



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES
E INFORMÁTICOS

TEMA:

**“IMPLEMENTACION Y CONFIGURACION DE UNA INTRANET CON
SU RESPECTIVA SEGURIDAD EN EL EDIFICIO DEL CENTRO DE
INVESTIGACION Y DESARROLLO DE LA FUERZA AEREA
ECUATORIANA.”**

Proyecto de pasantía de grado previo a la obtención del Título de Ingeniero en
Sistemas Computacionales e Informáticos.

AUTOR:

Darwin Ivan Chamorro Salazar

TUTOR:

Ing. David Guevara

Ambato – Ecuador

Julio 2007

APROBACIÓN DEL TUTOR

En calidad de tutor del proyecto de pasantía de grado sobre el tema:

“IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA INTRANET CON SU RESPECTIVA SEGURIDAD EN EL NUEVO EDIFICIO DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE LA FUERZA AÉREA ECUATORIANA”, de **Darwin Iván Chamorro Salazar**, estudiante de la Carrera de Ingeniería en sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Universidad Técnica de Ambato, considero que dicho proyecto de pasantía de grado reúne los requisitos y méritos suficientes de conformidad con el artículo 68 del capítulo IV de Pasantía del reglamento de graduación de Pregrado de la Universidad Técnica de Ambato.

Ambato, Julio 2007

Ing. M.Sc. David Guevara

AUTORÍA

El presente trabajo de investigación: “IMPLEMENTACIÓN Y CONFIGURACIÓN DE UNA INTRANET CON SU RESPECTIVA SEGURIDAD EN EL NUEVO EDIFICIO DEL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE LA FUERZA AÉREA ECUATORIANA”. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Julio 2007

Sr. Darwin Iván Chamorro Salazar

C.C. 180336955-0

DEDICATORIA

Quiero dedicar este trabajo que representa, mi último esfuerzo en esta carrera a las personas más importantes de mi vida, Mis padres, quienes con su esfuerzo y cariño han hecho posible este logro, el cual no es mió sino suyo en realidad.

También a mis hermanos por el apoyo que me brindaron durante tantos años de estudio, por su cariño y comprensión, pero sobre todo por haberme ayudado a formarme en lo poco que hoy soy.

AGRADECIMIENTO

A mis padres Napoleón Chamorro y Gladis Salazar por darme la vida y ser la luz que ilumina cada uno de mis días, a mis hermanos por estar siempre conmigo para apoyarme, a mi familia por sus palabras de aliento, a mis amigos quienes han compartido conmigo esta etapa estudiantil y han estado en las buenas y en las malas.

A todos mis profesores en la Facultad quienes han compartido generosamente sus conocimientos en especial al Ing. David Guevara.

A los directivos y empleados del Centro de Investigación y Desarrollo de la FAE quienes hicieron muy grata mi estancia en la institución a lo largo del proyecto.

A las autoridades de la Facultad que supieron abrirme las puertas A todas las personas quienes directa o indirectamente han contribuido en la consecución de esta meta.

Índice

Aprobación del Tutor.....	i
Autoría.....	ii
Dedicatoria.....	iii
Agradecimiento.....	iv
Índice.....	v
Índice de tablas.....	ix
Índice de ilustraciones.....	x
Índice de figuras.....	xi
Resumen Ejecutivo.....	xiii
Introducción.....	xiv

CAPITULO I

GENERALIDADES

1.1 Tema de Investigación.....	1
1.2 Antecedentes.....	1
1.3 Planteamiento del problema.....	3
1.4 Justificación.....	4
1.5 Objetivos.....	5
1.5.1 General.....	5
1.5.2 Específicos.....	6

CAPITULO II

MARCO TEÓRICO

Índice de tablas

Tabla	Página
Tabla 1. Personal CID-DIAF.....	2
Tabla 2. Capas del sistema operativo.....	17
Tabla 3. Información Técnica de Windows 2003 Server.....	18
Tabla 4. Tipos de registros definidos para el árbol.....	29
Tabla 5. Especificaciones técnicas del Servidor HP ProLiant ML350 G5 Server series.....	40
(a) Procesador y memoria.....	40
(b) Almacenamiento.....	40
(a) Destacados.....	41
Tabla 6. Costos del sistema actual.....	52
Tabla 7. Comparativa de los sistemas operativos de red.....	57

Tabla 8: Características de Windows Server 2003.....	66
--	----

Índice de Ilustraciones

Ilustración	Página
Ilustración 1. Organigrama estructural del CID-DIAF.....	3
Ilustración 2: Ejemplo de una red Intranet Extranet.....	22
Ilustración 3: Arquitectura para la Web.....	64
Ilustración 4. Plataforma Computacional.....	65
Ilustración 5: Pagina principal.....	69
Ilustración 6: Página de Acceso a la Intranet.....	69

Índice de Figuras

Figura	Página
Figura 1. Nombre DNS del Servidor.....	72
Figura 2. Nombre NetBios del Servidor.....	73
Figura 3. Dirección IP del DNS del Servidor.....	73
Figura 4. Pantalla de resumen de la configuración DNS.....	74
Figura 5. Crear una nueva interfaz.....	75
Figura 6. Actualización de los Servicios de Ruteo.....	76
Figura 7. Resumen de configuración los Servicios de Ruteo.....	77
Figura 8. Proceso de instalación del Servicio DHCP (1).....	78
Figura 9. Proceso de instalación del Servicio DHCP (2)	79
Figura 10. Registro de información en el Servidor.....	80
Figura 11. Cuadro de resumen de servicios instalados.....	80
Figura 12. Opción de configuración de zonas.....	81
Figura 13. Ventana de DNS Manager.....	81
Figura 14. Asistente para configurar nuevas zonas.....	82
Figura 15. Opción de configuración de tipo de zona.....	82
Figura 16. Ámbito de replicación del DNS.....	83
Figura 17. Nombre de la zona del DNS.....	83
Figura 18. Tipo de actualización de la zona del DNS.....	84
Figura 19. Cuadro de resumen de la configuración de la zona	84
Figura 20. Cuadro de bienvenida de la configuración de la zona inversa.....	85
Figura 21. Dirección IP de la zona Inversa para el DNS.....	85
Figura 22. Cuadro de resumen de la configuración de la zona inversa.....	86
Figura 23. Asistente para agregar servicios en servidor.....	87
Figura 24. Cuadro de propiedades de Documentos.....	89
Figura 25. Consola de administración de servidores de archivos.....	90
Figura 26. Cuadro de propiedades de la impresora.....	91
Figura 27. Creación de carpeta compartida FTP.....	94
Figura 28. Asistente para agregar el servicio FTP.....	94
Figura 29. Proceso de instalación del servicio FTP.....	95
Figura 30. Cuadro de resumen de instalación del servicio FTP.....	95
Figura 31. FTP Manager.....	96
Figura 32. Cuadro de propiedades del contenido WEB.....	97
Figura 33. Consola de comandos para crear un usuario FTP.....	98
Figura 34. Carpetas creadas para el servicio FTP.....	98
Figura 35. Cuadro de Propiedades del Sitio Web.....	99
Figura 36. Opción de añadir remover programas de Windows 2003 Server.....	100
Figura 37. Cuadro de dialogo para añadir servicios a Windows 2003 Server.....	101

Figura 38. Cuadro de selección de componentes.....	101
Figura 39. Proceso de instalación de los servicios IIS.....	102
Figura 40. Instalación exitosa de los servicios IIS.....	102
Figura 41. IIS Manager.....	103
Figura 42. Instalación de Microsoft Exchange Server desde un disco de instalación.....	105
Figura 43. Cuadro de Acuerdo de licencia de Microsoft Exchange Server.....	105
Figura 44. Cuadro de selección de componentes de Microsoft Exchange Server.....	106
Figura 45. Cuadro de Acuerdo de licencia de Microsoft Exchange Server.....	108
Figura 46. Cuadro propiedades de las políticas de correo electrónico.....	109
Figura 47. Opción añadir una nueva cuenta.....	109
Figura 48. Dialogo añadir una nueva cuenta SMTP.....	110
Figura 49. Cuadro de propiedades de Dirección SMTP.....	110
Figura 50. Dialogo modificar una cuenta SMTP existente.....	111
Figura 51. Administrador del sistema de Exchange.....	111
Figura 52. Cuadro de dialogo de las propiedades de almacenamiento del sistema.....	112
Figura 53. Cuadro de resumen de las propiedades de almacenamiento del sistema.....	113
Figura 54. Administrador del sistema de Exchange.....	113
Figura 55. Cuadro de dialogo para creación de una nueva unidad organizativa.....	114
Figura 56. Cuadro de dialogo para creación de un nuevo usuario.....	115
Figura 57. Cuadro de dialogo creación de contraseña para el usuario.....	115
Figura 58. Administrador de Servicios de Windows 2003 Server.....	116
Figura 59. Cuadro de propiedades del servicio POP3.....	117
Figura 60. Proceso para iniciar el servicio POP3.....	118
Figura 61. Tipo de inicio del servicio POP3.....	118
Figura 62. Administrador de servicios de Exchange.....	119
Figura 63. Cuadro de Propiedades del Servidor virtual SMPT.....	119
Figura 64. Cuadro de Propiedades del Servidor virtual SMPT, tipo de autenticación.....	120
Figura 65. Cuadro Asistente para correo de Internet.....	121
Figura 66. Asistente para correo de Internet.....	121
Figura 67. Cuadro de dialogo para añadir el servicio de Firewall.....	122
Figura 68. Instalación exitosa del servicio de Firewall.....	123

Resumen Ejecutivo

El Centro de Investigación y Desarrollo de la FAE se ha visto en la necesidad de optimizar los procesos flujo de información en su edificio central con el objetivo de conseguir mayor productividad de sus empleados así como también de reducir costos en proceso que se hacen manualmente.

La institución cuenta con el respaldo de un sistema de Cableado Estructurado, que no ha sido explotada en todo su potencial, lo que facilita enormemente la realización del presente proyecto

El proyecto de “Implementación y Configuración de una Intranet con su respectiva seguridad en el Nuevo Edificio del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana” esta orientado a cumplir las estas expectativas que tiene la institución

El presente trabajo investigativo destaca las siguientes etapas:

Determinación de los requerimientos, donde se detalla las demandas y exigencias con las que se debe cumplir la intranet se ven reflejadas en el análisis estructurado y en el análisis del sistema se establece las técnicas y procedimientos para satisfacerlos, las cuales son tomadas en cuenta en el diseño del sistema.

La fase de implementación es la más importante puesto que en el transcurso de la misma se deben realizar las pruebas respectivas para verificar la funcionalidad, estabilidad e integridad del proyecto y realizar ajustes respectivos de ser necesario. Finalmente la puesta en marcha y la capacitación que esta orientada específicamente al futuro administrador del sistema.

Introducción

El presente proyecto tiene como objetivo el manejo y optimización de las comunicaciones dentro del centro administrativo de Centro de Investigación y Desarrollo (CID) de la Fuerza Aérea Ecuatoriana, así como el control del flujo de información mediante la implementación de las políticas internas de gestión, las cuales integran:

- Control de Usuarios
- Control de Acceso
- Seguridades

De esta manera, se ha dividido el presente trabajo en los capítulos necesarios, los cuales están enfocados a dar una idea clara del esfuerzo por diseñar e implementar un proyecto de utilidad para el Centro de Investigación y Desarrollo. así tenemos en el primer capítulo un resumen de los antecedentes de la empresa que en principio nos proporciona los lineamientos para la ejecución del proyecto citado, se describen en síntesis, el ambiente de trabajo, los objetivos que persigue la empresa así como su metodología de trabajo.

En el segundo capítulo se exponen ciertos conceptos que van desde los aspectos más generales a lo que es una intranet, pasando por los sistemas operativos de red, conexiones de red, etc.

En el tercer tenemos el Análisis de los requisitos del sistema y el análisis de los datos proporcionados para el diseño del proyecto. El diseño y análisis del mismo se detalla en el cuarto capítulo con el modelamiento del flujo de datos, las especificaciones de dichos datos, etc.

El quinto capítulo está destinado al desarrollo mismo del proyecto y a las pruebas respectivas, a partir de lo cual se obtienen las conclusiones y recomendaciones que serán enunciadas respectivamente en el sexto capítulo.

Además de los anexos se adjunta un apéndice y un glosario de términos que son utilizados en el presente documento y que son necesarios aclararlos a fin de entender ciertos conceptos que representan en el presente proyecto.

De esta manera pongo a su consideración este proyecto y espero que brinde la utilidad y la funcionalidad para la cual fue creado, y porque no llegue a constituirse como una herramienta que brinde a la empresa lineamientos necesarios para un proyecto futuro, además que promover la eficacia, eficiencia y efectividad de los procesos de flujo de información que se desarrollen.

CAPITULO I

GENERALIDADES

1.1 Tema de Investigación

“Implementación y Configuración de una Intranet con su respectiva seguridad en el Nuevo Edificio del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana.”

1.2 Antecedentes de la Institución

La dependencia tecnológica extranjera no permite que los países subdesarrollados tengan un legado trascendente en la creatividad e innovación científica, más todavía cuando asistimos a la impresionante evolución de las grandes potencias, de las cuales dependemos, en cosas que con estudio e ingenio son susceptibles de ser solucionadas con nuestros propios recursos.

Preocupados por este tipo de dependencia tecnológica y conscientes de que el advenimiento de un nuevo siglo implica tomar una actitud frontal en el apoyo a la investigación y desarrollo científico para el engrandecimiento de la Nación, se propone crear el Centro de Investigación y Desarrollo de la FAE, cuya misión, enmarcada dentro de los grandes objetivos institucionales, sea la de dar soluciones a los requerimientos técnicos-operacionales en el menor tiempo posible optimizando los escasos recursos que dispone el País.

1.2.1 Nombre

Ala de Investigación y Desarrollo N° 12 de la Fuerza Aérea Ecuatoriana

1.2.2 Misión

Solventar los requerimientos tecnológicos de la Fuerza Aérea, Fuerzas Armadas y el País, con el fin de disminuir la dependencia tecnológica extranjera, fortalecer el Poder Aeronáutico del País y colaborar con el desarrollo nacional.

1.2.3 Visión

Constituirse en la primera institución militar a nivel del país que desarrolle tecnología aeronáutica enteramente nacional

1.2.4 Diseño de la Institución

1.2.4.1 Situación del Personal del Reparto

Personal CID-DIAF	
Oficiales	9
Aerotécnicos	10
Empleados Civiles	1
TOTAL	20

Tabla 1. Personal CID-DIAF

1.2.4.2 Organigrama Estructural del Centro de Investigación y Desarrollo



Ilustración 1. Organigrama estructural del CID-DIAF

FAE¹

1.3 Planteamiento del Problema

Para el Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana, como en todo centro de investigación del mundo, se ha vuelto imperativo contar con una infraestructura de comunicaciones plenamente desarrollada. Su elemento central lo constituye una Intranet; plataforma indispensable para la Red de Área Local del nuevo edificio del Centro.

1

Esta infraestructura básica permitirá brindar los múltiples servicios de comunicación local y gestión de información a todas las dependencias del Centro, además de permitir su presencia activa en la red mundial Internet.

Se propone un diseño basado en una implementación gradual, pero con posibilidades concretas de expansión no traumática y al mismo tiempo ir brindando los múltiples servicios de datos.

A continuación se va a exponer el proyecto propuesto así como algunos conceptos que aclararán y fundamentan la necesidad de inversión en una infraestructura para redes, y finalmente, una breve descripción del estado actual de la red.

Delimitación

La institución se encuentra ubicada en la ciudad de Latacunga, Provincia de Cotopaxi, denominada Centro de Investigación y Desarrollo perteneciente a la Fuerza Aérea Ecuatoriana, el desarrollo de esta investigación cuenta con el apoyo del departamento de electrónica con el soporte de 2 personas, el departamento de personal con aproximadamente 10 personas, quienes colaboran en la ejecución del proyecto.

El problema esta enfocado a implementar una Intranet en el nuevo edificio con sus respectivas políticas y estándares de tal forma que el trabajo administrativo y lógico del Centro de Investigación y Desarrollo sea optimizado, resultando en beneficios directos para la institución tanto en el aspecto económico como en el aspecto laboral.

1.4 Justificación

Para el CID, la intranet va ha ser un recurso indispensable, dada la gran cantidad de datos que genera.

La meta del CID es implementar la Intranet con todos los servicios y facilidades que la misma ofrece en el nuevo edificio administrativo creado para el efecto para lo cual se da por entendido que esta ya implementado el cableado estructurado; tomando en cuenta la misma distribución de los departamentos y las políticas y estándares debidamente documentadas en su tiempo.

Esta Intranet puede resolver, el problema de la distribución de información para todos los empleados, así pues se pueden publicar manuales, planes de acción, procedimientos, material de formación, listas de precios, información comercial, anuncios, etc. Y son accesibles para el empleado de forma inmediata, y con un ahorro considerable respecto a los métodos clásicos, panfletos, circulares, notas informativas, etc. Además cualquier actualización de datos es inmediata y no supone ninguna carga para el CID como los métodos tradicionales.

Se necesita también aprovechar la potencia de una intranet para tener acceso rápido a cualquier documento de la empresa, siempre que se tenga el nivel de privilegios adecuado. Además de la seguridad. Solo tendrán acceso a los recursos aquellos empleados que lo necesiten realmente. Siguiendo con la potencia y velocidad de acceso a datos de una intranet, el tiempo empleado en realizar cualquier búsqueda de datos de cualquier departamento de la empresa se reduce considerablemente, por lo que la productividad del CID mejora.

1.5 Objetivos

1.5.1 General

Implementar una Intranet para el nuevo edificio del Centro de Investigación y Desarrollo de la FAE.

1.5.2 Específicos

- Analizar la situación actual para conocer los requerimientos que conlleva a la construcción de este proyecto.
- Diseñar la Intranet basada en los requerimientos de cableado estructurados y sus normas.
- Evaluar las soluciones elegidas desde el punto de vista de la seguridad
- Conseguir una comunicación interna fluida sin duplicidad de mensajes ni distorsiones, con eficacia y con un ahorro de tiempo ejemplar.
- Minimizar costos administrativos.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes Investigativos

Las fuentes bibliográficas de la facultad y la ciudad no ofrece información actualizada acerca de las últimas tecnologías disponibles para intranets en entornos reales, puesto que, la tecnología informática y de comunicaciones avanza a una velocidad impresionante, tal es el caso que en este momento se habla de casas y ciudades inteligentes administradas en un dispositivo central.

Actualmente en Ecuador existen muchas empresas proveedoras de soluciones intranets para empresas, instituciones públicas e instituciones educativas, como por ejemplo:

Expertweb (<http://www.expertweb.com.ec>): que se especializa en el desarrollo e integración de sistemas con tecnología web.

Pupila::box: (<http://pupilabox.net.ec/>): que es un grupo de desarrolladores informáticos especializados en la rama de Internet y de desarrollo de soluciones tecnológicas basadas en software libre.

Ocitel. S. A. (<http://www.ocitel.net/>): que es una empresa especializada en el desarrollo de sitios web, montaje y configuración de servicios de acceso a Internet, capaz de brindar la asesoría y el soporte que las empresas requieren al mejor precio y proveer los servicios y equipos necesarios para que el aprovechamiento del acceso a Internet sea eficiente y adecuado.

Dichas empresas trabajan bajo normas y estándares propios y con materiales instrumentos y dispositivos propios, que en otras palabras quiere decir que no pueden hacer uso de los recursos existentes o previamente adquiridos por el cliente, sin contar que requieren una inversión económica considerable. Por lo que la mejor opción es crear una solución que utilice los recursos existentes en la institución militar sea de menor coste y tenga el desempeño esperado.

2.2 Fundamentación Legal

El Ala de Investigación y Desarrollo N° 12 de la Fuerza Aérea Ecuatoriana, acantonada en Latacunga, Provincia de Cotopaxi, inició su funcionamiento como tal el 1 de enero de 1988, mediante decreto N° 5, publicado en el Registro Oficial reservado N° 323-S, del 3 de agosto de 1997, en el que se establece la nueva organización del reparto.

En las áreas de aplicación que serán tratadas en el CID-FAE, se han considerado únicamente las que se consideran esenciales dentro del contexto de la Fuerza Aérea, dejando abierto el incremento de otras, de acuerdo a la proyección que vaya adquiriendo el Centro. A pesar de haber establecido subdivisiones en diferentes áreas, estas se interrelacionan y complementan unas con otras, debido a la naturaleza interdisciplinaria de los proyectos lo cual hace difícil tratarlas en forma individual.

▪ Situación del personal

a) **ÁREA AERONÁUTICA:**

1) **AERODINAMICA**

Diseño.

Comportamiento.

Modificaciones.

Flujo (Subsónico, Transónico, Supersónico).

2) ESTRUCTURAS

Diseño

Análisis

Reparaciones mayores y menores

Asesoría

3) INGENIERIA.

Diseño de sistemas hidráulicos

Construcción.

Tratamientos térmicos

Mecanismos

4) MATERIALES COMPUESTOS

Diseño en fibra de vidrio, kevlar, carbono y honey comb.

Reparaciones de planos de vuelo de aviones supersónicos.

Modificaciones.

Fibras y Resinas.

5) PROPULSION

Optimización.

Hélices.

6) PERFORMANCES, ESTABILIDAD Y CONTROL

Estudio de performances de aeronaves.

Determinación de vuelos de prueba.

Determinación de maniobrabilidad de aeronaves.

Control de aeronaves y misiles.

7) ADQUISICIÓN DE DATOS

Análisis de datos aerodinámicos.

Comportamiento en tiempo real.

b) **ÁREA ELECTRÓNICA:**

1) **GUERRA ELECTRÓNICA**

Inteligencia de señales

Medidas electrónicas de apoyo

Contra medidas electrónicas (ECM)

Contra contramedidas electrónicas (ECCM).

2) **CONTROL**

Guiado y navegación.

Sensores y actuadores.

Armamento.

3) **COMUNICACIONES**

Electromagnetismo y antenas,

Sistemas Satelitales,

Radio enlaces (HWF, VHF, UHF, Microondas),

Telefonía,

Redes Digitales,

Sistema Celular,

Fibra Óptica.

4) **SISTEMAS ELECTRONICOS:**

Sistemas Digitales

Procesamiento Digital Señales.

Computación

Opto-electrónica

Instrumentación

Aviónica

Electrónica de Potencia.

c) **ÁREA DE ARMAMENTO**

1) SISTEMAS DE ARMAMENTO

Sistemas de armamento

Sistemas de escape

Misiles.

Equipos de apoyo.

2) MATERIAL BÉLICO

Bombas

Espoletas

Modificaciones material convencional.

Diseños

3) MANTENIMIENTO MAYOR

Cañones

Director de tiro

Armamento terrestre

4) EXPLOSIVOS Y MUNICIONES

Cargas militares

Propelentes

El Control de Calidad esta implícito en todas las áreas.

2.2.2. Relación de dependencia del CID

El CID estará directamente subordinado al Jefe de Estado Mayor de la FAE.

2.2.3. Organización del Sistema Informático

El sistema informático esta organizado de la siguiente manera:

Dirección:

Director: 1 Computador

Secretaria: 1 Computador

Aeronáutica:

Investigación: 2 Computadores

Proyectos: 3 Computadores

Aviónica:

Servidor: 1 SERVIDOR

Investigación: 3 Computadores

Proyectos: 3 Computadores

Electrónica:

Circuitos: 2 Computadores

Diseño: 1 Computador

Estructuras: 1 Computador

Bodega:

Inventario: No tiene computador

Talleres:

Control: 1 computador

En total son 19 equipos de computación de los cuales 17 están conectados en red (grupo de trabajo) mediante una red LAN ETHERNET clase C, para lo que se utiliza un Switch Marca DLink de 24 puertos, a excepción del computador de Talleres.

No existe un departamento de Informática que se encargue de la administración de la Red ni del soporte para el equipo informático.

Además en un departamento no apropiado se encuentra el equipo SERVIDOR con las siguientes características:

Servidor ProLiant ML350 Generation 3 de HP

Procesador: Xeon

Disco Duro: 2 HDD Seagate 70 Gb, Serial Ata, 7.200 rpm

Memoria Ram: 1 DDR Kingstom de 1Gb

DVD Rom HP

Monitor HP

Puerto Frontal USB 2.0

Sistema Operativo: Windows 2003 Server Entrerprice

El cual actualmente esta siendo utilizado para compartir el servicio de Internet ADSL de 512/256 de Velocidad contratado con la Empresa ANDINANET.

2.3 Categorías Fundamentales

Sistema

“Un conjunto de entidades caracterizadas por ciertos atributos, que tienen relaciones entre sí y están localizadas en un cierto ambiente, de acuerdo con un cierto objetivo”.

Un **sistema informático** es la síntesis de hardware y software. Un sistema informático típico emplea un ordenador que usa dispositivos programables para almacenar, recuperar y procesar datos. El ordenador personal o PC resulta de por sí un ejemplo de un sistema informático.

Muchos sistemas informáticos pueden interconectarse, esto es, unirse para convertirse un sistema mayor. El interconexionado de sistemas informáticos puede tornarse dificultoso debido a las incompatibilidades.

Sistema operativo

Un **sistema operativo** (SO) es un conjunto de programas destinados a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera eficiente. Comienza a trabajar cuando se enciende el ordenador, y gestiona el hardware de la máquina desde los niveles más básicos.

Un sistema operativo se puede encontrar normalmente en la mayoría de los aparatos electrónicos que podamos utilizar y que utilicen microprocesadores para funcionar, ya que gracias a estos podemos entender la máquina y que ésta cumpla con sus funciones (teléfonos móviles, reproductores de DVD, autoradios... y computadoras)

•Funciones Básicas

Los sistemas operativos, motivados por su condición de capa software que posibilita y simplifica el manejo de la computadora, desempeñan una serie de funciones básicas esenciales para la gestión de la máquina. Entre las más destacables, cada una ejercida por un componente interno (módulo en núcleos monolíticos y servidor en microkernels), podemos reseñar las siguientes:

1. Gestionar los recursos de la máquina ejecutando servicios para los procesos (programas)
2. Brindar una interfaz al usuario, ejecutando instrucciones (comandos).

•Componentes

- Gestión de procesos.
- Gestión de memoria.
- Gestión de archivos y directorios.
- Gestión de la E/S (Entrada/Salida).
- Seguridad y protección.
- Comunicación y sincronización entre procesos.
- Intérprete de órdenes

•Características

- Administración de tareas:
 - o Monotarea: Si solamente puede ejecutar un proceso en un momento dado. Una vez que empieza a ejecutar un proceso, continuará haciéndolo hasta su finalización o interrupción.
 - o Multitarea: Si es capaz de ejecutar varios procesos al mismo tiempo. Este tipo de S.O. normalmente asigna los recursos disponibles (CPU, memoria, periféricos) de forma alternativa a los procesos que los solicitan.

- Administración de usuarios:
 - o Monousuario: Si sólo permite ejecutar los programas de un usuario al mismo tiempo.
 - o Multiusuario: Si permite que varios usuarios ejecuten simultáneamente sus programas, accediendo a la vez a los recursos del ordenador.

- Manejo de recursos:
 - o Centralizado: Si permite utilizar los recursos de un solo ordenador.
 - o Distribuido: Si permite utilizar los de más de un ordenador al mismo tiempo.

Estructura de un sistema operativo

Estructura modular.

También llamados sistemas monolíticos. Este tipo de organización es la más común. No existe estructura alguna. El sistema operativo se escribe como una colección de procedimientos, cada uno de los cuales puede llamar a los demás cada vez que así lo requiera. Cuando se usa esta técnica, cada procedimiento del sistema tiene una interfaz bien definida en términos de parámetros y resultados y cada uno de ellos es libre de llamar a cualquier otro, si este último proporciona cierto cálculo útil para el primero. Sin embargo incluso en este tipo de sistemas es posible tener al menos algo de estructura. Los servicios (llamadas al sistema) que proporciona el sistema operativo se solicitan colocando los parámetros en lugares bien definidos, como en los registros o en la pila, para después ejecutar una instrucción especial de trampa de nombre “llamada al núcleo” o “llamada al supervisor”.

Esta organización sugiere una organización básica del sistema operativo:

- 1.- Un programa principal que llama al procedimiento del servicio solicitado.
- 2.- Un conjunto de procedimientos de servicio que llevan a cabo las llamadas al sistema.
- 3.- Un conjunto de procedimientos utilitarios que ayudan al procedimiento de servicio.

Estructura por microkernel.

Las funciones centrales de un SO son controladas por el núcleo (kernel) mientras que la interfaz del usuario es controlada por el entorno (shell). Por ejemplo, la parte más importante del DOS es un programa con el nombre "COMMAND.COM" Este programa tiene dos partes. El kernel, que se mantiene en memoria en todo momento, contiene el código máquina de bajo nivel para manejar la administración de hardware para otros programas que necesitan estos servicios, y para la segunda parte del COMMAND.COM el shell, el cual es el interprete de comandos.

Estructura por anillos concéntricos (capas).

El sistema por “capas” consiste en organizar el sistema operativo como una jerarquía de capas, cada una construida sobre la inmediata inferior. El primer sistema construido de esta manera fue el sistema THE (Technische Hogeschool Eindhoven), desarrollado en Holanda por E. W. Dijkstra (1968).

El sistema tenía 6 capas. La capa 0 trabaja con la asignación del procesador y alterna entre los procesos cuando ocurren las interrupciones o expiran los cronómetros. Sobre la capa 0, el sistema consta de procesos secuenciales, cada uno de los cuales se podría programar sin importar que varios procesos estuvieran ejecutándose en el mismo procesador, la capa 0 proporcionaba la multiprogramación básica de la CPU.

5	El operador
4	Programas del usuario
3	Control de entrada/salida
2	Comunicación operador-proceso
1	Administración de la memoria y del disco
0	Asignación del procesador y multiprogramación

Tabla 2. Capas del sistema operativo

Estructura cliente – servidor.

En este modelo, lo único que hace el núcleo es controlar la comunicación entre los clientes y los servidores. Al separar el sistema operativo en partes, cada una de ellas controla una faceta del sistema, como el servicio a archivos, servicios a procesos, servicio a terminales o servicio a la memoria, cada parte es pequeña y controlable. Además como todos los servidores se ejecutan como procesos en modo usuario y no en modo núcleo, no tienen acceso directo al hardware. En consecuencia si hay un error en el servidor de archivos, éste puede fallar, pero esto no afectará en general a toda la máquina.

Sistemas operativos de red.

La principal función de un sistema operativo de red es ofrecer un mecanismo para transferir archivos de una máquina a otra. En este entorno, cada instalación mantiene su propio sistema de archivos local y si un usuario de la instalación A quiere acceder a un archivo en la instalación B, hay que copiar explícitamente el archivo de una instalación a otra.

Internet proporciona un mecanismo para estas transferencias, a través del programa protocolo de transferencias de archivos FTP (File Transfer Protocol).

Los Sistemas Operativos de red son aquellos sistemas que mantienen a dos o más computadoras unidas a través de algún medio de comunicación

(físico o no), con el objetivo primordial de poder compartir los diferentes recursos y la información del sistema.

El primer Sistema Operativo de red estaba enfocado a equipos con un procesador Motorola 68000, pasando posteriormente a procesadores Intel como Novell Netware.

Los Sistemas Operativos de red más ampliamente usados son: Novell Netware, Personal Netware, LAN Manager, Windows NT Server, UNIX, LANtastic.

Windows Server 2003

Windows Server 2003	
Pantalla de inicio	
<i>Desarrollador</i>	Microsoft
<i>Familia de S.O.</i>	Windows NT
<i>Modelo de desarrollo</i>	Software propietario
<i>Núcleo</i>	NT
<i>Tipo de núcleo</i>	Híbrido
<i>Licencia</i>	Microsoft CLUF (EULA)
<i>Última versión estable</i>	R2 / 6 de diciembre de 2005
<i>Estado actual</i>	En desarrollo
<i>Sitio web</i>	Web Windows Server 2003

Tabla 3. Información Técnica de Windows Server 2003

Windows Server 2003 es la versión de [Windows](#) para [servidores](#) lanzada por [Microsoft](#) en el año [2003](#). Está basada en el núcleo de [Windows XP](#), al que se le han añadido una serie de servicios, y se le han bloqueado algunas características. En términos generales, Windows Server 2003 es un Windows XP simplificado, no con menos funciones, sino que estas están deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor.

Características

Sus características más importantes son:

Sistema de archivos NTFS:

Cuotas

Encriptación y compresión de archivos, carpetas y unidades completas.

Permite montar dispositivos de almacenamiento sobre sistemas de archivos de otros dispositivos al estilo unix

Gestión de almacenamiento, backups: incluye gestión jerárquica del almacenamiento, consiste en utilizar un algoritmo de cache para pasar los datos menos usados de discos duros a medios ópticos o similares más lentos, y volverlos a leer a disco duro cuando se necesitan.

Windows Driver Model: Implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware

ActiveDirectory Directorio de organización basado en [LDAP](#), permite gestionar de forma centralizada la seguridad de una red corporativa a nivel local.

