (GPMC), que seguramente estará disponible como componente complementario en Windows Server 2003, proporciona el nuevo marco para administrar la Directiva de grupo.

3. **Rendimiento del servidor**
Windows Server 2003 demuestra un rendimiento enormemente superior sobre las versiones anteriores de los sistemas operativos de servidor Windows. El rendimiento de los archivos y del servidor Web es dos veces más rápido que en Windows NT Server 4.0.

4. **Restauración de instantánea de volúmenes**
Esta función permite configurar copias de datos vitales en un momento determinado, sin que se interrumpa el servicio. Estas copias pueden usarse posteriormente para restaurar el servicio, para archivo o para restauración. Los usuarios pueden recuperar versiones archivadas de sus documentos, que se mantienen de forma no visible en el servidor. La productividad queda mejorada gracias a la posibilidad de recuperar documentos de una forma más óptima.

5. **Servicios de Internet Information Server 6.0 y Microsoft .NET Framework**
Servicios de Internet Information Server (IIS) 6.0 es un servidor Web de funciones completas que posibilita la creación de aplicaciones Web y servicios Web XML. La arquitectura de IIS 6.0 ha sido completamente reconstruida, con un nuevo modelo de proceso de tolerancia a errores que mejora significativamente la confiabilidad de las aplicaciones y los sitios Web.

Ahora, IIS puede aislar una aplicación Web individual o varios sitios en un proceso autocontenido (llamado un "grupo de aplicaciones") que se comunica directamente con el núcleo del sistema operativo. Esta función aumenta el rendimiento y la capacidad de las

aplicaciones, proporcionando a la vez más espacio libre en los servidores, con lo que se reducen de forma efectiva los requisitos de hardware. Estos grupos de aplicaciones autocontenidos impiden que una aplicación o un sitio interrumpan los servicios Web XML u otras aplicaciones Web del servidor.

IIS también incorpora funciones de supervisión del estado con el fin de descubrir, recuperar e impedir errores en las aplicaciones Web. En Windows Server 2003, Microsoft ASP.NET usa de forma nativa el nuevo modelo de proceso de IIS. Estas funciones avanzadas de detección y estado de las aplicaciones también están disponibles para las aplicaciones ya existentes que se ejecuten en Internet Information Server 4.0 y en IIS 5.0, sin que la inmensa mayoría de las aplicaciones necesiten ninguna modificación.

NET Framework proporciona el modelo de programación para crear, distribuir y ejecutar aplicaciones basadas en Web y servicios Web XML en esta plataforma de gran estabilidad. Proporciona un entorno productivo, basado en estándares y multilenguaje para integrar las inversiones ya existentes con las aplicaciones y servicios de nueva generación, así como la agilidad para resolver los retos de la distribución y el funcionamiento de las aplicaciones a escala Internet.

6. **Servicios de Terminal Server**

Los Servicios de Terminal Server permiten entregar aplicaciones basadas en Windows, o el propio escritorio de Windows, virtualmente a cualquier dispositivo informático, incluyendo aquellos dispositivos que no ejecutan Windows. Si los usuarios ejecutan una aplicación en Terminal Server, la ejecución de la aplicación se produce en el servidor, y únicamente se transmite a través de red la información del teclado, el ratón y la pantalla. Los usuarios sólo ven su propia sesión individual, administrada de forma transparente por el sistema operativo del servidor, y que permanece independiente de cualquier otra sesión cliente.
El Escritorio remoto para administración crea el modo de administración remota de los Servicios de Terminal Server de Windows 2000.

Terminal Server puede mejorar las posibilidades de implantación de software de la empresa en una gran variedad de situaciones que serían difíciles de resolver usando las tecnologías tradicionales de distribución de aplicaciones.

7. **Organización de clústeres (compatibilidad con ocho nodos)**
Disponible únicamente en Windows Server 2003 Enterprise Edition y Windows Server 2003 Datacenter Edition, este servicio proporciona una alta disponibilidad y escalabilidad para aplicaciones vitales como bases de datos, sistemas de mensajería y servicios de archivos e impresión. La organización en clústeres funciona habilitando múltiples servidores (nodos) para que permanezcan en comunicación constante. En caso de que uno de los nodos del clúster no esté disponible debido a un error o a que se están realizando tareas de mantenimiento, otro nodo comenzará inmediatamente a proporcionar servicios, un proceso denominado conmutación por error. Los usuarios que estén teniendo acceso al servicio continuarán sus actividades, sin saber que ahora el servicio lo proporciona un servidor distinto (nodo).

