**UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA**
**"FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA"**

# "DISEÑO DE POLÌTICAS DE SEGURIDAD EN UNA RED UTILIZANDO WINDOWS 2003 SERVER PARA LOS SERVICIOS ACTIVE DIRECTORY, DHCP, DNS, TERMINAL SERVICE, WEB SERVICE, FTP, DE LA COMISION PORTAL WEB"

**INFORME PRÁCTICO DE SUFICIENCIA**

PARA OPTAR EL TÍTULO DE:

**INGENIERO DE SISTEMAS E INFORMÁTICA**


Presentado por el Bachiller:

**Alan Alberto García Panduro**

Asesor:
**BR. Alejandro Reategui Pezo**



**NAUTA – PERU**
**2007**

**Informe Técnico del Examen de Suficiencia previa actualización académica aprobado en sustentación publica, por el jurado examinador, designado por el Presidente de la Comisión de Gobierno de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonia Peruana.**

ING. JUAN MANUEL VERME INSUA
Presidente

ING. CESAR AUGUSTO PALACIOS CHAVEZ
Miembro

ING. FERNANDO JAVIER SALAS BARRERA
Miembro

**Asesor:**

BR. ALEJANDRO REATEGUI PEZO

# INTRODUCCÌON

La competitividad entre las empresas avanza cada día más y más, sobre todo por que cada vez las tecnologías crecen y son las empresas que adoptan estas y se automatizan, las que sacan una ventaja importante a sus competidores.

La Comisión de Portal Web - UNAP, al ser un organismo de educación no debe ser ajena a esto; es por eso que el presente proyecto busca aprovechar las tecnologías existentes para un diseño de servicios de red integrados basados en Windows 2003 Server en las diversas áreas de la institución.

Esto no solo le permitirá la automatización de procesos, sino también el crecimiento de la imagen institucional, sin dejar de mencionar el ahorro económico que implica la ejecución de sus procesos.

Uno de los factores importantes de este proyecto es que a través de una red integrada se podrá ejecutar aplicaciones cliente servidor e implementar una base de datos que se actualizará constantemente, lo que permitirá acceso a información actualizada y al instante, lo que es un punto importantísimo para la toma de decisiones de cualquier organización.

## DEDICATORIA

*"A Dios por guiarme en cada etapa de mi vida, y darme las fuerzas necesarias para seguir adelante"*

*"En memoria a mi señor Padre por que fue su deseo el verme un hombre profesional y capaz en la vida de poder emprender todas mi metas."*

*"A mi señora madre por el amor, el apoyo incondicional, la confianza que puso en mi, por que si no fuera por ella no estaría donde estoy ahora.*

*"A todos mis hermanos por su granito de arena que pusieron hacia mi persona para llegar hacer un hombre de bien.*

*"A un gran amigo muy especial que me brindo su apoyo y que compartimos muchas noches de estudio en nuestra vida universitaria"*

*Alan.*

## PRESENTACION

Señores miembros del jurado:

De conformidad a lo estipulado por el Reglamento de Grados y Títulos de la Facultad de Ingeniería de Sistemas e Informática – Universidad Nacional de la Amazonia Peruana, presento a vuestra distinguida consideración el siguiente Informe titulado:

**"Diseño de Políticas de Seguridad en una red utilizando Windows 2003 Server para los servicios: Active Directory, DHCP, DNS, Terminal Server, Web Service, FTP, de la Comisión Portal Web "**

Con el propósito de optar el título de ingeniero de sistemas e informática.

El presente informe se ha realizado basado en los conocimientos adquiridos durante los años de estudio en las aulas universitarias, en la consulta bibliográfica y en la información recibida por parte de los Docentes de la escuela de Ingeniería de Sistemas e Informática de la Universidad Nacional de la Amazonia Peruana con el deseo de brindar un aporte que sirva de base para mayores estudios e investigaciones.

Y esperando que me disculpen los vacíos u omisiones involuntarias que el presente informe contiene, y en espera de su justo criterio de revisión, anticipo a Uds. así como a todos aquellos Profesores de la mencionada Facultad que contribuyeron a mi formación profesional, mi más sincero agradecimiento.

Iquitos, Junio del 2007

Alan Alberto García Panduro

## AGRADECIMIENTO

*Expreso mi mas cordial y fraternal agradecimiento a los Docentes de la Escuela de Ingeniería de Sistemas e Informática por los conocimientos y enseñanzas impartidas durante mi permanencia universitaria; quienes lograron mi sólida formación académica y profesional.*

*El presente informe a sido elaborado bajo el asesoramiento del Docente Alejandro Reategui Pezo, a quien agradezco por su valioso apoyo en la dirección durante la realización del presente informe.*

*Así mismo expreso mi mas fraterno agradecimiento a todas las personas en general que pusieron su confianza y apoyo incondicional para llegar a alcanzar unos de mis grandes anhelos en mi vida profesional.*

**INDICE**

**Título: "Diseño de políticas de seguridad en una red utilizando Windows 2003 Server para los servicios: Active Directory, DHCP, DNS, Terminal Server, Web Service, FTP, para una Infraestructura de Servicios de Red Integrados para mejorar la gestión administrativa de la Comisión Portal Web – UNAP"**

**Autor: BR. Alan Alberto García Panduro.**

## RESUMEN

La seguridad de la información dentro de las organizaciones en nuestro país, hoy en día aún es tomada como una necesidad con poca relevancia, en la cual no se pretende invertir, avanzamos pensando que nadie pretenderá interesarse por vulnerar la poca o nula seguridad que se pone al servicio de la protección de nuestra información. Tomar conciencia de esta negligencia o ligereza es un gran punto para empezar.

La oficina de la Comisión de Portal Web de la Universidad Nacional de la Amazonia Peruana, es el Ente que toma la iniciativa de desarrollar políticas de seguridad en la red institucional de la Universidad, empezando de esta manera a darle mayor importancia al respaldo de la información patrimonio de la institución.

Con el presente trabajo se pretende diseñar políticas y estrategias de seguridad, haciendo uso de servicios diseñados para tal fin, con una plataforma de software robusta, como lo es Microsoft, definiendo normativas de seguridad, que garanticen confidencialidad, integridad y disponibilidad de la información a la comunidad universitaria.

Teniendo en cuenta que la Universidad cuenta con una plataforma de hardware y comunicación que le permiten salir a internet de forma independiente con servidores propios, poniendo a disposición de todos sus usuarios múltiples servicios inherentes a un portal web y otros propios de la labor académica y administrativa de la institución.

Es así también, que haciendo uso de herramientas y políticas ya establecidas, se combina las estrategias planteadas en el presente, con una metodología denominada "HIBRIDA" por estar compuesta de diversas fases de otras metodologías usadas para el desarrollo de una Infraestructura de Servicios de Red e Implementación de Políticas de Seguridad en base a Windows 2003 Server, tales como Microsoft Corporation, IGAPE, TIM EVANS y @System.

De esta manera se construye un producto sólido que sirva para la mejor administración en seguridad y fortalecer el nivel que es necesario para salvaguardar la información de la Institución.

**Title:** **Design of safety policies in a network using Windows 2003 Server for the services: Active Directory, DHCP, DNS, Terminal Server, Web Service, FTP, for an Infrastructure of Services of Network Integrated to improve the administrative management of the Commission Portal Web – UNAP.**

**Author: BR. Alan Alberto García Panduro.**

## ABSTRACT

The safety of the information inside the organizations in our country, nowadays still is taken as a need by few relevancy, in which is not tried to invert, we advance thinking that nobody will try to be interested for damaging small or void safety on that it puts to the service of the protection of our information. Be aware of this negligence or lightness is a great point to begin.

The office of the Commission of Portal Web of the National University of the Peruvian Amazonia, it is the Entity that takes the initiative to develop safety policies in the institutional network of the University, beginning to attach greater importance to the support of the information patrimony of the institution.

With the present work one tries to design policies and safety strategies, using services designed for such a end, with a robust platform of software, since it is Microsoft, defining safety regulations, which guarantee confidentiality, integrity and availability of the information to the university community.

Bearing in mind that the University relies on a platform of hardware and communication that they allow it to go out to Internet of independent form with their own servers, putting at the disposal of all users multiples services inherent in a portal web and others own works academic and administrative services of the institution.

It is like that also, that using tools and already established policies, one combines the strategies raised in the present, with a methodology called "HYBRID" for is composed of diverse phases of other methodologies used for the development of an Infrastructure of Services of Network and Implementation of Policies of Security on the basis of Windows 2003 Server, such as Microsoft Corporation, IGAPE, TIM EVANS and @System.

Thus builds a solid product to better management in safety and to strengthen the level that is necessary to safeguard the information of the Institution.