Autenticación Kerberos5

DNS con registro de IP's dinámicamente

Políticas de seguridad

Servidores

Los servidores que maneja Windows 2003 son:

Servidor de [archivos](#)

Servidor de impresión

Servidor de aplicaciones

Servidor de [correo](#) ([SMTP/POP](#))

Servidor de terminal

Servidor de [Redes privadas virtuales \(VPN\)](#) (o acceso remoto al servidor)

Controlador de Dominios (mediante [Active Directory](#))

Servidor [DNS](#)

Servidor [DHCP](#)

Servidor de [Streaming](#) de [Video](#)

Servidor [WINS](#)

Mejoras en el manejo de políticas de seguridad

[Active Directory](#) ya no utiliza NetBIOS sino que es necesaria la presencia de un [DNS](#) que soporte Service Records (detección de servicios ofrecidos por una máquina a través de un [DNS](#))

Versiones

Actualmente existen cuatro versiones de Windows 2003. Las versiones son:

Web Edition Diseñado para los servicios y el hospedaje Web.

Standard Edition El más versátil de todos, ofrece un gran número de servicios útiles para empresas de cualquier tamaño.

Enterprise Edition Para empresas de mayor tamaño que la Standard Edition.

Datacenter Edition Para empresas que requieran bases de datos más escalables y un procesamiento de transacciones de gran volumen.

Intranet

Uno de los mayores problemas de la gestión de la información interna de las empresas es la variedad de plataformas y sistemas informáticos existentes en cualquier organización, y los problemas para compartir información entre ellos. Una de las grandes ventajas de Internet, que explica su éxito internacional es que da cabida a todo tipo de equipos,

(mac, pc, unix, vax, etc.) fabricantes, redes, tecnologías y medios físicos de transmisión. Con estas premisas, una idea muy interesante es utilizar las tecnologías de Internet dentro de una organización. En ello se basan las llamadas Intranet, es decir, se aprovechan de las herramientas de Internet para su utilización interna dentro de las redes corporativas de la empresa.

El WWW

Al igual que en Internet, la pieza clave de la Intranet es el World Wide Web, pero de forma que la información de la empresa esté accesible sólo a los miembros de la organización, quienes, en consecuencia disponen de navegadores WWW para acceder a los datos internos de la empresa.

En las Intranet también se utiliza correo electrónico, aunque este es interno, es decir, sin necesidad de tener acceso a Internet.

Igualmente se utilizan el resto de herramientas de Internet: listas de distribución, boletines de noticias, transferencia de ficheros, acceso remoto, charlas interactivas, videoconferencia...

Push y Pull

La información puede hacerse llegar al usuario de diferentes formas. Se habla de tecnologías push y pull. Con el correo electrónico, la información se "empuja" (push) al destinatario, que es pasivo. En el navegador o en los boletines de anuncios, los interesados succionan (pull) la información del sistema. El usuario es activo

Un ejemplo

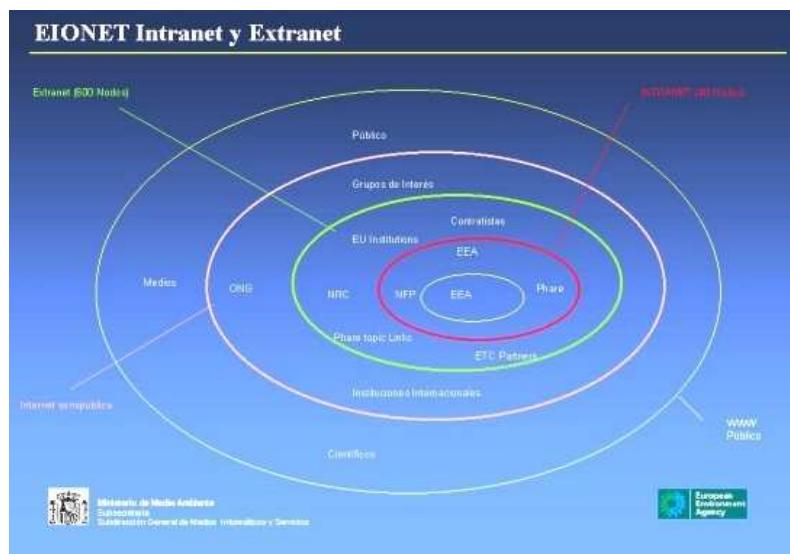


Ilustración 2. Ejemplo de una red Intranet Extranet

Esta red debe cumplir varios objetivos:

1. Permitir análisis integrado del estado del medio ambiente y cumplimiento de directivas de información.
2. Coordinación de proyectos.
3. Conectar a suministradores de datos y clientes.
4. Acceso público a documentos medioambientales y bases de datos.
5. Medio de coordinación de iniciativas internacionales y nacionales.

Parte pública

Acceso público a la mejor información disponible. Bases de datos en línea

Intranet

Red Virtual Privada. Permitir análisis integrado del estado del medioambiente y directivas de información.

Permitir puntos de encuentro y decisión.

Preparación conjunta de publicaciones.

Extranet

Permite acomodar nuevos miembros con flexibilidad.

Conecta con proveedores y clientes. Permitir análisis integrado del estado del medioambiente y el cumplimiento de las directivas de "reporting".

Conectar a los proveedores de información.

Conectar a los clientes. Permitir acceso a bases de datos.

Factores que influyen en el establecimiento de una Intranet

Los factores que influyen poderosamente en el establecimiento de una Intranet pueden resumirse como sigue:

1. Coste asequible, tanto de su puesta en marcha como de uso. Es una forma muy eficiente y económica de distribuir la información interna, sustituyendo los medios clásicos. Reduce los costes de distribución de información interna, sustituyendo los medios clásicos.
2. Fácil adaptación y configuración a la infraestructura tecnológica de la organización, así como gestión y manipulación. Disponible en todas las plataformas informáticas.
3. Adaptación a las necesidades de diferentes niveles: empresa, departamento, área de negocio, etc. Centraliza el acceso a la información actualizada de la organización, al mismo tiempo que puede servir para organizar y acceder a información de la competencia dispuesta en Internet.
4. Sencilla integración de multimedia.
5. Posibilidad de integración con las bases de datos internas de la organización.
6. Rápida formación del personal.
7. Acceso a la Internet, tanto al exterior, como al interior, por parte de usuarios registrados con control de acceso.
8. Utilización de estándares públicos y abiertos, independientes de empresas externas, como pueda ser TCP/IP o HTML.

¿Qué información compartir en la Intranet?

Las experiencias de Intranet realizadas en diferentes organizaciones revelan que los contenidos informativos accesibles a través de los mismos responden, en general, a los siguientes bloques:

- 1) Acceso a directorios internos: búsqueda de teléfonos, direcciones, agendas, programaciones, etc.
- 2) Acceso a las bases de datos de la empresa.
- 3) Publicación de documentos internos: informes económicos, listas de precios, publicaciones y manuales de producto, etc. Distribución de aplicaciones.
- 4) Creación de aplicaciones sencillas de trabajo en equipo.

A. Uso en las funciones empresariales

Sin pretender ser exhaustivos a continuación exponemos algunas aplicaciones de la Intranet en diversos departamentos de la empresa.

Contabilidad

Mediante una intranet se pueden integrar las funciones contables y financieras del día a día.

- A. **Capturar datos contables** Determinados programas de contabilidad utilizan el navegador para esta función.
- B. Medio para que la información contable esté disponible para los usuarios internos, satisfaciendo el requisito de oportunidad.
- C. Dar a conocer las políticas contables de la empresa
- D. Informar sobre clientes que presentan problemas y estado de pagos.

Marketing

Mediante una intranet se puede informar al personal de ventas e incluso puede ser una forma de interactuar.

- Información sobre productos, precios, promociones, etc.

- Información de disponibilidad de producto y plazos de entrega.
- Servicio postventa para los clientes. En este caso vía extranet.

Recursos Humanos

- Publicación de boletines, foros, eventos, etc.
- Tramitación de documentos como curriculum, roles, etc.
- Canalizar información confidencial
- Formación en la empresa vía Intranet

Producción

- Compartir archivos, planos, documentos
- Documentación y control de los procesos de trabajo
- Posibilidad de integrar herramientas de trabajo en grupo

Seguridad

- Confidencialidad. Garantizar que los datos no sean comunicados incorrectamente.
- Integridad. Proteger los datos para evitar cambios no autorizados.
- Autenticación. Tener confianza en la identidad de usuarios.
- Verificación. Comprobar que los mecanismos de seguridad están correctamente implementados.

Disponibilidad. Garantizar que los recursos estén disponibles cuando se necesiten.

Cortafuegos

La tecnología más habitual es emplear un cortafuegos, o firewall que **permite controlar el acceso de usuarios a ciertas zonas de una red.** Generalmente los cortafuegos se interponen entre el servidor de WWW (que es público y, por tanto, no está protegido) y la red interna, que debe

ser confidencial. Estos cortafuegos actúan como una pared de seguridad de la intranet y puede hacerse de diversas maneras.

Problema: Aunque una INTRANET sea una red privada en la que se tengan grupos bien definidos y limitados ésta no se encuentra exenta de ataques que pudiesen poner en riesgo la información que maneja, ya que la mayoría de éstos son provocados por sus mismos usuarios.

Antecedentes: La mayoría de las estadísticas de seguridad en cómputo indican que cerca del 80% de los fraudes relacionados con las computadoras provienen de los usuarios internos, por esto las intranets son las más vulnerables a ataques de ésta índole.

Según el CSI (Computer Security Institute) el 90 % de las empresas entrevistadas detectaron ataques a sus computadoras, el 70 % reporto que los más comunes fueron virus, robo de laptops y ataques de abuso de la red de sus empleados.

Modelo de Solución:

- o Políticas de Seguridad
- o Control de Acceso
- o Transacciones Seguras
- o Virus
- o Cantidad de Seguridad a Implementar
- o Políticas de Seguridad

¿Qué son las políticas de seguridad?

Políticas de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos tanto de usuarios como administradores, describe lo que se va a proteger y de lo que se esta tratando de proteger,

éstos documentos son el primer paso en la construcción de Firewalls efectivos.

Extranet

La Extranet consiste en permitir que personas ajenas a la empresa, como nuestros clientes o proveedores puedan acceder a parte de la Intranet de la organización. Es decir, técnicamente se trata de que el cortafuegos permita también el acceso a usuarios externos, lo que complica los aspectos relativos a la seguridad.

Naturalmente, no tienen acceso a todos los directorios o documentos sino sólo a partes concretas, por ejemplo, se les puede permitir acceso a información sobre los productos y precios.

Colaboración.

Desde el punto de vista de la gestión empresarial se pueden enmarcar las Extranet en el **nuevo contexto el que se contemplan las transacciones en las empresas, que implica integrar a los clientes y proveedores en la cadena de producción**, estableciendo más asociaciones con ellos, y que implica un mayor intercambio de información. Además demandan información oportuna -en tiempo real, a ser posible- y fiable -tomada de la fuente de donde surge-. Este marco de negocios, más propicio a la colaboración, arranca de conceptos bien establecidos como el Just in Time, mediante el cual los proveedores tienen que estar sincronizados con los clientes para que los pedidos estén siempre a tiempo.

¿Qué información incluir?

Tenemos que posicionarnos en un sector concreto -un banco, una institución pública - y plantearnos las siguientes preguntas: a los clientes y proveedores.

- ¿Qué información podría interesarles?
- ¿Puedo dársela?
- En definitiva: ¿Qué necesidades de información tratan de satisfacer las Intranet?

Algo básico que casi todas las Extranet incluyen es información sobre los productos, las tarifas, condiciones comerciales y promociones.

Servicios a configurar:

El Domain Name System (DNS)

DNS es una base de datos distribuida que traduce los nombres de los hosts a direcciones IP y viceversa. Es también un mecanismo estándar en Internet para el almacenamiento de muchos otros tipos de información sobre los hosts, por ejemplo si un host no puede recibir mail directamente, y se hace cargo otro host, esta información es comunicada con un registro MX en el DNS

Existen varias características de los DNS que los determina como un factor decisivo: Packet Filtering, Proxying, los datos que contiene y los problemas de seguridad.

Packet Filtering: Existen dos tipos de actividades que realiza un DNS: lookups y zonas de transferencia. Los Lookups ocurren cuando un cliente del DNS le consulta información: por ejemplo, la dirección IP de un nombre de host dado o el mail Exchange para un host dado. Las zonas de transferencia ocurren cuando un servidor de DNS requiere del servidor primario toda la información que posea acerca de una parte dada del árbol de nombres del DNS (la zona). Este tipo de transferencia ocurre solamente entre servidores que proveen la misma información.

Características de Proxying de un DNS.

El DNS esta estructurado de tal manera que los servidores actúan siempre como proxies para los clientes. También es posible usar un “feature” llamado forwarding de manera tal que el DNS Server es efectivamente un Proxy para otro Server.

Existen varios tipos definidos de tipos de registros definidos para el árbol, entre los cuales podemos destacar:

Tipo de registro	Uso:
A	Traduce un nombre de host (hostname) en un a dirección IP.
PTR	Traduce una dirección IP en un nombre de host (hostname).
CNAME	Traduce el alias de un host a su hostname (nombre “canónico”).
NS	Delega una zona del árbol del DNS a algún otro Server.
SOA	Denota “Start Of Authority” para una zona de un árbol de DNS.
TXT	Registros no-estructurados de texto.

Tabla 4. Tipos de registros definidos para el árbol DNS

De hecho existen 2 árboles de datos del DNS: uno para obtener información vía hostname (como es la dirección de IP, el registro CNAME, el registro HINFO o el registro TXT que corresponde a un hostname dado), y uno para obtener información a través de dirección IP dada (el hostname).

Problemas de seguridad del DNS.

Respuestas falsas a consultas de DNS (Bogus answers): El primer problema de seguridad con el DNS es que muchos servidores y clientes pueden ser afectados por el ataque de un hacker haciéndoles creer información falsa. Esto se debe a que muchos clientes y servidores no verifican que todas las respuestas que obtienen están relacionadas con una

pregunta que realmente haya realizado, o bien si las respuestas que obtienen están siendo recibidas del servidor al cual fueron formuladas. Los servidores en particular, pueden “cachear” estas respuestas falsas si que sean verificadas y responder a su vez consultas con esta información falsa que se encuentra cacheada.

Esta falta de chequeo de los servidores puede permitir a los atacantes dar información falsa a los clientes y servidores. Por ejemplo, un hacker podría usar esta capacidad para cargar la cache del Server con información que dice que su dirección de IP mapea a un hostname de un host “confiable” para acceso sin password vía login.

Configuración del DNS para ocultar información interna.

La capacidad de forwarding de un DNS Server nos permite armar un esquema en el cual es posible brindar a los hosts internos una visión irrestricta de los datos internos y externos del DNS, y al mismo tiempo restringir una muy limitada visión de la información interna desde el exterior. Entre varios factores, existen 2 por los cuales este tipo de configuración es necesaria:

- Evitar el acceso externo a información acerca de los hosts internos
- Porque se desea proveer de cierta información a los hosts externos y otra información diferente a los hosts internos (por ejemplo, se desea que los host internos envíen mail directamente a hosts internos y los mails que se reciben de hosts externos sean tratados de manera diferente -manejados por otro servidor, por ejemplo-).

La primera etapa para llevar a cabo la ocultación de información interna del DNS configurar n DNS Server que se encargue de resolver el acceso

externo y establecer allí que información se desea, pueda ser accedida externamente. Dicho servidor es establecido como authoritative para nuestro dominio. Luego debemos establecerlo como el servidor para nuestro dominio que es nombrado en los registros del Name Server mantenidos por el dominio padre.

La información que contendrá este servidor acerca de nuestro dominio será aquella que se desee revelar al exterior. Esta información incluye información de IP básica sobre los siguientes hosts:

- Las máquinas que se encuentran en el perímetro de la red (las que constituyen el firewall).
- Cualquier máquina que deba ser contactada directamente por alguien desde fuera de nuestro dominio. Se necesitará además publicar los registros MX para cualquier host o nombres del dominio que sean utilizados como parte de direcciones de email en mensajes de email y Usenet Eventualmente puede publicarse información falsa para cualquiera de las máquinas que deban ser contactadas externamente en forma directa.
- Sin embargo, si se utiliza exclusivamente proxying para conectar hosts internos con el resto del mundo, simplemente necesita incluir en la información del DNS sobre el /los hosts que están corriendo un proxy Server, El resto del mundo podrá conocer solamente las direcciones las direcciones de los servidores proxy y nada más.

Configuración de un DNS para uso interno.

Las computadoras internas necesitan utilizar información verdadera acerca del dominio en el cual funcionan, y no la información falsa que pueda darse a conocer a través de un DNS que atiende las necesidades de interacción el resto del mundo. Esto se realiza a través de un servidor de DNS estándar funcionando en algún host interno. Las máquinas internas

pueden necesitar averiguar sobre una dirección externa o bien traducir el hostname de un servidor remoto de FTP a una dirección de IP.

La primera posibilidad de lograr esto es permitiendo el acceso a información de DNS externa configurando el DNS interno para que consulte a un servidor de DNS remoto para resolver las consultas de las maquinas internas sobre direcciones externas- Tal configuración no obstante, requiere abrir cualquier filtrado de paquetes para permitir que el DNS interno pueda establecer contacto e intercambiar información (-se trata de un intercambio basado en UDP-) con un DNS externo.

Correo electrónico

El servicio de correo electrónico es actualmente, en conjunto con el de acceso a Web sites, el servicio fundamental en Internet. Los objetivos en cuanto al uso de este servicio incluyen la posibilidad de enviar y recibir mail entre la red e Internet y también disponer de alguna forma de correo corporativo.

Hay varias alternativas en cuanto a los sistemas de mail corporativo, que van desde soluciones propietarias (CC Mail, Microsoft Mail, Microsoft Exchange) a sistemas con tecnología de Internet. Aunque existen gateways entre los sistemas propietarios y el correo de Internet es razonable utilizar, con el ánimo de simplificar la administración y de no mediar otras restricciones, la misma tecnología tanto para el correo corporativo como para el de Internet.

SMTP – POP3.

El Simple Mail Transfer Protocol usado para intercambiar mail entre mail servers. Básicamente, un servidor SMTP acepta mail y decide basándose en la dirección de retorno si debe entregarlo localmente o si debe forwardearlo a otro host. SMTP es un sistema 'store-and-forward', particularmente adaptado al funcionamiento en un firewall (todo servidor SMTP funciona como proxy).

El Post Office Protocol se utiliza entre clientes y servidores (a diferencia del SMTP, usado entre servidores) para obtener el contenido del mailbox de un usuario.

WWW

Puede considerarse que el servicio de WWW es el responsable del crecimiento explosivo de Internet en los últimos años, particularmente a partir de la distribución de browsers gráficos como el NCSA Mosaic y el Netscape Navigator. Es entonces imprescindible poder contar con la capacidad de brindar este servicio como punto de presencia en Internet, y de utilizarlo como herramienta de trabajo (y esparcimiento).

El protocolo HTTP (HyperText Transfer Protocol) utilizado para brindar este servicio es muy sencillo conceptualmente, ya que se establece una conexión por cada requerimiento al servidor. Estas conexiones no tienen estado y son básicamente un pedido seguido de una respuesta. Por estas características este protocolo está particularmente adaptado al uso de proxies. Además la mayoría de los clientes soportan el protocolo SOCKS, así como el uso de proxies de HTTP como discutiremos en esta parte, brindando una amplia gama de alternativas al momento de implementar una solución. Es por lo tanto muy sencillo brindar una solución para el uso del servicio de web.

Aunque disponemos ya de un servidor SOCKS en el firewall, que podría perfectamente servir al propósito de utilizar el servicio de web, nos inclinamos por el uso de una solución basada en proxies HTTP. Los beneficios de utilizar estos proxies radican en la posibilidad de realizar caching de las páginas accedidas, con el consiguiente aumento de performance en el acceso, y de realizar restricciones basadas en el protocolo HTTP, más que en los hosts involucrados en la comunicación como sería en el caso de SOCKS (el puerto de comunicación es el mismo en general).

El producto utilizado como proxy de HTTP es el Squid, por dos razones: es de uso gratuito y es uno de los más conocidos.

Como siempre, deberá existir en el firewall algún proxy que nos provea de conectividad con Internet. En el caso del servicio de web, el uso del caching es muy beneficioso sobre todo en nuestra situación, donde disponemos de una única conexión con Internet.

FTP

Para realizar una sesión de FTP, se utilizan diferentes conexiones: una se usa para transportar comandos entre el cliente y el servidor, y la otra para transportar los datos. El canal de comandos utilizado por el servidor se encuentra en el puerto 21, y el de datos en el 20. El cliente, utiliza puertos por encima del 1023 tanto para el canal de datos como para el de comandos. También se pueden utilizar conexiones en modo “pasivo” en donde el cliente no identifica el canal de datos, y es el servidor el que utiliza un canal superior al 1023, que es utilizado exclusivamente por el cliente.

En una configuración de red como la anterior, no existen muchas alternativas para proveer el servicio de FTP.

La alternativa más sencilla es poseer un servidor de FTP en la entrada de la red, en donde éste puede ser accedido por los clientes de la red, como desde fuera. Esto posee varias desventajas anteriormente mencionadas: la sobrecarga del servidor principal (que contiene a todos los servicios), y algunos inconvenientes de seguridad, ya que puede ser accedido desde el exterior.

TELNET

Continuando con la configuración de red anteriormente mencionada, se está ante un problema similar al anterior. Los usuarios que acceden a la red desde el exterior, sólo pueden conectarse con un servidor de telnet

Por lo general, es conveniente disponer de servidores de FTP en las maquinas en las que se posee terminales. De esta manera, un usuario conectado a cualquier terminal de la red desde el exterior, podría tener la posibilidad de obtener archivos de cualquier servidor de FTP de la red; estos archivos serían almacenados temporalmente en la terminal, para luego ser obtenidos por el usuario nuevamente vía FTP.

Existen muchos otros servicios que pueden ser deseables proveer por la red. Siempre y cuando estos servicios utilicen diferentes puertos de comunicación, se puede configurar al servidor de socks para mapear el servicio a un maquina (servidor) específica.

DCHP

Cada computadora en una red TCP/IP debe tener asignado un nombre y dirección de IP únicos. Esta dirección de IP identifica a la computadora y la subred a la cual pertenece. Cuando una computadora es movida a una subnetwork diferente, la dirección de IP debe ser cambiada para reflejar la nueva Network ID.

DHCP es un protocolo diseñado para reducir la complejidad en la configuración de computadoras para TCP/IP. El RFC 1541 identifica los dos elementos más importantes del DHCP:

- a. un protocolo de comunicación de parámetros de configuración de TCP/IP entre un servidor de DHCP y sus clientes.
- b. un método para la alocaión dinámica de direcciones de IP para los clientes de DHCP.

Wins

Microsoft Windows Internet Name service (WINS) es una implementación del servicio de mapeo de nombre NetBIOS a una dirección de IP. WINS permite que los clientes basados en Windows pueda fácilmente localizar recursos compartidos en una red con TCP/IP. Los servidores de WINS mantienen bases de mappings de nombres de recursos estáticos y dinámicos a direcciones de IP. Dado que WINS soporta entradas de nombre y direcciones de IP dinámicas, puede ser utilizado con DHCP para proveer administración y configuración sencillas en redes TCP/IP basadas en Windows.

Packet Filtering

Packet filtering es un mecanismo de seguridad de redes que funcionan controlando que datos pueden fluir desde y hasta una red.

Un router debe decidir una decisión de ruteo sobre cada paquete que recibe sobre como enviarlo a su destino final. En general, los paquetes no llevan consigo información para ayudar al router en esta decisión, aparte de la dirección de IP destino (- salvo algunos paquetes poco comunes denominados “source routed packets”). En la determinación de como enviar el paquete, el router habitualmente se preocupa solamente de resolver el problema de cómo realizar el envío.

La utilización de packet Filtering o “filtrado de paquetes” permite el control (habilitación o deshabilitación) de las transferencias de datos basados en:

- La dirección en la cual los datos se (supuestamente) envían.
- La dirección en la cual los datos son dirigidos.
- La sesión y los protocolos de aplicación utilizados para la transferencia de datos.

La mayoría de los sistemas de filtrado de paquetes no hacen nada respecto de los datos en si, porque no realizan ningún tipo de decisiones basados en el contenido. Un filtrado de paquetes permite establecer reglas del siguiente tipo:

- No permitir que nadie utilice el TELNET (un protocolo de aplicación) para loguearse desde el exterior de la red
- Permitir que cualquiera envíe mails utilizando el sendmail (otro protocolo de aplicación).
- Que una computadora pueda enviarnos NEWS vía NNTP (otro protocolo de aplicación) pero solamente esa computadora.
- Sin embargo, existen ciertas cosas que no se pueden realizar con esta técnica:
- Que un usuario pueda realizar un TELNET desde el exterior pero no otros usuarios.
- Esto se debe a que el concepto de usuario no es algo que el sistema de filtrado sea capaz de reconocer. Otro ejemplo de esto podría ser:
- Poder transferir algunos archivos y otros no.

Una de las principales ventajas que provee esta técnica es simplicidad: permite establecer en un solo lugar, políticas de seguridad para toda una red. Por otra parte, ciertas protecciones sólo pueden ser provistas a través de esta técnica y solamente si estas se implementan en determinados puntos de accesos de la red. A continuación enumeramos las principales ventajas de Packet Filtering:

- Un solo Router de Screening puede ayudar a proteger toda una red.
- Packet Filtering no requiere del conocimiento del usuario o cooperación
- Está disponible en una gran variedad de routers.

Sin embargo existen ciertas desventajas:

- Loas herramientas actuales de filtrado no son perfectas.
- Algunos protocolos so especialmente conflictivos para el “filtrado”.
- Algunas políticas no pueden ser fácilmente llevas a cabo por algunos routers

Configuración de los servidores

DNS

El DNS Server en el firewall (NS1.company.com) será authoritative del dominio company.com.

Tendrá registros para los dominios que quieran hacerse públicos, y será el nameserver primario de la zona company.com.

Habrá al menos otro nameserver (NS2.othercompany.com), secundario, con conectividad directa a Internet que transferirá la zona company.com desde DNS1.

Asumiendo que tenemos una sola dirección de IP para nuestro firewall, tendremos que dejar que el proveedor de nuestro enlace maneje el DNS reverso para nuestra única dirección (i.e. no tendremos control sobre esto).

Servidor HP ProLiant ML350 G5 Server series

Visión General

El servidor HP ProLiant ML350, el servidor de torre más vendido en el mundo, es lo más nuevo en quinta generación con notables mejoras a la confiabilidad, expandabilidad, ambiental, y características de rendimiento.

Características

Si hubiera una palabra para describir las características del nuevo servidor HP ProLiant ML350 G5, sería "Dual". Dual-socket, procesadores Intel Xeon 5000 Dual- y Quad-Core sequence, conectores en caliente duales redundantes, ventiladores duales redundantes, y el mas pequeño, ligero y silencios chasis "Dual" para que uses drivers como 2.5" (SFF) o 3.5" (LFF) SAS o SATA.

Rendimiento

- Procesadores en secuencia Intel Xeon 5000 Quad- and Dual-Core con mas de 1333 M^a FSB, y 8MB L2 cache con EM64T
- Ocho DIMMS PC2-5300F DDR2 Fully-Buffered a 667MHz
- Zloty PCI Express y 3 PCI-X o 2 PCI Express y 5 PCI-X usando el extensor opcional PCI-X

Opciones

- Suministro de electricidad Hot Plug Redundant
- Sistema de ventiladores Redundantes
- Puerto serial y paralelo
- 8 Bahías de disco duro - 2.5" Small Form Factor (SFF) o 6 - 3.5" Large Form Factor (LFF) Universal Hot Plug SAS o bahías de disco duro SATA

Diseño y Conectividad

- Nuevo bezel frontal diseñado para un acceso flexible a discos media removibles y discos duros
- En total seis puertos USB 2.0 incluyendo dos en el frente
- 5 bahías Media para mayor flexibilidad

Especificaciones

Tabla 5. Especificaciones técnicas del Servidor HP ProLiant ML350 G5 Server series

(a) Procesador y memoria

PROCESADOR Y MEMORIA	
Procesadores disponibles	Intel Dual-Core Xeon 5000 series Intel Dual-Core Xeon 5100 series Intel Quad-Core Xeon 5300 series
Corazón de procesadores	Quad
Cache	4MB L2 cache
Multi-procesador	2
Velocidad máxima de bus	1333 MHz
Tipo de memoria	PC2-5300F DDR2 FB-DIMMs
Memoria Standard	512 MB (1 x 512 MB) or 1 GB (2 x 512 MB)
Memoria Maxima	16 GB (8 x 2 GB) – Dual-Core Models 32 GB (8 x 4 GB) – Quad-Core Models
Protección avanzada de memoria	Advanced ECC Online Spare

(b) Almacenamiento

ALMACENAMIENTO	
Tipo de almacenamiento	Hot plug 2.5" SAS Hot plug 2.5" SATA Hot plug 3.5" SAS Hot plug 3.5" SATA
Máximo de drivers internos	8 - 2.5" (SFF) o 6 – 3.5" (LFF)
Bahías media removibles	5
Slots de Expansión	6
Controlador de	Smart Array E200i Controller

almacenamiento	-64MB Cache (RAID 0/1) Entry Model -128MB BBWC (RAID 0/1/5) Base Models
----------------	--

(c) Destacados

DESTACADOS	
Factor de Forma	Torre o Rack
Altura de Rack	5U
Red	NC373i Multifunction Gigabit Network Adapter con TCP/IP Offload Engine
Administración remota	Integrated Lights-Out 2 (iLO 2)
Suministro de energía redundante	Opcional
Ventiladores redundantes	Opcional
Garantía Años (partes)	3/3/3

o **Hipótesis**

La Implementación y Configuración de una Intranet con su respectiva seguridad en el Edificio del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana orientada a la administración y control de los proceso y la información de la institución con eficiencia y optimizando recursos ayudara a la misma a cumplir con sus metas y objetivos para la cual fue creada.

2.5 Señalamiento de Variables de la Hipótesis

Variable Independiente

Implementación y Configuración de una Intranet

Variable Dependiente

Administración y control de los procesos de información de la institución.

CAPITULO III

METODOLOGÍA

3.1 Enfoque

La recolección de datos para el desarrollo del proyecto estará enfocada cuantitativamente puesto que se estará en permanente contacto con el personal de la institución quienes colaboraran para la comprobación de la hipótesis.

3.2 Modalidad

La investigación es de campo puesto que estudiaremos directamente los hechos en el lugar en el que se producen, los acontecimientos, tomando contacto en forma directa con la realidad, para obtener información de acuerdo a los objetivos del proyecto, además considerando que el objetivo del proyecto es el desarrollo de software la investigación también posee modalidad especial.

3.3 Nivel o Tipo de Investigación

Para el desarrollo del proyecto la investigación requerida iniciará en un nivel exploratorio, hasta llegar a un nivel explicativo que nos permita comprobar experimentalmente la hipótesis.

3.4 Población y Muestra

Debido a que el universo de la población esta reducido a aproximadamente 20 personas la muestra esta conformada por el mismo grupo.

3.5 Instrumentos para el Registro de Datos

Los instrumentos que utilizaremos para la recolección y registro de datos será cuaderno de notas, fichas de campo, escalas estimativas, y como técnicas la observación entrevista.

3.6 Procesamiento de la Información

Los datos recogidos se transforman siguiendo los siguientes procedimientos:

- o Revisión de la información recogida.
- o Repetición de la recolección de la información en ciertos casos individuales para corregir fallas.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis de resultados

Los resultados se obtuvieron luego de realizar entrevistas (Ver Anexo 2) al personal que labora en el CID-FAE, especialmente al oficial con mayor rango, y los encargados de las respectivas jefaturas como la de electrónica, aeronáutica, que se consideran que son las personas relacionadas directamente con el problema de investigación.

De las entrevistas realizadas se obtuvieron criterios respecto a la forma de manejar y distribuir la información y de compartir los recursos en red dentro de la entidad, mismos que se detallan a continuación:

Los equipos están conectados por medio de un switch marca Dlink Ethernet Dgs-1248 48 puertos 10/100/1000 mbps, en una configuración de GRUPO DE TRABAJO, las identificaciones de los equipos están asignados al azar o a conveniencia del usuario responsable de dicho equipo.

Los datos (archivos y carpetas) se comparten de manera intuitiva es decir de acuerdo a las necesidades del día, sin ninguna política de control de acceso, es decir que, cualquier empleado puede acceder a cualquier información en la red, mientras éste se mantenga compartido.

La información rutinaria, tales como reportes, formularios, informes, noticias, se comparte ya sea verbalmente o en hojas impresas. Además tomando en cuenta que la finalidad del Centro de Investigación y Desarrollo es el desarrollo de proyectos aeronáuticos con tecnología propia, se debe recalcar que existe información de

carácter confidencial que no es manejada con el debido recelo y delicadeza que se merece.

Excesiva centralización de la información en algunas áreas, como por ejemplo, la Secretaria, Departamento de Electrónica, Gerencia.

Excesivo flujo de documentos impresos hacia la Gerencia, así mismo hay información que llega tarde o no llega al lugar adecuado.

Muchos directivos no saben exactamente qué información necesitan para trabajar.

Dificultad por parte de los usuarios (empleados) para utilizar algunos programas de propósito específico para la gestión de información.