Windows Server 2003, Enterprise Edition y Windows Server 2003, Datacenter Edition admiten configuraciones de clúster de servidor de hasta ocho nodos.

8. **Compatibilidad con PKI integrada utilizando Kerberos Versión 5**
Mediante el uso de los Servicios de Certificate Server y las herramientas de administración de certificados, se puede implementar nuestra propia infraestructura de claves públicas (PKI). PKI permite implementar tecnologías basadas en estándares, como la posibilidad de inicio de sesión con tarjeta inteligente, la autenticación de clientes (mediante SSL y TLS), el correo electrónico seguro, las firmas digitales y la conectividad segura (mediante la Seguridad de protocolo Internet (IPSec).

Mediante los Servicios de Certificate Server, es posible configurar y administrar entidades emisoras de certificados que emiten y revocan certificados X.509 V3.

Kerberos versión 5 es un protocolo de autenticación de red estándar del sector ampliamente probado. La compatibilidad con Kerberos versión 5 proporciona a los usuarios un proceso de inicio de sesión rápido y único que les permite obtener el tipo de acceso que necesitan a los recursos empresariales, así como a otros entornos compatibles con este protocolo. La compatibilidad con Kerberos versión 5 incluye ventajas adicionales, como la autenticación Mutua (el cliente y el servidor deben proporcionar autenticación) y la autenticación delegada (se hace un seguimiento integral de las credenciales del usuario).

9. **Administración desde la línea de comandos**
La familia de Windows Server 2003 proporciona una infraestructura de línea de comandos significativamente mejorada, permitiendo realizar la mayoría de las tareas de administración sin usar una interfaz gráfica de usuario.

Globalmente, la mejor funcionalidad de línea de comandos de la familia de Windows Server 2003, en combinación con secuencias de comandos listas para su uso, rivaliza con la eficacia de otros sistemas operativos asociados frecuentemente a un mayor costo de propiedad.

10. **Servicios de archivos inteligentes: Sistema de archivos de cifrado, Sistema de archivos distribuido y Servicio de replicación de archivos**
El Sistema de archivos de cifrado (EFS) permite que los usuarios cifren y descifren archivos para protegerlos de intrusos que puedan obtener acceso físico no autorizado a sus datos confidenciales almacenados (por ejemplo, mediante el robo de un portátil o de una unidad de disco externo).

El cifrado es transparente: Los usuarios pueden trabajar con archivos y carpetas cifrados de la misma forma que con cualquier otro archivo o carpeta. Si el usuario de EFS es la misma persona que cifró el archivo o la carpeta, el sistema descifrará automáticamente el archivo o la carpeta cuando el usuario lo utilice más adelante.

El Servicio de replicación de archivos (FRS) es una mejora significativa respecto a la función de replicación de directorios de Windows NT Server 4.0. Por ejemplo, FRS proporciona replicación de archivos de varios principales en árboles de directorios designados entre servidores designados.

Antes de realizar la migración de la organización del dominio de Windows NT 4.0 a un directorio activo de Windows 2003 Server es importante evaluar los controladores del dominio y servidores existentes, planear su proceso de la migración, y diseñar su nuevo dominio 2003 del servidor de Windows.

Planear una migración a Windows 2003 Server implica los pasos siguientes:

. Seleccionar una trayectoria de la migración
· Asignar papeles del servidor
· Diseñar el nuevo dominio 2003 del servidor de Windows
. etc

También es imprescindible que Windows NT 4.0 Server tenga el Service Pack 5 ó posterior instalado para poder realizar la migración.

Es importante planificar las asignaciones futuras del papel de todos los servidores. Esto implica determinar los pasos siguientes:

· Documentación de los servidores en su ambiente actual y los servicios que cada servidor proporcionarán
· Asignación de los papeles del servidor en el nuevo ambiente, y la documentación de esas asignaciones
· Planeamiento de la capacidad básica para verificar que se tiene suficiente capacidad en los servidores
· Evaluación de la configuración de red existente (incluyendo IP ADDRESS y la información del adaptador de la red para cada servidor)

La migración a Windows 2003 Server se ha de planificar para que se realice durante fin de semana (por si surge cualquier problema o incidencia durante la instalación). Se migrarán tanto el servidor principal de la Mutua como los secundarios (actualmente utilizados únicamente como servidores de impresión).