# CAPÍTULO I

# GENERALIDADES

# I. Generalidades

## 1. Título

"Diseño de políticas de seguridad en una red utilizando Windows 2003 Server para los servicios: Active Directory, DHCP, DNS, terminal Server, Web Service, FTP, para una Infraestructura de Servicios de Red Integrados para mejorar la gestión administrativa de la Comisión Portal Web - UNAP

## 2 Autor:

García Panduro, Alan Alberto

## 3. Tipo de investigación

### a. De acuerdo a la orientación

Aplicada

### b. De acuerdo a la técnica de contrastación

Cuasiexperimental

## 4. Régimen de la investigación:

Libre

## 5. Localidad e institución donde se desarrollara el proyecto:

Localidad: Iquitos - Perú
Unidad orgánica: Comisión Portal Web - UNAP

## 6. Cronograma de ejecución del proyecto

| Etapas | Fecha inicio | Fecha término | Dedicación (Meses) |
|---|---|---|---|
| Recolección de datos | 02/01/2007 | 31/01/2001 | 1 |
| Análisis de datos | 02/01/2007 | 10/01/2007 | 1 |
| Elaboración del informe | 14/01/2007 | 02/05/2007 | 5 |

## 7. Fecha de inicio

02 de Enero del 2007

## 8. Fecha de término

30 de Abril del 2007

**9. Horas semanales dedicadas al proyecto**

14 horas semanales

**10. Recursos**

**Recursos disponibles**

**Personal**

- **Tesista**

  1 Bach.en Ingeniería de Sistemas e Informática

- **Asesor**

  Docente de la FISI - UNAP

**Bienes**

- **Materiales**
  - Material de escritorio
  - Lapiceros de tinta
  - Lápices
  - Cartucho de tinta para impresora
  - Regla x 30 cm.
- **Equipos de desarrollo**
  - 1 computadora personal: procesador Intel Pentium IV 3.0 GHz, 512 MB RAM, 160 GB de Disco Duro.
  - 1 Impresora Lexmark Z515
  - 1 Escáner Canon Lide 25

**Servicios**

- Grabado de CD
- Escaneado
- Internet

**Recursos no disponibles**

**Bienes**

- **Materiales de oficina**
  - Papel bond A4 x 80 gr.
  - Papel Bulky
  - Fólder de plástico
  - Fólder manila
  - Correctores
  - Resaltadotes
  - Archivadores

- **Material PAD**
  - Memoria 128 Mb Kingston Data Traveler USB 2.0
  - CDs grabables

- **Software**
  - Microsoft Windows Server 2003
  - Microsoft Office XP Profesional.
  - Microsoft Project 2003
  - Etrust firewall

**Servicios**

- Transporte
- Fotocopiado
- Espiralado
- Empastado
- Telefonía

## 11. Personal

**Tesista**

- 01 Bach. en Ingeniería de Sistemas e Informatica

**Asesor**

- Docente de la FISI - UNAP

## 12. Materiales y equipos

| Especificaciones | Cantidad |
|---|---|
| **Material de oficina** | |
| Papel Bond A4 x 80 gr. (x1000) | 01 |
| Papel Bulky (x100) | 04 |
| Lapiceros de tinta (x10) | 01 |
| Lápices (x10) | 01 |
| Regla x30 cm. | 02 |
| Correctores papermate | 02 |
| Resaltadores Faber Castell | 02 |
| Archivadores | 02 |
| Folders de plástico | 02 |

| | |
|---|---|
| **Material PAD** | |
| Memorias 256 Mb Kingston Data Traveler USB 2.0 | 01 |
| CDs grabables LG | 10 |
| **Equipos de desarrollo** | |
| Computadora personal Pentium IV | 01 |
| Impresora Lexmark Z515 | 01 |
| Escáner Canon Lide 25 | 01 |
| **Software** | |
| Microsoft Windows Server 2003 | 01 |
| Microsoft Office Xp Professional | 01 |
| Microsoft Project 2003 | 01 |
| **Otros** | |
| Cartucho de tinta B/N | 02 |
| Cartucho de tinta a color | 02 |

## 13. Locales

- Biblioteca especializada de la Facultad de Ingeniería de sistemas e Informática de la Universidad Nacional de la Amazonia Peruana
- Cabinas de ineternet FISINET- de la UNAP.
- Domicilio del investigador.

## 14. Presupuesto

**Cuadro N° 01**

| **Personal** | | | | |
|---|---|---|---|---|
| **Descripción** | **Cantidad** | **Sueldo Mensual (S/.)** | **Meses** | **Sueldo Total (S/.)** |
| Investigadores | 01 | 600 | 01 | 600.00 |
| Asesor | 01 | 800 | 01 | 800.00 |
| | | | **Total** | **1400.00** |

**Fuente: Elaboración propia**

**Cuadro N° 02**

| Material de Oficina | | | | |
|---|---|---|---|---|
| **Unidad de medida** | **Descripción** | **Cantidad** | **Precio Unitario (S/.)** | **Precio Total (S/.)** |
| Millar | Papel Bond A4 x 80 gr. | 01 | 24.00 | 24.00 |
| Ciento | Papel Bulky | 04 | 2.50 | 10.00 |
| Unidad | Lapiceros de tinta | 10 | 1.00 | 10.00 |
| Unidad | Lápiz | 10 | 0.50 | 5.00 |
| Unidad | Regla Artesco | 01 | 1.00 | 1.00 |
| Unidad | Corrector papermate | 02 | 2.50 | 5.00 |
| Unidad | Resaltador Faber Castell | 02 | 2.50 | 5.00 |
| Unidad | Archivadores | 02 | 4.50 | 9.00 |
| Unidad | Folders de plástico | 02 | 3.50 | 7.00 |
| | | | **Total** | **76.00** |

**Fuente: Elaboración Propia**

**Cuadro N° 03**

| Material PAD | | | | |
|---|---|---|---|---|
| **Unidad de medida** | **Descripción** | **Cantidad** | **Precio unitario (S/.)** | **Precio total (S/.)** |
| Unidad | Memorias 128 Mb Kingston Data Traveler | 01 | 80.00 | 80.00 |
| Unidad | CDs grabables LG | 10 | 0.80 | 8.00 |
| | | | **Total** | **88.00** |

**Fuente: Elaboración propia**

**Cuadro N° 04**

| Equipos de desarrollo | | | | |
|---|---|---|---|---|
| **Unidad de medida** | **Descripción** | **Cantidad** | **Precio unitario (S/.)** | **Precio total (S/.)** |
| Unidad | PC Pentium IV 3.0 GHz | 01 | 1874.00 | 1874.00 |
| Unidad | Impresora Lexmark z515 | 01 | 170.00 | 170.00 |
| Unidad | Escáner Canon Lide 25 | 01 | 181.00 | 181.00 |
| | | | **Total** | **2225.00** |

**Fuente: Elaboración Propia**

**Cuadro Nº 05**

| Servicios | | | | |
|---|---|---|---|---|
| **Unidad medida** | **Descripción** | **Cantidad** | **Precio unitario (S/.)** | **Precio total (S/.)** |
| | Transporte | Global | 0.50 | 210.00 |
| Páginas | Fotocopiado | 1600 | 0.05 | 80.00 |
| Unidad | Espiralado | 06 | 2.50 | 15.00 |
| Unidad | Empastado | 04 | 8.00 | 32.00 |
| Unidad | Escaneado | 20 | 1.00 | 20.00 |
| Minuto | Telefonía | Global | 0.5 | 40.00 |
| Hora | Internet | 100 | 1.00 | 100.00 |
| | | | **Total** | **497.00** |

**Fuente: Elaboración propia**

**Cuadro Nº 06**

| Software | | | |
|---|---|---|---|
| **Descripción** | **Cantidad** | **Costo de licencia (S/.)** | **Precio total (S/.)** |
| ▪ Microsoft Windows Server 2003 | 1 | 999 | 999 |
| ▪ Microsoft Office XP Professional. | 1 | 200 | 200 |
| ▪ Microsoft Project 2003 | 1 | 150 | 150 |
| | | **Total** | **1349.00** |

**Fuente: Elaboración propia**

**Cuadro Nº 07**

| Presupuesto Total | |
|---|---|
| **Descripción** | **Total (S/.)** |
| Personal | 1400.00 |
| Material de oficina | 76.00 |
| Material PAD | 88.00 |
| Equipos de desarrollo | 2225.00 |
| Servicios | 497.00 |
| Software | 1349.00 |
| **Total presupuesto** | **5,635.00** |

**Fuente: Elaboración propia**

## 15. Financiación

El desarrollo del proyecto será financiado en su totalidad por el Tesista.

# CAPÍTULO II
# FUNDAMENTO TEÓRICO

# II. Fundamento teórico

## 1. Realidad problemática

La Comisión de Portal Web cuenta con una infraestructura dentro de la Universidad Nacional de la Amazonia Peruana. Debido al flujo constante de información, esta área se ve en la imperiosa necesidad de comunicarse permanentemente una con otra y es por tanto un problema relevante la falta de comunicación e interconexión eficiente entre todas ellas, mas aún por no contar con una infraestructura de servicios de red integrados, lo que afecta la gestión de los procesos claves en el momento oportuno. Estos inconvenientes traen como consecuencia una ineficiente transmisión de la información y un inadecuado control de seguridad.

Esto lleva a la necesidad de diseñar un sistema de comunicación que permita optimizar los procesos administrativos y de comunicaciones existentes, y dar un sostenimiento a la información de una manera eficiente, eficaz y efectiva para la toma de decisiones.

### 1.1 Problemática General

La comisión del Portal Web no cuenta físicamente en su local con los respectivos equipos informáticos y con los servicios de una adecuada infraestructura de red con políticas de seguridad.

### 1.2 Problemática específica

- ✓ No cuenta con el software adecuado para implementar una política de seguridad que garantice la información y el servicio que brinda dentro de la red local y hacia el Internet.
- ✓ Carece de seguridad en la red local, como por ejemplo, acceso de usuarios a la red, permisos o políticas de seguridad para el manejo y utilización de las computadoras.
- ✓ Carece de una infraestructura de hardware para garantizar la seguridad de la información que llega y sale al Portal, para su difusión al Internet.
- ✓ La inexistencia de un esquema o estructura lógica y física de la seguridad para el Internet.

# 2. Antecedentes y marco teórico

## 2.1 Antecedentes

En 1996 algo de la fama de Internet se desplazó hacia la última evolución en las redes: la *intranet.* Una intranet es una tecnología resultante de la combinación de Internet con una red de área local (LAN), es decir, una red cuyo ámbito geográfico es menor de una milla. Por tanto, la intranet se adapta a todos los pasos adelante que da internet.

La conexión de ordenadores individuales o redes a internet no es un invento nuevo. Así es como crece internet. Pero, anteriormente, la mayoría de los sistemas conectados a internet lo estaban con el único propósito de compartir información con el resto de la comunidad electrónica. Los sistemas de internet estaban abiertos para casi todo el mundo. La utilización de internet tan solo como medio para comunicar dos o más redes privadas fue un giro revolucionario.

En base a este diseño se propondrán las potencialidades de los servicios de Windows 2003 Server, para el buen funcionamiento y desempeño de las actividades administrativas, las cuales se verán mejoradas que administrara la infraestructura de red

# 3. Marco teórico

## 3.1 Intranet

**¿Qué es una infraestructura de servicios de red?**

Una infraestructura de servicios de red (intranet) es una red privada que la tecnología Internet usó como arquitectura elemental. Una red interna se construye usando los protocolos TCP/IP para comunicación entre las distintas estaciones de trabajo, que pueden ejecutarse en muchas de las plataformas de hardware y en proyectos por cable. El hardware fundamental no es lo que construye una infraestructura de servicios de red, lo que importa son los protocolos del software. Las infraestructuras de servicios de red pueden coexistir con otra tecnología de red de área local. Por lo tanto, las herramientas usadas para crear una Intranet son idénticas a las mismas de internet y las aplicaciones Web. La diferencia principal de la intranet es que al acceso a la información publicada esta restringido a clientes dentro del grupo de la intranet.