Se han tomado en cuenta los criterios antes mencionados por considerarse los más relevantes y los que merecen una atención en cuanto al futuro diseño e implementación de la intranet que se encargara de la óptima gestión de la información que se origina en esta institución.

De esta manera presento la siguiente propuesta que tiene como meta optimizar los procesos de compartimiento de información y recursos dentro de la empresa, además tomando en cuenta diversas concepciones teóricas que lo fomentan: como medio de comunicación, como sistema de información, como mediación tecnológica; solución cuyo estudio esta detallado en el Capitulo VI

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La Implementación y Configuración de una Intranet con su respectiva seguridad en el Nuevo Edificio del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana fue fundamentada en necesidades de dicha institución, para optimizar los procesos de distribución de datos y recursos logrando el ahorro de tiempo y la satisfacción del usuario.

El proyecto es muy factible de ejecutarlo puesto que el Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana, cuenta con el recurso económico, los equipos y personal capacitado para la implementación y posterior administración y mantenimiento de una intranet como la que se ha propuesto en esta investigación

El diseño cumplió con la expectativas para el cual se formuló el proyecto, de esta manera logrando el objetivo principal el cual era el diseño e implantación, en forma rápida, fácil y económica de una Intranet, atendiendo a los estándares vigentes en cuanto a requerimientos en la interconexión de equipos en un ambiente de trabajo reducido y de esta manera obtener todas las potencialidades de una Intranet, sin dejar de lado los costos de los materiales.

La Intranet ofrece una facilidad de utilización al usuario independientemente de la estación de trabajo para acceder a la información que necesite y por lo

tanto, el entorno de trabajo está siempre dispuesto para funcionar sin preparación previa

El Incremento de la productividad constituye uno de los aspectos principales a tener en cuenta a la hora de considerar los costos de la Intranet y es difícil de cuantificar. Este incremento está dado por la velocidad y la facilidad de acceso e intercambio de información. La Intranet también permite flexibilidad en el tiempo de consulta de la información, aspecto este sumamente importante en la institución.

La administración de la Intranet estará a cargo de un administrador de redes o una persona que tenga los conocimientos necesarios para realizar las tareas asignadas, lo cual será una ventaja para la empresa

El administrador de red ahora disponen de una gran cantidad de información de la institución on-line, fácilmente accesible desde cualquier lugar y se hace latente el ahorro de tiempo y dinero que permite la Intranet, además por la posibilidad de reducción de gran cantidad de material impreso y otras vías ineficientes de compartir información

5.2 Recomendaciones

Se recomienda a los miembros que conforman la Institución continuar con el desarrollo de este tipo de proyectos informáticos que mejoren su desempeño como entidad pionera en tecnología y desarrollo como su nombre hace referencia.

Proteger la información de la base de datos del sistema puesto que se registra allí toda la información sobre los descuentos del personal, por lo que se hace necesario el establecimiento de procedimientos para el respaldo de la misma y así evitar dificultades en su manejo.

Proteger la información corporativa delicada, y asegurar que personas ajenas a la institución no perjudiquen a los sistemas informáticos y a los datos, mediante firewalls que protegen a la Intranet de Internet.

Tomando en consideración los servicios de la Intranet a disposición de todos los usuarios a través de la página Web creemos que es fundamental para la formación, el aprendizaje de estas herramientas y otras que no están incluidas dentro del sitio, pero que son muy útiles en el trabajo diario, por lo que sugerimos que el administrador de redes realice las capacitaciones pertinentes no solo para los usuarios directos, sino además para todo el personal que labora dentro de la institución.

CAPITULO VI

PROPUESTA

“Implementación y Configuración de una Intranet con su respectiva seguridad en el Nuevo Edificio del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana.”

6.1 Datos Informativos

Nombre:

Centro de Investigación y Desarrollo de la Fuerza Aérea
Ecuatoriana

Ubicación:

Latacunga, Avenida Amazonas y Antonio Clavijo.

Tipo Empresa:

Estatal

6.2. Antecedentes de la Propuesta

El análisis que se acaba de detallar permite plantear una alternativa de solución informática que optimice los procesos de la institución en cuanto a flujo de información y seguridad tomando en cuenta la reducción de costos y optimización de recursos que este al alcance de todos los empleados con acceso a ella, solución que se detalla en el Análisis del Sistema.

6.3 Análisis del Sistema

6.3.1 Análisis de Riesgos

6.3.1.1 Plan de Riesgos

6.3.1.1.1 Riesgos de Proyecto

Riesgo: Información inexacta brindada por colaboradores de la institución para el desarrollo del sistema.

Estrategia Proactiva.- Pedir a los personeros de la institución que se me asigne una persona que sea guía y que tenga conocimientos suficientes para que facilite la información requerida para el desarrollo del proyecto.

Estrategia Reactiva.- Pedir a los personeros de la institución que se me den las facilidades necesaria sobre la información y ciertos recursos que serán utilizados en el desarrollo del proyecto.

Riesgo: Exista una confusión en la determinación de los requerimientos del proyecto que puedan influir en la elaboración del mismo.

Estrategia Proactiva.- Documentar los pedidos de la persona encargada del asesoramiento para evitar futuras confusiones.

Estrategia Reactiva.- Realizar las modificaciones de acuerdo a las nuevas peticiones de la persona encargada.

Riesgo: Alteración de los requerimientos en el transcurso del proyecto.

Estrategia Proactiva.- Definir concretamente los requerimientos del sistema en la sección de análisis antes de iniciar el desarrollo del mismo.

Estrategia Reactiva.- Establecer nuevos plazos y reasignar los recursos necesarios para cubrir los nuevos requerimientos del proyecto.

6.3.1.1.2 Riesgos Técnicos

Riesgo: Que las personas involucrada tengan una perspectiva equivocada

acerca de los alcances del proyecto.

Estrategia Proactiva.- Establecer bajo documentos los límites y restricciones con el representante de la institución en el proceso de desarrollo del sistema.

Estrategia Reactiva.- Orientar y asesorar a los futuros usuarios acerca de los alcances reales del proyecto desarrollado.

Riesgo: Que la institución no facilite los recursos establecidos en el análisis del proyecto.

Estrategia Proactiva.- Mediante el previo análisis determinar los requerimientos físicos, económicos y humanos para el desenvolvimiento del proyecto.

Estrategia Reactiva.- Realizar un reajuste a fin de cumplir con los requerimientos fijados.

Riesgo: Daños en el Software de desarrollo del proyecto.

Estrategia Proactiva.- Realizar instalaciones de Software apropiadas de acuerdo a las capacidades del Hardware y realizar un monitoreo constantemente el estado del software para evitar posibles retrasos en el desarrollo del proyecto.

Estrategia Reactiva.- Reinstalar el software.

Riesgo: Incumplimiento de los plazos establecidos para la entrega del proyecto.

Estrategia Proactiva.- Planificar el tiempo para desarrollar cada una de las actividades planeadas para la ejecución del proyecto.

Estrategia Reactiva.- Reajustar los recursos de tiempo y esfuerzo del desarrollador para evitar el retraso en el desarrollo del proyecto.

Riesgo: Retrasos por desabastecimiento de energía eléctrica.

Estrategia Proactiva.- Respalda la información constantemente.

Estrategia Reactiva.- Realizar nuevamente lo que se ha perdido.

Riesgo: Posibles daños no intencionados en el software por parte del personal por desconocimiento.

Estrategia Proactiva.- Respalda la información periódicamente y informar al personal acerca de los avances del proyecto.

Estrategia Reactiva.- Reestablecer los cambios realizados a la mayor brevedad posible.

Riesgo: Posibles daños en el hardware usado por el desarrollador.

Estrategia Proactiva.- Monitoreo del estado del hardware y mantenimiento periódico para evitar novedades en el desarrollo del proyecto.

Estrategia Reactiva.- Reparar o reemplazar el hardware con la mayor brevedad posible.

6.3.2 Estudio de Factibilidades

6.3.2.1 Factibilidad Económica

Los costos que involucran el desarrollo del sistema se obtuvieron mediante el proceso de estimación de costos que se detalla a continuación

COSTO DEL SISTEMA ACTUAL

Tabla 6. Costos del sistema actual

Cantidad	Personal	Dólares Mensual
1	Encargado del Servidor	400.00
1	Mensajero	180.00
Gasto Personal (GP)		580.00

Cantidad	Equipo de Computo	Valor	Depreciación	Total
----------	-------------------	-------	--------------	-------

			(15%)	
1	Servidor	1500 USD	50 0	1000
Gasto Equipo de Cómputo (GE)				1000

Materiales Directos	Dólares Mensual
Materiales de Oficina	70.00
Servicios de terceros	50.00
Gasto Materiales Directos (GMD)	120.00

Varios	Dólares Mensual
Mantenimiento de Instalaciones	10.00
Mantenimiento de Computadores	50.00
Útiles de Limpieza	10.00
Gasto Varios (GV)	70.00

COSTO DEL SISTEMA ACTUAL	
GASTOS	Dólares Mensual
Gasto Personal (GP)	580.00
Gasto Equipo de Cómputo (GE)	1000.00
Gasto Materiales Directos (GMD)	120.00
Gasto Varios (GV)	70.00
SUBTOTAL	1770.00
Gastos Indirectos (0.67%)(SUBTOTAL)	11.85
TOTAL	1758.15

SON MIL SETECIENTOS CINCUENTA Y OCHO DOLARES CON QUINCE CENTAVOS AMERICANOS.

COSTO DEL SISTEMA DE INTRANET

Tabla 7. Costos del sistema de Intranet

Cantidad	Personal	Dólares Mensual
1	Administrador de Redes	550.00
Gasto Personal (GP)		550.00

Cantidad	Equipo de Computo	Valor	Depreciación (15%)	Total
1	Servidor	1500 USD	50 0	1000
Gasto Equipo de Cómputo (GE)				1000

Materiales Directos	Dólares Mensual
Materiales de Oficina	60.00
Gasto Materiales Directos (GMD)	60.00

Varios	Dólares Mensual
Mantenimiento de Instalaciones	10.00
Mantenimiento de Computadores	20.00
Útiles de Limpieza	10.00
Gasto Varios (GV)	40.00

COSTO DEL SISTEMA DE INTRANET	
GASTOS	Dólares Mensual
Gasto Personal (GP)	550.00
Gasto Equipo de Cómputo (GE)	1000.00
Gasto Materiales Directos (GMD)	60.00
Gasto Varios (GV)	40.00
SUBTOTAL	1650.00
Gastos Indirectos (0.67%)(SUBTOTAL)	11.05
TOTAL	1638.94

SON MIL SEISCIENTOS TREINTA Y OCHO DOLARES CON NOVENTA Y CUATRO CENTAVOS AMERICANOS.

Beneficios

La variación en cuanto al costo del sistema de trabajo actual y del sistema nuevo (Intranet) es CIENTO DIECINUEVE DOLARES CON VEINTIUN CENTAVOS AMERICANOS, observamos que la cantidad de ahorro económico es mínima pero se debe tomar en cuenta que se reemplaza el equipo de impresión obsoleto por un centro de impresión nuevo y veloz por ende los beneficios de productividad se incrementan en un 75% a largo plazo además debemos considerar que se reduce una plaza de trabajo innecesaria.

Otro beneficio a tomar en cuenta es que el entorno de trabajo toma un nuevo aspecto aumentando la eficiencia de los usuarios de la Intranet dentro de la institución.

Debo mencionar además el ahorro de recursos y la preparación de la empresa en una tecnología fundamental para la supervivencia en la Nueva Economía, en las áreas funcionales de servicio al cliente, producción y operaciones, ingeniería, recursos humanos, administración, contabilidad y finanzas, que son un potenciales proyectos a implementar a futuro.

Un beneficio clave es la habilidad de entregar información actualizada de manera rápida y costo eficiente a toda la base de usuarios. La Intranet pone información vital al alcance de todos los empleados con acceso a ella. Otra característica que vale la pena mencionar, es la consistencia, porque la información es la misma a lo largo y ancho de la empresa.

6.3.2.2 Factibilidad Técnica

Software

Mediante el siguiente cuadro comparativo podemos hacer la elección mas coherente de la mejor alternativa para que sea la plataforma sobre la cual desarrollar la Intranet

Sistema Operativo de Red

Parámetros	Microsoft Windows 2000 Server	Microsoft Windows 2003 Server R2	Linux Red Hat Enterprise Server
Menor Costo de Adquisición			X
Conocimientos del Administrador de Redes	X	X	
Confiabilidad			X
Robustez			X
Mayor Seguridad		X	X
Menor Costo de Administración		X	X
Mayor Capacidad de Almacenamiento		X	X
Disponibilidad como plataforma Web		X	X
Licencia adquirida	X	X	
Firewall	X	X	X
Plataforma .NET		X	X

Tabla 5. Comparativa de los sistemas operativos de red

Analizando los resultados de la comparativa notamos que la mejor opción la tenemos en Linux Red Hat Enterprise Server por sus características, pero hay una razón fundamental por la que se optó por Windows 2003 Server R2: que la institución tiene adquirida la licencia para Microsoft Windows 2003 Server R2 lo que significa un ahorro económico importante para la misma.

Hardware

Se cuenta con un equipo Servidor ProLiant ML350 Generation 3 de HP cuyas características se muestran en el Anexo 1.

(Ver Anexo 1)

6.3.2.3 Factibilidad Operacional

El personal de la institución nos brinda una amplia apertura informativa con respecto a las actividades que se desarrollan dentro de la misma.

La persona designada para nuestro asesoramiento y orientación, es un técnico que tiene como tarea secundaria la administración del servidor.

6.3.2.3.1 Parámetros de Desarrollo

Equipo Humano

Ivan Chamorro

Equipo Hardware

La maquina en las que desarrollará el proyecto tienen las siguientes características:

- Servidor ProLiant ML350 Generation 3 de HP
- Procesador: Xeon
- Disco Duro: 2 HDD Seagate 70 Gb, Serial Ata, 7.200 rpm
- Memoria Ram: 1 DDR Kingson de 1Gb
- DVD Rom HP
- Monitor HP
- Puerto Frontal USB 2.0

Software:

- Microsoft Windows 2003 Server R2
- Microsoft Exchange Server 2003
- Macromedia Dreamweaver MX

6.3.3 Análisis FODA

Se efectuará un análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) sobre la implementación de un sistema de información con estas características:

6.3.3.1 Fortalezas

- Seguridad en la información entregada:

La información restringida se accede por niveles a través de contraseñas y protocolos de seguridad.

- Pertinencia de la información:

La documentación publicada de la institución será la que ésta estima conveniente y oportuna.

- **Ahorro de insumos:**

El mejoramiento de los procesos asociados a la obtención y difusión de la información permiten significativamente ahorrar papel, tinta y personal para impresión en comparación a los procesos tradicionales.

- **Escalabilidad:**

Permite rediseñar el sistema sin realizar ningún cambio posterior importante.

6.3.3.2 Oportunidades

- **Incorporación de Herramientas Multimedia:**

Se pueden incorporar todos los avances tecnológicos frecuentes de Internet en cuanto a herramientas multimedia (texto, gráficas, sonido y video).

- **Integración de Aplicaciones:**

Se presenta un único lugar virtual donde es posible centralizar y constituir en un todo las aplicaciones existentes.

- **Personal Mejor y Más Informado:**

A través de la implementación de algún mecanismo comunicacional eficiente es posible difundir las actividades y noticias importantes.

- **Reducir el tiempo de Aprendizaje de los Usuarios:**

La centralización de información junto a adecuadas metodologías que apoyen la gestión del aprendizaje disminuirá el tiempo de capacitación de los usuarios.

- **Cobertura:**

El sistema a través de la red permite llegar a todos los departamentos en los que esta repartida la institución.

- **Calidad de Servicio:**

Dada la rapidez en la obtención y difusión de la información como su tratamiento en línea, se procurará mejor calidad de servicio.

6.2.5.3 Debilidades

- Escasez de Equipamiento Computacional:

El 65% del equipo computacional de la institución tiene características de cierta manera obsoletas para la actualidad.

6.2.5.4 Amenazas

- Difusión del Servicio:

Si existe una deficiente estrategia de difusión del servicio, la utilidad de la Intranet pasará desapercibida para el usuario.

- Problemas de Comunicaciones:

La calidad del servicio debe ir acompañada de un buen desempeño de las herramientas de comunicaciones de esta tecnología (cableado, enlaces, equipos, etc.)

- Capacitación Tecnológica de los Usuarios:

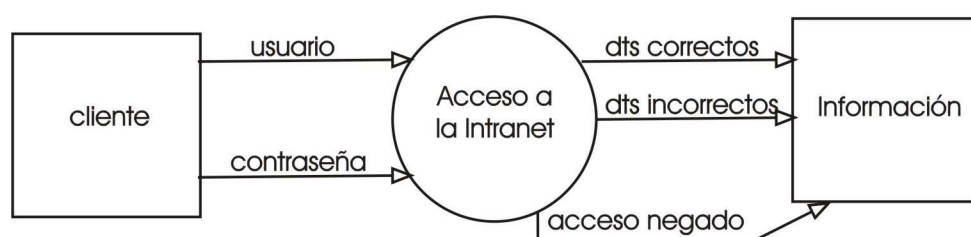
Hay una cierta parte del personal que posee escasa capacitación en materia computacional, específicamente en tecnologías de Internet e Intranet lo que podría dilatar el uso masivo de la Intranet.

6.3.4 Análisis estructurado

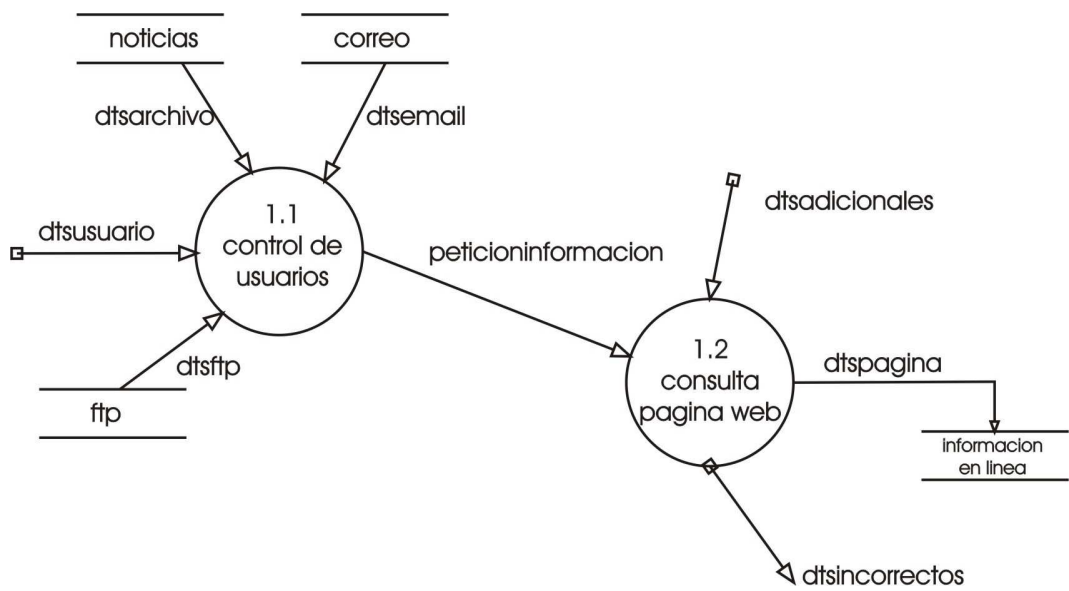
6.3.4.1 Diagrama de Flujo de Datos

“Implementación y Configuración de una Intranet con su respectiva seguridad en el Nuevo Edificio del Centro de Investigación y Desarrollo de la Fuerza Aérea Ecuatoriana.”

Nivel 0:



Nivel 1:



6.4 Diseño del Sistema

6.4.1 Modelo de la Solución Propuesta

La solución estudiada propone desarrollar una Intranet, la cual funcionará sobre un servidor Web que además tendrá las funciones de servidor de correo interno, servidor FTP, cortafuegos y servidor de archivos donde se encuentra la información y documentos a publicar. Así el acceso a la información podrá ser realizada desde cualquier computador que se encuentre conectado a la Red y que tenga acceso.

Para desarrollar la Intranet se utilizarán la plataforma Windows 2003 Server y una mezcla de otras.

La información se administrará de la siguiente forma:

El administrador del servidor subirá la información a la Intranet; el personal accederá a dicha información desde sus respectivos equipos a través de un login con usuario y contraseña.

6.4.1.1 Identificación de Usuarios y Roles

Dentro del esquema de la Intranet existirán 3 tipos de usuarios:

- Administrador: El usuario: **Administrador** es aquel que tiene derechos ilimitados sobre la información del sistema. En este caso el Administrador de Red.
- Directivo: El usuario: **Directivo** es aquel que tiene derechos ilimitados sobre la información del sistema y además por políticas de la institución tiene voz de mando sobre el usuario administrador. En este caso el personal militar de mayor rango: Mayor, Capitán.
- Usuario Final: El usuario: **Usuario Final** es aquel que tiene derechos de consulta sobre la información del sistema que el administrador le

otorgue. En este caso demás personal militar, el personal administrativo y el personal civil de los diferentes departamentos

De los cuales podemos de derivan los roles a continuación:

Administrador del Sistema:

- Apagar el equipo servidor
- Configurar los programas que se inician junto con el sistema.
- Administrar cuentas de usuarios.
- Administrar los programas y la documentación instalada.
- Configurar los programas y los dispositivos.
- Configurar la zona geográfica, fecha y hora.
- Administrar espacio en discos y mantener copias de respaldo.
- Configurar servicios que funcionarán en red.
- Solucionar problemas con dispositivos o programas.
- Revisar archivos log, solucionar y prevenir inconvenientes de seguridad.

Directivos

- Apagar el equipo servidor
- Administrar cuentas de usuarios.
- Administrar los programas y la documentación instalada.
- Administrar espacio en discos y mantener copias de respaldo.
- Revisar archivos log, solucionar y prevenir inconvenientes de seguridad.
- Supervisar las acciones del Administrador
- Pedir informes al Administrador

Usuarios Finales

- Apagar el equipo a su cargo
- Mantener su equipo en optimo funcionamiento

- Compartir la documentación requerida
- Administrar espacio en discos y mantener copias de respaldo en su equipo.
- Revisar, solucionar y prevenir inconvenientes de seguridad en su equipo.
- Permitir la supervisión y monitoreo de su equipo por parte del Administrador o del Directivo, en caso de ser requerido.

6.4.2 Arquitectura

La arquitectura del modelo (Ilustración 1) se compone por un Servidor de Archivos donde se almacenarán los datos de la Intranet, un Servidor de páginas Web, el cual será el punto de conexión de los usuarios. Este servidor recibirá los requerimientos de los clientes y procesará las respuestas realizando la conexión al servidor de base de datos en caso de ser necesario.

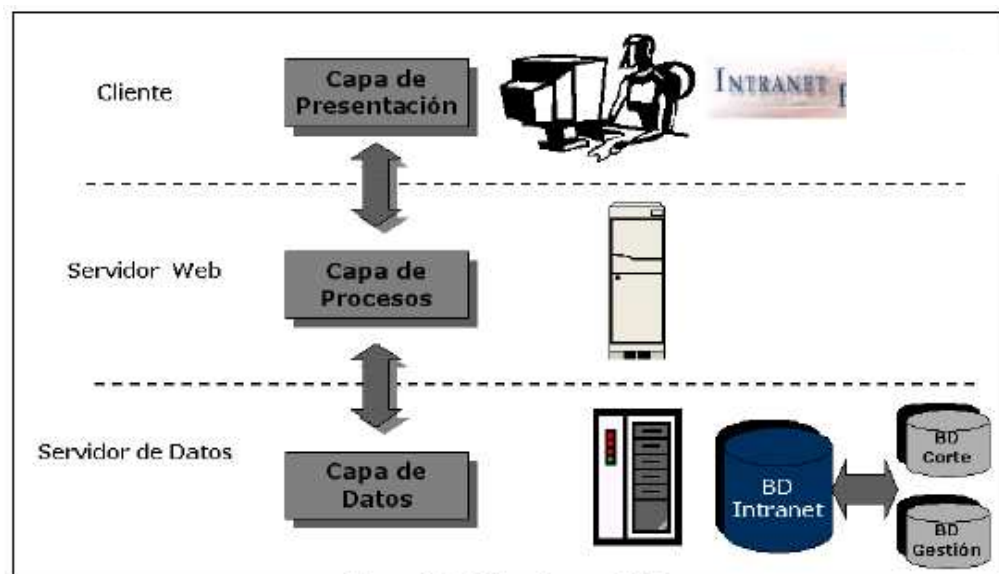


Ilustración 4.1: Arquitectura WEB.

Ilustración 3: Arquitectura para la Intranet

6.4.3 Tecnología para la Implantación de la Solución

Para implementar la arquitectura anterior mencionada se utilizó una mezcla de componentes (Ilustración 2):



Ilustración 4.2: Plataforma Computacional.

Ilustración 4. Plataforma Computacional

Sistema Operativo	: Microsoft Windows 2003 R2
Servidor Web	: IIS 6.0
Navegador	: Internet Explorer 5.0 o superior

6.4.3.1 Microsoft Windows 2003 R2

Microsoft Windows Server 2003 R2 hace más fácil y más efectivo de costos extender la conectividad y control de usuarios, ubicaciones, datos, y aplicaciones dentro de la organización. Windows Server 2003 R2 tiene como ventajas las mejores en estabilidad y seguridad de un código base probado capaz de extender la conectividad y el control en nuevas áreas. Ofrece todos los beneficios de las plataformas Windows además que mejora enormemente la administración de accesos, soluciones de servidor, configuración y administración de almacenamiento, y desarrollo de aplicaciones dentro y fuera los límites tradicionales de la organización.

Algunas características de Windows Server 2003 R2 son ⁽¹⁾:

Características	Windows Server 2003 Web Edition	Windows Server 2003 Standard Edition	Windows Server 2003 Enterprise Edition	Windows Server 2003 Datacenter Edition
Servicios de Directorio Activo	Sí	Sí	Sí, incluido metadirectorio	Sí, incluido metadirectorio
Servicios de Ficheros	Limitado **	Sí	Sí	Sí
Servicio de Impresión	No	Sí	Sí	Sí
Clustering	No	No	8 Nodos	8 Nodos
Servicios de Balanceo de Carga	Sí	Sí	Sí	Sí
Servicios IIS	Sí - Servidor web dedicado a este propósito	Sí	Sí	Sí
Servicios de Fax	No	Sí	Sí	Sí
Cortafuegos básico	No	Sí	Sí	No
Servicios de Terminal	Administración Remota	Servidor, Administración Remota	Servidor, Administración Remota	Servidor, Administración Remota
			Session Directory	Session Directory
Límite VPN		1 000 conexiones concurrentes	Ilimitada	Ilimitada
Windows System Resource Manager	No disponible	No disponible	Sí	Sí

Tabla 8: Características de Windows Server 2003

6.4.3.2 Microsoft Internet Information Server (IIS) 6.0

Los servicios de Microsoft Internet Information Server proporcionan capacidades de servidor Web integrado, confiable, escalable, seguro y administrable en una Intranet. IIS 6.0 incorpora mejoras significativas en la arquitectura para cubrir las necesidades de los clientes.

IIS 6.0 introduce muchas características nuevas para la administración, disponibilidad, confiabilidad, seguridad, rendimiento y escalabilidad de los servicios de aplicaciones Web. IIS 6.0 y Windows 2003 Server proporcionan la solución para servidores Web más confiable, productiva, conectada e integrada ⁽²⁾.

(1, 2) Tomado del Manual de Windows 2003 Server, Microsoft TechNet Community 2002

6.4.4 Macromedia Dreamweaver MX

Macromedia Dreamweaver MX, un producto que permite a los desarrolladores diseñar y crear código para una completa gama de soluciones, desde sitios Web hasta aplicaciones para Internet, sin comprometer el enfoque principal del producto para los usuarios solo de HTML. Dreamweaver MX combina en un único entorno de desarrollo accesible y potente las reconocidas herramientas de presentación visual de Dreamweaver, las características de rápido desarrollo de aplicaciones Web de Dreamweaver UltraDev y ColdFusion Studio, y el extenso soporte de edición de código de HomeSite. Dreamweaver MX ofrece una completa solución abierta para las tecnologías Web y estándares de hoy, incluyendo la accesibilidad y servicios Web ⁽³⁾.

6.4.5 Tecnología en el Cliente

Sistema Operativo: Windows Xp

Uno de esos servicios consiste en crear la infraestructura lógica que permitirá grabar datos en los discos y disquetes, así como generar, abrir, eliminar y mover archivos.

La oferta de sistemas operativos disponible para computadoras personales en la actualidad no es demasiado amplia. La mayoría de las pc`s cuentan con el famoso y popular Windows 9*/00/NT/XP/ME/SE.

Para la implementación de la Intranet del Poder Judicial, se utilizará en el cliente MICROSOFT WINDOWS XP.

1 Navegador de la Solución

Los clientes de la solución tendrán instalados la versión 6.0 de Internet Explorer.

(3) Tomado de <http://www.adobe.com/es/devnet/dreamweaver/>

1 **6.4.6 Descripción del Sitio Web**

El sitio Web diseñado presenta diferentes canales de navegación, los cuales serán descritos a continuación.

1 **6.4.6.1 Inicio**

Es la presentación de la institución, se describe de manera general lo que es la institución.

6.4.6.2 Misión

Se describe concretamente la misión que tiene la empresa dentro del entorno militar.

6.4.6.3 Visión

Se describe la visión, las metas, objetivos que desea lograr la institución.

6.4.6.4 Áreas

Se resume la forma en que está organizada la institución, sus niveles jerárquicos, sus departamentos y oficinas.

6.4.6.5 Intranet

Es la página donde los clientes podrán identificarse y acceder a la Intranet y utilizar los servicios que brinda la misma. Consta de un cuadro de texto para usuario y otro para contraseña y un botón de aceptar.

2 **6.4.6.6 Contactos**

3

Es el área donde se muestra información de contacto de la institución: teléfonos, dirección, dirección electrónica, etc.

6.4.6.7 Contenidos

A continuación se muestra la página principal de la Intranet del CID.

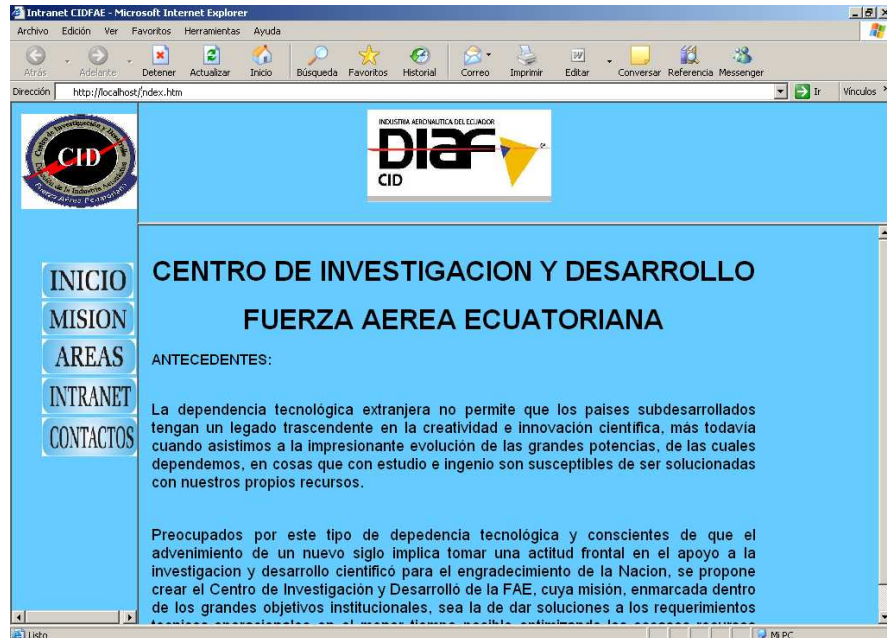


Ilustración 5: Pagina principal

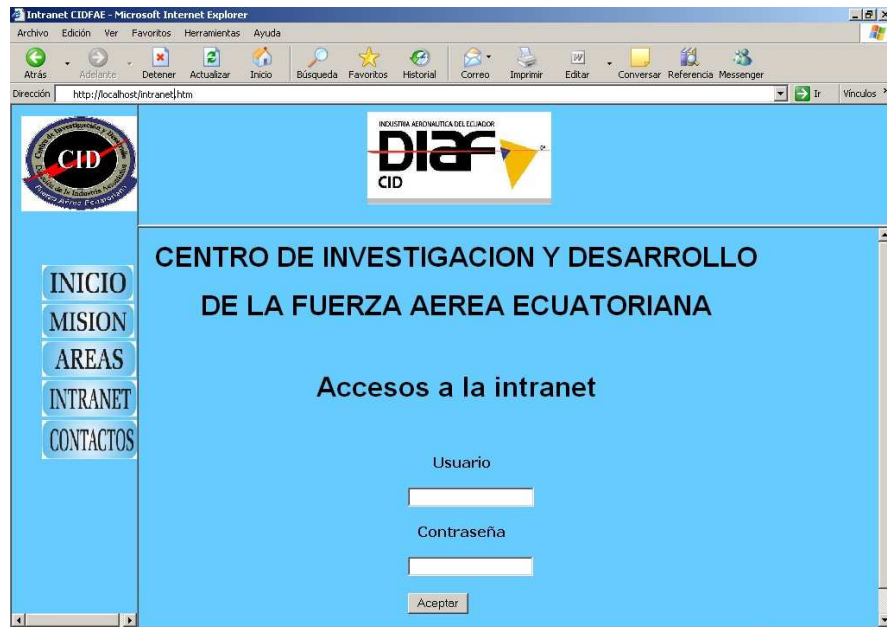


Ilustración 6: Página de Acceso a la Intranet

6.5 Implementación

6.5.1 Levantar servicios de Windows 2003 Server

Partimos que los servicios de Windows 2003 Server están integrados en una herramienta centralizada: el Directorio activo (Active Directory).