3.1.1. Seguridad

La migración a Windows 2003 Server nos proporciona una conexión segura a la red corporativa y los recursos soportando protocolos estandarizados 802.1x, una infraestructura integrada de clave pública (PKI), acceso basado en contraseña o certificado y seguridad de autentificación extensible (EAP) integrado. Los avances que nos permiten una conectividad segura, tanto cableada como inalámbrica incluyen:

- Inicio de Sesión Única. Perfecciona la confidencialidad de la constraseña y simplifica su administración.
- Autentificación Kerberos. Proporciona un inicio de sesión único y rápido a los recursos de Windows.
- Servicios de Autentificación a Internet (IAS). Se hace más sencilla la implementación de soluciones paa el control del acceso a la red.
- Tarjetas inteligentes.
- Servicios de Certificación. Se utilizarán para crear y administrar autoridades de certificación Cas.
- Matriculación y Renovación automática de Certificado. Reducirá el tiempo y la energía consumida en el manejo de una infraestructura PKI y disminuye el riesgo de la pérdida de datos mediante un acceso no autorizado.
- Implementación PKI más sencilla. Quedan reducidos el número de recursos que se necesita para administrar certificados X.509.
- EAP Protegidos (PEAP). Mediante el empleo del Protocolo de Autentificación Extensible Protegida, PEAP, tenemos la opción de utilizar contraseñas de dominio de Windows para la comunicación inalámbrica, autenticada y cifrada.

Además, dispone de una garantía antivirus y de protección de contenido. Se consigue una mejora tecnológica más segura en la migración a Windows 2003 Server, ganando capacidad para controlar el impacto de riesgos.

3.2. 2ªfase: Migración de las aplicaciones de los servidores

Windows 2003 Server consolida el servidor de aplicaciones: las DLL simultáneas hacen mucho más facil la consolidación de aplicaciones mediante la resolución de conflictos entre aplicaciones que requieren diferentes versionesde la misma DLL. Las DLL simultáneas permiten la coexistencia de aplicaciones y mejoran la confiabilidad de nuestro sistema.

Principales aplicaciones a actualizar tras realizar la migración de los servidores a Windows 2003 Server son las siguientes:

Veritas Backup Exec 8.5: *Veritas Backup Exec for Windows Servers 9.1*
actualización a la version 9.0 (nueva interfaz gráfica de usuario que integra las funciones en una vista tipo navegador y consola de administración alternativa basada en Web para servidores Windows Server 2003).

Los agentes y las opciones del alto rendimiento proporcionan flexibilidad para proteger rápidamente los datos del servidor, protección automatizada de los datos críticos que residen en el servidor. La protección automatizada avanzada del servidor de Microsoft SQL, etc

Cliente Norton Antivirus Corporate Edition 7.01: actualización a la versión 9.0.
La edición corporativa de Symantec AntiVirus proporciona la protección escalable.La exploración de la memoria permite detectar amenazas y terminar los procesos sospechados en memoria antes de que estropeen, exploración de los email entrantes entregados a través de clientes del correo POP3 tales como Microsoft Outlook, Eudora, y correo de Netscape, etc.

Permite que los administradores revisen la red para determinar qué nodos son vulnerables a los ataques del virus. Los administradores pueden manejar a grupos del cliente y del servidor lógicamente.

Systems Management Server v1.2: actualización a Microsoft Systems Management Server 2003.
Se obtiene un ahorro de costes significativo, actualizaciones más sencillas, y mejoras sustanciales en la distribución de software, generación de informes y rendimiento. Entre las principales funcionalidades que incorpora esta nueva versión destaca la implantación de dispositivos móviles, identificación y análisis de vulnerabilidades, directorio activo, etc

Esta solución de licencia completa utiliza las probadas tecnologías de Symantec. Asegura la mejor protección frente a virus basados en Internet, caballos de Troya, códigos ActiveX y subprogramas Java dañinos. Proporciona una detección, análisis y reparación de virus rápida, fiable y sin intervención humana. La consola de gestión central permite una facilidad aún mayor de la gestión

Microsoft Office 97:

actualización a Microsoft Office 2003.
Microsoft Office 2000 ofrece nuevas y potentes herramientas de acceso y análisis de la información aplicaciones auto-reparables; todas las aplicaciones de Office 2000 comparten HTML como formato de archivo complementario binario tradicional.