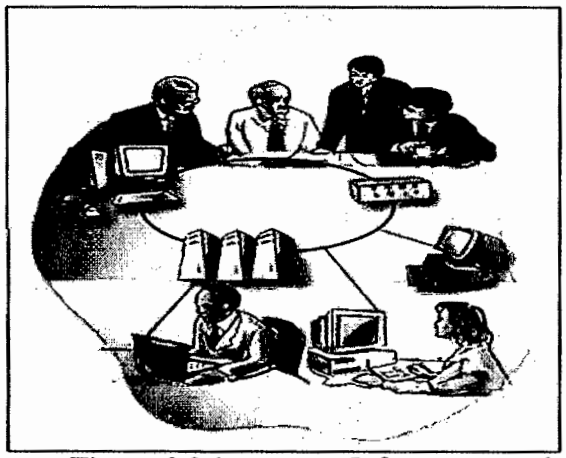


**Figura 2.2.1** : Infraestructura de servicios de red
**Fuente** : [URL 11]

**¿Porqué usar una infraestructura de servicios de red?**

Una infraestructura de servicios de red básica puede ser instalada en horas o días y puede servir como un "depósito de información" para la compañía completa. [URL 02].

- **Características y beneficios**

  La infraestructura de servicios de red tiene las siguientes características: [URL 02]:

  - Rápido diseño y fácil navegación.
  - Escalabilidad (se construye según la necesidad y los requerimientos).
  - Accesible para la mayoría de las plataformas de cómputo.
  - Integra la estrategia de cómputo distribuido.
  - Adaptable a los sistemas de información propietarios.

  **Los beneficios de una infraestructura de servicios de red**

  Más que ser un híbrido entre Internet y una red, mejora las capacidades de ambos, proporcionando algunos beneficios, entre los más importantes:

  - La capacidad de enviar información rápidamente.
  - Utilización y aprendizaje sencillos.
  - Escalabilidad, es decir, puede crecer con suma facilidad.
  - Usuarios simultáneos ilimitados.
  - Barata, multiplataforma y comunicaciones privadas seguras.

- Sistema abierto, es decir, sus protocolos son conocidos, facilitando el desarrollo de software por parte de cualquiera, no estando limitado a sistemas de propietario.
- Se pueden emplear todos los servicios que se utilizan en Internet.

Las infraestructuras de servicios de red toman prestado lo mejor de las redes y los sistemas de información tradicionales y lo combinan con la arquitectura abierta y los servicios de información de internet. Ahora hay nuevas aplicaciones que antes eran impensables, se denominan *soluciones intranet.*

Nadie los había previsto, pero internet se ha impuesto en las mentes más deprisa de lo que sus promotores habían imaginado. Posteriormente los fantasmas se han desencadenado, salvo que representaría el futuro de los sistemas de información.

➢ **Nuevo paradigma de la información**

La intranet propone el concepto de usar el paginador de Web como la interfaz de información universal. Las ventajas de este nuevo paradigma son [URL 02]:

- Reduce el tiempo de aprendizaje de los usuarios.
- Simplifica la instalación de aplicaciones.
- Presenta diferentes tipos de información: texto, gráficas, sonido y video.
- Actúa como "front-end" para las aplicaciones cliente-servidor.
- Permite el acceso a bases de datos.

**Componentes de una infraestructura de servicios de red**

Los componentes de una infraestructura de servicios de red se tomaron prestados inicialmente de las redes tradicionales y de internet. Según avanza esta área de los servicios de información se desarrollan productos específicos para el entorno de la intranet. Las partes de una intranet pueden dividirse en cuatro grandes áreas:

- **TCP/IP**

  TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en internet se encuentran conectados ordenadores de clases muy diferentes y con *hardware* y *software*

incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de *hardware* [URL 03].

- **Servicios de información**

  Los servicios de información forman el corazón de una intranet. Un servicios de información es cualquier paquete software o aplicación que pueda recibir, almacenar y enviar información a o desde uno o más clientes, en otras palabras, cualquier aplicación que permita la interacción con datos o personas mediante una intranet [URL 04].

- **Clientes**

  Los clientes son las herramientas software necesarias para acceder al mundo de la información que está disponible mediante servidores de información. Los clientes también se denominan utilidades de acceso, aplicaciones de estación de trabajo e interfaces de usuario, pero, independientemente del término que se utilice, todos ellos realizan funciones muy básicas. El cliente más habitual en una intranet siempre será el navegador Web [URL 04].

## 3.2 Conceptos básicos de redes

- **Arquitectura cliente/servidor**

  El secreto para comprender el funcionamiento de internet o de cualquier infraestructura de servicios de red es considerar la red poblada por dos tipos de aplicaciones informáticas: servidores y clientes. Los servidores son aplicaciones que proporcionan recursos. Los clientes son aplicaciones que se utilizan para acceder a los recursos que proporcionan los servidores. Internet soporta, el que en la actualidad se considera su servicio estrella, el World Wide Web, al que a menudo se conoce como "el Web" o "WWW". El Web consta de muchos servidores repartidos por todo el internet, estos servidores responden a peticiones de información, que se organiza en "páginas" [URL 04].

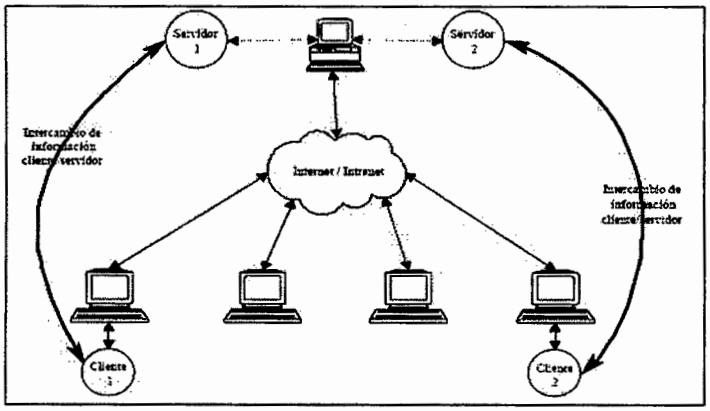



**Figura 2.2.2** : Arquitectura cliente/servidor
**Fuente** : [URL 04]

- **Servidor Web**

Cuando uno navega en internet, en realidad está asistiendo ante la charla entre el navegador web y el servidor web, que hablan un mismo idioma (http) [URL 05].

- **Servicios de acceso remoto (RAS)**

RAS conecta al usuario con una red remota a través de una línea telefónica. Una vez hecha la conexión, la línea telefónica se hace transparente y el acceso a los recursos de red se efectúa como si la computadora estuviera conectada directamente a la red.

- **DNS**

Sistema de nombre de dominio. DNS traduce un nombre alfabético común en su dirección IP numérica. Un servidor DNS permite a los usuarios localizar ordenadores en internet, manteniendo una base de datos de nombres de host y direcciones IP [URL 08].

- **DHCP**

Dynamic Host Configuration Protocol (DHCP). El protocolo dinámico de la configuración del anfitrión (DHCP) es un internet protocol para automatizar la configuración de las computadoras que utilizan TCP/IP. DHCP se puede utilizar para asignar automáticamente direcciones del IP, para entregar parámetros de la configuración del apilado de TCP/IP tales como el subnet mask y para omitir la rebajadora, y para proporcionar la otra información de la configuración tal como las direcciones para los servidores de impresión, tiempo y de noticias.

# CAPÍTULO III
# PROPUESTA DISEÑO DE POLÍTICAS DE SEGURIDAD

## 3. Disposiciones Generales

### Objetivo

Esta política tiene como objeto definir la normativa de seguridad de la red de comunicaciones del Portal Web que garantice la confidencialidad, integridad y disponibilidad de la información en los usos requeridos por la comunidad universitaria.

### Ámbito de aplicación.

Las medidas expuestas en este documento afectan a todo el personal docente e investigador, al personal de administración y servicios y en general, a todos los miembros de la comunidad universitaria que accedan a la red de comunicaciones.

En lo que respecta a los equipos informáticos, su ámbito de aplicación son todos los nodos (ordenadores personales, servidores, impresoras, etc.) conectados a la red de comunicaciones del Portal Web.

En cuanto a los temas abordados, se incide sobre tres aspectos:

- ✓ La infraestructura de red.
- ✓ La heterogeneidad de los colectivos de usuarios que comparten esa infraestructura, y por tanto, de sus necesidades de seguridad.
- ✓ La política de uso de la red por parte de los usuarios que, aunque su ámbito supera al de este documento, ha sido incluida por sus repercusiones directas sobre la seguridad de la red.

## 3.1 Infraestructura de Red

**Gestión de la red de comunicaciones.**

El diseño de la red de comunicaciones se realizará con el apoyo del personal necesario para una correcta definición de los requerimientos técnicos y funcionales de la red.

Corresponde al personal coordinar el diseño y la gestión de la red de comunicaciones de la Comisión Portal Web:

- ✓ El diseño físico y lógico de la red.
- ✓ La gestión de los enlaces de comunicaciones.
- ✓ La gestión del cableado de los locales (facultades).
- ✓ La gestión de las medidas de seguridad de la red.

## 3.2 Zonas de seguridad

**Finalidad.**

Dentro de la red de comunicaciones del portal Web existen varios entornos que comparten una misma infraestructura, pero que debido a los requerimientos de seguridad impuestos por su finalidad, deben mantenerse claramente separados. En este apartado se describe cada uno de estos entornos, que dan origen a las diferentes zonas de seguridad de la red.

**Internet**

Pertenecen a esta zona todos los nodos ubicados fuera de la red de la Universidad, que acceden o que son accesibles desde la red Internet.