Active Directory® es un servicio de directorio que almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red. Por ejemplo, Active Directory almacena información acerca de las cuentas de usuario (nombres, contraseñas, números de teléfono, etc.) y permite que otros usuarios autorizados de la misma red tengan acceso a esa información ⁽⁴⁾.

(4) Tomado <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9d684f0-90b1-4c67-8dca-7ebf803a003d.msp?mfr=true>

Se puede usar Active Directory para crear los siguientes objetos.








Icono	Objeto	Descripción
	Usuario	Un objeto de usuario es un objeto que es un principal de seguridad en el directorio. Un usuario puede iniciar sesión en la red con estas credenciales y a los usuarios se les puede conceder permisos de acceso.
	Contacto	Un objeto de contacto es una cuenta que no tiene ningún permiso de seguridad. No se puede iniciar sesión como contacto. Los contactos se suelen utilizar para representar a usuarios externos con fines relacionados con el correo electrónico.
	Equipo	Objeto que representa un equipo en la red. Para las estaciones de trabajo y servidores con Windows NT, ésta es la cuenta de equipo.
	Unidad organizativa	Las unidades organizativas se utilizan como contenedores para organizar de manera lógica objetos de directorio tales como usuarios, grupos y equipos, de forma muy parecida a como se utilizan las carpetas para organizar archivos en el disco duro.
	Grupo	Los grupos pueden contener usuarios, equipos y otros grupos. Los grupos simplifican la administración de cantidades grandes de objetos.
	Carpeta compartida	Una carpeta compartida es un recurso compartido de red que se ha publicado en el directorio.
	Impresora compartida	Una impresora compartida es una impresora de red que se ha publicado en el directorio

Tabla 7. Objetos de Active Directory

Se procede a levantar los siguientes servicios sobre la plataforma Windows 2003 Server:

6.5.1.1 Directorio Activo y DNS

Un servidor DNS nos va a servir para la resolución de nombres cuando queramos acceder a las web que tenemos alojadas en nuestra intranet.

Servidor DNS

Servicio de Ruteo y Acceso remoto

Servidor DHCP

Configurando de la siguiente manera según lo planteado en la etapa de análisis:

Nombre de dominio del directorio activo: CID-DIAF.COM. Fig 1

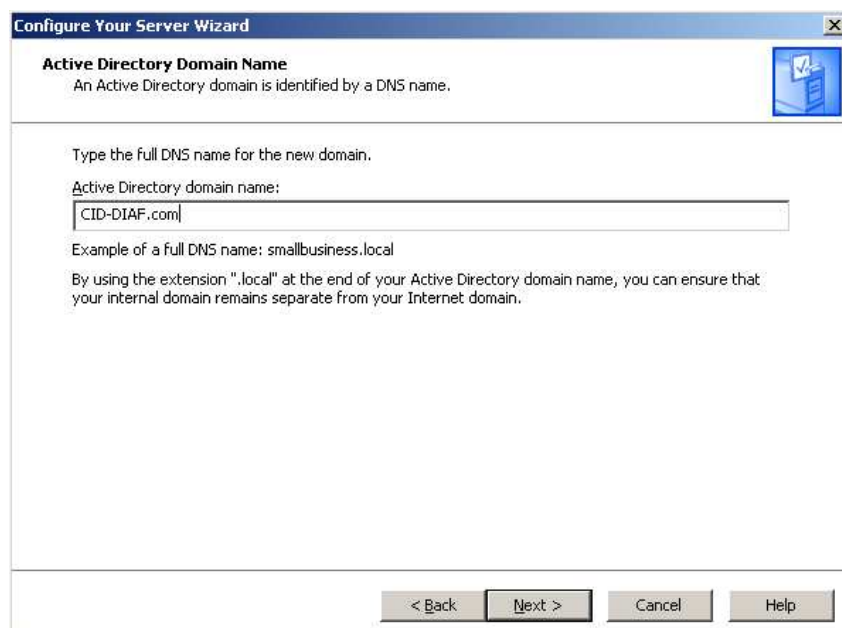


Figura 1. Nombre DNS del Servidor

Nombre de dominio NetBIOS: CID-DIAF. Fig 2

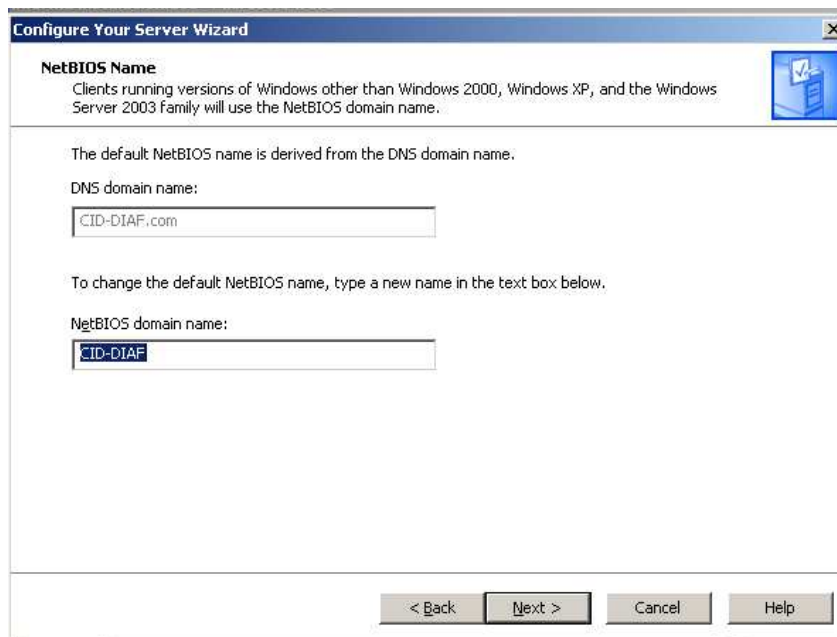


Figura 2. Nombre NetBios del Servidor

Dirección IP del DNS: 192.168.0.1. Fig 3.

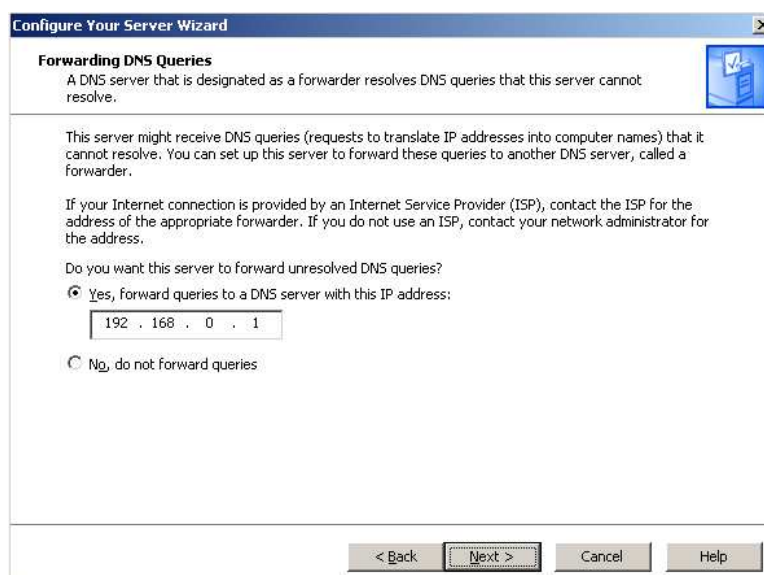


Figura 3. Dirección IP del DNS del Servidor

Así tenemos la siguiente información al finalizar el Asistente. Fig 4.

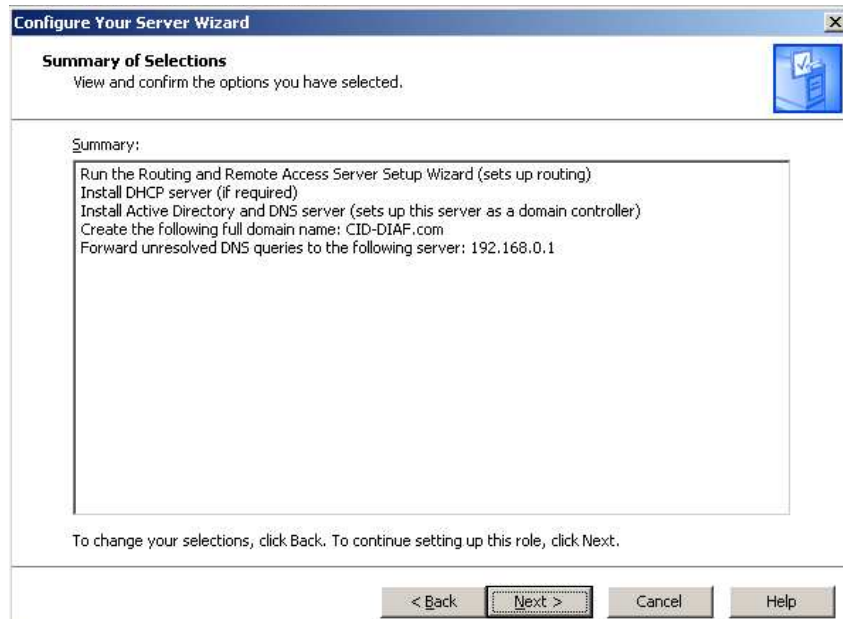


Figura 4. Pantalla de resumen de la configuración DNS

Configuración del Ruteo y Acceso Remoto:

Elegimos la primera tarjeta de red a la cual se le asignara una IP pública, y habilitamos la seguridad de esta tarjeta por medio de un Firewall y creamos una nueva interfase de demanda para Internet. Fig 5.

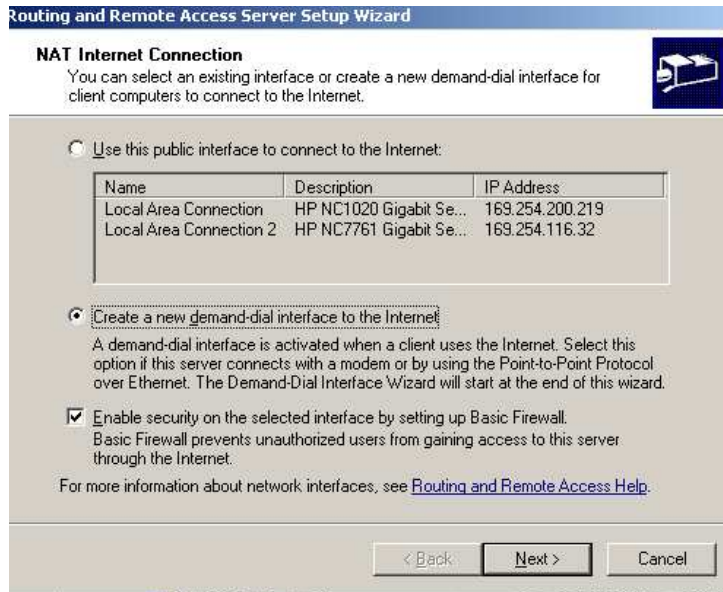


Figura 5. Crear una nueva interfaz

Seleccionamos la tarjeta de red que tendrá el acceso a Internet:

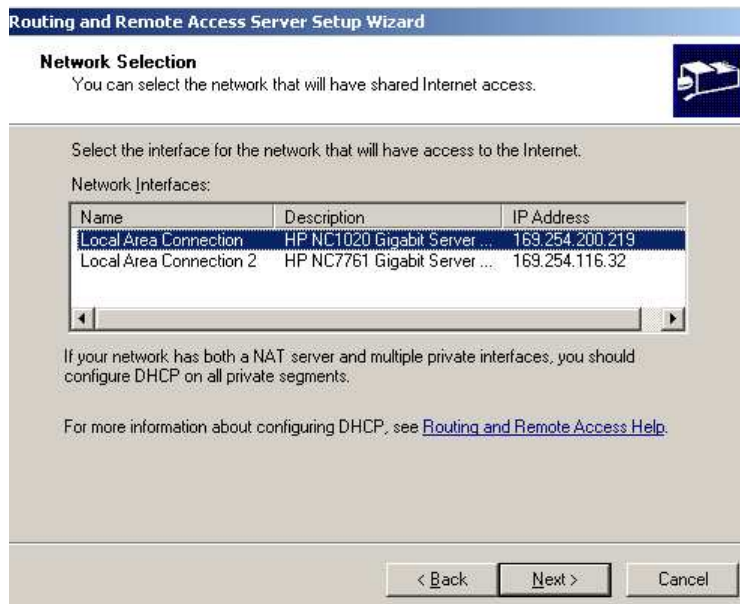


Figura 6. Selección de la Tarjeta de Red

Esperamos mientras el Asistente actualiza los servicios levantados. Fig 6.

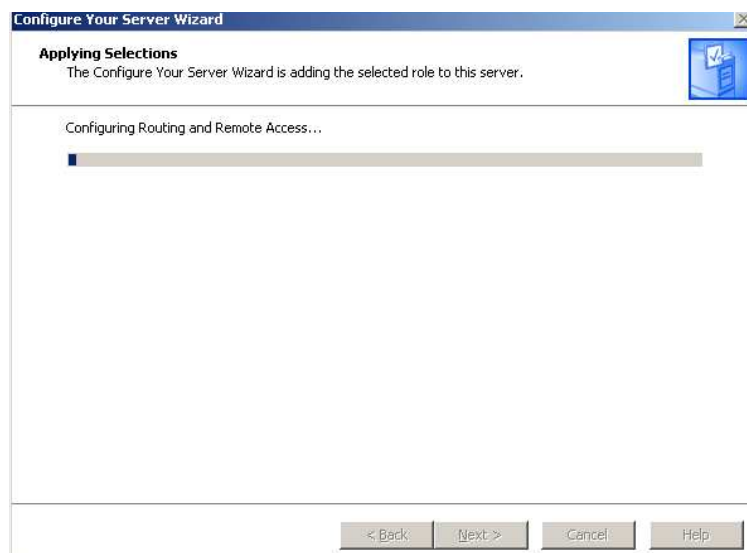
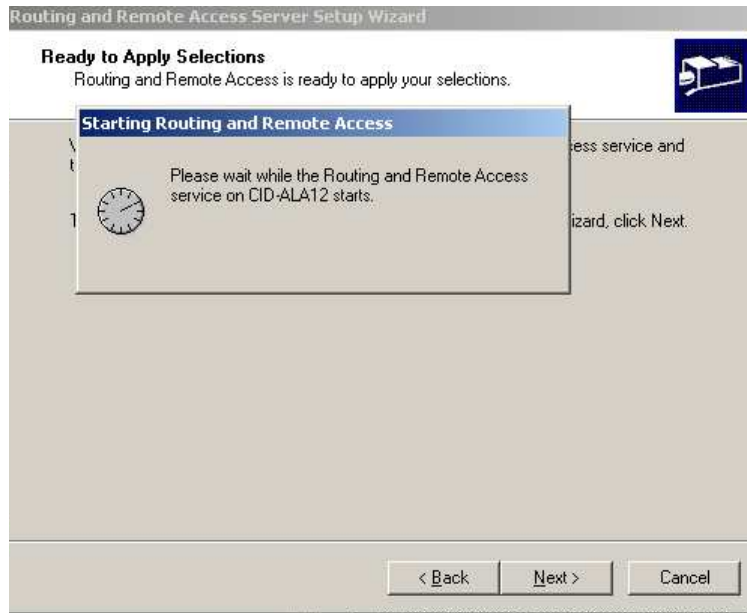


Figura 6. Actualización de los Servicios de Ruteo

Finalizamos el asistente de Ruteo y Acceso Remoto

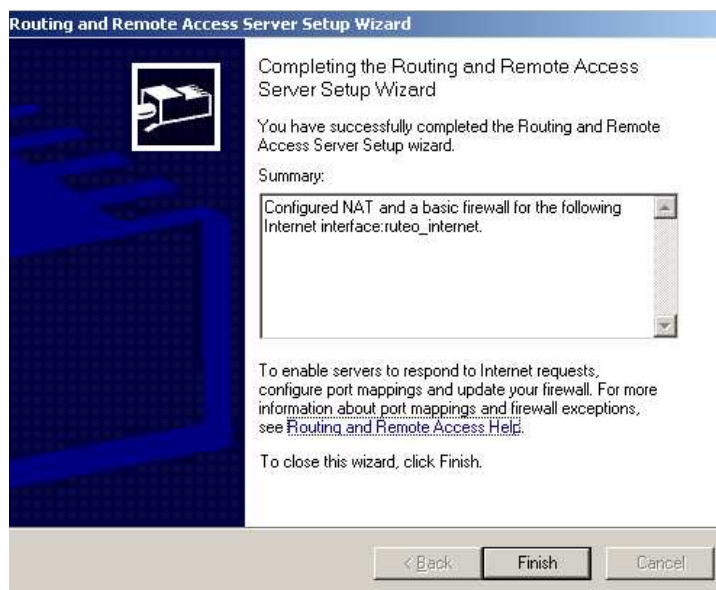


Figura 7. Resumen de configuración los Servicios de Ruteo

6.5.1.2 Instalación del Servidor DHCP

Cada computadora en una red TCP/IP debe tener asignado un nombre y dirección de IP únicos. Esta dirección de IP identifica a la computadora y la subred a la cual pertenece. Cuando una computadora es movida a una subnetwork diferente, la dirección de IP debe ser cambiada para reflejar la nueva Network ID.

DHCP es un protocolo diseñado para reducir la complejidad en la configuración de computadoras para TCP/IP. El RFC 1541 identifica los dos elementos más importantes del DHCP:

- un protocolo de comunicación de parámetros de configuración de TCP/IP entre un servidor de DHCP y sus clientes.
- un método para la alocaión dinámica de direcciones de IP para los clientes de DHCP.

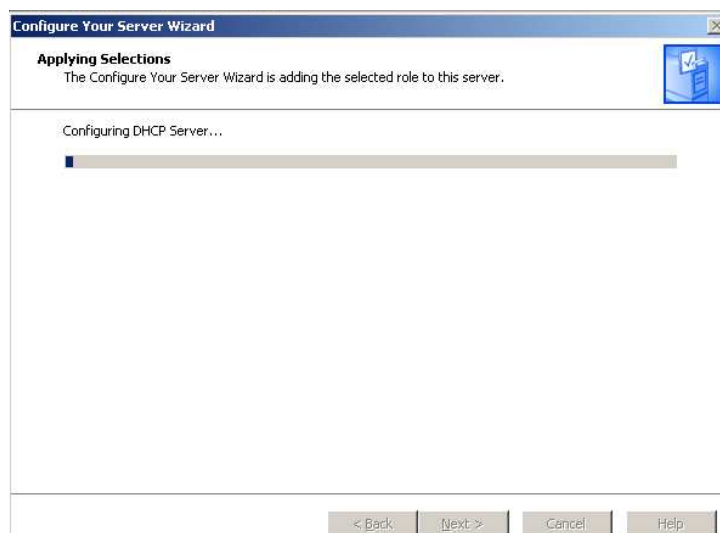
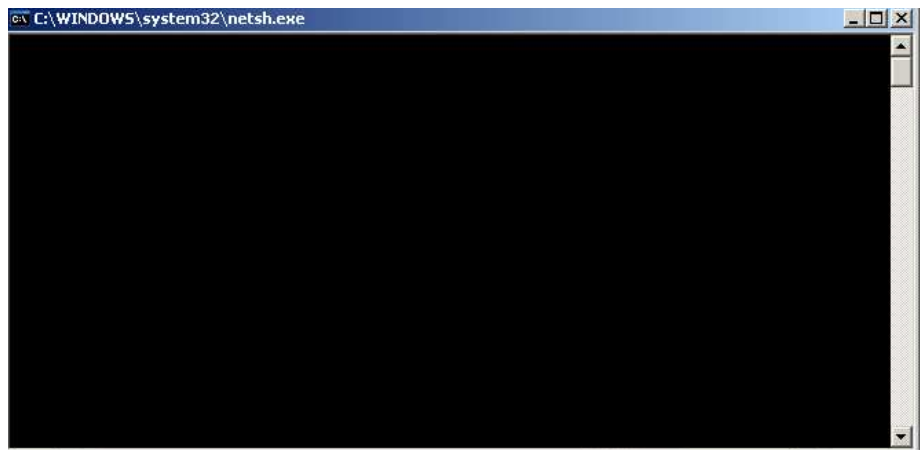
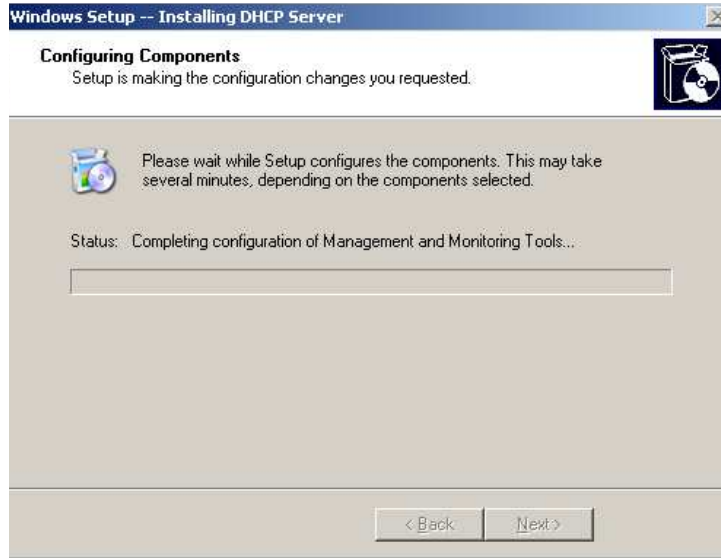


Figura 8. Proceso de instalación del Servicio DHCP (1)

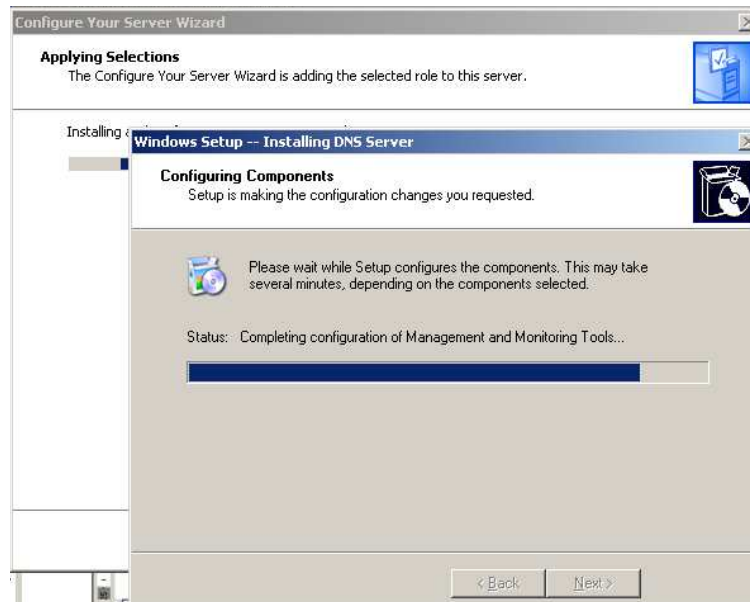
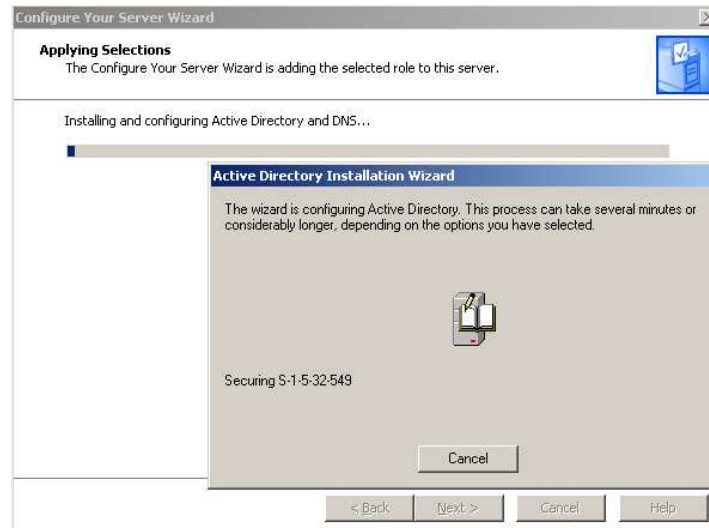


Figura 9. Proceso de instalación del Servicio DHCP (2)

Esperamos que el Asistente actualice el Directorio Activo

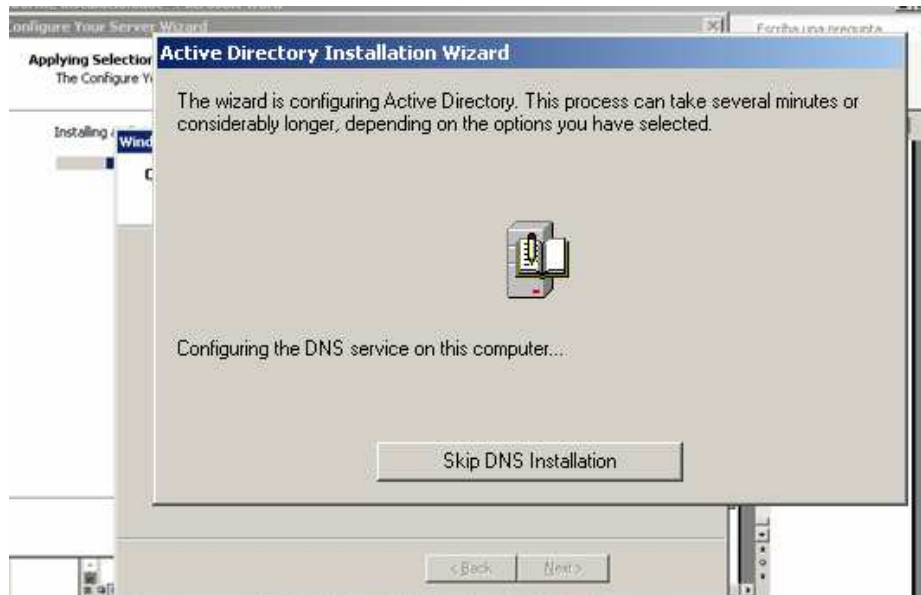


Figura 10. Registro de información en el Servidor

Observamos y verificamos la información en el cuadro de resumen

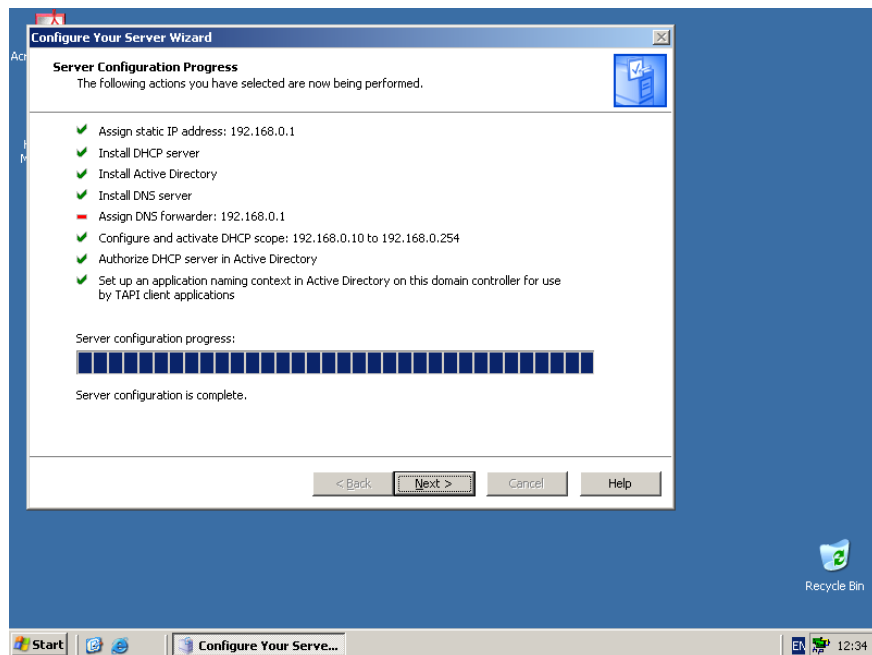


Figura 11. Cuadro de resumen de servicios instalados

Finalizamos configurando la zona de envío y la zona reversa en el DNS

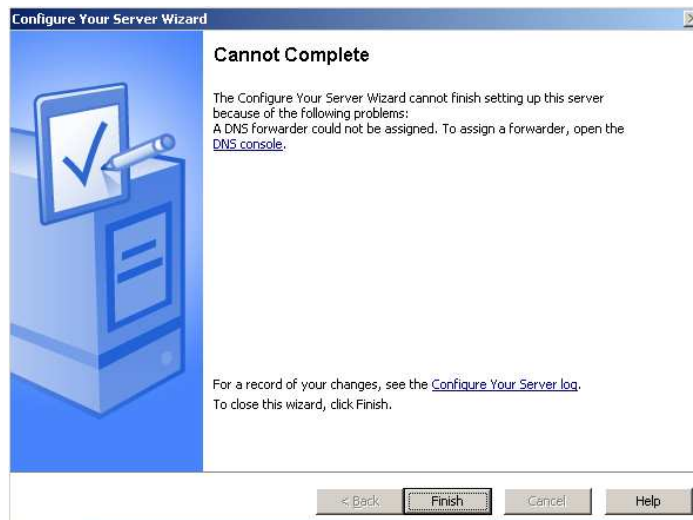


Figura 12. Opción de configuración de zonas

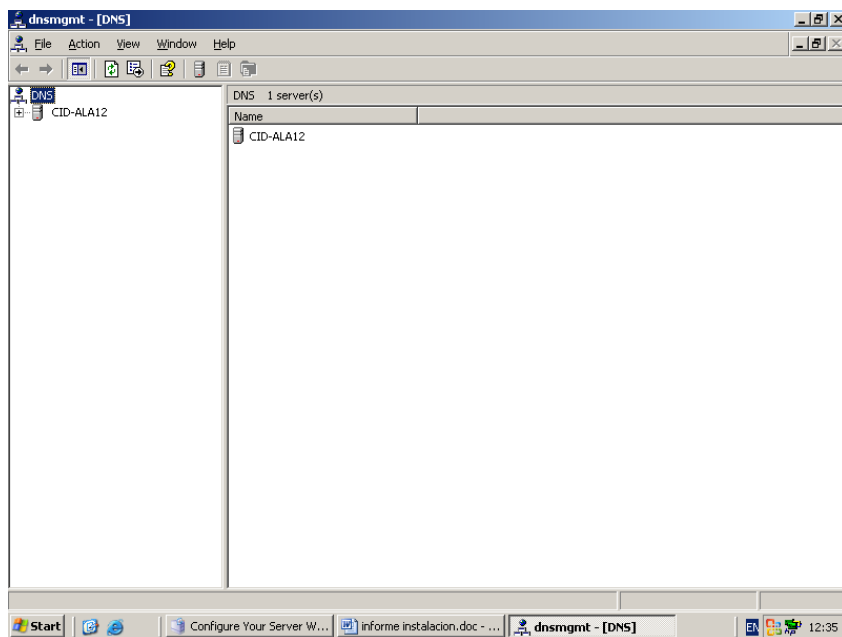


Figura 13. Ventana de DNS Manager

Abrimos el Asistente para crear nuevas Zonas:



Figura 14. Asistente para configurar nuevas zonas

Configuramos una nueva zona primaria:

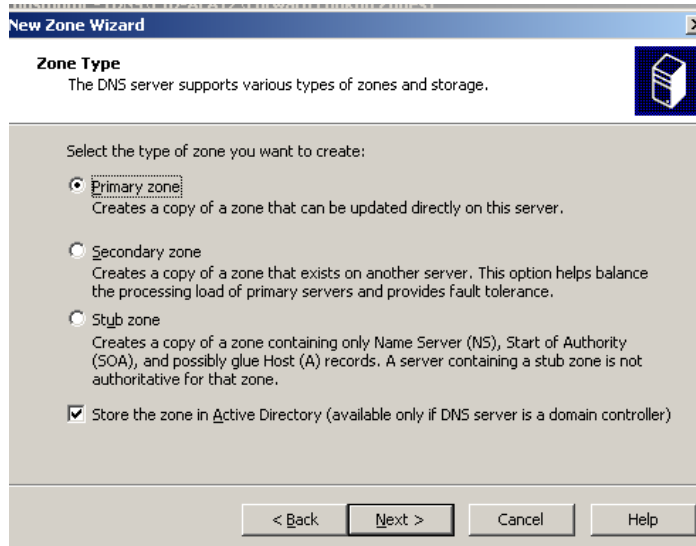


Figura 15. Opción de configuración de tipo de zona

Seleccionamos que la Zona sea replicada a todos los controladores de Dominio en le Dominio del Directorio Activo de CID-DIAF.com