Las licencias de Microsoft otorgan al usuario derecho legal a utilizar un software. Por cada programa de software de Microsoft que se utiliza, se otorga una licencia al usuario y ésta se documenta en el Contrato de Licencia de Usuario Final. Un usuario de software, necesita una licencia. El acuerdo de licencia da al usuario el derecho de utilizar el software.

Se escogerá entre una de estas dos opciones:

Enterprise Agreement (EA): Para grandes clientes corporativos con más de 250 PCs. Un único precio por ordenador de sobremesa proporciona los derechos a actualizar a las versiones nuevas de los productos para los que se adquiere una licencia.

Enterprise Agreement Suscripción (EAS): Ofrece a los grandes clientes corporativos con más de 250 PCs la opción de suscribirse a licencias de software de Microsoft, en vez de ser los propietarios

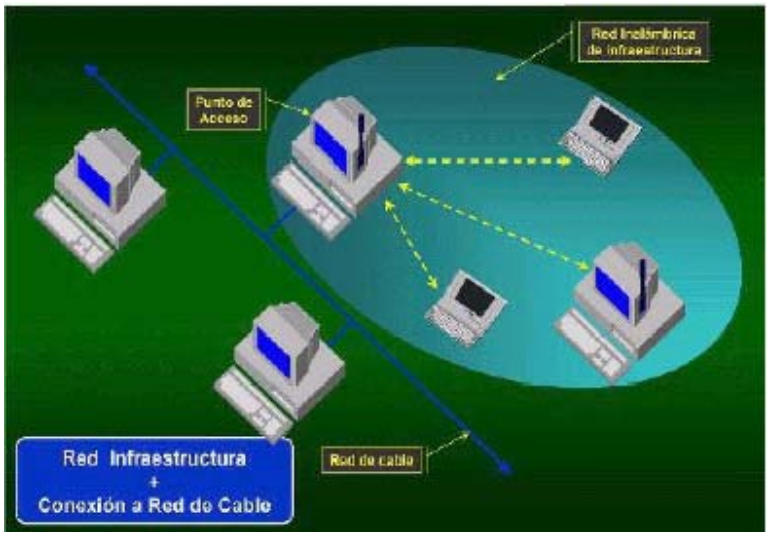
Las aplicaciones sanitarias que se tienen en estos momentos no necesitarán ningún cambio con la migración a Windows 2003 Server.

3.3. 3ªfase: Recableado edificio principal y edificios adyacentes. Instalación de nuevos elementos

La actualización a Windows 2003 Server es una buena elección para la implantación, total o parcial, de una tecnología Wireless en la red corporativa ya que el soporte inalámbrico no es posible utilizando Windows NT 4.0.
Se optará por mezclar la red cableada (LAN) y la inalámbrica (WLAN), y constituir una Red Híbrida; es relativamente fácil crearla, y seguiríamos teniendo las ventajas de la velocidad que nos brinda la parte cableada y expanderíamos las posibilidades con la parte inalámbrica.

Todas las plantas serán cableadas con UTP Clase 6, a excepción de los puntos Wireless (portátiles y algún caso puntual de estación de sobremesa). Y el cableado entre plantas se realizará con Fibra Óptica.

Respecto a la tecnología Wireless, se escoge el estándar IEEE 802.11g; además, donde se va a implantar es un espacio cerrado (el edificio en sí) y y por tanto, la interferencia con los alrededores es mínima.
La red inalámbrica operará en la modalidad *Grupo de trabajo extendido o Red de Infraestructura*: la red inalámbrica conectada a la red cableada, como complementaria. Se implementará como *Puente constituído por un/varios Punto de Acceso*. Así, proporciona la posibilidad, al portátil y/o equipo conectado, de desplazarse dentro de la subred inalámbrica: cuando pierden contacto con su punto de acceso, pasan a buscar otro sin perder la comunicación.



Todas las comunicaciones se centralizan en el backbone que comunica todas las plantas y termina en el servidor.

El sistema cableado será la parte principal y la inalámbrica la que proporcionará movilidad adicional a ciertos equipos y puestos de la organización, para que se pueda desplazar con facilidad dentro de las oficinas.

Se procederá a realizar un recableado general del edificio principal en una primera fase, y luego, posteriormente, en una segunda fase se extenderá a los edificios secundarios.