**Servidores públicos (DMZ)**

Pertenecen a esta zona todos aquellos nodos que ofrecen servicios al resto de Internet, como servidores de correo, de DNS, o Web.

Se permite todo el tráfico excepto el que se lista a continuación:

- ✓ El tráfico IP con origen en direcciones no pertenecientes al rango de direcciones públicas de la Universidad o en direcciones reservadas.
- ✓ El tráfico de correo electrónico.
- ✓ Las comunicaciones específicas de los sistemas operativos corporativos (compartición de carpetas, impresión, etc.)

- ✓ El tráfico de gestión del equipamiento de red (SNMP, etc.)
- ✓ Las comunicaciones de servidores de bases de datos (Microsoft SQL-Server, Oracle, Mysql, etc.)
- ✓ El tráfico orientado a saltar las medidas de seguridad de este conjunto de restricciones (SOCKS, etc.)

## 3.3. Planteamiento de Solución

Dicho planteamiento está basado en una arquitectura de seguridad típica utiliza para proteger.

Esta propuesta consta de dos puntos centrales: los equipos informáticos y el software que se utilizará para tal fin, en base a esto se detalla la propuesta de solución para políticas de seguridad.

### 3.3.1 Software y Características a utilizar

**Sistema Operativo Microsoft Windows Server 2003**

**¿Qué es el Microsoft Windows Server 2003?**

Windows Server 2003 es un sistema operativo de red de propósitos múltiples, capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida.

**Características Windows 2003 Server**

- Está construido sobre la robustez y fiabilidad de Microsoft Windows 2000 Server.

- Las características mejoradas del Active Directory permiten realizar tareas fácilmente, entre las que destacan: la habilidad de renombrar dominios, la posibilidad de redefinir el esquema, una replicación más eficiente, la selección de múltiples objetos, arrastrar y soltar para mover objetos, almacenar consultas de usuario y permitir búsquedas basadas en criterios específicos.

- No instala Internet information services de manera predeterminada, debe ser instalado solo para los sistemas que proporcionan servicios Web. Internet Information Services (IIS) 6.0 está configurado para incrementar la seguridad del servidor Web.

- Agrega dos nuevas características para la recuperación de desastres, recuperación automática del sistema (recupera la configuración de un servidor caído) y recuperar copias de archivos (recupera copias de archivos en el tiempo).

**Beneficios en Microsoft Windows Server 2003**

➢ **Seguridad:**

Microsoft Windows Server 2003 es el sistema operativo de servidor más rápido y más seguro que ha existido. Windows Server 2003 ofrece fiabilidad al:

- Proporcionar una infraestructura integrada que ayuda a asegurar que su información de negocios estará segura.
- Proporcionar fiabilidad, disponibilidad, y escalabilidad para que usted pueda ofrecer la infraestructura de red que los usuarios solicitan.

➢ **Productividad:**

Microsoft Windows Server 2003 ofrece herramientas que le permiten implementar, administrar y usar su infraestructura de red para obtener una productividad máxima.

Microsoft Windows Server 2003 realiza esto al:

- Proporcionar herramientas flexibles que ayuden a ajustar su diseño e implementación a sus necesidades organizativas y de red.
- Ayudarle a administrar su red proactivamente al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones.
- Ayudar a mantener bajos los gastos generales al permitirles a los usuarios trabajar más por su cuenta.

➢ **Conectividad:**

Microsoft Windows Server 2003 puede ayudarle a crear una infraestructura de soluciones de negocio para mejorar la conectividad con empleados, socios, sistemas y clientes.

Windows Server 2003 realiza esto al:

- Proporcionar un servidor Web integrado y un servidor de transmisión de multimedia en tiempo real para ayudarle a crear más rápido, fácil y seguro una Intranet dinámica y sitios de Internet.

- Proporcionar un servidor de aplicaciones integrado que le ayude a desarrollar, implementar y administrar servicios Web en XML más fácilmente.
- Brindar las herramientas que le permitan conectar servicios Web a aplicaciones internas, proveedores y socios.

**¿Por qué utilizar Microsoft Windows Server 2003?**

- Como servidor de archivos es de un 100% a un 139% más rápido que Windows 2000 Server y un 200% más que Windows NT Server 4.0
- Como servidor Web es de un 100% a un 165% más rápido y seguro que Windows 2000 Server [URL 09].
- Las características mejoradas de Active Directory permiten realizar tareas más fácilmente, entre las que destacan la habilidad de renombrar dominios, la posibilidad de redefinir el esquema y una replicación más eficiente.
- Mayor disponibilidad a través del Windows System Resource Manager, de las actualizaciones del sistema automáticas y gracias a un servidor cuyos parámetros le confieren la máxima seguridad por defecto.
- Ofrece la mejor conectividad, facilitando al máximo la configuración de enlaces entre delegaciones, acceso inalámbrico seguro y acceso remoto a aplicaciones a través de los Terminal Services, así como en su integración mejorada con dispositivos y aplicaciones.

**Requerimientos de instalación de Windows 2003 Server**

Antes de la instalación deberá evaluar las características y condiciones para determinar si lo que necesita es una actualización o una instalación nueva. Para ello debemos tener en cuenta lo siguiente:

**Requerimientos de Hardware**

| | Standard Edition | Enterprise Edition | Datacenter Edition | Web Edition |
|---|---|---|---|---|
| Velocidad CPU | 550 MHz | 733 MHz | 733 MHz | 550 MHz |
| RAM | 256 MB | 256 MB | 1 GB | 256 MB |
| Espacio de Disco | 1.5 GB | 1.5 GB (x86)<br>2.0 GB (Itanium) | 1.5 GB (x86)<br>2.0 GB (Itanium) | 1.5 GB |

**FIGURA 2.2.3 : Requerimiento de Hardware**
**FUENTE : [05]**

**Requerimientos de software**

Debemos contar con:

- ✓ La edición de Windows Server 2003 que se va a instalar.
- ✓ Controladores del servidor.
- ✓ Controladores de las interfaces de disco, red, video, etc.
- ✓ El Service Pack actualizado para Windows Server 2003. (Llamado así a la actualización, o solución a problemas específicos de un sistema operativo o una aplicación).

**Determinación de las opciones de partición de discos**

Deberá elegir una de las siguientes opciones:

- ✓ Crear una nueva partición en un disco duro sin particiones.
- ✓ Crear una nueva partición en un disco duro con particiones.
- ✓ Instalar en una partición existente.
- ✓ Eliminar una partición existente para crear más espacio en el disco

**Elección de un sistema de archivos**

El sistema de archivos recomendado para Windows Server 2003 es NTFS, porque permite:

- ✓ Seguridad de archivos y carpetas
- ✓ Compresión de disco
- ✓ Cuotas de disco
- ✓ Cifrado de archivos

### 3.3.2 Metodología

La metodología que se usará en el presente proyecto, denominada "HIBRIDA" por estar compuesta de diversas fases de otras metodologías usadas para el desarrollo de una Infraestructura de Servicios de Red e Implementación de Políticas de Seguridad en base a Windows 2003 Server, tales como Microsoft Corporation, IGAPE, TIM EVANS y @System. La Metodología HIBRIDA consta de las siguientes fases:

1. **Evaluar Sistemas y Definir Requisitos de Usuario**
   (Microsoft Corporation - Fase – 1 [URL 10])
   - Definir requisitos de usuario. (Levantamiento de Observaciones)
   - Definir requisitos del sistema. (Mencionar los Servicios de Red)

- Definir requisitos propietarios de servidor. (Infraestructura de Hardware)
- Definir las funcionalidades (Requerimientos Funcionales: Describir los Servicios).
- Definir riesgos y aproximación a la gestión de riesgos (Ver en Internet).
- Coordinaciones con el equipo de trabajo (Líder del Proyecto, Analistas, Usuarios, Otros) → Cuadro de responsabilidades de cada participante

2. **Diagnóstico de la infraestructura de servicios de red de la Empresa: (IGAPE - fase 1)**
   - Ordenadores existentes: tamaño y funcionalidad.
   - Herramientas ofimáticas: grado de utilización, nivel de formación de los usuarios y número de licencias disponibles.
   - Puntos de conexión requeridos para la infraestructura de servicios de red.
   - Red de área local: idoneidad del sistema operativo de red, tamaño y capacidad el servidor, puntos de conexión existentes y capacidad de expansión, organización del cableado de red, número de tarjetas de conexión a red local existentes.
   - Infraestructura de comunicaciones: central telefónica, módems, líneas de transmisión de datos existentes, accesos a Internet existentes.
   - Infraestructura de servicios de red (Lo que actualmente existe: ¿Qué servicios de red tiene?)

3. **Definición de la Infraestructura de Servicios de Red necesaria: (IGAPE - fase 2)**
   - Nuevos ordenadores.
   - Nuevas licencias ofimáticas.
   - Implantación, si procede, de la red de área local.
   - Equipamiento auxiliar: impresoras, tarjetas, módems.
   - Diseño lógico
   - Diseño físico

- Infraestructura central de red (Servicios de red principales: DNS, WINS, Active Directory, DHCP, FTP.)

**4. Implementación de la Infraestructura de servicios de Red.**
**(TIM EVANS - fase 3 [01])**

Una vez considerados los asuntos administrativos precedentes, el enfoque será el diseño y contenido de la Intranet.

- Servicio TCP/IP
- Servicio DNS
- Servicio WINS
- Servicio de Active Directory
- Servicio DHCP
- Servicio de archivos
- Servicio de impresión
- Servicio de aplicaciones
- Servicio de correos
- Servicio de mensajería instantánea
- Servicio de Terminal Server
- Servicio de seguridad

**5. Visionamiento**

(Microsoft Solution Framework - Fase 1 [URL 10])

- Definir Visión y Alcance del proyecto
- Definir requisitos de Usuario.
- Definir requisitos del sistema.
- Definir requisitos propietarios de servidor.
- Definir las funcionalidades
- Definir riesgos y aproximación a la gestión de riesgos.
- Desarrollar el plan del proyecto.
- Coordinaciones con el equipo de trabajo

**6. Planeamiento**

**(IGAPE - fase 1 y Microsoft Solution Framework – fase 2)**

- Ordenadores existentes: tamaño y funcionalidad.
- Herramientas ofimáticas: grado de utilización, nivel de formación de los usuarios y número de licencias disponibles.