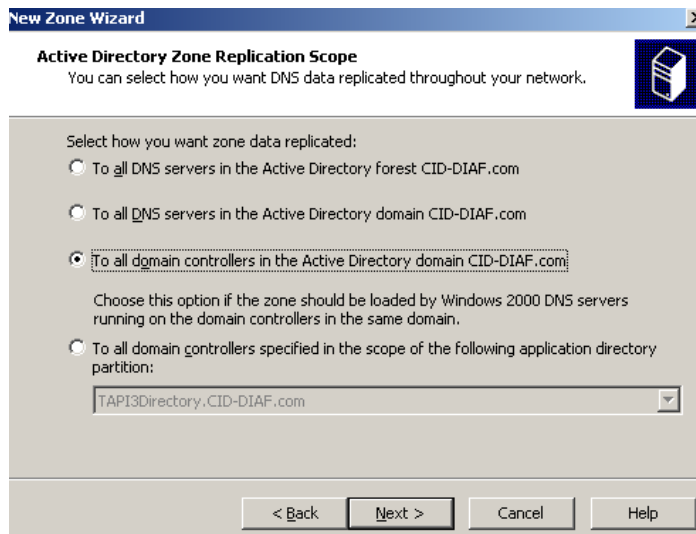


Figura 16. *Ámbito de replicación del DNS*

Nombre de la Zona: edificioCID

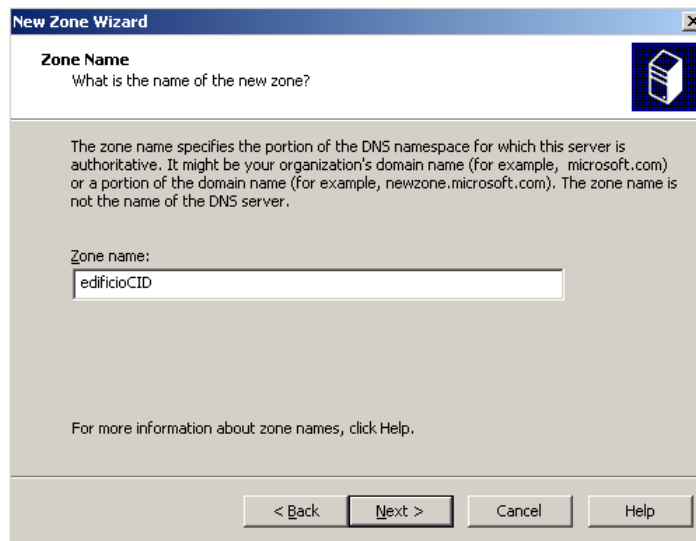


Figura 17. *Nombre de la zona del DNS*

Controlamos que las actualizaciones sean solo de tipo Seguras

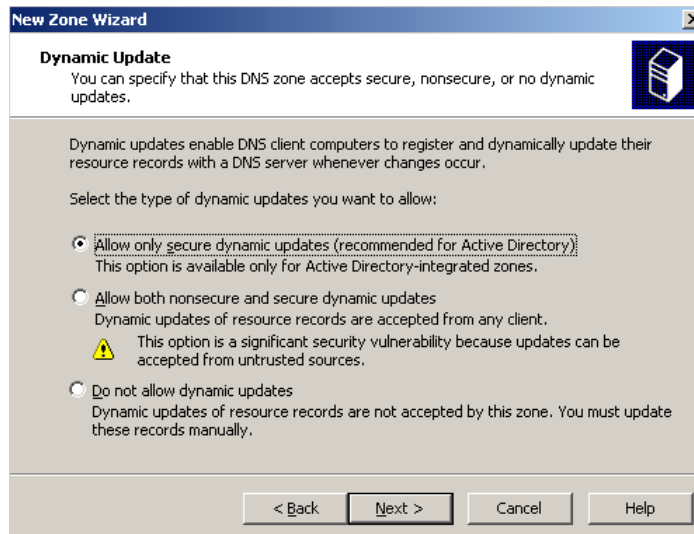


Figura 18. Tipo de actualización de la zona del DNS

Verificamos que los datos sean correctos y finalizamos el Asistente



Figura 19. Cuadro de resumen de la configuración de la zona

Configuramos la Zona Inversa Mediante el asistente:



Figura 20. Cuadro de bienvenida de la configuración de la zona inversa

Ingresamos la dirección de red para la zona reversa: 192.168.0

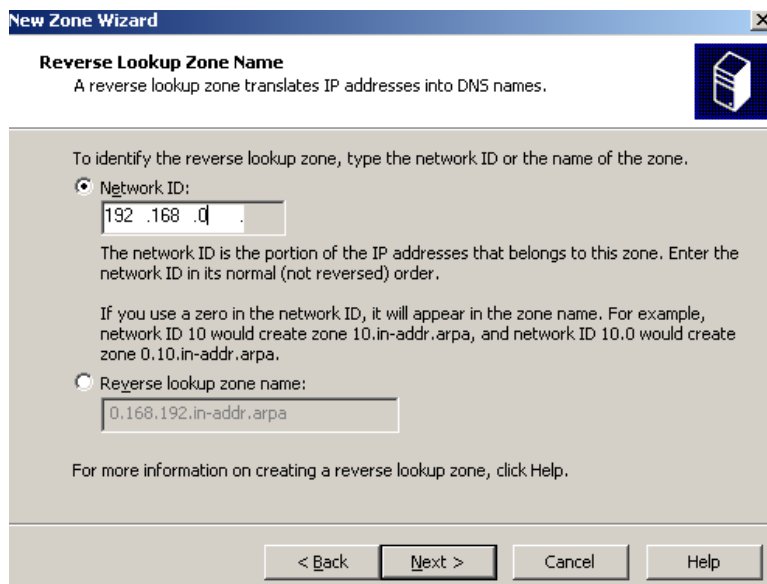


Figura 21. Dirección IP de la zona Inversa para el DNS

Habilitamos solo actualizaciones seguras.

Verificamos la Información en el asistente y finalizamos:



Figura 22. Cuadro de resumen de la configuración de la zona inversa

6.5.1.3 Configuración Servidor de Archivos

6.5.1.3.1 Instalación

Windows Server 2003 tiene instalado de manera predeterminada el cliente para Compartir impresoras y archivos Microsoft.

Es posible crear un servidor de archivos de Windows Server 2003 manualmente o bien utilizando los asistentes incluidos en la herramienta Asistente para configurar un servidor.

Instalación mediante el Asistente

Clic en **Inicio**, **Herramientas administrativas** y luego clic en **Asistente para configurar su servidor**.

Clic en **Siguiente** dos veces, y seleccionar la función de **Servidor de archivos**, y hacer clic en Siguiente.

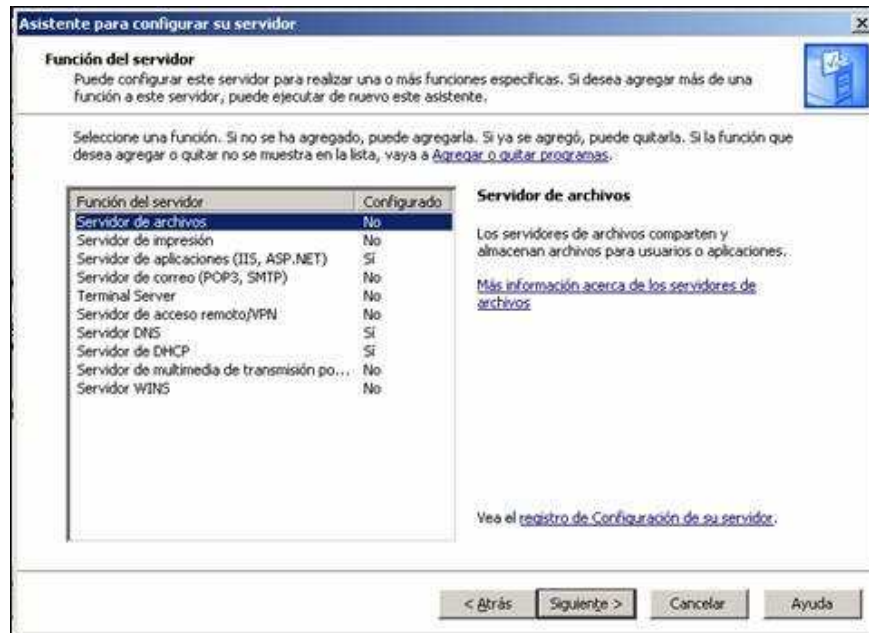


Figura 23. Asistente para agregar servicios en servidor

Activamos la casilla de verificación **Habilitar la administración de cuota** en la pantalla para establecer cuotas de disco, para establecer el uso de espacio es necesario activar la casilla de verificación.

Luego seleccionamos **Limitar espacio de disco a** y escribimos el límite de cuota que se va asignar a los nuevos usuarios del volumen. También, podemos especificar un nivel de advertencia. De manera opcional, es posible seleccionar el registro para cuando suceda un exceso del límite de cuota o advertencia de límite. Otra opción que tenemos es seleccionar es la de denegar espacio de disco a usuarios que hayan excedido el límite de cuota. Con esta opción el usuario que se excedió no podrá seguir escribiendo.

No seleccionamos la activación del servicio de Index Server. Clic en **Siguiente**.

Revisamos el Resumen de las selecciones y clic en **Siguiente**. Luego de un momento aparece el Asistente para compartir una carpeta. Hacer clic en **Siguiente**.

En ruta de la carpeta clic en **Examinar** y navegar hasta la carpeta que vamos a compartir, en este caso: D:\CARPETACID. Clic en **Crear nueva carpeta** si se desea compartir un nuevo recurso. Clic en **Aceptar** y luego en **Siguiente**.

Definimos el nombre del recurso compartido que será el mismo nombre de la carpeta y agregamos una descripción.

Establecemos los permisos. Los mismos definen el nivel de acceso al recurso compartido. La descripción de los permisos es:

- Acceso de solo lectura a todos los usuarios.
- Acceso total a los administradores y solo lectura a los demás usuarios.
- Acceso total a los administradores y acceso de lectura y escritura a los demás usuarios.
- Usar permisos personalizados

Para personalizar los permisos, seleccionamos esta opción y hacemos clic en Personalizar, hacemos clic en **Agregar** y escribir el nombre del usuario o grupo, seleccionar los permisos (control total, cambiar, leer) clic en **Aceptar** y luego en **Finalizar**.

Aparece el siguiente mensaje: “El uso compartido se completo correctamente”.

Hacemos clic en **Finalizar** en la pantalla con el mensaje: “Este servidor es ahora un servidor de archivos”.

6.5.1.3.2 Asignación de Permisos

Ejecutamos el Explorador de Windows.

Hacer clic con el botón secundario del mouse sobre la carpeta a configurar y luego hacer clic en **Compartir y seguridad**.

Clic en la ficha **Seguridad** y luego en **Agregar** y escribir el nombre de usuario o grupo de dominio que se desea agregar. Clic en **Aceptar**. Fig 24

Seleccionamos los permisos que se desean asignar y hacer clic en **Aceptar**.



Figura 24. Cuadro de propiedades de Documentos

Administración de un Servidor de Archivos

La consola Administración de servidores de archivos se compone de los siguientes complementos: Recursos compartidos: Ver y administrar todas las carpetas compartidas.

- Sesiones: Usuarios conectados al servidor.
- Archivos Abiertos: Ver todos los archivos abiertos por los usuarios.
- Desfragmentador de disco: Analizar la desfragmentación de volúmenes.

- Administrador de discos: Administrar discos y volúmenes.

Al contar con estos complementos en una sola consola, se puede administrar los recursos compartidos, volúmenes y discos de manera centralizada.

Pasos para iniciar la consola Administración de servidores de archivos:

Clic en Inicio, Herramientas Administrativas y, Administre su servidor.

Clic en la opción Administrar este servidor de archivos. Nos aparecerá la consola Administración de servidores de archivos. Fig. 25

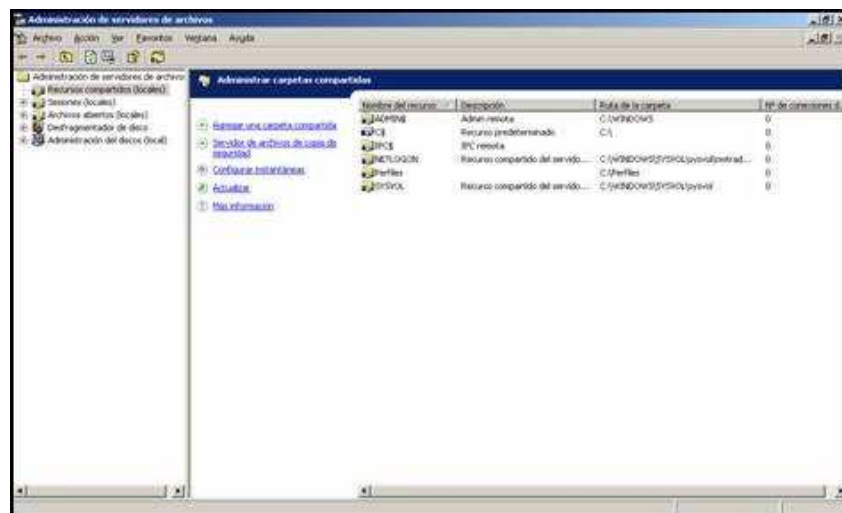


Figura 25. Consola de administración de servidores de archivos

6.5.1.4 Instalación del Servidor de Impresión

6.5.1.4.1. Impresora Minolta Magicolor 2480MF

Características: Ver Anexo 3

6.5.1.4.2. Instalación de impresora

Entrar a **Impresoras y faxes**.

Opción **Agregar impresora**.

Seleccionar la opción que describe la impresora en este caso una **impresora local** y clic en **Siguiente**.

Seleccionamos un puerto existente. Clic en Siguiente.

Seleccionar el fabricante y el modelo de impresora. Elegimos Utilizar disco puesto que es una impresora que no esta en la lista. Hacer clic en Siguiente.

Realizamos la instalación de la impresora: Minolta Magicolor 2480MF

Asignamos un nombre a la impresora: Centro de Impresiones. Clic en Siguiente.

Procedemos a compartir la impresora

Ir a impresoras y faxes, clic derecho y propiedades

Ir a la pestaña Compartir Asignar un nombre para compartir y aceptar. Fig 26.

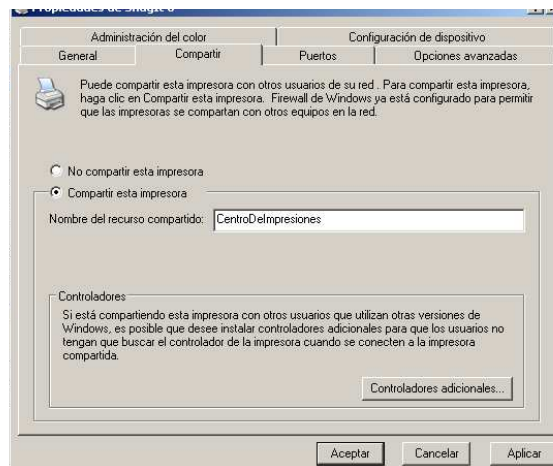


Figura 26. Cuadro de propiedades de la impresora

Podemos asignar permisos específicos accediendo a la pestaña **Seguridad**.

Clic en la ficha Seguridad y luego Agregar, escribimos el nombre de usuario o grupo de dominio que se desea agregar según las reglas establecidas y clic en Aceptar.

Seleccionamos los permisos que se desean asignar y clic en Aceptar.

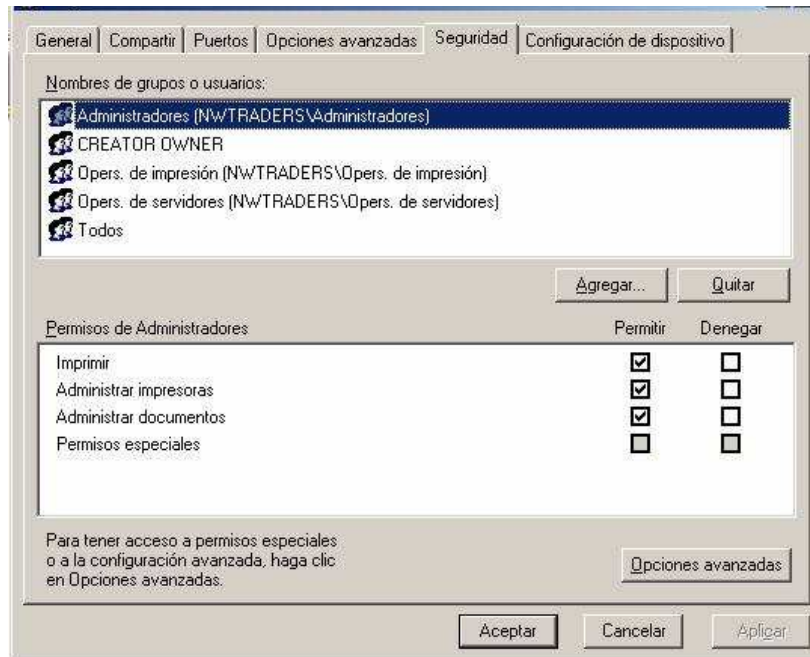


Figura 26. Cuadro de propiedades de seguridad de la impresora

6.5.2 Configuración del Servidor FTP

6.5.2.1. Instalación

Para realizar una sesión de FTP, se utilizan diferentes conexiones: una se usa para transportar comandos entre el cliente y el servidor, y la otra para transportar los datos. El canal de comandos utilizado por el servidor se encuentra en el puerto 21, y el de datos en el 20. El cliente, utiliza puertos por encima del 1023 tanto para el canal de datos como para el de comandos. También se pueden utilizar conexiones en modo “pasivo” en donde el cliente no identifica el canal de datos, y es el servidor el que utiliza un canal superior al 1023, que es utilizado exclusivamente por el cliente.

La alternativa más sencilla es poseer un servidor de FTP en la entrada de la red, en donde éste puede ser accedido por los clientes de la red, como desde fuera. Esto posee varias desventajas: la sobrecarga del servidor principal (que contiene a todos los servicios), y algunos inconvenientes de seguridad, ya que puede ser accedido desde el exterior.

Utilizando un proxy socks en el proxy server, se puede configurar al servidor de FTP en algún lugar interno de la red, en el cual pueda ser accedido por los clientes internos, y por los externos a través del proxy.

La mejor alternativa es la de disponer un servidor de FTP global de la red, el cual puede ser accedido tanto desde fuera como desde las subredes, y servidores locales internos.

La seguridad es inmediata: los servidores locales son totalmente seguros, ya que no existe el acceso a los mismos por agentes externos, y la seguridad del servidor general está dada por el Proxy.

Así comenzamos por crear una carpeta que será compartida para el servicio FTP. Fig 27

Nombre de la carpeta: ARCHIVOSFTP

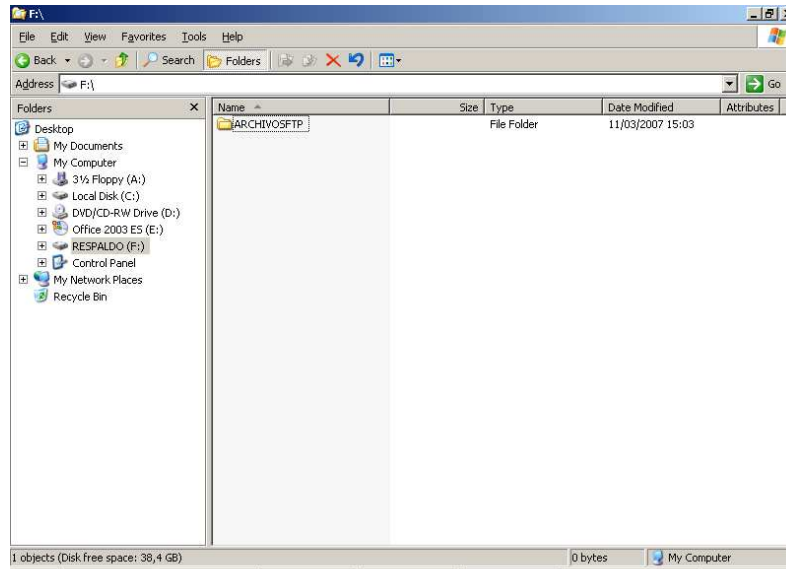


Figura 27. Creación de carpeta compartida FTP

Mediante el asistente de instalación de servicios procedemos a instalar el servicio FTP. Fig 28

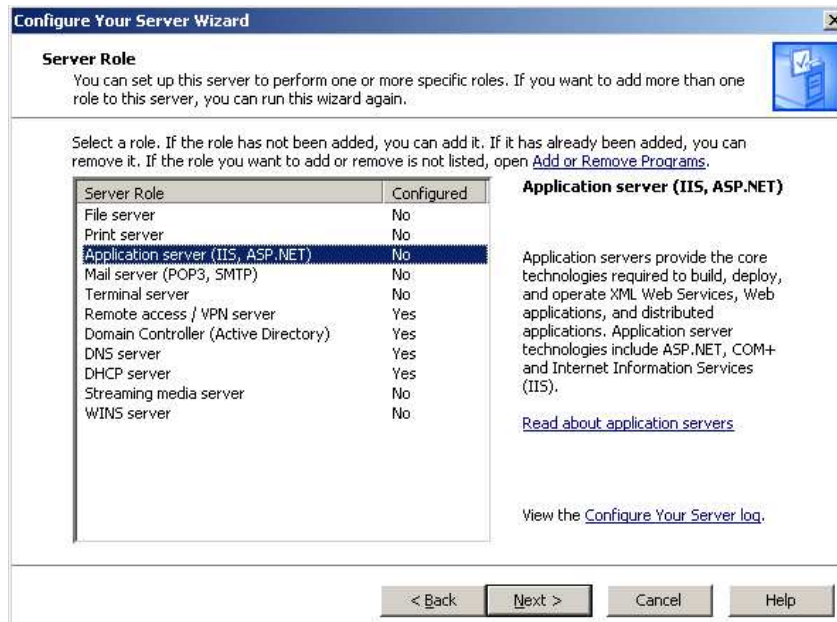


Figura 28. Asistente para agregar el servicio FTP

Elegimos la opción File Server y continuamos.

Esperamos que el asistente termine de instalar el Servicio.



Figura 29. Proceso de instalación del servicio FTP

Verificamos si la información es correcta en el asistente y finalizamos.

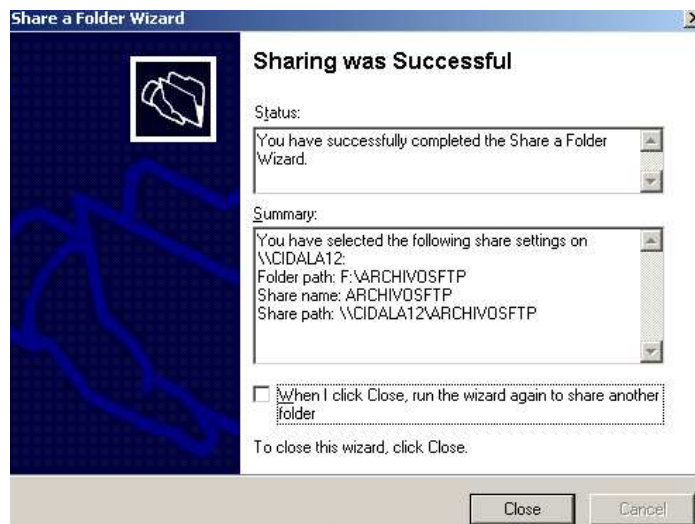


Figura 30. Cuadro de resumen de instalación del servicio FTP

6.5.2.2. Configuración del sitio FTP

Vamos a utilizar la característica que incorpora IIS6 denominada **Aislar Usuarios**. Este modo autentica a los usuarios contra cuentas locales o de dominio antes de permitirles el acceso al directorio particular correspondiente a su nombre de usuario. Todos los directorios principales de los usuarios se encuentran en un mismo directorio raíz FTP, en el que cada usuario únicamente puede obtener acceso y está restringido a su directorio particular.

Borramos el sitio FTP predeterminado. Fig 31.

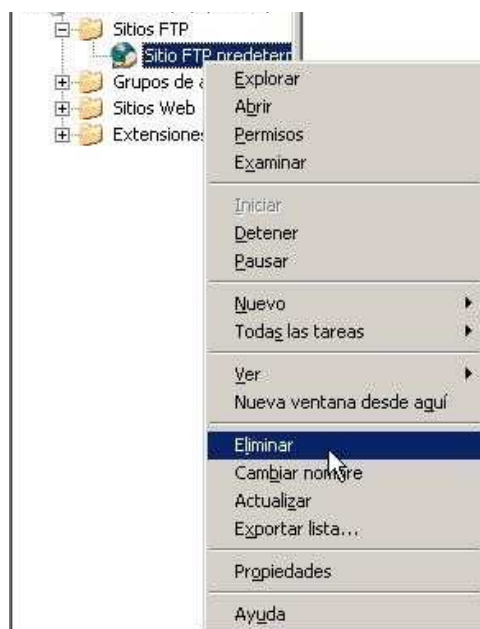


Figura 31. FTP Manager

Creamos un nuevo sitio FTP haciendo click derecho en **Sitios FTP**, **Nuevo** y luego **Sitio FTP**, click en **Siguiente** para aceptar la pantalla de bienvenida.

Escribimos una descripción que identifique claramente al sitio "Sitioftp" y click en **Siguiente**.

Asignamos una dirección IP que será la misma que usamos para levantar los otros servicios y dejamos el puerto 21 como puerto estándar.

Click en **Siguiente**. Elegimos la opción **Aislar Usuarios** para permitir que cada usuario deje el contenido en su propio directorio y no pueda acceder a ningún otro y click en **Siguiente**.

Elegimos la ruta del directorio raíz que en nuestro caso será D:\ftp\SitioWeb1.

Click en **Siguiente** y elegimos **lectura y escritura**.

Click en **Siguiente** y luego en **Finalizar**.

Click derecho en el sitio recientemente creado y vamos a propiedades. En la pestaña “**Cuentas de Seguridad**” y deshabilitamos la opción “**Permitir conexiones anónimas**”, aceptamos y finalizamos. Fig 32

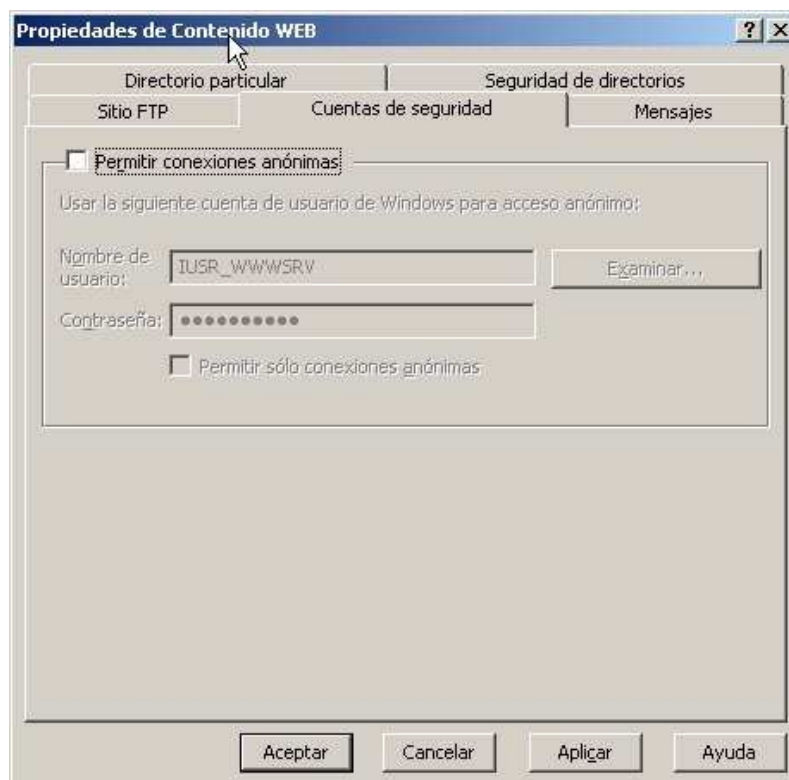


Figura 32. Cuadro de propiedades del contenido WEB

Creamos un usuario por cada sitio web para el cual se cargará contenido. Vamos a crear un usuario de prueba. Esto lo hacemos mediante consola.

Inicio>Ejectuar>command y aceptar:

Tecleamos lo siguiente:

```
C:\> net user SitioWeb1 P@ssw0rdC0mpleX /add
```

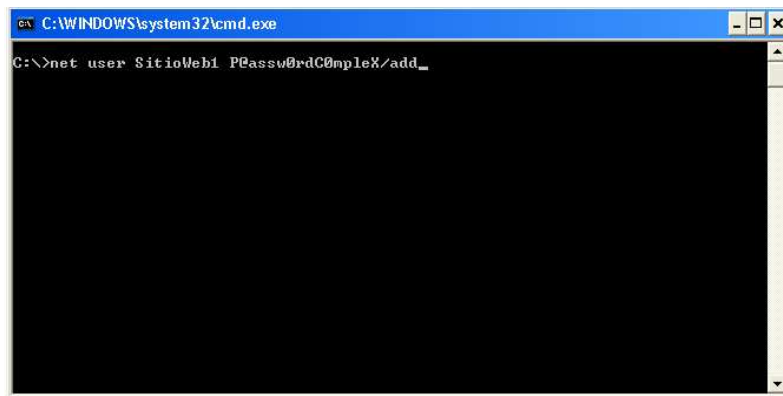


Figura 33. Consola de comandos para crear un usuario FTP

En el directorio raíz creamos una subcarpeta llamada LocalUser.

Dentro de **LocalUser** creamos una carpeta por cada usuario autorizado a subir contenido. En nuestro ejemplo crearemos las carpetas sitioweb1. Fig 34



Figura 34. Carpetas creadas para el servicio FTP

Click derecho en cada carpeta y en la pestaña “**Seguridad**” asignamos permisos de lectura y escritura únicamente al usuario creado anteriormente, y que coincida con el nombre de la carpeta. Fig 35.

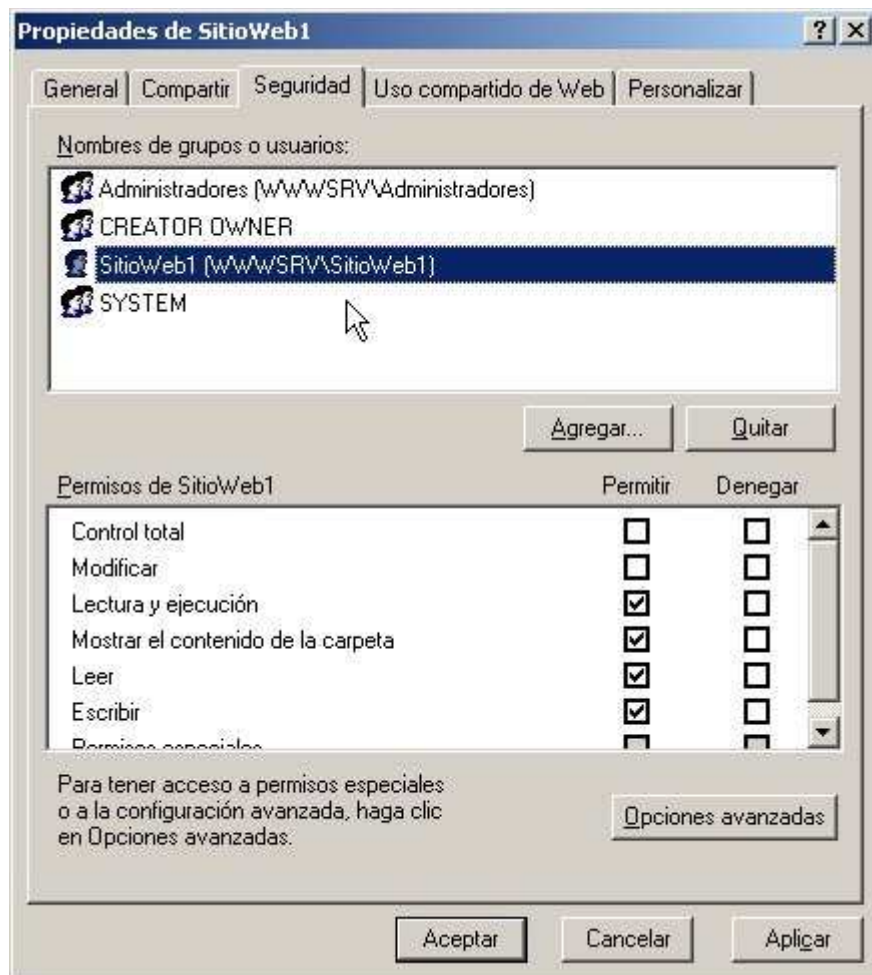


Figura 35. Cuadro de Propiedades del Sitio Web

Verificamos que ningún otro usuario tenga permisos en esa carpeta a excepción de Administradores, System y Creator Owner.

Probamos el procedimiento iniciando una sesión ftp con uno de los usuarios creados recientemente.