El proceso se caracterizará por los siguientes puntos:

- Cableado horizontal del edificio: se recableará con cable UTP Cat 6 combinado con tecnología Wireless.
- Cableado vertical del edificio: se utilizará Fibra Óptica.
- Cableado entre los edificios: se utilizará Fibra Óptica.

Al tratarse de oficinas, y no de hospital, no nos encontramos con la imposibilidad legal de implantar una red WIFI en una planta de cuidados intensivos.

Desde el punto de vista lógico, como ya he comentado, la red presenta una topología en estrella concentrándose los cables de red de cada planta en un banco de switches central.

Se intentará seguir un orden cronológico y estructurado. Para acometer la instalación de todos los elementos que compondrán la red de acceso del edificio de relativas dimension, es es necesario tener en cuenta ciertos aspectos previos al inicio de la instalación.

Se enumeran a continuación las tareas, que de forma cronológica y estructurada, se van a contemplar para permitir que el proyecto de instalación pueda ser completado entorpeciendo el menor tiempo posible la funcionalidad usual de las instalaciones de la organización.

1. Estudio de las necesidades concretas:
    - Necesidades espaciales de explotación
    - Necesidades lógicas: número de usuarios que podrán acceder al sistema en un momento inicial
    - Necesidades de seguridad

2. Inspección del edificio: estudio inicial y análisis de las instalaciones. Un grupo de técnicos e instaladores deberán tener acceso físico tanto a los planos como a las diferentes plantas del edificio.

3. Planificación de la instalación:
    - Clasificación de instalaciones de los puntos de acceso
    - Puntos Wireless necesarios y cableado del resto (Fibra o Cat 6)
    - Planificación de las fases de la instalación
    - Planificación de la topología lógica de red para todos los puntos de identificación y el servidor

4. Pedido de material y preparación de equipos:
    - Relación de componentes electrónicos que componen el hardware
    - Adquisición de tarjetas Wireless y puntos de acceso
    - Material para cableado UTP-6

5. Instalación:
    - Instalación de los puntos de identificación
    - Ubicación de la estación de control del sistema con las debidas exigencias de seguridad
    - Instalación de las comunicaciones
    - Instalación y ubicación de los switches necesarios que ampliarán la red ya preinstalada
    - Instalación de los enlaces WIFI

<u>Instalación de nuevos elementos</u>

Cableado UTP Cat 6 para el cableado horizontal de cada planta.
Fibra óptica: para el cableado vertical del edificio, entre plantas y distribuidores y para el cableado entre el edificio principal y los secundarios.

Tecnología Wi-Fi: para la implantación de tecnología Wireless en ciertos puestos de trabajo harán falta los siguientes elementos:

- Para ordenador sobremesa una tarjeta PC Card Wireless (LAN Standard IEEE 802.11g) y si es un portátil, una tarjeta PCMCIA Wireless
- Adaptador Wireless Ethernet o base inalámbrica
- Punto de acceso: elemento que es la estación base que generalmente tiene conectividad con la red cableada Ethernet

3.4. 4ªfase: Renove de servidores y/o plataformas corporativas

Servidores actuales:
Los actuales servidores de los que dispone la Mutua en estos momentos presentan las suficientes características como para aplicar el plan de actualización planteado y por tanto, actualmente no es necesario el renove de los mismos, aunque sí se puede puede plantear para un futuro.

El servidor IBM Netfinity 5500 esta hecho para crecer a medida que crece la organización; posee poder, escalabilidad y control para manejar las diversas aplicaciones. Además, ofrece soporte para SMP de dos procesadores e integra avanzados procesadores Intel.

Lo mismo ocurre con los servidores IBM Netfinity 3000, utilizados únicamente como servidores de impresión. Pero en el caso del Servicio de Prevención, hará falta añadir una unidad de cinta en el servidor para realizar los nuevos Backups.

Plataformas corporativas:
Se realizó un renove de ciertas plataformas corporativas hace un par de años. Respecto a las estaciones de sobremesa, los procesadores que tienen los equios IBM Netfinity son Celerones a 600 Mhz – 766 - 1000 - 1200 y, en menor medida, algún PII a 433 y 466 Mhz.

Respecto a los portátiles, también se realizó un renove, y actualmento son portátiles IBM Thinkpad Pentium III 1133 y Celeron a 1.2 GHz y Toshiba Satelite Celeron 300.