- Puntos de conexión requeridos para la infraestructura de servicios de red.
- Red de área local: idoneidad del sistema operativo de red, tamaño y capacidad el servidor, puntos de conexión existentes y capacidad de expansión, organización del cableado de red, número de tarjetas de conexión a red local existentes.
- Infraestructura de comunicaciones: módems, líneas de transmisión de datos existentes, accesos a Internet existentes.
- Infraestructura de servicios de red

7. **Desarrollo:**

**(IGAPE - fase 2)**

- Definición actual de la red
- Nuevos ordenadores.
- Nuevas licencias ofimáticas.
- Implantación, si procede, de la red de área local.
- Equipamiento auxiliar: impresoras, tarjetas, módems.
- Diseño lógico
- Diseño físico
- Infraestructura central de red

8. **Estabilización.**

Una vez terminado el desarrollo de la intranet se procede a las respectivas pruebas para la Infraestructura de servicios de red a implementar.

- Criterios y consideraciones de análisis
- Cálculos de utilización de la infraestructura de red
- Pruebas de rendimiento de la infraestructura de red

9. **Pruebas e Implantación (@System – fase 4)**

- Detección de errores
- Aceptación del cliente
- Instalación y soporte de clientes

### 3.3.3 Hardware y Arquitectura de Red de Comunicaciones

En base a lo señalado se propone una arquitectura de seguridad tal como se ve en la figura siguiente:

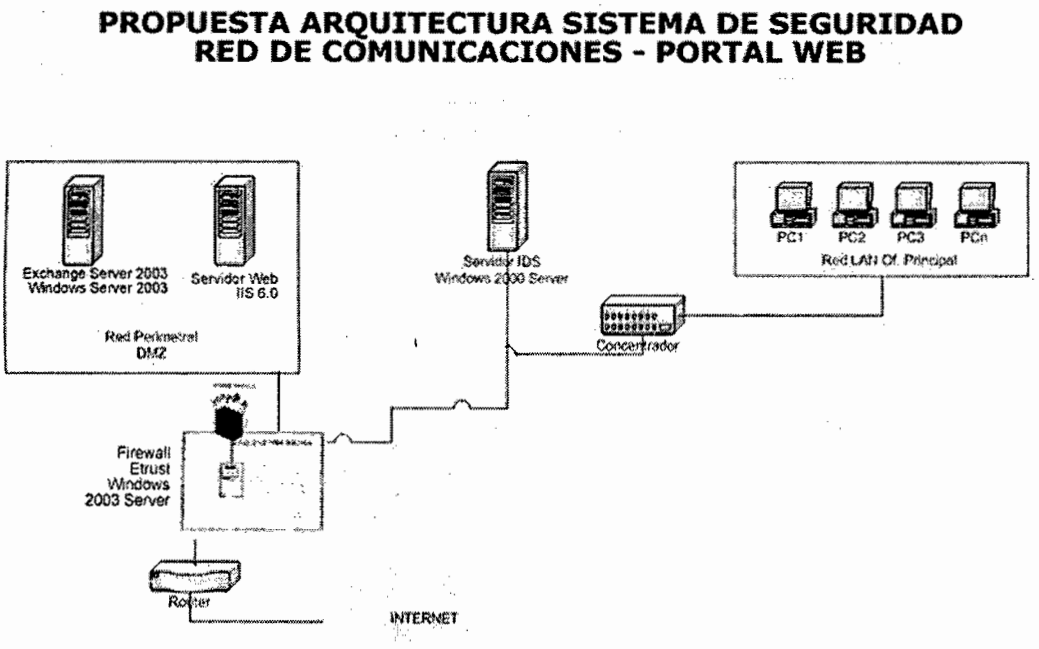



*Figura: Arquitectura Sistema de Seguridad – Portal Web*

**¿Que necesitamos?**

Hardware

- Una PC (Preferentemente servidor, con tres tarjetas de red, que hará las veces de servidor, el cual estará conectado a Internet, a la red Lan y el DMZ)
- 2 Switches

Software

- Etrust http://www.ca.com/ (software que nos permitirá crear las tres zonas detalladas líneas arriba)
- Windows Server 2003

**Nota**:

Se recomienda diseñar y probar el modelo antes de poner en producción.

### 3.3.3.1 Topología del firewall

La topología básica más fiable es la de crear tres zonas: (ver figura anterior)

- ✓ Zona Internet
- ✓ Zona DMZ (Desmilitarized Zone)
- ✓ Zona de Red Privada
- ✓ Estas tres Zonas son creadas por el firewall

**La Zona Internet**: Es el contacto del firewall con el mundo Internet.

**Zona desmilitarizada DMZ**, es la zona creada por el firewall, donde se coloca los equipos que proveen servicio público, como son; servidor de Web, servidor de correos, servicios de ftp, y cualquier servicio público como servidor de terminales, etc.

El firewall en la zona DMZ pone los servidores de uso público, pero están protegidos contra ataques, porque los servidores de esta zona están a través de direcciones ficticias, que representan a direcciones reales y los accesos son restringidos a las funciones que el usuario les permite.

**Zona privada**, es la correspondiente a la red del usuario, como intranets, recursos propios, aplicaciones, servidores de base de datos y cualquier otra aplicación del usuario.

La zona privada, si es la zona totalmente protegida, a esta zona ningún acceso externo esta permitido, solo esta permitido salidas a los usuarios que la institución permita.
Todos los tráficos entre las redes internas, son controlados.

### 3.3.3.2 Firewall

Un firewall de Internet es un sistema que fuerza políticas de seguridad en las comunicaciones, entre Internet y la red privada o intranet.

Un firewall pone en acción un juego de reglas de acuerdo a las políticas de seguridad de la institución que lo usa. Basado en estas reglas, el firewall inspeccionará él tráfico de red, de acuerdo a los tipos de servicios, direcciones de red, con el objetivo de permitir o negar dicho tráfico. La seguridad de perímetro es usualmente instalado sobre los Gateway de la red, de tal forma que todo él tráfico entre la red interna y red externa pueda ser examinado.

Alcances de los Firewalls

- ✓ Proporciona un punto donde concentrar las medidas de seguridad.
- ✓ Ayuda a llevar a cabo la política de seguridad.
- ✓ Permite desactivar servicios que se consideran inseguros desde Internet.
- ✓ Permite restringir fácilmente el acceso o la salida desde/hacia determinadas maquinas.
- ✓ Permite el registro de información sobre la actividad entre la red interna y el exterior.
- ✓ Aísla secciones internas de la red de otras.

Limitaciones de los Firewalls

- ✓ No puede proteger de enemigos internos.
- ✓ La información confidencial no solo puede exportarse a través de la red.
- ✓ Las acciones indebidas sobre maquinas (accesos no autorizados, introducción de virus, etc.) se pueden realizar aun mas fácilmente desde la red interna.
- ✓ No puede impedir ni proteger conexiones que no pasan a través del firewall.
- ✓ No puede proteger contra nuevos tipos de ataque que no tiene catalogados.
- ✓ No puede impedir la entrada de virus.

**Tipos de firewall**

**Firewall de filtrado de paquetes**: Desarrolla filtrado basado en conexiones TCP. Este firewall desarrolla el filtrado para determinar si una conexión TCP esta permitido basado en las reglas de control establecidas. Un firewall que esta basado en filtro de estados TCP, combina el alto nivel de seguridad de los proxys, con la performance de los filtros de paquete.

**Firewall proxy**: Aplicación independiente, todo el tráfico se recibe en el cortafuegos y después lo redirige. Cuenta con un cache. Existen proxys transparentes.
Es realizado por juegos de servicios de Proxy, siendo un Proxy una aplicación que corre sobre el gateway y se pone en cascada con la aplicación real, para protegerlo, pero requiere loguearse al proxy. Sus desventajas:

- ✓ Baja performance, por las conexiones en cascada
- ✓ Pocas aplicaciones soportadas, pocas aplicaciones tienen escritas proxys.
- ✓ Impacto operacional, requiere código de aplicación o del usuario final para el acceso.
- ✓ Limitada seguridad

### 3.3.3.3Diseño de las reglas del firewall

**Reglas en el firewall**

Las reglas en un Firewall se crean de igual forma como se a mencionado con anterioridad, tenemos una condición que debe de cumplirse para que el paquete de entrada o salida tenga los permisos para poder llegar a su destino. Los valores que debemos de utilizar para crear una regla se muestran a continuación:

Las reglas son las que van a decidir que pasa y que no pasa, que se registra y que no se registra.
Entonces para un firewall básico, que trabaje con servicios y direcciones ip lo que necesitamos es conocer los servicios que hay en cada puerto y las direcciones que pueden ingresar o no a nuestra red.

Por ejemplo tenemos los siguientes servicios en sus respectivos puertos:

- ✓ WWW 80
- ✓ ssl 443
- ✓ ftp 21
- ✓ ssh 22
- ✓ telnet 23
- ✓ smtp 25
- ✓ pop3 110
- ✓ dns 53

Ahora que ya sabemos esto, vamos a definir nuestro firewall, con los servicios que vamos a dejar funcionar y que no va a funcionar.
Primero debemos elegir la política que vamos a utilizar, generalmente entre:

- ✓ Bloqueo todo y permito solo algo
- ✓ Permito todo y bloqueo solo algo

*1)* ***Política por defecto ACEPTAR***: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.

*2)* ***Política por defecto DENEGAR:*** todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

Como es obvio imaginar, la primera política facilita mucho la gestión del firewall, ya que simplemente nos tenemos que preocupar de proteger aquellos puertos o direcciones que sabemos que nos interesa; el resto no importa tanto y se deja pasar.

En cambio, si la política por defecto es DENEGAR, a no ser que lo permitamos explícitamente, el firewall se convierte en un auténtico MURO infranqueable. El problema es que es mucho más difícil preparar un firewall así, y hay que tener muy claro como funciona el sistema y que es lo que se tiene que abrir sin caer en la tentación de empezar a meter reglas super-permisivas.