6.5.3. Configuración del Internet Information Server (IIS 6.0)

Windows Server 2003 viene también con la plataforma ASP.NET 1.1 que están diseñada para integrarse con el IIS 6.0.

El IIS 6.0 y el ASP.NET 1.1 no vienen agregados en el disco de instalación de Windows 2003 Server, por lo tanto iniciaremos desde su instalación

Nos dirigimos a la opción Añadir y Quitar programas del panel de control como se muestra en la imagen. Fig 36

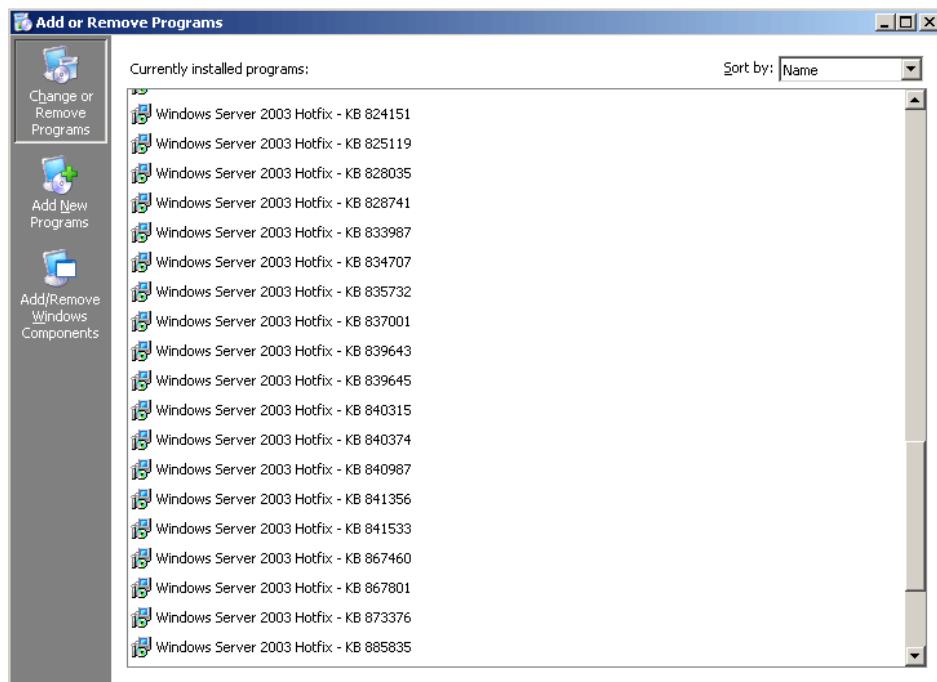


Figura 36. Opción de añadir remover programas de Windows 2003 Server

Click en Añadir/Remover componentes de Windows lo que iniciara un asistente como se muestra abajo.

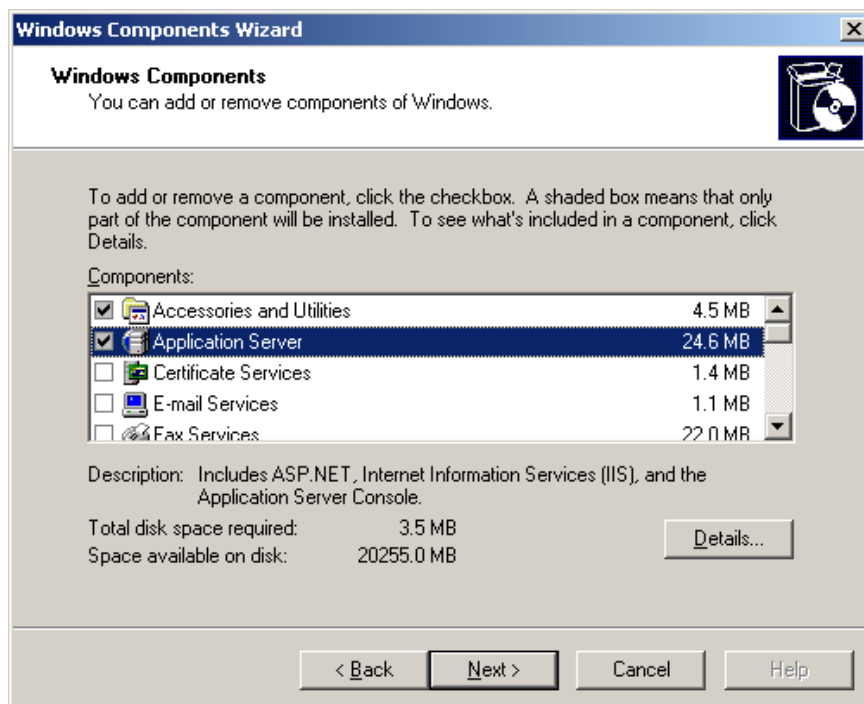


Figura 37. Cuadro de dialogo para añadir servicios a Windows 2003 Server

Doble click sobre **Aplicación Services** para acceder a una nueva ventana donde elegiremos los servicios que necesitamos: **IIS y ASP.NET**. Fig 38

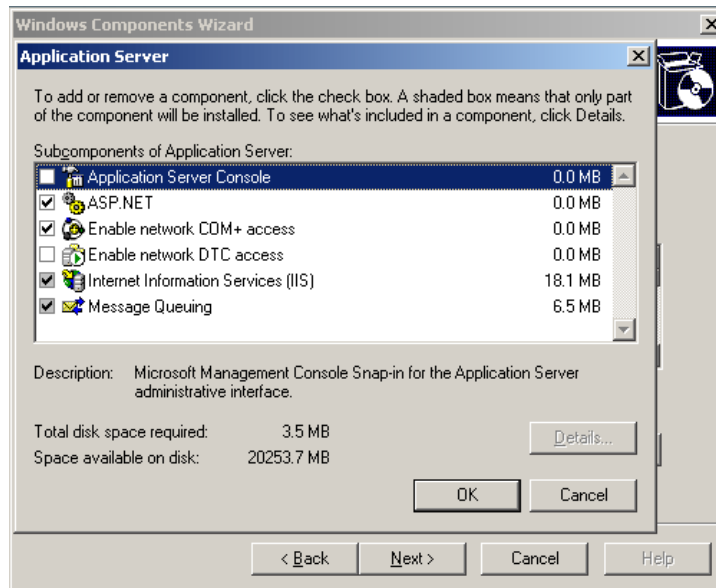


Figura 38. Cuadro de selección de componentes

Aceptamos y esperamos a que el asistente termine la instalación. Fig 39

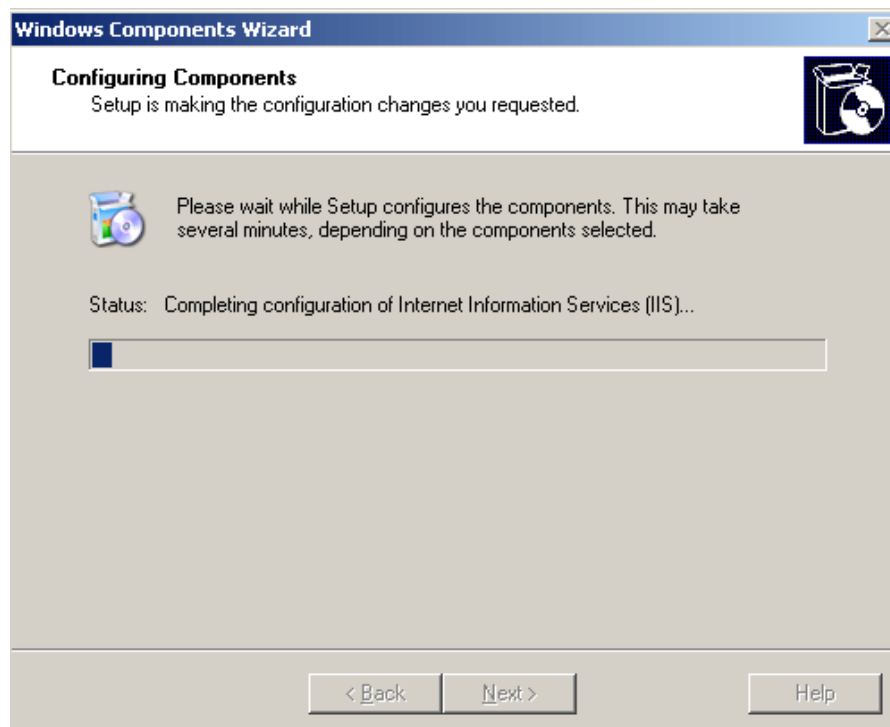


Figura 39. Proceso de instalación de los servicios IIS.

Cuando la instalación finalice el asistente mostrara un mensaje de instalación exitosa, y finalizamos.



Figura 40. Instalación exitosa de los servicios IIS.

De esta manera ya tenemos instalado el IIS 6.0, accedemos desde el panel de control, Herramientas Administrativas, Internet Information Service para su posterior configuración.

6.5.3.1 Crear el sitio Web en IIS 6.0

Por defecto el IIS 6.0 viene con un sitio Web predeterminado, pero para el efecto del proyecto vamos a crear uno con los parámetros establecidos en los capítulos anteriores.

Procedemos a eliminar el sitio Web predeterminado. Fig 41.

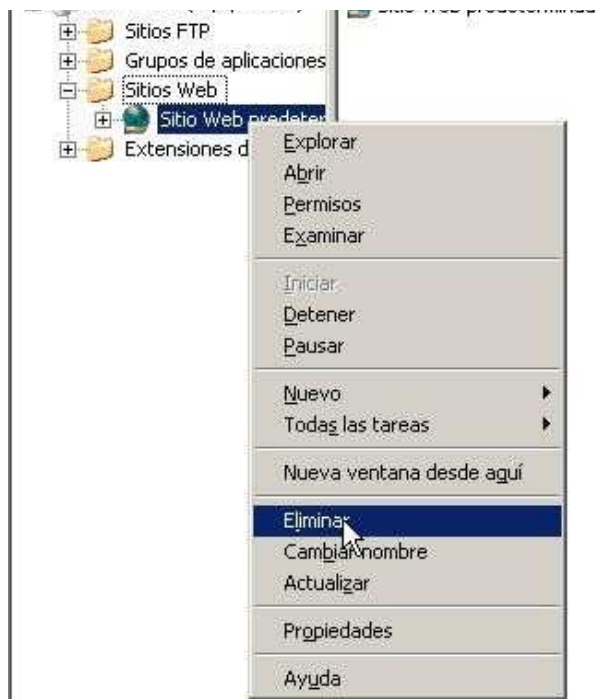


Figura 41. IIS Manager.

Creamos un sitio nuevo haciendo click derecho en el nodo **Sitios Web**, **nuevo**, y luego **Sitio Web**, para iniciar el asistente de creación de sitios.

Click en **Siguiente** para pasar la pantalla de bienvenida. Escribimos el nombre del sitio que será: SITIOWEBCID y click en **Siguiente**. Luego elegimos una dirección IP en *Escriba la dirección IP para este sitio Web* que será la que nos asigne el proveedor de Internet en caso de querer tener acceso. Elegimos el puerto, típicamente puerto 80 y Asignamos el Encabezado host en la caja de texto *Encabezado de host para este sitio web (predeterminado ninguno)*: www.cid-fae.com, click en **Siguiente**.

Elegimos la ruta de acceso donde el contenido del sitio estará ubicado que será en la dirección: D:\SITIOWEBCID y dejamos habilitado **Permitir accesos anónimos a este sitio web** puesto que va un sitio público, y click en **Siguiente**.

En la pantalla *Permisos de acceso al sitio web* elegimos solo **Leer** puesto que el contenido será solo estático (html).

Elegimos opcionalmente *Ejecutar secuencias de comandos (por ejemplo ASP)*, puesto que posteriormente se puede agregar páginas con contenido dinámico. Click en **Siguiente** y luego en **Finalizar**.

6.5.4. Configuración de Microsoft Exchange Server 2003

6.5.4.1 Instalación

Insertamos el Disco de Exchange Server 2003 en la unidad de CD-ROM. En el menú **Inicio**, clic en **Ejecutar** y escribimos `E:\setup\i386\setup`, donde *E* es la unidad de CD-ROM. Fig 42.

Doble clic en SETUP.EXE

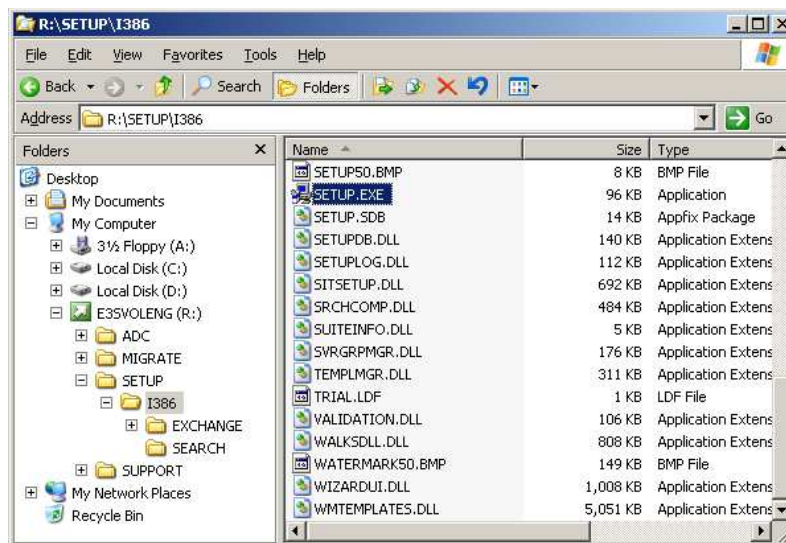


Figura 42. Instalación de Microsoft Exchange Server desde un disco de instalación.

Se abre un asistente de instalación pasamos la pantalla de bienvenida

Aceptamos el contrato de licencia. Fig 43

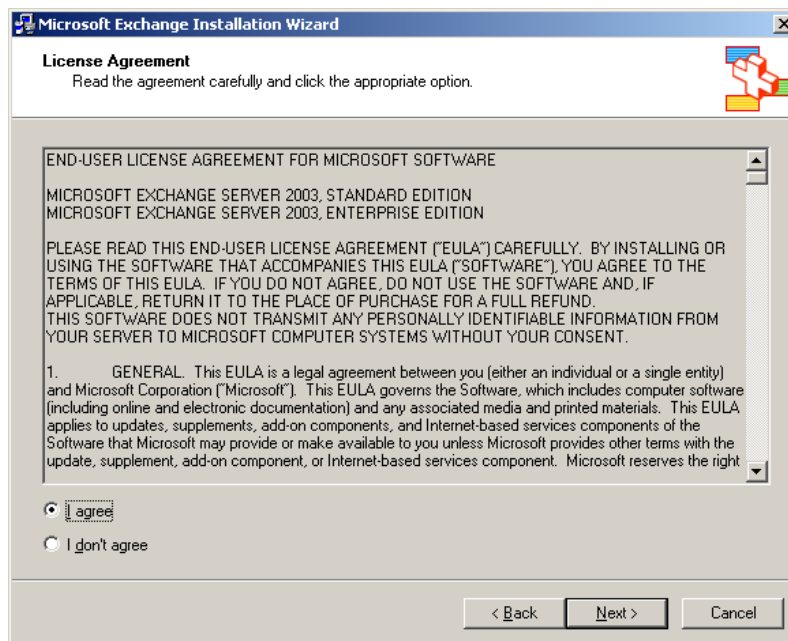


Figura 43. Cuadro de Acuerdo de licencia de Microsoft Exchange Server.

Seleccionamos los componentes que deseamos instalar y dejamos el directorio por defecto. Fig 44.

Microsoft Exchange Messaging and Collaboration Services y Microsoft Exchange System Management Tools

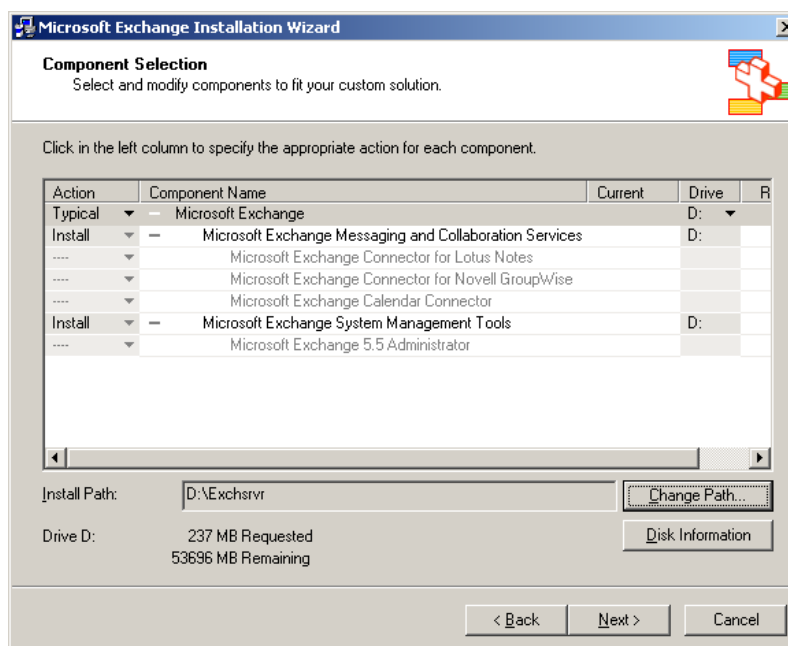


Figura 44. Cuadro de selección de componentes de Microsoft Exchange Server.

En tipo de instalación Elegimos:

Crear una nueva organización Exchange

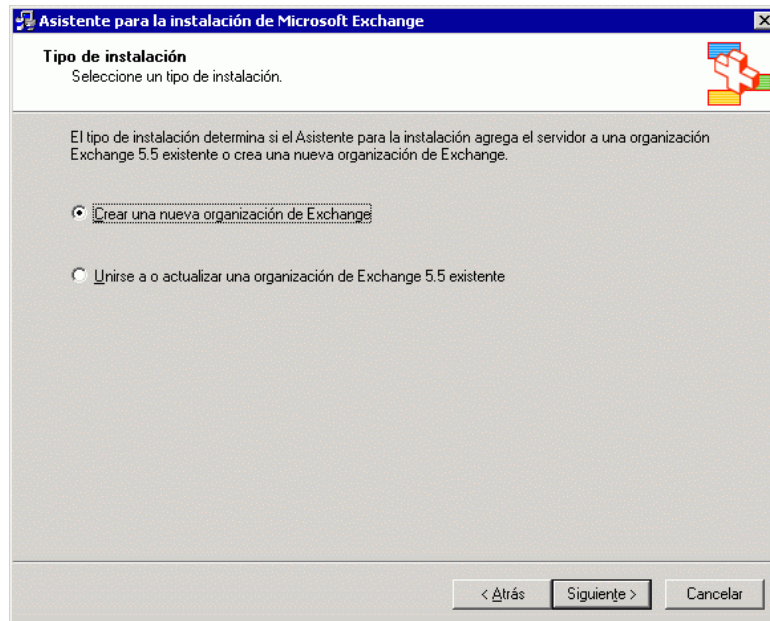


Figura 45. Cuadro de Acuerdo de licencia de Microsoft Exchange Server.

En el cuadro **Nombre del servidor Exchange**, escribimos el nombre de un servidor Exchange que hemos creado, que será el siguiente: cid_srv_web

En la página cuenta de servicio elegimos una contraseña para la cuenta de servicio que es la siguiente: adminTI01. Fig 46.

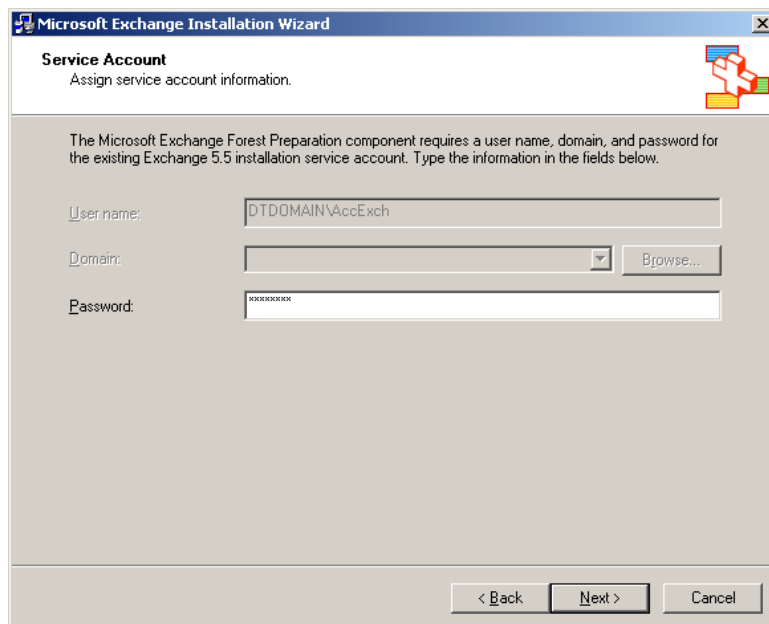


Figura 46. Cuadro de Información de cuenta de Microsoft Exchange Server.

Verificamos la información en la ventana de Resumen de la instalación, y click en Siguiente.

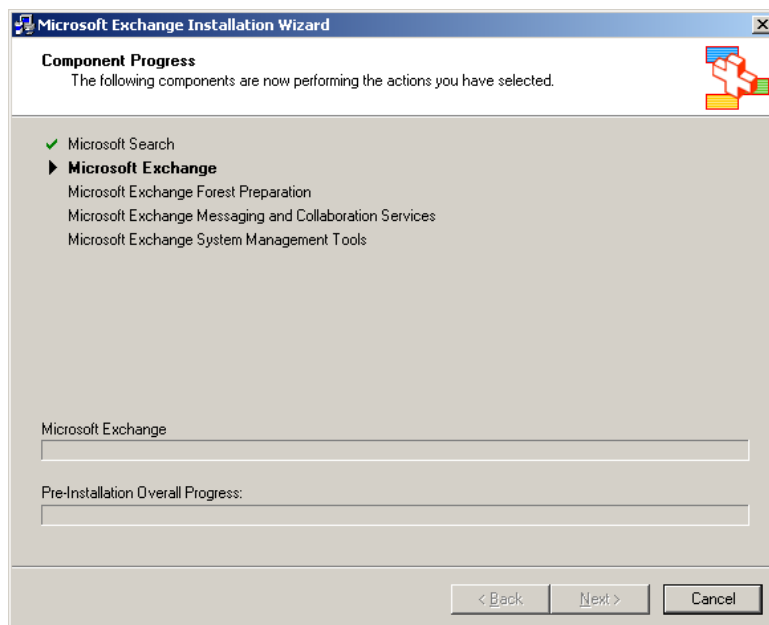


Figura 45. Cuadro de resumen de instalación de Microsoft Exchange Server.

Finalizamos el asistente.

6.5.4.2. Configuración del servidor de correo

Múltiples Dominios

Empezamos dando correo a todos los dominios que queramos. Abrimos el Administrador del sistema. Vamos hacia Destinatarios/Directivas de destinatarios. En la política por defecto vamos a modificar unas cosas:

Vamos a "Direcciones de correo electrónico (directiva)"



Figura 46. Cuadro propiedades de las políticas de correo electrónico

Pulsamos en nueva. Fig 47



Figura 47. Opción añadir una nueva cuenta

Dirección de SMTP



Figura 48. Dialogo añadir una nueva cuenta SMTP

El nombre del dominio precedido de una @. Repetir este paso y los dos anteriores tantas veces como dominios queramos servir.



Figura 49. Cuadro de propiedades de Dirección SMTP

Es importante decir en este paso que NO. Cuando damos a Aplicar, nos aparece este interrogante, decir que NO

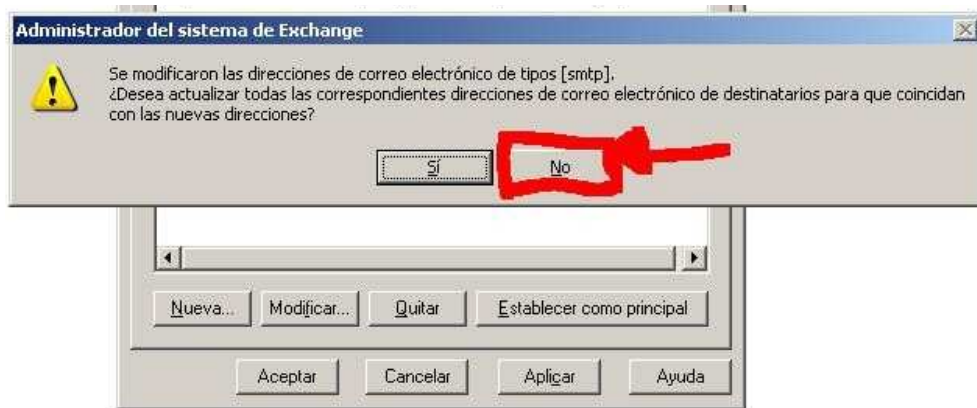


Figura 50. Dialogo modificar una cuenta SMTP existente

Almacenamiento de buzones

Partimos de la base de que no se ha creado todavía ninguna cuenta. Para que cada buzón este en el sitio que corresponda nos vamos a Servidores/"nombre del servidor"/ Primer grupo de almacenamiento. Fig 51:



Figura 51. Administrador del sistema de Exchange

Dejar todo por defecto. El almacén por defecto se guarda en: c:\Archivos de programa\Exchsrvr\MDBDATA



Figura 51. Propiedades de almacenamiento del sistema de Exchange

Seleccionamos la opción SI para montar el almacén

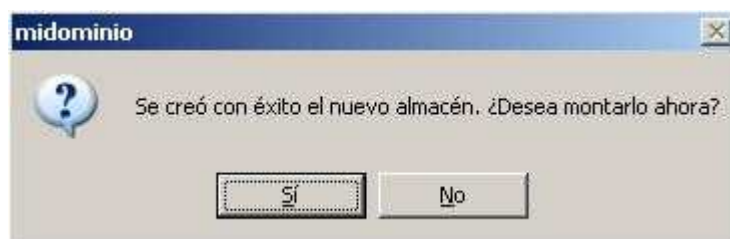


Figura 52. Cuadro de dialogo de las propiedades de almacenamiento del sistema

Montando el nuevo almacén

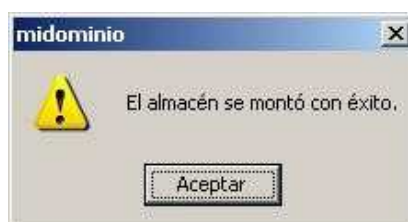


Figura 53. Cuadro de resumen de las propiedades de almacenamiento del sistema

Comprobamos que almacén esta creado.



Figura 54. Administrador del sistema de Exchange

Como no hemos añadido ningún buzón, estos son los que están por defecto.

Alta de usuarios

Lo primero abrir "Usuarios y equipos de Active Directory" que se encuentra en Inicio/Programas/Microsoft Exchange/usuarios y equipos. Una vez abierto:

Creamos una nueva unidad organizativa

Dentro de la unidad organizativa creamos un usuario, de estas dos maneras, o bien desde el icono de arriba o con el botón derecho "nuevo\usuario"



Figura 55. Cuadro de dialogo para creación de una nueva unidad organizativa

Rellenamos a nuestro gusto o exigencias

Para las contraseñas por defecto en Windows 2003 han de ser de un mínimo de 7 caracteres, con alguna mayúscula y algún número.



Figura 56. Cuadro de dialogo para creación de un nuevo usuario

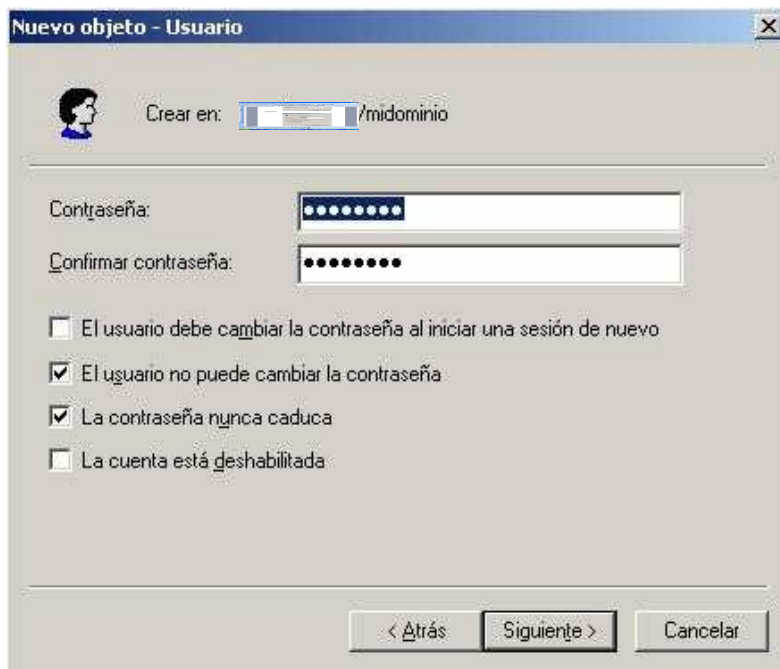


Figura 57. Cuadro de dialogo creación de contraseña para el usuario

Le asociamos un buzón de Exchange

Aquí buscamos el almacén donde queremos que este el usuario.

Finalizamos

Iniciar el servicio POP3

Este servicio por mucho que se intente activar desde la consola de administración de Exchange no se va a poder, o va no ha sido capaz. Pero

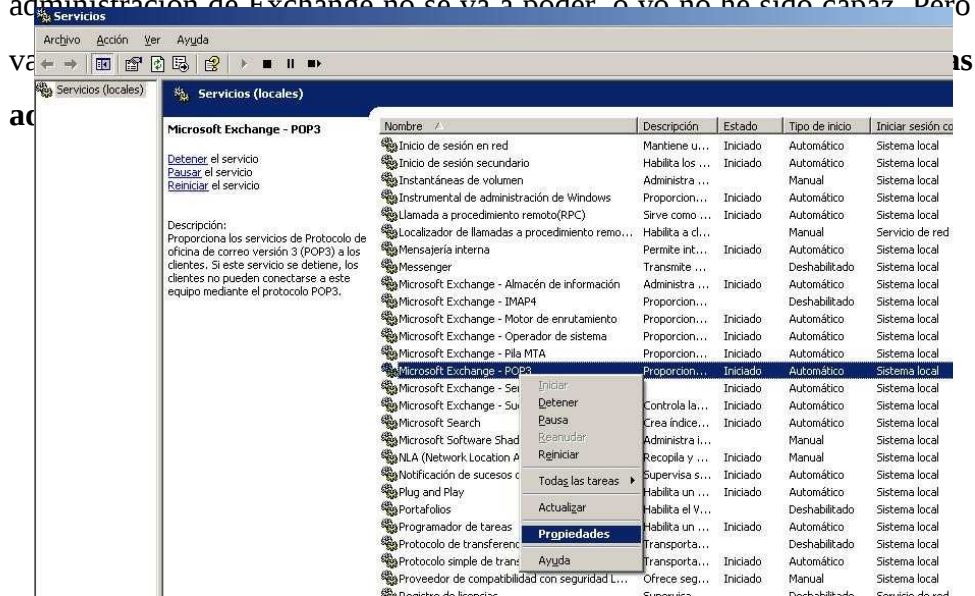


Figura 58. Administrador de Servicios de Windows 2003 Server

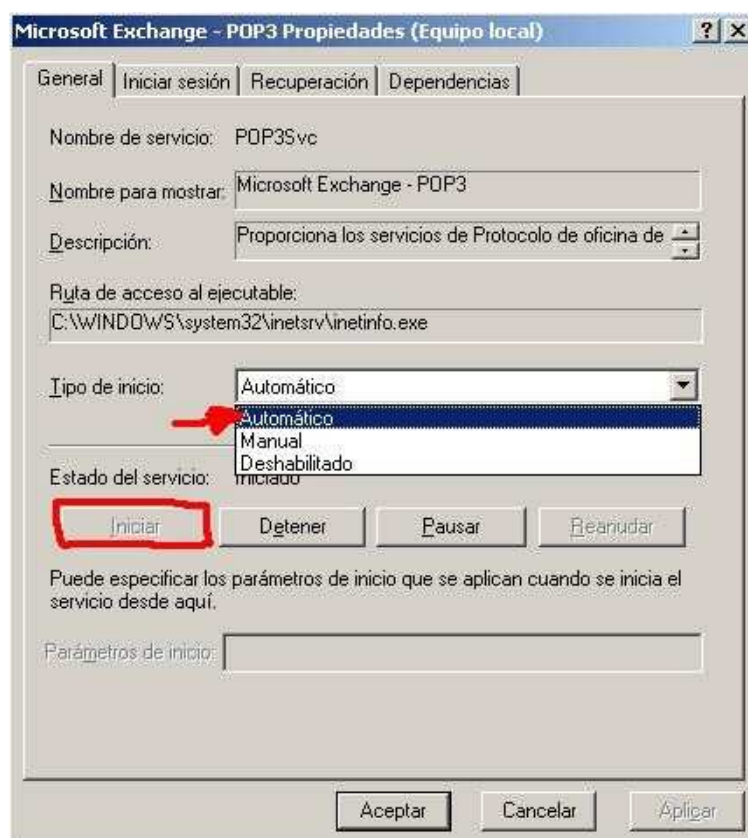


Figura 59. Cuadro de propiedades del servicio POP3

No tiene mas, y una vez levantado desde aquí ahora si que podemos detener pausar y volver a iniciar desde el administrador de sistema de Exchange.