Hace unos meses, a raiz de la implantación de Windows 2000 en las plataformas corporativas, se procedió a ampliar la memoria RAM a 128 Mb o más en aquellos equipos que no la tenían.
Y el disco duro es indiferente, ya que únicamente se utiliza para la instalación cliente de ciertas aplicaciones, sistema operativo, configuración de colas, etc, pero nada que requiera unas características especiales.

3.5. 5ªfase: Formación de los usuarios

3.5.1. Formación de los usuarios

El objetivo de la formación de los usuarios de la organización es el buen uso de los sistemas de información, evaluación de las necesidades, cumplimiento de la política de seguridad, etc. Las acciones formativas se centrarán en varios aspectos, tales como:

- Conocimientos básicos de un ordenador: cpu, monitor, teclado, ratón, conexión de red, etc.
- Introducción a Windows 2000
- Utilización de ficheros, carpetas ...
- Introducción a los paquetes ofimáticos (Microsoft Office) para su correcto manejo
- Introducción a las utilidades y aplicación práctica de internet
- Utilización del correo Lotus Notes
- Configuración de las impresoras

3.5.2. Creación de una FAQ en la Intranet

Las siglas FAQ significan Frequently Asked (o Answered) Questions, preguntas frecuentemente preguntadas o contestadas. Son recopilaciones de información que son generalmente el resultado de ciertas preguntas comúnmente hechas. Están ordenadas por temas, por grupos, etc, y casi todas tienen un formato de preguntas y tipografía**.** No requieren formato, pero sin embargo la FAQ debe ser legíble.
Es altamente recomendable utilizar un formato consistente y fácil de leer. La gramática y la ortografía son también importantes. Una mala gramática puede provocar ambigüedades y hacer difícil, para el usuario, entender lo que se está explicando. Además, el espacio ocupado debe ser mínimo.

Algunos formatos para crear una FAQ son:

formato ASCII plano

estandar de documento html para uso en la World Wide Web

La creación de una faq en la Intranet de la Mutua con las dudas más frecuentes que tienen los usuarios en cuanto al uso de los equipos informáticos, las aplicaciones, etc, es una opción muy acertada, dado el número actual de empleados y la diversidad de los programas utilizados.
La FAQ se podría subdividir en dos grandes bloques:

Dudas de software

Dudas de hardware

En el bloque de dudas de software se podría incluir lo siguiente:
problemas de cambio de contraseña, contraseña de acceso a aplicaciones como Lotus Notes, Intranet, software sanitario ..., renovación de certificados, dudas sobre el uso de aplicaciones Corporativas, etc

Y en el bloque de dudas de hardware:
problemas de conexión física del equipo (corriente, cable de red,...), cambio y/o traslado de periféricos, ...

4. ANÁLISIS DE COSTES

4.1. Costes de hardware

4.1.1. Servidores

Tal y como se ha planteado el plan de actualización de las oficinas de la Mutua, en principio no se hará ningún renove de los servidores.
Respecto a la ampliación de los mismos, en el servidor de dominio principal no se realizará ninguna modificación, en los servidores secundarios tampoco, a excepción del servidor existente en el edificio del Servicio de Prevención, que, además de servidor de impresión, también almacenará ficheros y, por tanto, necesitará una unidad de cinta para realizar los Backups

- Unidad de cinta IBM: Dispositivo de almacenaje de alta densidad. Permite la instalación interna económica. Puede almacenar hasta 40GB de datos en modo nativo y comprimidos hasta 80GB

- Cinta DLT IV IBM

Cinta Backup Servidor IBM Servicio de Prevención	Coste
IBM 40/80 Gb DLTVS80 Type Drive 	1415 €
IBM Cintas BM DLT 4 MEDIA (5 unid) 	230 € * 2 paquetes 460 €
TOTAL	1875 €

4.1.2. Plataformas

Estaciones corporativas IBM Netfinity:
Respecto a la conexión en red, las estaciones de sobremesa no necesitarán ninguna ampliación, ya que se ha optado por un cableado estructurado Categoría 6, y por tanto se pueden aprovechar las actuales tarjetas de red (Ethernet 3 Com) que llevan incorporadas.

Y a nivel del hardware propio de la máquina, tampoco, como bien se ha mencionado; no es necesario renove y/o ampliación de CPU, RAM, HD, etc.