La primera forma, de bloquear todo y permitir solo algo es la más recomendada. Así que vamos ahora a definir que es ese algo que vamos a permitir:

- ✓ Permitir servicios Web
- ✓ Permitir resolución de nombres o DNS
- ✓ Permitir accesos ssh
- ✓ Permitir revisar correo (pop3)
- ✓ Permitir enviar correo (smtp)
- ✓ Permitir Web seguro (ssl)

En nuestros firewall, generalmente debemos tener 3 tarjetas de red conectadas para que sea efectivo el filtro, una a la red externa y otra a la red interna, y las reglas deciden que pasa y que no pasa.

Entonces el esquema de nuestras reglas sería el siguiente:

- ✓ Permitir todo en la red interna
- ✓ Bloquear todo en la red externa
- ✓ Permitir todo a la DMZ o maquinas con privilegios y salir rápido
- ✓ Permitir acceso Web (puerto 80) de toda mi red interna a cualquier host y conservar el estado y salir rápido

- ✓ Permitir acceso Web seguro (puerto 443) de toda mi red interna a cualquier host y conservar el estado y salir rápido
- ✓ Permitir acceso correo (puertos 25 y 110 ) de toda mi red interna a cualquier host y conservar el estado y salir rápido
- ✓ Permitir resolver nombres (puertos 53 ) de toda mi red interna a cualquier host y conservar el estado y salir rápido
- ✓ Permitir acceso a ssh (puerto 22) de cualquier host a firewall y conservar estado y salir rápido.

### 3.3.3.4 Agregar reglas (Políticas de Seguridad) al firewall con Etrust

Después de la instalación, su cortafuego no es todavía activo. Una vez que usted cree y despliegue su primera regla del cortafuego, el cortafuego llega a ser activo. Por defecto, ningún tráfico permitido a menos que fuera permitido específicamente por el cortafuego.
Pues usted camina con este ejemplo, usted creará una política corporativa típica de la seguridad que esté conforme a las reglas siguientes:

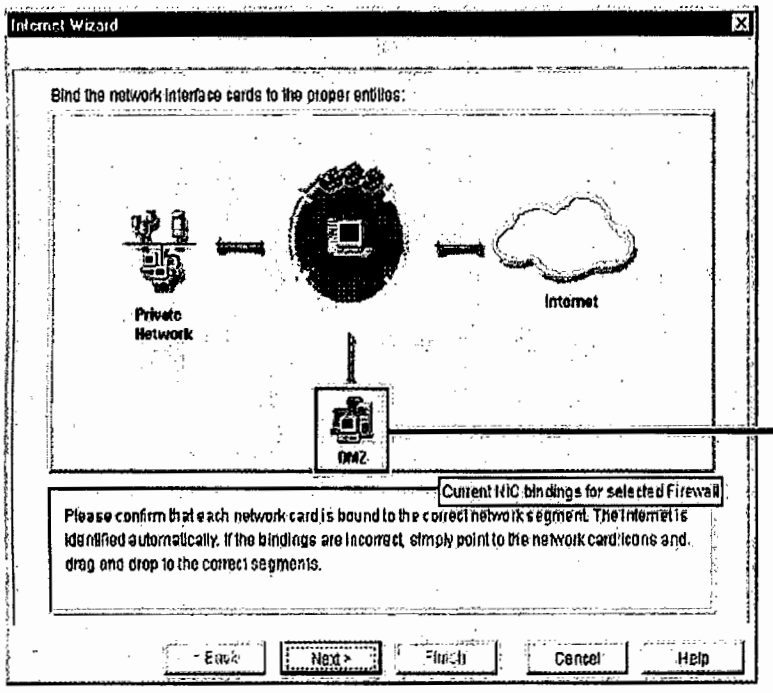
- ✓ Nadie en el Internet se permite conectar con las redes internas
- ✓ Se permite a los usuarios internos de la red tener WWW y los accesos al Internet, tráfico del ftp del E-mail se permiten al DMZ
- ✓ Todas las preguntas del DNS que vienen del Internet al servidor del DNS en el DMZ se permiten. Este servidor del DNS no contendrá ninguna información interna del anfitrión. El anfitrión interno utilizará un DNS interno dentro de la red interna, que no está conforme a reglas del cortafuego. Ese DNS interno será permitido a los accesos el DNS en el DMZ para la resolución externa
- ✓ La conectividad del E-mail a y desde el Internet está a través del servidor del E-mail en el DMZ
- ✓ Todo el tráfico de WWW y del ftp del Internet al servidor de WWW en el DMZ se permite.

**Usando el internet wizard de Etrust**

Seleccionar el cortafuego que representa su motor del cortafuego en el cristal izquierdo

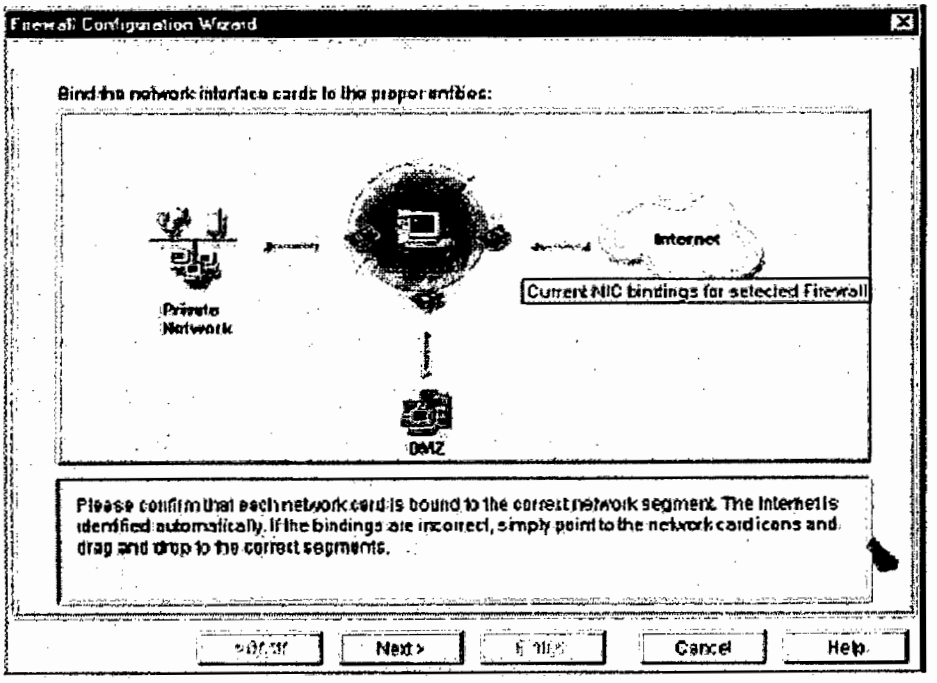
Hacer click en la imagen  "luanch Internet Wizard", seleccionar del menú de Herramientas.

La ventana del mago del Internet aparece que exhibe su topología de la red



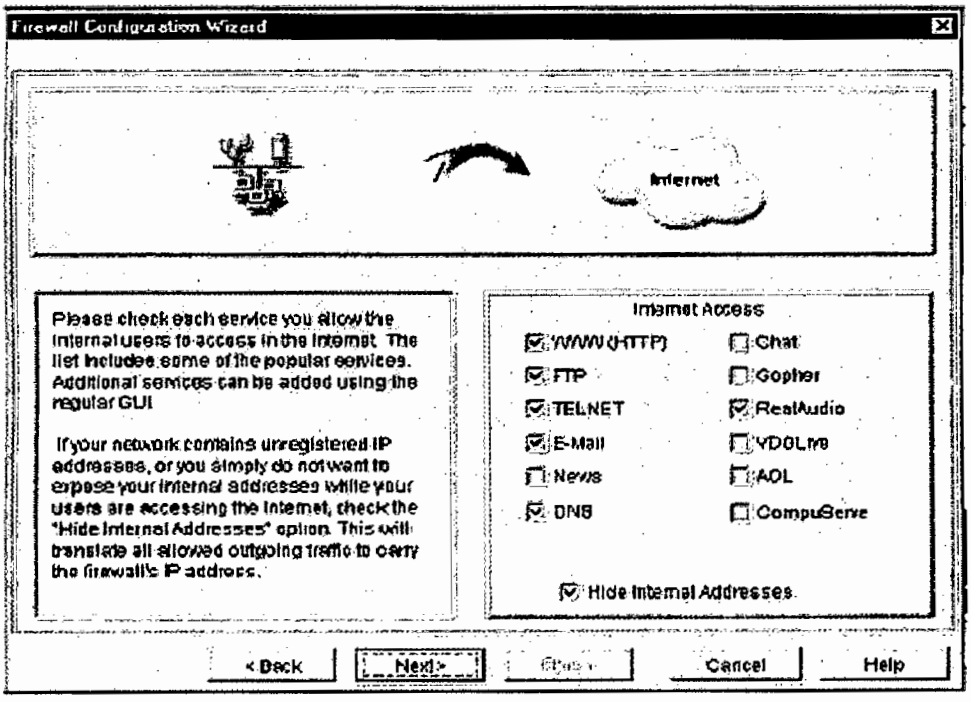

La DMZ, representa la zona en donde residen todos los servicios públicos del Internet. Cualquier paquete de la información que se mueve entre su red privada, el DMZ, y el Internet debe ir a través del cortafuego

Hacer clic y arrastrar el icono de la tarjeta de la red  apropiado a su entidad asociada de la red, y siguiente:

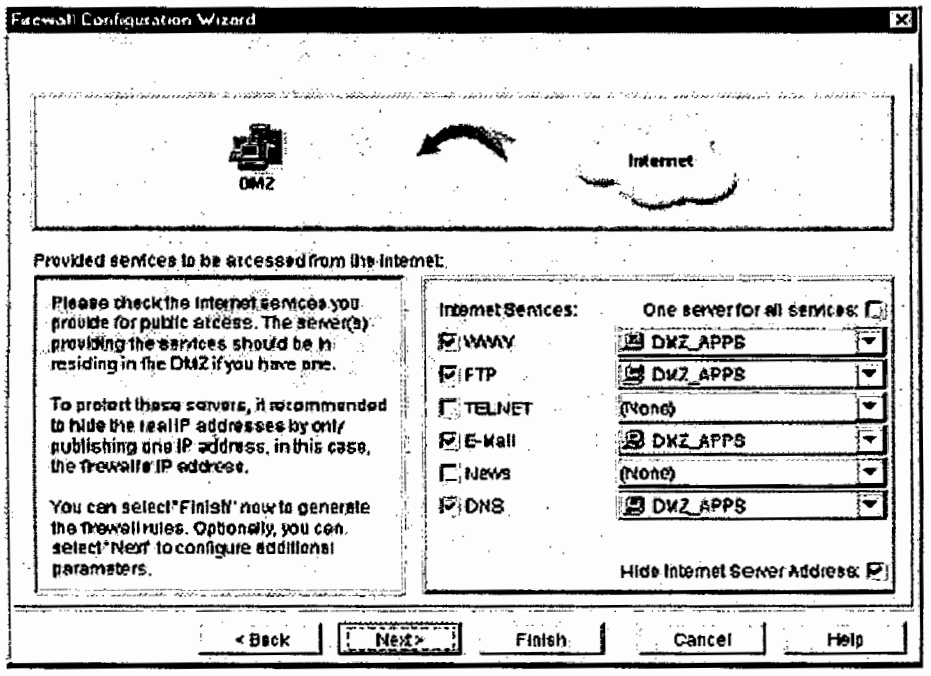


**Nota:** Su pantalla parecerá diferente de la que esta' demostrada arriba, dependiendo del número de las tarjetas de la red que usted tiene.