Administración de Exchange

Servidor virtual POP3: se puedes cambiar el nombre eso no cambia nada. A continuación las capturas de pantalla de como debe estar.

Abrimos Servicios yendo a **Inicio > Panel de Control > Herramientas Administrativas > Servicios**

Seleccionamos Microsoft Exchange POP3. Fig 60

Click derechos y **Propiedades**

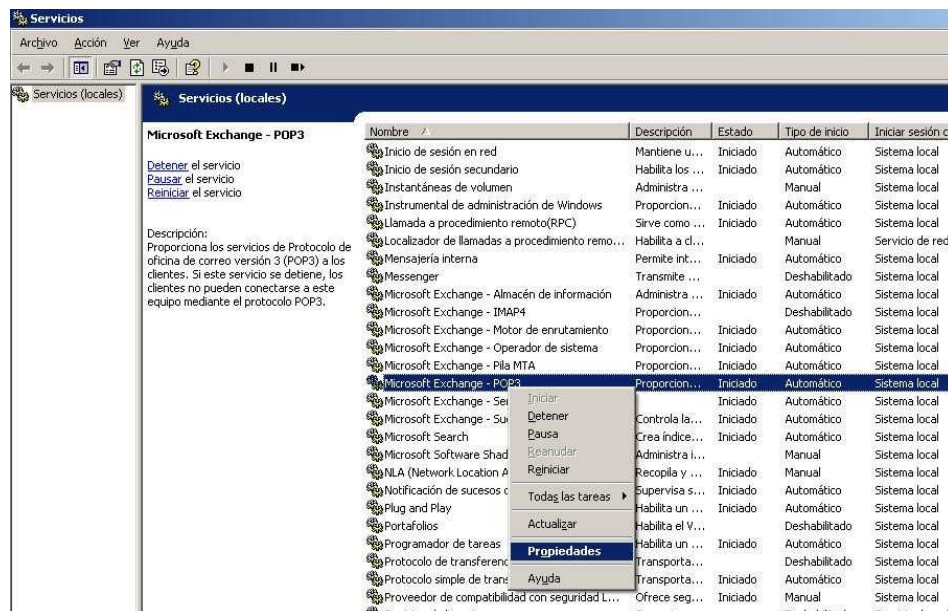


Figura 60. Proceso para iniciar el servicio POP3

En la pestaña general, en tipo de inicio seleccionamos **Automático** y luego click sobre el botón **Iniciar**

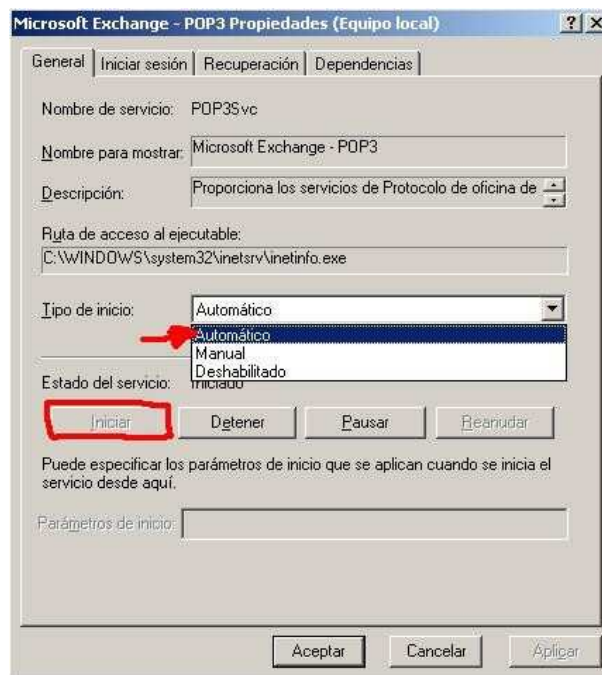


Figura 61. Tipo de inicio del servicio POP3

Servidor virtual SMTP

En el administrador de Exchange nos dirigimos a la siguiente ruta:

Servidores > Protocolos > SMTP

Y seleccionamos el servidor virtual SMTP predeterminado

Clic derecho en **propiedades**



Figura 62. Administrador de servicios de Exchange

En la pestaña general verificamos la asignación de la IP

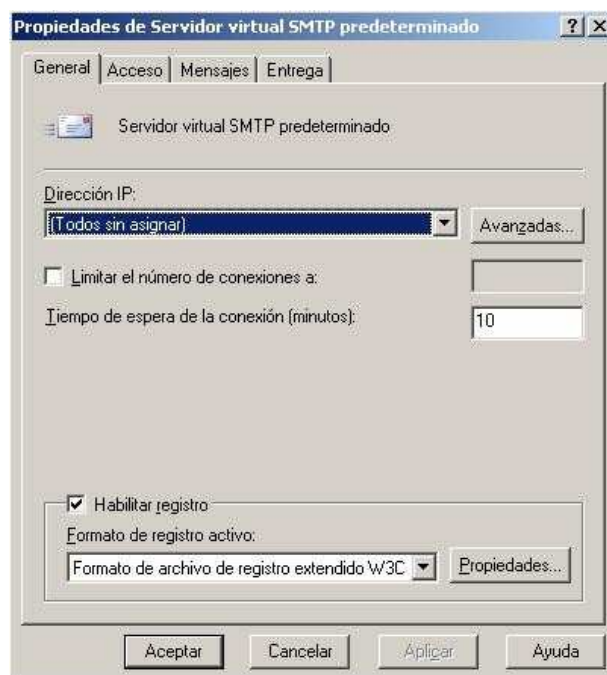


Figura 63. Cuadro de Propiedades del Servidor virtual SMTP

En la pestaña **Acceso** en **Opciones Avanzadas** vamos a **Autenticación** y seleccionamos las casillas de **Acceso anónimo**, **Autenticación Basica** y **Autenticación de Windows** integrada menos la casilla de **Resolver Correo electrónico anónimo**.

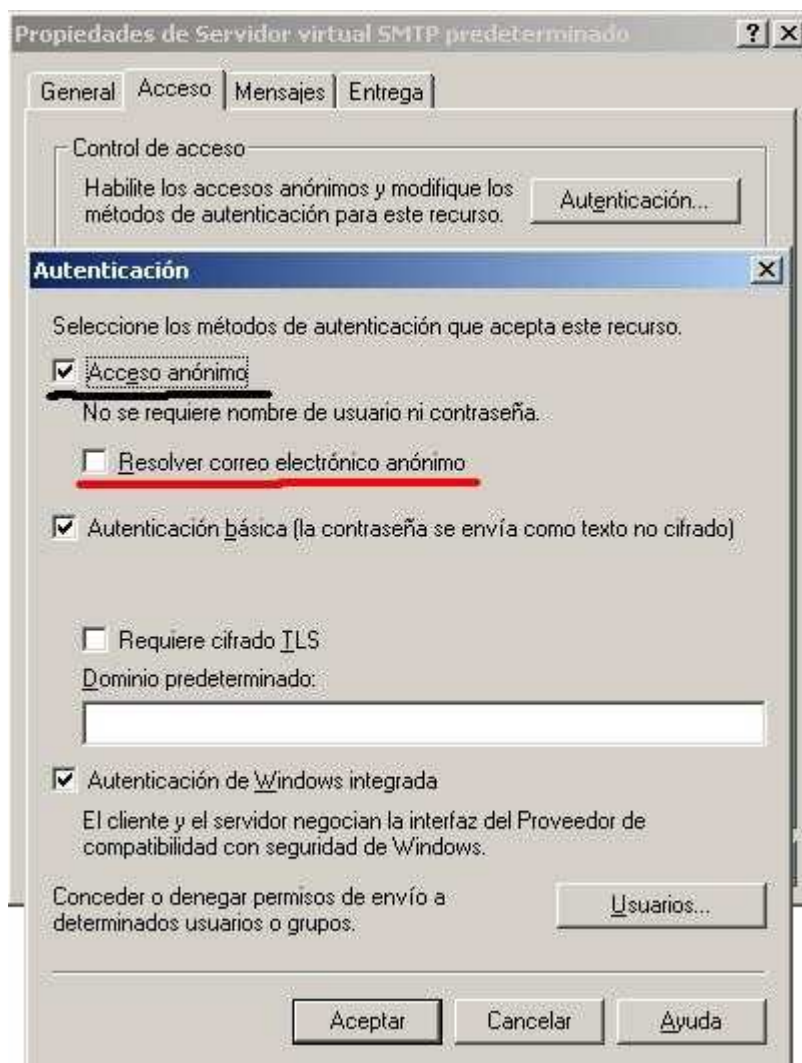


Figura 64. Cuadro de Propiedades del Servidor virtual SMTP, tipo de autenticación

Atención: hay que permitir acceso anónimo para poder recibir correo. Lo que no hay que dejar es "resolver correo electrónico anónimo", eso es propagar SPAM.

Finalmente damos opciones para restringir a lo máximo el correo electrónico no deseado o SPAM

Subir el Conector SMTP

Subir el conector SMTP es necesario para enviar y recibir correo tanto interno como externo (de Internet). La mejor manera de configurar es

eliminarlo y luego crearlo con el asistente, que además te configura los servidores virtuales POP3 y SMTP. Fig 65.



Figura 65. Cuadro Asistente para correo de Internet

Y seguir los pasos del asistente.

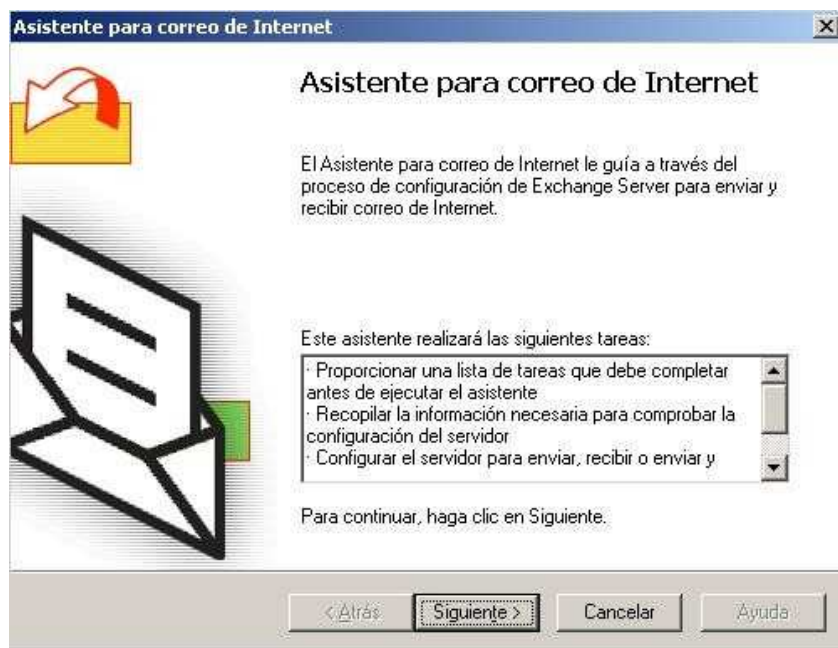


Figura 66. Asistente para correo de Internet

6.5.4.3 Configuración del Firewall de Windows 2003 Server

6.5.4.3.1 Instalación

Lo más recomendable para configurar Windows Firewall en un Windows Server 2003 R2, es utilizar SCW, Security Configuration Wizard es una herramienta que puede reducir la superficie de ataque en los equipos en que se ejecute. Podemos utilizarla para iniciar y configurar Windows Firewall, aunque no lo hace directamente, sino ayudando creando una política de seguridad basada en reglas de configuración para un servidor, después de creada puede ser editada o aplicada a un o más servidores.

Abrir el panel de control y pulsar en agregar y quitar programas.
Elegir componentes de Windows

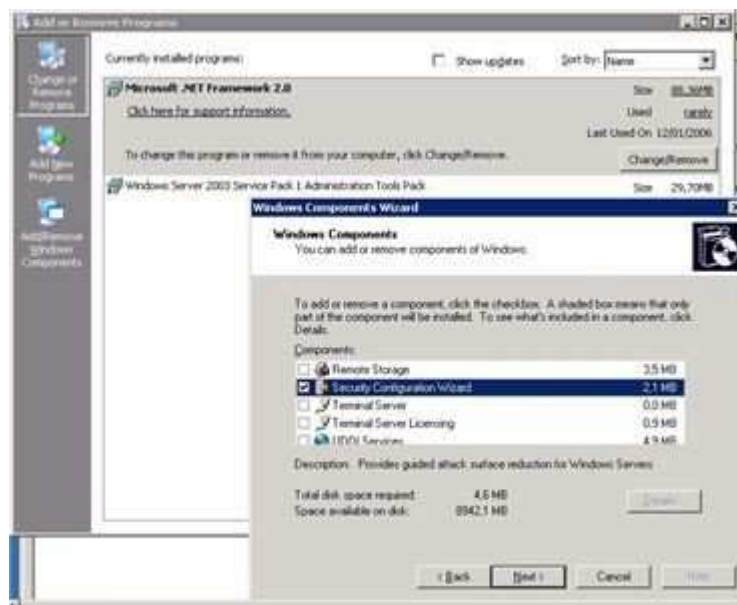


Figura 67. Cuadro de dialogo para añadir el servicio de Firewall

Marcamos SCW y pulsamos en el botón **Next**.

Cuando finalice la instalación se nos informará de ello y finalizamos.



Figura 68. Instalación exitosa del servicio de Firewall

6.5.4.3.2 Configuración del Firewall

Para configurar el Firewall debemos usar el SCW

El Asistente de Configuración de la Seguridad (SCW, Security Configuration Wizard) nos permite configurar de forma rápida y fácil los servidores basados en Microsoft Windows de acuerdo con sus requerimientos funcionales: servidor Web, controlador de dominio u otros, y simultáneamente configura las políticas de seguridad para minimizar la vulnerabilidad a ataques.

1. Abrimos el SCW, y seguimos los pasos hasta llegar a la página de **Network Security**.
2. Borrarnos la selección que tenemos en el check box **Skip this section**, y click **Next**.
3. Bajo la lista de **Select the ports to open**, revisamos los puertos que SCW añadirá a la liste de excepciones del Firewall. Para eliminar

- un puerto de la lista de excepciones, borramos la selección del check box al frente del puerto.
4. Si queremos añadir puertos adicionales o aplicaciones a la lista de excepciones de Firewall, click en **Add**, y hacer lo **siguiente**:
 - a. Para añadir un Puerto a la lista de excepciones, en **Port number**, ingresamos el numero de puerto, seleccionar TCP o UDP o ambos, y click en **OK**.
 - b. Para añadir una aplicación a la lista de excepciones, click sobre la pestaña **Approve Application**, y en **Application path**, ingresar la dirección y el nombre del archivo ejecutable (.exe), y click en **OK**.
 5. Click en **Next**.
 6. En la pagina Confirm Port Configuration, verificamos la configuración de puertos que SCW usara para configurar el Firewall, y click en **Next**.
 7. En la pagina Registry Settings, seleccionamos el check box **Skip this section**, y click en **Next**.
 8. En la pagina Audit Policy, seleccionamos el check box **Skip this section**, y click en **Next**.
 9. En la pagina Internet Information Services, seleccionamos el check box **Skip this section**, y click en **Next**.
 10. En la pagina **Save Security Policy**, click en **Next**.
 11. Ingresamos un nombre y una descripción para las políticas de seguridad, y click en **Next**.
 12. Click en **Apply now** para aplicar las políticas de seguridad y configurar Firewall, y click en **Next**.
 13. Luego que el SCW ha aplicado las políticas de seguridad, click en **Next**, y click en **Finish**.

6.6 Configuración de la seguridad de la intranet

6.6.1 Introducción

Problema: Aunque la Intranet es una red privada en la que tenemos grupos bien definidos y limitados ésta no se encuentra exenta de ataques que pudiesen poner en riesgo la información que manejara, ya que la mayoría de éstos son provocados por sus mismos usuarios.

Antecedentes: La mayoría de las estadísticas de seguridad en cómputo indican que cerca del 80% de los fraudes relacionados con las computadoras provienen de los usuarios internos, por esto las intranets son las más vulnerables a ataques de ésta índole.

Modelo de la Solución:

- a. Políticas de Seguridad
- b. Control de Acceso
- c. Transacciones Seguras
- d. Virus
- e. Cantidad de Seguridad a Implementar

Presentación de la Solución.

- f. Políticas de Seguridad

¿Qué son las políticas de seguridad?

Políticas de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos del sistema de cómputo, las responsabilidades y derechos tanto de los usuarios como del administrador, describe lo que se va a proteger y de lo que se esta tratando de proteger, éstos documentos son el primer paso en la construcción de Firewalls efectivos.

6.6.2. Metodología de desarrollo

El esquema de políticas de seguridad llevara ciertos pasos, para garantizar su funcionalidad y permanencia en la institución. La propuesta es seguir los pasos se detalla a continuación:

Preparación – Recopilación de todo tipo de material relacionado con cuestiones de seguridad en la organización:

Recursos a proteger: Personal, información, hardware, software, documentación, consumibles, etc.

Uso externo, por ejemplo:

Protección de acceso externo

Acceso remoto de usuarios autorizados

Restricciones de acceso a la información importante

Uso interno, por ejemplo:

Restricción de la información a grupos, departamentos o usuarios.

Acceso inautorizado

¿De quién necesito protegerlo? De cualquiera que constituya una amenaza, ya sea interna o externa en cualquiera de estos rubros:

- Acceso no autorizado: Utilizar recursos de cómputo sin previa autorización
- Daño a la información: Modificación o eliminación de la información en el sistema
- Robo de información: Acceso a cierta información sin previa autorización
- Divulgación de la información: Publicar detalles del sistema, como podrían ser las contraseñas, secretos, investigaciones, etc.

- Negación del servicio: Obligar al sistema a negar recursos a usuarios legítimos

En general, se tiene que lograr que las políticas de seguridad cumplan con todos los servicios de seguridad:

Autenticación

Confidencialidad

Integridad

No repudio

Disponibilidad de los recursos a personas autorizadas

Control de Acceso

6.6.3 Redacción de las políticas de seguridad

6.6.3.1 Definiciones

6.6.3.1.1 Gerencia

Como Gerencia se incluyen los oficiales de mayor rango dentro de la institución como son: Mayores, Capitanes y Tenientes, que tienen la responsabilidad de aprobar, evaluar los mecanismos, estándares, guías y procedimientos creados en sus respectivos Departamentos a cargo.

6.6.3.1.2 Departamento de Informática

El departamento de Informática provee a la institución igualdad de acceso a los recursos de Tecnologías de Información (TI) y facilita su uso e integración en los procesos de investigación, administrativos y de servicios de la institución.

El objetivo principal del departamento es establecer y promulgar políticas, guías, procedimientos y estándares de TI que faciliten y promuevan el uso de las TI en forma integrada para satisfacer las

necesidades de los usuarios de TI en la institución. El departamento es responsable por la administración, desarrollo y mantenimiento de la infraestructura de comunicación de data, voz y video en el recinto. Además, es responsable de proveer a la comunidad del Recinto acceso a la Intranet e Internet.

6.6.3.1.3 Personal Técnico de Informática

El personal técnico de informática comprende al personal de los departamentos, proyectos especiales que manejan recursos o servicios de tecnologías de información. Estos son responsables de administrar equipo, manejo de usuarios, seguridad, entre otros.

6.6.3.1.4 Usuarios

Bajo usuario se incluye toda aquella persona que utiliza cualquiera de los recursos de tecnología de información del recinto, ya sea de forma permanente o temporera.

6.6.3.1.5 Sistemas Centralizados

Servicios ofrecidos por el departamento de informática a toda la institución, entre ellos la Intranet, Mantenimiento, Instalación, Sistema Administrativo, etc.

6.6.3.1.6 LAN (Local Area Network)

Es la red de comunicación de data, voz y video de la institución.

6.6.3.2 Principios y Filosofía

6.6.3.2.1 Apoyo Institucional

El departamento de informática contará con el apoyo y recursos fiscales institucionales para poder presentar e implantar los mecanismos necesarios para cumplir con esta política.

6.6.3.2.2 Desarrollo de Políticas Existentes

El CID (Centro de Investigación y Desarrollo) tiene la responsabilidad de crear políticas, procedimientos y estándares de seguridad de Tecnología de información, a tenor con la Política sobre el Uso Ético Legal de las Tecnologías.

6.6.3.2.3 Educación

El CID tiene la responsabilidad de concienciar sobre los deberes, responsabilidades y derechos de los usuarios sobre el acceder, utilizar, manejar, resguardar y disponer de la información, sistemas y equipo que manejan.

6.6.3.2.4 Niveles Razonables y Costo Efectividad en la Seguridad

- a. No todos los recursos necesitan los mismos niveles de seguridad, por lo cual esta política busca establecer los indicadores razonables para que el Jefe de la Unidad de Informática con su Personal Técnico puedan determinar los niveles de costo efectividad adecuados y funcionales de seguridad, control de acceso y privacidad necesarios para sus recursos de información.
- b. El CID es una Institución Militar de Desarrollo de proyectos de tecnología propia, la cual incluye áreas de Investigación, Desarrollo de Proyectos y Administrativa, por ello se deben de ajustar los niveles y requisitos de seguridad a base de requerimientos de entidades reguladoras, en este caso su inmediato superior que es el Estado Mayor de la Fuerza Aérea.

6.6.3.2.5 Prácticas de Seguridad Comúnmente Aceptadas

Los requisitos y recomendaciones mencionadas en esta política buscan estar acorde con la Prácticas Comúnmente Aceptadas para Instituciones de Investigación.

6.6.3.2.6 Responsabilidad Institucional del Departamento de Informática

El Departamento de Informática es la oficina responsable por velar que se cumplan con todos los requisitos y aspectos de seguridad y privacidad según requerido por leyes estatales y entidades afines, Oficinas de Auditoría Interna y entidades Militares, y otras entidades reguladoras.

6.6.3.3 Propósito

- a. Establecer elementos uniformes para el cumplimiento de los estatutos reglamentarios pertinentes y con el uso adecuado de tecnologías de información en todo el CID.
- b. Proveer los procedimientos necesarios para el uso adecuado de las tecnologías garantizando la protección de la información, los derechos de autor y las amenazas en distintos niveles a la seguridad y privacidad de información de los usuarios.
- c. Coordinar con todos los departamentos la mejor estrategia y los procedimientos para determinar los niveles, prácticas óptimas y funcionales de seguridad, uso de los equipos y programas en el CID.
- d. Establecer los mecanismos para divulgar los requisitos y especificaciones mencionados en la Política Institucional, relacionados con los distintos niveles de privacidad y seguridad.

6.6.3.4 Alcance

- a. Esta política cubre a todos los miembros de la comunidad del CID, entre ellos los militares, civiles, investigadores, personal administrativo, personal destacado en facilidades externas e individuos asociados de forma alguna con el CID y cualesquiera que solicite acceder a alguno de los sistemas o fuentes de información del CID.
- b. En adelante esta política establecerá las obligaciones y responsabilidades de las personas que utilizan cualquiera de los recursos de Tecnologías de
- c. Información del Recinto (*Usuario*); aquellos responsables de proveer, mantener, administrar y dar apoyo a los recursos de tecnología de información (*Personal Técnico de Informática*); y aquellos que tienen la responsabilidad gerencial o administrativa de departamentos (*Gerencia*).
- d. Este documento no busca restringir, limitar o excluir prácticas existentes en los sistemas de información del CID. El contexto bajo el cual se crea esta política es en el marco de establecer una base o principios básicos aceptables de procedimientos de seguridad y operacionales que promuevan la uniformidad en los trabajos y estrategias para proteger los datos y recursos de información del CID.

6.6.3.5 Políticas

6.6.3.5.1 Elementos Generales

- a. Todo usuario es responsable del uso y contenido de la (s) computadora (s) y otras tecnologías de información asignadas para su uso.

- b. El departamento de informática proveerá las guías para el uso de la *Intranet*, mediante capacitaciones.
- c. El departamento de informática es la oficina que administra y mantiene directamente la red de comunicación del CID y la seguridad global que impera en esta.
- d. Por la naturaleza de los servicios en la red de comunicación del CID, el departamento de informática integra el concepto de Red Privada y Red Extranet, las cuales permiten ubicar los servicios estratégicamente, a base de sus necesidades de acceso, seguridad y otras peculiaridades.
- e. Se considera *abuso de recurso de información* cuando un usuario utiliza, accede o modifica información, equipo o ambas para actividades personales y no oficiales acorde con la Política Institucional y Procedimiento. Esto comprende acceso no autorizado, violación de derecho de autor, uso de la red para acceder o descargar archivos no relacionados con las tareas y/o funciones oficiales, entre otras.
- f. El Departamento de Informática utiliza el Procedimiento de Manejo de Incidente, donde se establece que se interviene con la PC o equipo que esté en *abuso de recurso de información acorde con la Política Institucional*, y se toman las medidas para notificar a la Gerencia sobre el incidente y determinar la acción apropiada o correctiva a tomar.

6.6.3.5.2 Adquisición de equipo y programado

- a. El Departamento de Informática evaluará y autorizará la adquisición de programado o equipo, para evaluar su conectividad con la red de comunicación del CID.
- b. El Departamento de Informática en coordinación con los departamentos, colaborará en la integración del nuevo equipo o programado a la red de comunicación del CID de forma óptima y aceptable, que no resulte en conflicto alguno.

6.6.3.5.3 Privacidad y Confidencialidad

- a. Todo sistema de datos localizado en una estación de trabajo servidor deberá tener un mecanismo de control de acceso, privilegio y registro de bitácora (Log). Es responsabilidad del personal técnico de informática el implantar los mecanismos para cumplir con este requisito. Esto requiere incluir las notificaciones de “Prohibido el Acceso no Autorizado” y una notificación de privacidad.
- b. El Departamento de Informática por su parte es responsable de responder por el control de acceso, seguridad y aspectos relacionados de *Sistemas Centralizados* que el Departamento de Informática administra.
- c. El Departamento de Informática es también responsable de responder por el control de acceso, seguridad y aspectos relacionados con la red de comunicación del CID.

6.6.3.5.4 Responsabilidades

6.6.3.5.4.1 Responsabilidades del Departamento de Informática

- a. El departamento de informática en conjunto con otro personal gerencial relacionado creará los programas de educación y publicación de manejo de información en forma general, además de proveer cualquier información que sea de carácter público sobre mecanismos adoptados.
- b. El departamento de informática en coordinación con los Directivos y con su respectivo personal técnico de informática, tendrá los criterios y la discreción de otorgar la cualificación a la hora de brindar el acceso y privilegio basado en el concepto de necesidad de saber y necesidad de tener.
- c. En el ejercicio de su responsabilidad de administrar la red de comunicación del CID, el departamento de informática debe analizar, evaluar, someter y recomendar para probar toda petición, plan de proyecto o propuesta alguna que requiera o proponga el integrar componente o programado alguno a la red de comunicación del CID.
- d. Por otro lado es responsabilidad del departamento de informática viabilizar las diferentes opciones que estén disponibles para hacer posible cualquiera de las peticiones de los individuos, Directivos, su respectivo personal técnico de informática, Administradores, Departamentos y/o Usuarios.
- e. El Departamento de informática ha de mantener la evidencia, historial y documentación relacionados a incidentes de seguridad, peticiones, cambios realizados, procedimientos y estándares de seguridad y privacidad.

6.6.3.5.4.2 Responsabilidades de los Usuarios

6.6.3.5.4.2.1 Acceso

- a. Los usuarios son responsables por el acceso a recursos de información de sus áreas de trabajos, entre estos archivos, computadoras y documentos internos. Esto también incluye el acceso a través de puertas y otro tipo de acceso requerido específicamente para su área. En caso de ser requerido por el usuario, el Departamento de Informática proveerá la orientación y guías para que el usuario cumpla con esta responsabilidad.
- b. El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo.
- c. Es responsabilidad del usuario implantar las medidas adecuadas para proteger la privacidad y acceso a la información guardada en su PC o Archivo Histórico acorde a las normas internas establecidas en su área de trabajo y procedimientos existentes.
- d. La autenticación de usuarios es requerida para el acceso a computadoras, computadoras portátiles y servicios centralizados.
- e. Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y cifrada.
- f. Está terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas

- g. Es requerido el notificar y coordinar con el Departamento de Informática o los Directivos que aplique la disposición de toda información contenida en cualquier equipo (incluyendo PC) que vaya a ser dado de baja o intercambiado con otra persona perteneciente a la CID.

6.6.3.5.4.2 Contraseña

- a. Se requiere que todo acceso a *Recursos Centralizados* sea mediante una cuenta de usuario ("username") y contraseña, esta última con un mínimo de ocho (7) caracteres.
- b. La autenticación es requerida para el acceso a computadoras y computadoras portátiles, incluyendo la opción de crear secciones o instancia ("profiles") para cada usuario por separado.

6.6.3.5.4.2.3 Virus y Vulnerabilidades

- a. Es requerido que el usuario utilice y apoye el uso de programados de actualización automática para su antivirus.
- b. Es responsabilidad del usuario utilizar las herramientas incluidas en los sistemas operativos para la actualización de vulnerabilidades, entre estas parches, "hotfix" y "service packs". También el usuario deberá observar y seguir las notificaciones del Departamento de Informática relacionados con los asuntos antes mencionados. El departamento de Informática enviará estas notificaciones vía email y a través de los boletines publicados en la página

- c. Los usuarios son responsables de realizar resguardo (backup) de la información de sus PC u otro equipo de información.

6.6.3.5.4.3 Responsabilidades del Personal Técnico de Informática

- a. Al Personal Técnico de Informática le aplican las observaciones mencionadas en la sección de Usuarios, dado a que ellos también utilizan recursos provistos por el CID a través del Departamento de Informática.
- b. El Personal Técnico de Informática es responsable de ejecutar el plan de resguardo (backup) para los sistemas que administra y el personal gerencial es el responsable de crear y mantener actualizado el plan de resguardo.
- c. El Personal Técnico de Informática estará encargado del apoyo técnico de seguridad a los usuarios.
- d. La información respaldada deberá ser almacenada en un lugar seguro y distante del sitio de trabajo

6.7 Pruebas

Las pruebas se realizaron tomando en cuenta los diferentes aspectos en los que la Intranet debe responder a las exigencias del entorno de la institución.

Así tenemos las siguientes pruebas.

6.7.1 Pruebas de Operatividad

En estas pruebas se verifico que la información que contenga la página de la intranet este siempre en condiciones operativas para quienes acceden a la

misma puedan recorrerla sin problemas, sin encontrar fallas, faltas, o cualquier tipo de anomalía, lo que demuestra el buen funcionamiento de la plataforma que esta atrás de la misma, en este caso: Sistema Operativo, Servicios de Red, Firewall, Políticas de Seguridad.

6.7.2. Pruebas de Integridad

Se verifico la integridad de la información que se muestra en una página Web que es uno de los factores más importantes de la seguridad, pues de esto depende el interés y la credibilidad de la página. La de integridad de la página se mantuvo frente a ciertas fallas de hardware o software, y frente a ciertos ataques de intrusos en el sistema.

6.7.3 Pruebas de Privacidad

Se verifico que la información clasificada como privada esta reservada a usuarios registrados y que existen restricciones usuarios que desean acceder si permisos o privilegios.

6.8. Mantenimiento de la Intranet

El mantenimiento de la Intranet radica en dos puntos:

1. *Actualización de la información:* La información presentada en la Intranet debe ser actualizada por el Administrador del Sistema, el cual es el responsable de este proceso. Se debe contar con el compromiso del personal del CID para la actualización de la Intranet mediante una adecuada capacitación, motivación y apoderamiento.

2. *Mantenimiento de las aplicaciones y de la plataforma tecnológica:* Esta tarea puede llevarse a cabo, a través del servicio que brinda el departamento de informática. El objetivo es garantizar el adecuado funcionamiento de servicios como la red, el correo electrónico y demás herramientas necesarias para el aprovechamiento óptimo de la Intranet. El

administrador del sistema dará soporte a cualquier problema presentado en las mismas, así como desarrollar nuevas funcionalidades y servicios a las aplicaciones existentes, demandadas por los directivos y responsables de los procesos dentro del CID.

Los directivos de la empresa, deben definir las nuevas labores del personal encargado del mantenimiento respectivo, para garantizar que este se realice exitosamente, y que no sea solo el compromiso de algunos miembros de la organización identificados con el proyecto.

Para llevar a cabo este mantenimiento, es necesario evaluar la necesidad de capacitación del personal en diferentes herramientas tecnológicas, las cuales permiten hacer esta labor desde el propio escritorio y en una forma más efectiva.

Es importante en esta fase contar con mecanismos de medición que retroalimenten el proceso de mantenimiento, para así fortalecer las áreas de la Intranet de más uso y eliminar o mejorar las de menor uso.

6.9 Adiestramiento del Personal

El personal que queda al frente de la Intranet es un Administrador de Redes, por lo tanto no podríamos hablar de una capacitación mas bien de una actualización de conocimientos, es así que se han tomado en cuenta los siguientes aspectos:

- **Sistema Operativo**

Ciertos parámetros de control y monitoreo del sistema operativo, en este caso hablamos de Microsoft Windows 2003 Server para la maquina servidor, Microsoft Windows 9x/XP/2000 para las maquinas clientes.