TOTAL	0 €

En el caso de que, excepcionalmente se necesite conectar inalámbricamente alguna estación corporativa Netfinity, se deberá incorporar a la misma un adaptador PCI Wireless:

- **Adaptador PCI sin cables IBM:** El Adaptador PCI sin cables 802.11b de IBM es la solución perfecta para equipos NetVista. Es un producto seguro (con cifrado de 128 bits) y de alta velocidad. El cifrado de 128 bits permite cifrar y descifrar paquetes de datos mientras se envían a través de la red LAN inalámbrica. El adaptador soporta el intercambio dinámico de claves 802.11e que cambia las claves de seguridad de forma aleatoria para aumentar la protección frente al acceso no autorizado a la red LAN.
El adaptador PCI de alta velocidad para redes LAN inalámbricas dispone de la certificación Wi-Fi y es compatible con los puntos de acceso estándar del sector.

Hardware Netfinity	Coste
IBM Adaptador PCI sin cables para LAN de alta velocidad + Software 	220 € * 12 unidades = 2640 €
TOTAL	2640 €

Estaciones corporativas portátiles (IBM o Toshiba):
A nivel de red, los portátiles, al decidirnos por la innovadora tecnología Wireless, precisarán :

- **Adaptador PCMCIA:** El adaptador IBM proporciona la potencia de la informática inalámbrica en los portátiles ThinkPad Serie R40 con tecnología inalámbrica. Se ha sometido a pruebas, se ha certificado su compatibilidad con Wireless Ethernet Compatibility Alliance y está autorizado a mostrar el logotipo Wi-Fi. Proporciona soporte para la seguridad estándar, incluidos el cifrado WEP de 128 bits.

En un principio se comprarán una docena de unidades, y, en función de las necesidades, se irá ampliando esta cantidad.

Hardware portatil	Coste
IBM Adaptador Mini-PCI 2100 3B para LAN inalámbrica/Intel PRO 	133 € * 12 unidades= 1600 €
TOTAL	1600 €

Y respecto a hardware de la estación, no requieren ninguna ampliación adicional.

4.1.3. Cableado

- **Cableado horizontal del edificio: UTP Cat 6 combinado con Wireless y cableado entre repartidores, plantas y edificios: fibra óptica**

La distribución física de los puestos actuales se mantendrá, por tanto no hará falta crear/añadir más rosetas en la pared de las actuales.

Cableado edificio	Coste
Cable de red Categoría 6 UTP 1Gbps (rollo 100m) 	60 € * 16 rollos = 960 €
Cable 8 fibras Fibra óptica interior 	6.38 €/metro * 60 metros = 380 €
Conector ST Multimodo y conector SC Multimodo 	8 € unidad * 20 unidades = 160 €
Conector RJ45 Cat6 	8 € unidad * 600 unidades = 4800
TOTAL	6300 €

4.1.4. Switches, routers, hubs.

- **Punto de acceso inalámbrico**: LAN inalámbrica de clase empresarial para poder acceder a la red desde cualquier lugar de la organización. 3Com Wireless 8250 Access Point crea una LAN inalámbrica que soporta hasta 253 usuarios simultáneos. El 8250 Access Point está diseñado de

"abajo hacia arriba", para servir como una plataforma modular y actualizable para brindar flexibilidad de configuración.

Se distribuye como punto de acceso 802.11g 2.4 GHz, con una sola modalidad de 54-Mbps. A medida que las necesidades aumenten, se podrá agregar soporte 802.11a a este punto de acceso para optimizar su rendimiento. Gracias a sus funciones integradas de seguridad, manejabilidad y confiabilidad es ideal.

Para proteger las comunicaciones y los datos confidenciales en la LAN inalámbrica, ofrece uno de los conjuntos de capacidades de autentificación y encriptación más avanzados y completos. La certificación Wi-Fi asegura interoperabilidad con los productos certificados con Wi-Fi de otros fabricantes.

- Bridge Inalámbrico: Los bridges de LAN Inalámbrica 802.11 de 3Com® permiten conectar redes cableadas e inalámbricas entre sí.

Puede conectar edificios a distancias de hasta 16 kilómetros. El wireless Ethernet bridge nos permite empezar con topologías de tipo punto-a-punto, para a continuación pasar otras de tipo punto-a-multipunto a medida que el crecimiento y las aplicaciones nos lo requieran.