Terminar la pantalla siguiente según lo ilustrado abajo para seleccionar los servicios que permitirán sus usuarios para utilizar a los accesos el Internet, y hacer click después

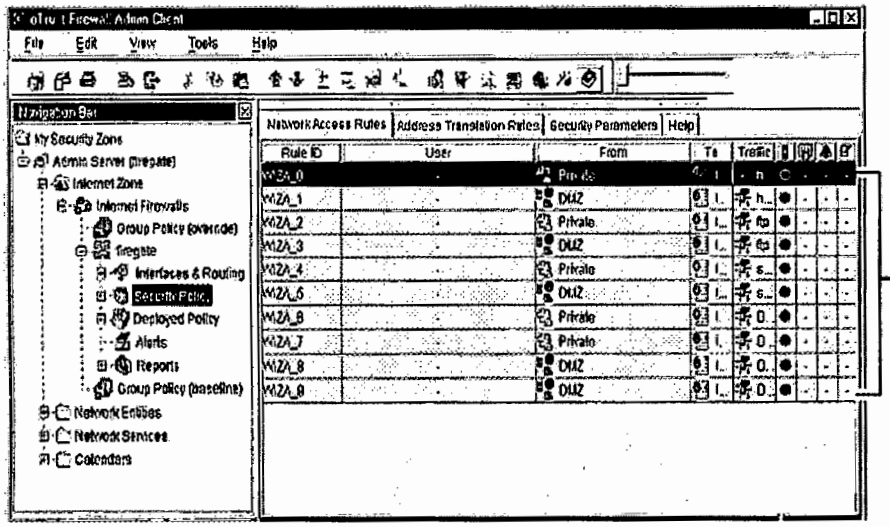



Seleccionar los servicios del Internet que usted proporcionará para el acceso público. Termi nar la pantalla según lo ilustrado en la página siguiente, substituyendo su Web Server con el que está demostrado.




Clic en Finish para finalizar las reglas del firewall.

Una caja de diálogo aparece que le alerta que todas las reglas previamente generadas del mago serán suprimidas
El mago del Internet procesa su política de la seguridad y crea las reglas correspondientes. Estas nuevas reglas aparecen en la tabla derecha de la pantalla del cliente del admin.




En este ejemplo, el mago del Internet creó 10 reglas. Derecho-tecleo una regla para corregirlo o para suprimir

# CAPÍTULO IV
# ESTUDIO DE FACTIBILIDAD

## 4. Justificación

### Justificación legal

### Justificación académica

Debido a que el ejecutor del proyecto tiene la base de conocimientos necesarios para poder desarrollar eficientemente el mismo, conocimientos adquiridos en los diferentes cursos desarrollados como Redes de Computadoras, Sistemas Operativos, etc;

Por otro lado este proyecto servirá para ostentar el grado de Ingeniero de Sistemas e Informática del ejecutor.

### Justificación institucional

El diseño de políticas de seguridad en base a Windows 2003 Server no solo automatizará de manera eficiente los procesos en la institución sino que también levantará la imagen institucional de la misma y la situará en la capacidad de competir de una mejor forma con otras de rubro similar, debido a las ventajas que obtendrán con la implementación de la misma.

### Justificación económica

El desarrollo de dicho proyecto no tiene un costo considerable, además el mantenimiento y el coste marginal de su uso constante es relativamente bajo. Por otra parte, la ganancia en términos monetarios, tiempo, y precisión de resultados resultantes del uso de la intranet y los servicios a levantarse en dicho sistema operativo son muy altos.

### Justificación tecnológica

El presente proyecto busca diseñar tecnológicamente el proceso de transferencia de información entre las distintas áreas de la institución donde se realizará el proyecto. Para llevar a cabo esto se ha tomado como base el uso de la tecnología de intranet y los servicios a levantarse en dicho Sistema Operativo.

### Justificación operativa

Con la ayuda de la intranet y de los servicios propuestos el personal se beneficiará gracias al fácil y rápido acceso a la información entre las áreas de la institución y ésta se verá beneficiada al tener información estructurada y actualizada en el momento oportuno.

**Justificación social**

Nuestra sociedad debe alinearse a las nuevas tendencias y provocar panoramas facilitadores, el uso de la intranet y del diseño propuesto permitirá a la institución brindar un servicio de mejor calidad para los estudiantes que se desempeñarán como futuros profesionales en la región y el país.

Los especialistas en esta área ven una oportunidad creciente de trabajo y negocio.

## 5. Objetivos

### 4.1 Objetivo general

Diseño de Políticas de Seguridad en una Red en Base a Windows 2003 Server es para mejorar la Gestión Administrativa de la Comisión de Portal Web - UNAP.

### 4.2 Objetivos específicos

- Mejorar la utilización de los recursos de hardware que la Comision de Portal Web - UNAP maneja y administra.
- Lograr agilidad, flexibilidad y adaptabilidad en el procesamiento de la información.
- Limitar los accesos a la información que cada departamento deba manejar
- Administrar y supervisar DNS
- Administrar y supervisar DHCP.
- Asignar direcciones IP mediante el Protocolo de configuración dinámica de host (DHCP).
- Configurar, administrar y supervisar el acceso a la red.

## 6. Definición de variables

**Definición conceptual**

- **Variable independiente:** Infraestructura de servicios de red integrados en base a Windows 2003 Server.
- **Variable dependiente:** Nivel gestión administrativa.
- **Variable interviniente:** Metodología HIBRIDA del Diseño de servicios de red basado en Windows 2003 Server.

**Definición operacional**

- Diseño de servicios de red integrados en base a Windows 2003 Server.
  Permite el acceso a la información publicada, y esta restringido a clientes dentro del grupo de la intranet.
- Nivel gestión administrativa
  Gestión que genera conformidad al brindar información a sus clientes.

# CAPÍTULO V
# METODOLOGÍA EMPLEADA

## 5.1 Enfoque

La metodología que se usará en el presento proyecto denominada "HIBRIDA" por estar compuesta de diversas fases de otras metodologías usadas para el desarrollo de un Diseño de servicios de red basado en Windows 2003 server, tales como Microsoft Solution Framework (MSF), IGAPE, TIM EVANS y @System.

## 5.2 Técnicas

Técnicas de extracción de información

- Entrevistas
- Observación

## 5.3 Herramientas

Para el desarrollo del proyecto se utilizaran diversas herramientas tales como:

**Hardware**

- Computadoras personales
- Impresora

**Software**

- Microsoft Windows Server 2003
- Microsoft Office System 2003.
- Etrust firewall

**Otros**

- Material de escritorio en general
- Acceso a internet

## 5.4 Fases de la Metodología

### 5.4.1 VISIONAMIENTO

La fase de *visionamiento* es el período durante el cual, el cliente defina los requisitos primordiales de alto nivel y los cometidos globales del proyecto.

El propósito principal es asegurar una visión común y alcanzar un consenso entre las diferentes unidades organizativas a crearse, esto es valioso para la organización y probablemente para tener éxito. Durante ésta fase, se enfoca en la creación de definiciones claras del problema.

### 5.4.1.1 Visión y alcance

- **Definición del problema**

  En la comisión Portal Web – UNAP, no existe interconexión entre sus áreas, además existe atrasos y pérdida de tiempo en la transmisión de información.

- **Visión**

  Ser de la comisión Portal Web una organización con mejor diseño de acuerdo a la propuesta plantead para sus diversos servicios, la UNAP – por medio de la Comision Portal Web logrará obtener un valor agregado en el servicio que brinda y una mejora en la ejecución de sus procesos lo que permitirá realizarlos más ágil y eficientemente.