- **Cableado y Herramientas de Red**

Todo lo concerniente a las Herramientas de Red, monitoreo, etc que seran de gran utilidad para el control sobre todo en las maquinas de los usuarios

- **Software**

Información actualizada acerca de las diversas posibilidades que se van abriendo en el mercado. Tanto por la posibilidad de actualizar o adquirir software nuevo que le permita agilizar la red o ahorrar costes como por el hecho de estar al tanto de nuevas amenazas y posibles soluciones.

- **Seguridad**

Aspectos de seguridad e integridad de los datos, utilizando herramientas de detección de intrusos, además de procedimientos básicos como revisión periódica de los archivos logs. Sin dejar de lado también los procedimientos para realizar copias de seguridad.

- **Programación**

El administrador de redes queda con los plenos conocimientos acerca de las herramientas de programación utilizados como lo es la herramienta de diseño de sitios Web Dreamweaver MX, además queda con precedente para explorar nuevas herramientas que se actualizan día a día.

La copia de toda la documentación generada a lo largo de este proyecto queda en manos del Administrador de redes, quien podrá hacer el uso que creyere conveniente.

BIBLIOGRAFIA

Libros

RAYA, José Luis y RAYA, Laura, **“INTRANETS Y TCP-IP CON MICROSOFT WINDOWS SERVER 2003”**, Primera Edición, 2004, Editorial PARACUELLOS DEL JARAMA, Madrid España.

GONZÁLEZ. María **“INTERNET PARA LA EMPRESA”**, Primea Edición, Ediciones ANAYA, México DF.

VV.AA, **“MANTENIMIENTO DE PORTALES EN INTERNET”**. Primera Edicion, BOOK'S EDICIONES, Buenos Aires Argentina

CARBALLAR, J.A, **“FIREWALL. LA SEGURIDAD DE LA BANDA ANCHA”**, **Primera Edición**, Editorial Ra-ma, 2001

VV.AA, **“MANUAL INTERNET EN LA ADMINISTRACION PUBLICA. NIVEL BASICO. FORMA CION”**, EDITORIAL CEP, Segunda Edición, Valladolid España.

Internet

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/default.mspx>

Información necesaria para planear, implementar y administrar Windows Server 2003

[http://msdn2.microsoft.com/es-es/library/ms181052\(VS.80\).aspx](http://msdn2.microsoft.com/es-es/library/ms181052(VS.80).aspx)

Nos da ciertas pautas para Habilitar los Servicios de Internet Information Server (IIS), desde la biblioteca MSDN2 de Microsoft

<http://www.slideshare.net/fergabram/introduccion-windows-2003-server/>

Presentación en diapositivas en línea de Microsoft TechNet, acerca de aspectos generales de la configuración y los servicios de Windows 2003 Server.

<http://msmvps.com/blogs/juansa/archive/2006/01/14/81040.aspx>

Información importante acerca de la configuración del servicio SWC y configurar las políticas de seguridad para el Windows Firewall.

http://www.auditoriasistemas.com/politicas_de_seguridad.htm

Lineamientos y conceptos generales acerca de la gestión de las políticas de seguridad informática.

<http://foro.elhacker.net/index.php/topic,32557.0.html>

Información detallada acerca de las características de un administrador de red

<http://www.frm.utn.edu.ar/nodo/Proyectos/pdf/Proyecto.pdf>

Universidad Tecnológica Nacional
Facultad Regional Mendoza
Proyecto: Red Global Sistema de Cableado Estructurado

<http://www.redclara.net/03/01.htm>

Enlace interesante acerca la implementación y manejo de la infraestructura de red

<http://www.axioma.co.cr/strucab/sctiaeia.htm>

Estándar ANSI/TIA/EIA-568-A de Alambrado de Telecomunicaciones para Edificios Comerciales

http://www.uleam-facci.com/archivos/1114552459Cableado_estructurado.pdf

Normas de Cableado Estructurado

<http://www.culminisnetwork.com/exchange/glue/public/es/Biblioteca%20de%20documentos1/1/Procedimiento%20Instalacion%20y%20Migracion%20de%20Exchange%20V.1.doc>

Procedimientos de Migración e Instalación de Exchange 2003

ANEXOS

ANEXO 1

CARACTERISTICAS DEL SERVIDOR HP ProLiant ML350 Generation 3

Características del Servidor

Procesadores

- Procesador Intel Xeon con tecnología Hyper-Threading;
- Memoria Caché de Transferencia Avanzada de nivel 2 e integrada con un mínimo de 512 KB;
- Bus frontal de sistema a 400/533 MHz;
- Funcionalidad de procesador doble.

Memoria del Sistema

- Detección y corrección de errores (AECC) para detectar y corregir errores en la memoria;
- Módulos DIMM PC2100 ECC DDR, ampliables a 8 GB;
- Compatibilidad con un máximo de cuatro módulos DIMM de DDR registrados PC2100 ECC a 200/266 MHz;
- Es posible instalar los DIMM de uno en uno o por parejas;
- Opción de configuración de memoria intercalada 2 X 1 (con módulos DIMM instalados por parejas idénticas) o configuración no intercalada admitidas.

Ranuras de Expansión

- Cinco ranuras de expansión: cuatro ranuras PCI-X de 64 bits a 100 MHz y una PCI de 32 bits a 33 MHz;
- Compatible a 3,3 voltios (compatible con 5 voltios en la ranura PCI de 32 bits).

Controlador de Almacenamiento

- Adaptador SCSI Ultra3 con canal doble integrado en el bus local PCI. El Controlador proporciona dos buses SCSI internos, dos buses SCSI externos o uno interno y otro externo.
- Tarjetas de Controlador opcionales para la compatibilidad con RAID, duplicación del Controlador o ampliación de la capacidad de almacenamiento disponible.

Controlador de Interfaz de Red

- Controlador de interfaz de red (NIC) Integrado con Conmutación Automática NC7760 Gigabit Server.
- Las opciones Embedded NIC Port 1 PXE Support (Soporte PXE Integrado para Puerto NIC 1) permiten al servidor arrancar desde la red y conectarse a un servidor PXE con imágenes de arranque. Una vez activado, el puerto NIC aparece en la lista IPL (Initial Program Load).

Puertos y Conectores

- Serie;
- Paralelo;
- Teclado;
- Ratón;
- USB (2).

Fuente de Alimentación

- Fuente de alimentación redundante 1+1 opcional de conexión en caliente que cumple con la Marca CE de 500 vatios con corrección del factor de alimentación y conmutación automática.

Vídeo

- Controlador de Vídeo ATI Rage XL integrado que proporciona una resolución máxima de 1.280 x 1.024 no entrelazada con 16,7 millones de colores.
- Admite resolución de gráficos SVGA, VGA y EGA.
- Memoria de vídeo SDRAM de 8 MB.

ANEXO 2

Encuesta realizada al Personal del Centro de Investigación y Desarrollo

UNIVERSIDAD TENCICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS

**PROYECTO DE IMPLEMENTACIÓN DE UNA INTRANET EN EL CENTRO DE
INVESTIGACIÓN Y DESARROLLO DE LA FAE**

OBJETIVO: Establecer el nivel de conocimientos relacionados con la Intranet

INSTRUCCIONES: Lea detenidamente y señale con una X la o las respuestas que crea convenientes.

1. ¿Hay una persona encargada de la administración de la Red dentro de la Institución?
SI NO

2. ¿Hay una persona encargada del mantenimiento y soporte técnico del Equipo Informático?
SI NO

3. ¿Cuantos puntos de red tiene su empresa?

De 1 a 15	16 a 30	31 a 50	50 a 100	Mas de 100 puntos
-----------	---------	---------	----------	-------------------

4. ¿Que tipo de estaciones de trabajo utilizan sus trabajadores? Por cada equipo

		PROCESADOR			
		PENTIUM 2	PENTIUM 3	PENTIUM 4	Xeon
SISTEMA OPERATIVO	Windows 2003				
	Windows 95/98				
	Windows XP				
	Windows 2000				
	DOS				
	Linux				

5. Resumen del nivel técnico promedio de los empleados? Siendo 1 muy pobre y 5 Excelentes.

AREA	NIVEL				
	1	2	3	4	5
Windows	1	2	3	4	5
Redes	1	2	3	4	5
Internet	1	2	3	4	5
Procesador de palabras	1	2	3	4	5
Hoja de cálculo	1	2	3	4	5
Desarrollo de páginas Web	1	2	3	4	5
Diseño Gráfico	1	2	3	4	5

6. ¿Tienen los empleados libre acceso a la información de la Institución?

SI

NO

7. ¿Tienen los empleados libre acceso a los servicios de Internet?

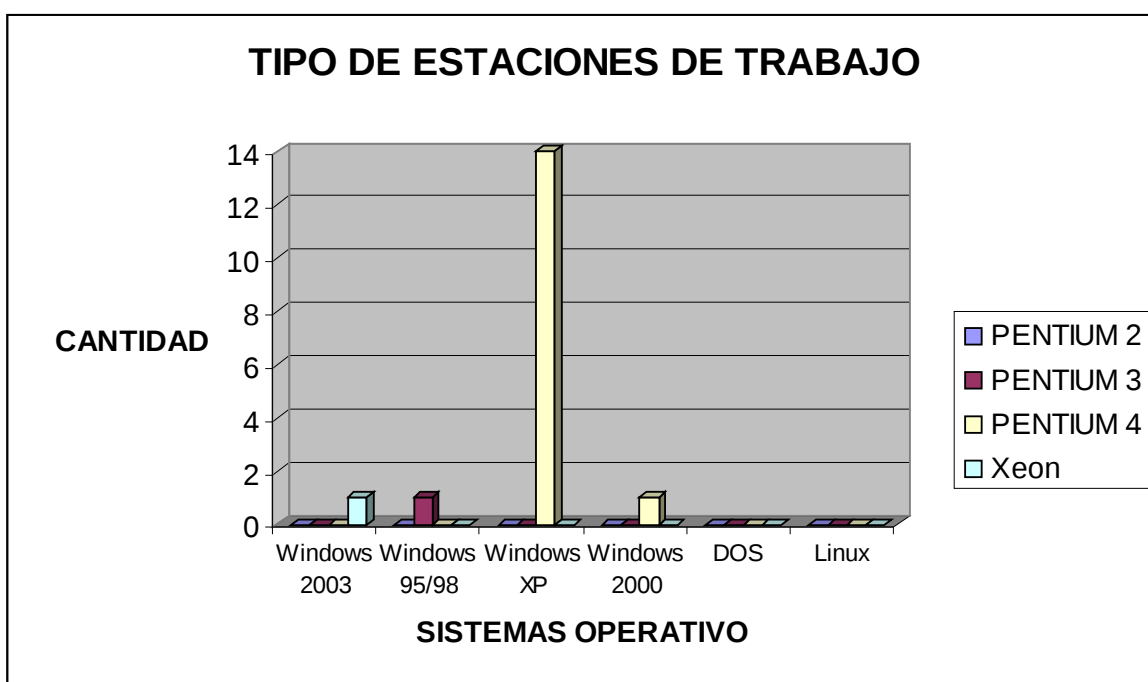
- a. Navegación
- b. Noticias
- c. Correo Electrónico
- d. Descargas
- e. Chat
- f. Ftp

Gracias por su colaboración

RESULTADOS FINALES DE LA ENCUESTA

1. Actualmente no existe una persona encargada de la administración de la Red
2. Existe un Ingeniero Electrónico encargado de realizar el mantenimiento y soporte técnico pero como tarea secundaria.
3. Actualmente existen 17 equipos conectados en la Red con una proyección a 30 equipos en los siguientes 10 meses
4. Resumen del cuadro de tipo de estaciones de trabajo que usan los trabajadores.

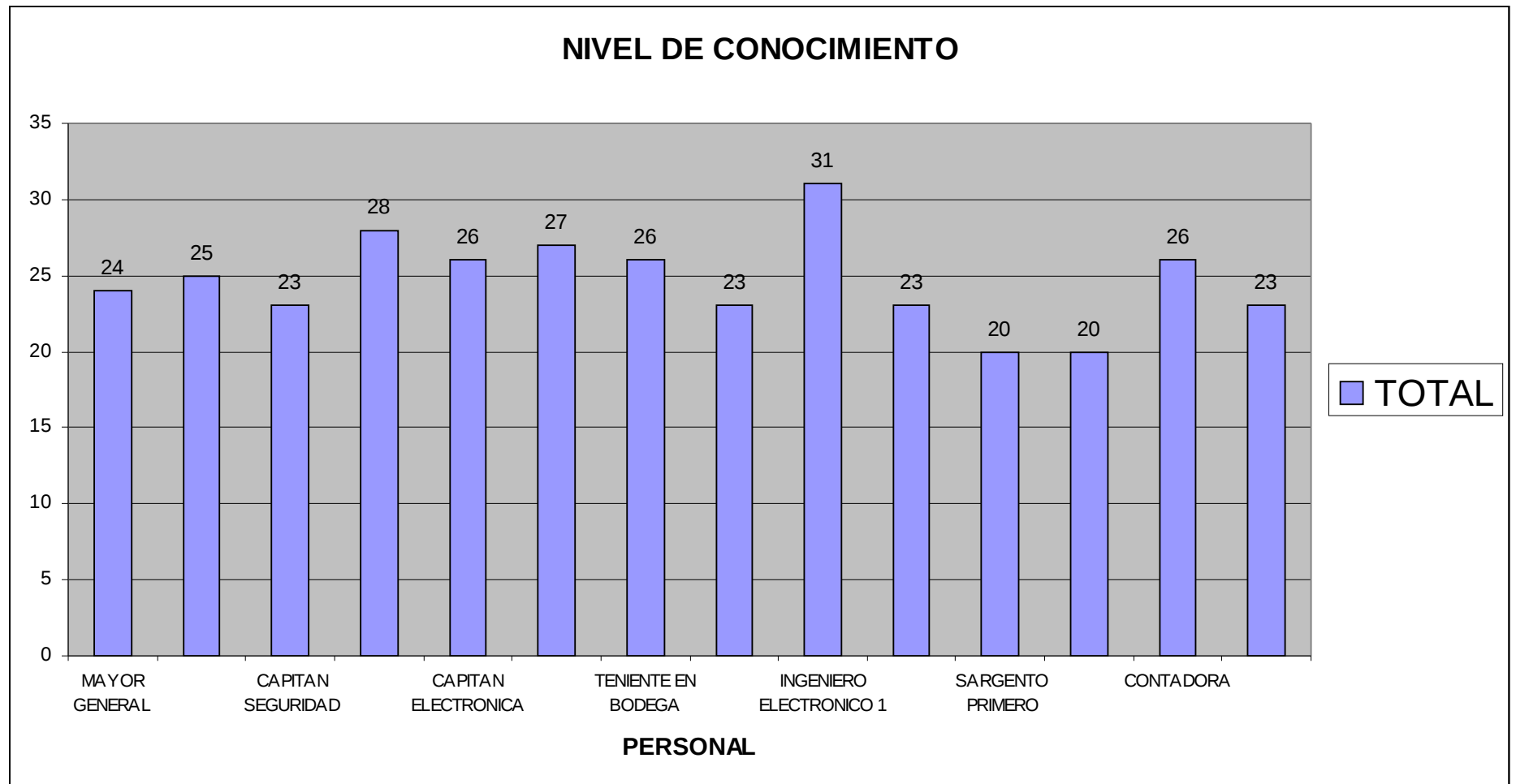
	PENTIUM 2	PENTIUM 3	PENTIUM 4	Xeon
Windows 2003	0	0	0	1
Windows 95/98	0	1	0	0
Windows XP	0	0	14	0
Windows 2000	0	0	1	0
DOS	0	0	0	0
Linux	0	0	0	0



Según el grafico tenemos que los usuarios están familiarizados con el entorno de Windows XP

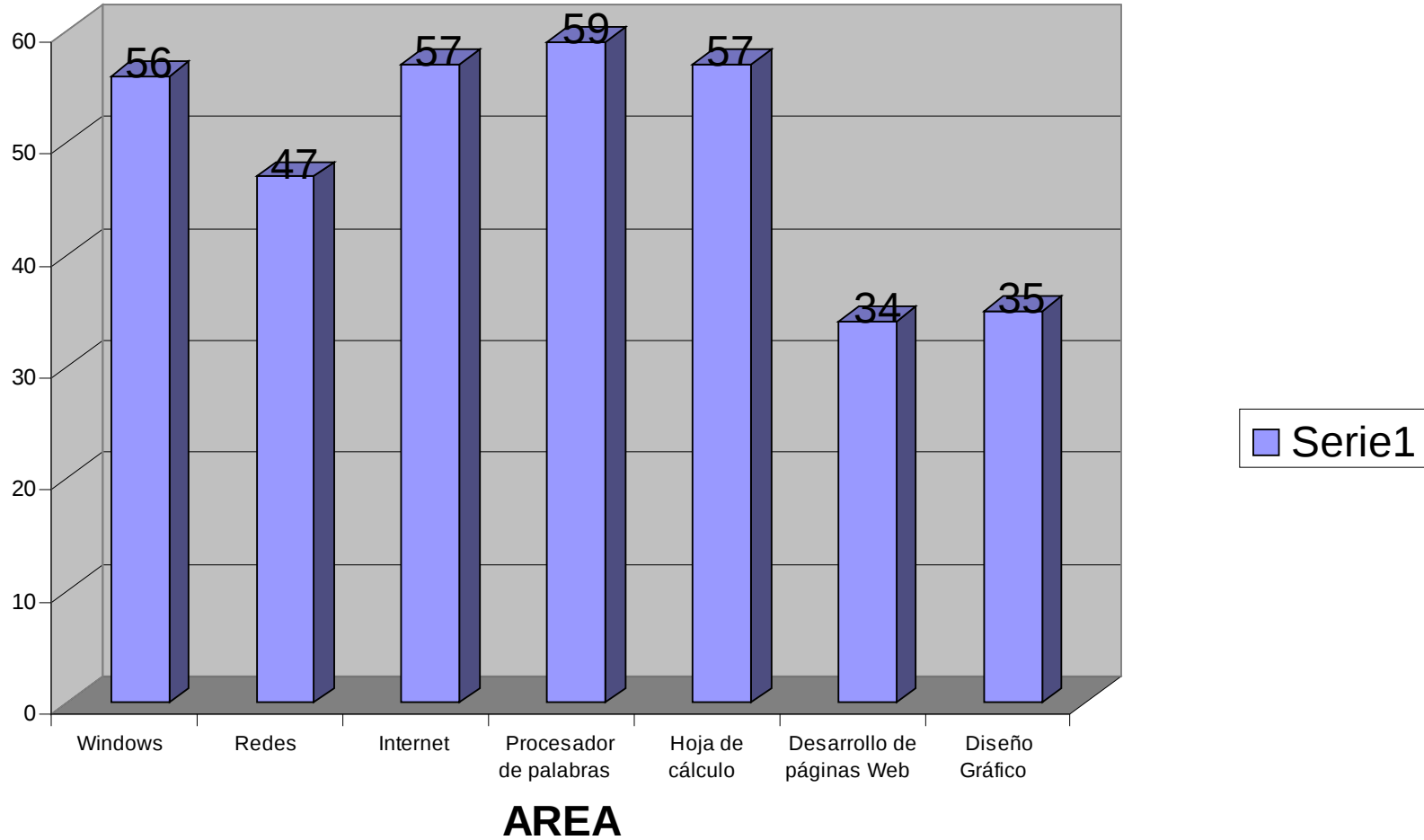
5. Resumen del nivel técnico promedio de los empleados:

PERSONAL	Windows	Redes	Internet	Procesador de palabras	Hoja de cálculo	Desarrollo de páginas Web	Diseño Gráfico	TOTAL
MAYOR GENERAL	4	3	4	4	4	3	2	24
MAYOR DE EJECUCION	5	3	5	4	4	2	2	25
CAPITAN SEGURIDAD	4	3	4	4	4	2	2	23
CAPITAN AVIONICA	5	5	5	4	4	2	3	28
CAPITAN ELECTRONICA	4	5	4	4	5	1	3	26
CAPITAN MANTENIMIENTO	5	4	5	4	5	2	2	27
TENIENTE EN BODEGA	4	4	5	5	4	2	2	26
TENIENTE DE TESORERIA	3	2	4	4	4	3	3	23
INGENIERO ELECTRONICO 1	4	5	5	4	4	5	4	31
INGENIERO ELECTRONICO 2	3	5	3	4	3	3	2	23
SARGENTO PRIMERO	4	2	3	4	3	2	2	20
SARGENTO SEGUNDO	3	2	3	4	3	2	3	20
CONTADORA	4	2	4	5	5	3	3	26
SECRETARIA GENERAL	4	2	3	5	5	2	2	23
TOTALES	56	47	57	59	57	34	35	



Del grafico podemos interpretar que el ingeniero en sistemas en jefe es el que mayor conocimiento presenta en todas las areas.

NIVEL DE CONOCIMIENTO



Del grafico podemos resumir que el personal por el ámbito de la institución esta más familiarizado en las áreas de procesamiento de texto, hojas de cálculo, pero presentan pocos conocimientos en el desarrollo de paginas web y el diseño grafico.

6. Se determino también que los usuarios tiene libre acceso a la información sin importar su nivel de importancia para la institución.
7. Esta pregunta nos demuestra que se accede al Internet para el uso de y Navegación y del Correo Electrónico en mayor proporción.

ANEXO 3

Glosario de Términos Informáticos

A

Actualizar: Volver a cargar o mostrar el contenido de una página Web o una ventana.

Aplicación: Programa que realiza una serie de funciones y con el cual trabajamos en el ordenador.

Árbol: Estructura de directorios o carpetas de un ordenador, del directorio raíz van partiendo diferentes ramas (subdirectorios o subcarpetas), donde se ubican los archivos.

Archivo: Documento generado con una aplicación que se almacena en una unidad.

Arquitectura: Término que se refiere al tipo de estructura hardware de la máquina y que también se aplica a la clasificación de los microprocesadores o el tipo de ranuras de expansión.

Asistente: Herramienta que nos guía y ayuda a través de varios pasos a realizar una tarea para mayor comodidad y sencillez.

B

Backup: Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información o ficheros en varios disquetes y que además la comprime.

Barra de herramientas: Conjunto de botones que representan las opciones de menú más comunes o las utilizadas con más frecuencia.

Base de datos: Sistema de almacenamiento de datos muy flexible que permite organizar la información de forma muy eficiente.

Botón Inicio: Botón que se encuentra a la izquierda de la barra de tareas del escritorio y mediante el cual ejecutamos cualquier tarea (iniciar programas, abrir documentos, obtener ayuda, buscar archivos o carpetas, configurar el sistema o las impresoras...

Botón secundario: Botón derecho del ratón. Muestra un menú emergente o contextual.

Buscador: Servidor de Internet que organiza los ficheros por grupos temáticos y que permite la localización de páginas Web mediante unas palabras clave que introduce el usuario, sin necesidad de conocer las direcciones de las citadas páginas.

C

Caché: Carpeta o memoria intermedia que almacena temporalmente los archivos del equipo.

Carpeta: Contenedor que sirve para almacenar archivos u otras carpetas.

Chat: Servicio de Internet basado en la comunicación en tiempo real y mediante teclado entre personas.

Clic: Pulsar un botón del ratón.

Cliente: Equipo que se conecta a otro equipo llamado servidor.

Comando: Orden que se da al ordenador para ejecutar una función concreta o un programa.

Correo electrónico: Mensajes, documentos, archivos que se envían personas a través de Internet o de una red.

Cortafuegos (firewall): Programa que protege a una red de otra red.

Cuadro de diálogo: Ventana mediante la que debemos proporcionar información a una aplicación.

Cursor: Señalizador que se controla mediante el ratón o teclado y mediante el cual nos movemos por Windows y las aplicaciones.

D

Dirección IP: Cadena numérica que identifica a una máquina en una red IP.

Dirección: Ubicación de un archivo.

Doble clic: Pulsar dos veces seguidas rápidamente el botón izquierdo del ratón. Si hacemos doble clic sobre una carpeta abrimos ésta mostrándonos su contenido en una ventana. Si el doble clic es sobre un acceso directo se ejecuta el programa que representa éste.

Documento: Archivo creado con una aplicación.

Dominio: Grupo de equipos conectados en red que comparten información y recursos.

Driver: Programa que gestiona los periféricos que se conectan al ordenador.

E

Ejecutable: Dícese del archivo que puede poner en marcha un programa.

e-mail: Nombre inglés que designa el correo electrónico.

Enlace: Conexión de un documento de Internet con otro que figura resaltado de manera especial, también llamado Hipervínculo o Hiperenlace.

Escalabilidad: Capacidad de ampliación de los ordenadores.

Extranet: Red basada en Internet de una compañía en la que comparte información y comunicación con agentes externos.

F

Firewall: Dispositivos de seguridad a entradas no autorizadas.

Frames (marcos): Areas rectangulares que subdividen las ventanas de algunas páginas Web, cada una de las cuales contiene un documento de hipertexto independiente de los demás.

G

Grupos de trabajo: Conjunto de equipos conectados en red y que comparten los mismos recursos.

H

Hardware: Partes duras de un ordenador o componentes de éste.

Hipertexto o Hiperenlace: Documento que contiene texto o imágenes que actúan como enlaces con otros textos o páginas cuando se pulsa sobre ellos.

Hipervínculo: Marca que nos permite el salto a otro lugar del documento o a otra ubicación que se puede encontrar en cualquier parte del mundo.

HTML (Lenguaje de Marcas de Hipertexto): Lenguaje utilizado para crear páginas Web.

HTTP: Protocolo de Transferencia de Hipertexto o entorno gráfico de las páginas Web.

I

Icono: Imagen que representa un archivo, una unidad, una carpeta u otro elemento.

Implementar: Implantar o instalar un sistema o diseño informático o incorporar una tecnología novedosa.

Importar: Transferir o enviar ficheros a otro programa distinto del que los generó.

Imprimir: Acción de plasmar en papel la información obtenida en pantalla (texto, gráficos, imágenes, etc.)

Iniciar sesión: Identificarse y obtener acceso a un equipo mediante nombre de usuario y contraseña.

Interfaz: Aspecto que presentan los programas tras su ejecución mediante el cual ejercemos la comunicación con éstos

IP: Dirección numérica y única de cada ordenador en Internet.

J

Java: Lenguaje de programación creado por Sun Microsystem para proporcionar más velocidad y facilidad de uso a Internet, es independiente de la plataforma utilizada y está disponible para cualquier navegador de la WWW que admita este lenguaje.

Joystick: Periférico en forma de palanca y con botones incorporados, diseñado especialmente para disfrutar de los videojuegos.

L

LAN (Red de Area Local): Grupo de equipos conectados en la misma ubicación.

Librería: Conjunto de módulos de programación o elementos que se utilizan para desarrollar y diseñar aplicaciones.

Link: Cada uno de los enlaces de un módulo con las librerías que utiliza. En Internet, conexión de un documento con otro mediante un clic sobre un texto marcado o un icono o imagen.

M

Microprocesador: Unidad de proceso y corazón del ordenador. Podríamos decir que es el jefe del ordenador, el cual procesa y distribuye el trabajo a los demás componentes del ordenador

Minimizar: Dícese de la acción llevada a cabo, mediante la pulsación sobre el botón del mismo nombre en una ventana, la cual hace que ésta se esconda en la barra de tareas y deje el espacio del escritorio listo para otro uso.

N

Navegador: Programa utilizado para acceder a los documentos almacenados en Internet.

Navegar: Recorrer el contenido de Internet.

O

Off-line: Proceso para poder ver páginas Web sin estar conectado a Internet. Se cargan al disco duro y se puede tener acceso a ellas más tarde.

On-line (en línea): Conexiones a la red donde las respuestas del sistema se generan de forma casi inmediata.

P

Página principal (Home Page): Página primaria o introductoria a Internet. También llamada página de inicio.

Página Web: Documento realizado en HTML y que es parte de un sitio Web.

Partición: Subdivisión que se realiza en el disco duro con el fin de obtener un mayor aprovechamiento de éste.

Password: Clave secreta personal.

Perfil: Conjunto de parámetros de Windows 98 para un determinado usuario.

Pirata: El que copia software ilegalmente y lo comercializa sin ningún tipo de licencia.

Portales: Páginas que se utilizan como punto de partida y que se estructuran por contenidos, índices y temas, además de ser potentes bases de datos o buscadores de información por Internet, es decir, localizadores de otras páginas de las cuales no conocemos su dirección, pero que las encontramos al teclear en éstos unas palabras clave.

Predefinido: Opción predefinida por defecto.

Programa: Grupo de instrucciones que sirven para realizar determinadas tareas. También llamadas aplicaciones.

Protocolo: Conjunto de normas que los equipos utilizan para comunicarse entre sí a través de una red y poder hablar el mismo idioma.

Proveedor de Servicios Internet (ISP): Organización que proporciona acceso a Internet mediante una tarifa y que nos ofrece una serie de servicios.

Proxy: Servidor que realiza la conexión a Internet y que sirve de puerta de entrada a los ordenadores cliente.

R

Routers: Dispositivos de red cuya misión principal es encaminar los paquetes de información que reciben en la dirección adecuada para que alcancen su destino.

Ruta de acceso (Path - Camino o Trayectoria): Forma para llegar hasta un lugar o una ubicación determinada, partiendo de una unidad específica, por carpetas y nombre de archivo.

S

Servidor: Equipo que controla el acceso de los usuarios a una red y les da servicio e información.

Sistema: Conjunto formado por el hardware y software que componen la parte esencial del ordenador.

Sitio Web: Grupo de páginas Web relacionadas entre sí.

Software: Partes blandas de un ordenador o soportes donde se almacenarán los datos generados con éste.

Spamming: Bombardeo de los buzones con correo basura o no deseado por parte de los spammer.

T

Tarjeta de red: Hardware que se inserta en un equipo para conectarlo a una red.

U

Unidad: Dispositivo físico de almacenamiento de los datos. Por lo general se les nombra mediante una etiqueta o nombre (A:, C:, D:).

URL: Localizador Uniforme de Recurso, dícese de la dirección de una página Web de Internet.

Usuario remoto: Persona que se conecta a una red mediante un módem y Acceso telefónico a redes.

V

Ventana: Forma rectangular que aparece en la pantalla y representa a una carpeta, una aplicación, un elemento.

Virus: Programas informáticos diseñados con mala intención, ya que se convierten en parásitos capaces de infectar a otros para incluir una copia evolucionada de sí mismos.

W

Web: World Wide Web, Internet. Zona gráfica compuesta por millones de páginas Web y a la cual accedemos por medio de un navegador.

Webmaster: Persona encargada de administrar una Web.

ANEXO 4

Características de la Impresora Minolta Magicolor 2480 MF



KONICA MINOLTA

magicolor® 2480 MF

TECHNICAL DATA

Print process

Print method: Electro photographic dual laser printing system
Print speed: 5 ppm colour/ 20 ppm monochrome
First page out: 12 seconds monochrome, 21 seconds colour
First copy out: 23 seconds monochrome, 52 seconds colour
Resolution: 2400 x 600 dpi
Monthly duty cycle: 35,000 sheets

Scan process

Scan technology: CCD Image sensor, flatbed
Resolution: 600 x 600 dpi (max.)
Max. scan size: Legal
Scan time: 9.4 seconds monochrome (600 dpi), 23 seconds colour (600 dpi)
Driver support: TWAIN and WIA
Document handling: ScanSoft PaperPort®

Copy process

Copy speed continuous: 5 cpm colour/20 cpm monochrome
Copy resolution: 600 dpi
Copies: 1-99
Zoom range: 50-200%

Hardware and software capabilities

Processor type: 108 Mhz Risc CPU
Memory: 96 MB RAM
Colour support: Enhanced Automatic Image Density Control (eAIDC), Automatic ICC-based colour matching, ICC device profiles

Interface support

USB 2.0 (High-Speed) 'Plug-N-Play' support, PictBridge (Digital Camera via special USB)

Operating system compatibility

Windows® XP, 2000, ME and 98SE

Paper handling

Standard paper input: 200-sheet
Optional paper input: 500-sheet lower paper feeder
Paper output: 200-sheet face-down output tray
Automatic document feeder: 50-sheet
Automatic duplexing (optional): Letter, A4, legal, Government legal
Paper sizes supported:
Multi-purpose tray: A4, A5, B5, letter, legal, J-Postcard, executive, Government letter/legal, folio, envelope C5/C6, envelope monarch, envelope DL, envelope COM10, double postcard, statement, UK Quarto, foolscap, letter plus, custom (92-216 mm x 210- 356 mm)
Lower paper feeder: A4
Printable area: 4mm from all edges
Print media: Plain paper (60-90 g/m2), thick stock (91-163 g/m2), recycled paper (60-90 g/m2), transparency, letterhead, postcard, glossy paper

Physical

Type: Laser printer with internal controller
Dimensions: (D) 475 mm x (W) 530 mm x (H) 466 mm
Weight: 28 kg without consumables; 35.2 kg shipped with consumables

ANEXO 5

Ubicación del Departamento De Informática

1. Servidor



2. Sistema central del cableado estructurado.