Elementos	Coste
3Com Wireless LAN Access Point 8250 	600 € * 8 unidades = 4800 €
3Com Wireless LAN Building-to-Builiding Bridge 	700 €
TOTAL	5500 €

4.2. Costes de software

4.2.1. Actualización de las aplicaciones

Aplicaciones a actualizar	Coste
Windows 2003 Server	1200 € * 2 servidores = 2400 €
Veritas Backup Exec 9	275 € * 2 servidores = 550 €
Cliente Norton Antivirus Corporate Edition 9	2450 € / 50 licencias
Microsoft Systems Management Server 2003	1300 € / 10 licencias
Microsoft Office 2003	Según Licencia por Volumen de Microsoft

4.2.2. Nuevas aplicaciones y/o utilidades

En un principio no se ha contemplado la incorporación de nuevo software para la Mutua, aunque no se descarta para un futuro.

TOTAL	0 €

BIBLIOGRAFIA

http://www.officeintegra.com.mx/cm2gj/html/cablescat.html

http://www.anixter.es/webaxeuk/ES.nsf/120af576a5ae6145c1256b25007c4ef1/445cfe2a240fbbd4c1256c0c00336402/$FILE/_p95n78sjfchqm6or9k9n20kq3acg42tj1f5gg_.doc

http://www.microsoft.com/Spain

http://www.microsoft.com/spain/servidores/windowsserver2003/evaluation/nt4/default.asp

http://www.microsoft.com/latam/technet/articulos/200005/art21/

http://www.istraining.com.mx/html/upgradeAWin2k3.htm

http://www.microsoft.com/spain/servidores/windowsserver2003/evaluation/nt4/nt4tows2003.asp

http://www.microsoft.com/spain/servidores/windowsserver2003/evaluation/nt4/tools.asp

http://www.pc.ibm.com/la/pymes/Netfinity_5000.pdf

http://catalog.blackbox.com/BlackBox/Templates/blackbox/mainscreen.asp

http://www.abox.com/documentos/wp_ciscointe.pdf

http://www.cablematic.com/

http://www.ibm.com

http://www.ten-informatica.com/precios.php#cables

http://www.cimabox.com/precios/precios.htm#2

http://www.preciomania.com/search_getprod.php/masterid=1617391

http://www.veritas.com/Products/www

http://www.pc-actual.com/Actualidad/Noticias/Infraestructuras/Soluciones/20031120036

http://www.microsoft.com/spain/servidores/smserver/default.asp

http://www.microsoft.com/spain/servidores/windowsserver2003/evaluation/nt4/default.asp

http://www.uap.edu.pe/fac/02/enlaces/manualhtmlegl/inei/Libro-5117.pdf

http://www.expansys.pt/accesory.asp?code=9148R0138U&atype=BLUEACCESS&count=91

CONCLUSIONES

Este proyecto ha intentado plasmar las diferentes opciones y vías con que cuenta la Mutua a la hora de actualizar su sistema informático. Tras estudiar la viabilidad de las diferentes propuestas, se han propuesto soluciones a todos los aspectos planteados.

Como es bien sabido, un plan de actualización informática conlleva la renovación y/o el cambio de los componentes principales de un servicio ya existente a fin de mejorarlo, ya sea porque se encuentre desfasado a causa de su propia antigüedad, o bien porque dé problemas, o porque incumpla las exigencias de la organización en ese momento.

En nuestro caso, se ha planteado esta actualización como consecuencia del incremento de personal y de servicios que ha vivido en los últimos tiempos la propia Mutua. El proceso de adaptación conlleva que el sistema de cableado de ciertas plantas del edificio principal no sea el adecuado para estos cambios, y que sea necesario establecer un programa de formación para los usuarios recién llegados, dado el volumen de personal que se ha alcanzado. También resulta vital proceder a la migración de ciertas aplicaciones para que cada uno de los empleados de la Mutua cuente con los programas necesarios para su desempeño habitual.

Este estudio, obviamente, quiere funcionar como un indicativo de la situación actual y de las posibles alternativas, y su futuro depende, en primer lugar, de su viabilidad técnica, y después de la económica y empresarial. En todo momento se han tenido en cuenta todas las variables y las opciones más aconsejables para una óptima inversión en términos de rentabilidad y economía. En ese sentido, las bases quedan sentadas.