- **Perfiles de usuario**

| Usuario | Perfil | Requerimientos |
|---|---|---|
| Directivos | - Administración de la Universidad.<br>- Usuario de toma de decisiones.<br>- Acceso a toda la información. | - Obtención de reportes de manera oportuna.<br>- Comunicación rápida con las demás áreas para agilizar la toma de decisiones |
| Operativos | - Encargados de la parte transaccional (generación de reportes).<br>- Acceso a casi toda la información. | - Consultas rápidas de la información.<br>- Realizar transacciones seguras, fáciles y rápidas con los datos. |
| Docentes | - Generación de evaluaciones<br>- Generación de material didáctico<br>- Evaluación de los alumnos. | - Proceso de evaluación eficiente y sencillo<br>Obtención de listado de alumnos en forma oportuna. |
| Estudiantes | - Acceso a cursos dictados<br>- Horarios<br>- Acceso a notas de los cursos<br>- Servicio de aplicaciones. | - Reporte de notas a tiempo<br>- Informe de horarios<br>Acceder a programas e información necesaria para el desarrollo de los cursos. |

**Cuadro N° 01** : Perfiles de Usuario
**Fuente** : Elaboración propia

- **Alcance del proyecto**

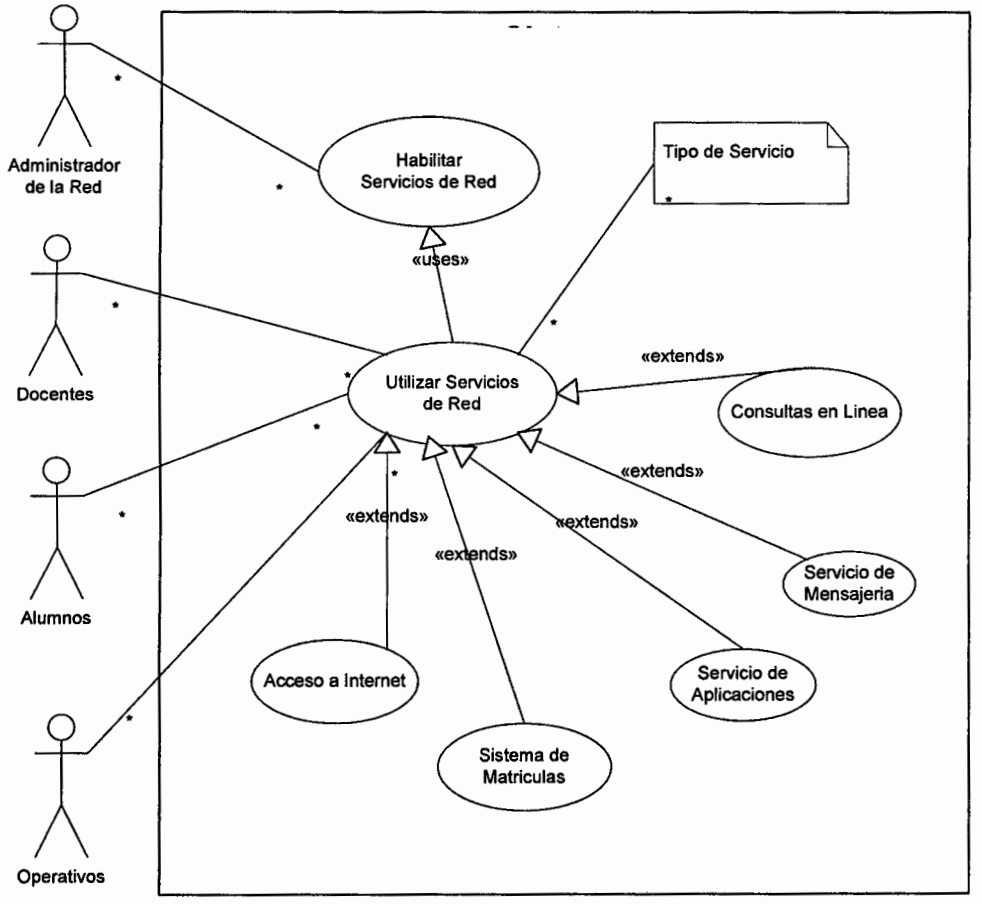



**Diagrama N° 01** : Caso de Uso del Alcance del Proyecto

**Fuente** : Elaboración Propia

- **Conceptualización de la solución**

El diseño de una Infraestructura de Servicios de Red, basados en Windows 2003 Server y sus servicios, debe contemplar los siguientes aspectos:

Debe interconectar eficientemente las diferentes áreas de la organización.

- Implementar el servidor DNS para una mejor organización de la red.
- Implementar el servidor de correos para obtener una mejor comunicación entre los usuarios de la red
- Implementar el servidor de aplicaciones para un mejor desempeño de las áreas de la organización.
- Implementar una aplicación web para el manejo de la información.

**Ventajas del diseño de una Infraestructura de Servicios de Red basado en Windows 2003 Server.**

Aunque a veces, difícilmente cuantificables, las ventajas que reporta un diseño de Infraestructura de Servicios de Red, basado en Windows 2003 server, integrados, son numerosas, y ya no son sólo económicas sino también en ahorro de tiempo y espacio físico.
En primer lugar, es un sistema que está operativo en cualquier sitio y sin limitación horaria, lo que permite que un trabajador pueda desempeñar su labor incluso fuera del local de trabajo y en horas distintas a las habituales. (Siempre y cuando tenga los permisos adecuados para el uso de dichos servcios).

Una Infraestructura de Servicios de Red integrados también es muy útil para evitar perder tiempo reuniendo a los trabajadores para darles una información determinada, ya que gracias a los foros o tablones de anuncios cualquier persona autorizada puede conocer las últimas novedades sobre las cosas que ocurren sin necesidad de interrumpir su jornada laboral.
Por supuesto, permite un claro ahorro económico en material de papelería y en telecomunicaciones; los informes, notas, comunicados e incluso las llamadas telefónicas se pueden sustituir por la pantalla del ordenador, de modo que todo esté más organizado y accesible a los usuarios de la Infraestructura de Servicios de Red integrados, gracias a los diferentes servicios que nos presenta Windows 2003 server (Como Mensajera Instantánea).
Una ventaja no menos destacable es la facilidad con la que se puede formar a los empleados en determinadas materias sin gastos en academias, profesores o sin necesidad de interrumpir a uno u otro compañero para que nos aclare una duda. Simplemente con una tutoría programada, el trabajador podrá aprender por sí mismo los conocimientos exigidos.

También se debe señalar la utilidad que representa este proyecto para facilitar ciertas informaciones a unos y privar de ella a otros; sólo con la introducción de nuestra clave personal, el sistema ya sabe qué contenidos puede mostrarnos y cuáles nos son vedados.

Y para terminar con una lista en la que nos podríamos extender mucho más, debemos tener en cuenta que un Diseño de infraestructura de servicios de red integrados, basados en Windows 2003 Server, se caracteriza por su fácil manejo para toda persona que esté familiarizada con el entorno Windows.

La única dificultad que podemos encontrar a la hora de ver los resultados es que los trabajadores tengan reticencias en su utilización. Problema que se puede solventar concienciando de la utilidad y comodidad del sistema. Una vez que la red está totalmente implantada en dicha institución, no se tardará en ver los beneficios que ésta reporta a los usuarios.

- **Objetivos del proyecto**

**Objetivos del negocio**

- Mejorar la calidad del servicio
- Interconectar las áreas de la institución.
- Incrementar la cartera de usuarios en unidades organizativas.
- Automatizar los procesos

**Objetivos del diseño**

- Mejorar la utilización de los recursos de hardware y software que la Comision Portal web – UNAP maneja.
- Lograr agilidad, flexibilidad y adaptabilidad en el procesamiento de la información.
- Limitar los accesos a la información que cada departamento deba manejar
- Administrar y Configurar los servicios DNS, DHCP, FTP, WEB, Active Directory, etc.
- Asignar direcciones IP mediante el Protocolo de configuración dinámica de host (DHCP).
- Configurar, administrar y supervisar el acceso a la red.

- **Factores críticos de éxito**

Los factores críticos de éxito son aquellos de los que dependerá el éxito o fracaso de la institución, y por lo tanto deben de tener una atención

especial para el buen desempeño de la funciones de los encargados en la institución.

**Factores críticos de éxito:**

- Disposición de entidades para firma de convenios, el nivel de participación de la dirección de la institución.
- El conocimiento y compromiso del personal administrativo, docente y de servicio con los objetivos propuestos, la eficacia de los programas de capacitación, el nivel de participación de la dirección de la institución.
- Costos de adecuar el diseño de la infraestructura, cultura de cuidado con el inmobiliario.

### 5.4.1.2 Estructura del proyecto

1. **Roles y responsabilidades del responsable y de el cliente**

   A continuación se presenta un cuadro de las personas involucradas y sus roles en el proyecto, tanto el ejecutor del proyecto y el cliente.

| Nombre | Rol |
|---|---|
| Alan Alberto García Panduro (Responsable) | Encargados del levantamiento de la información.<br>Análisis de la información<br>Implementación del Sistema de Servicios de Red, basado en Windows 2003 server.<br>Responsabilidad<br>Monitorear el correcto desarrollo del proyecto |
| Administrador Comision Portal Web - UNAP | Facilitar el acceso a la información y las instalaciones de la Empresa<br>Responsabilidad<br>Brindar apoyo y acceso oportuno. |

**Cuadro Nº 02** : Roles y responsabilidades del responsable y de Cliente.

**Fuente** : Elaboración propia

2. **Decisión de comunicaciones**

   Los archivos generados en este proyecto serán realizados únicamente por el responsable.

3. **Decisiones logísticas**

   Como practica de desarrollo se usará los conocimientos adquiridos por parte del responsable, en el diseño de la red.

   La definición del contenido de las especificaciones del producto fueron dadas por el ejecutor del proyecto.

4. **Decisiones de gestión de cambios**

   Los cambios o imprevistos que se presenten e el proyecto serán atendido por el ejecutor del proyecto

### 5.4.1.3 Análisis de riesgos

#### i) Definición de los riesgos

- No se tiene un acceso oportuno a la información que necesita hacer uso el ejecutor del proyecto.
- Falta de implementación de un plan para asegurar información sensible de la institución.

#### ii) Valoración de los riesgos

| Condición/ Descripción | Consecuencia | Probabilidad | Impacto | Prioridad | Mitigación |
|---|---|---|---|---|---|
| No se tiene un acceso oportuno a la información que necesita hacer uso el ejecutor del proyecto. | Retraso en la implementación de la Infraestructura de Servicios de Red, basado en Windows 2003 Server | 1 (Bajo) | 3 (Alto) | 0 | El ejecutor del proyecto debe identificar a la(s) personas encargadas de proveer esta información y solicitar su pronta atención. |
| Falta de implementación de un plan para asegurar información sensible de la institución. | Acceso a información confidencial de la institución | 1 | 3 | 1 | El equipo debe implementar ni veles de seguridad y autenticación de usuarios |

**Cuadro N°03** : Valoración de riesgos

**Fuente** : Elaboración propia

### 5.4.2 PLANEAMIENTO

Durante la fase de Visionamiento, el ejecutor recoge bastante información para determinar el alcance del proyecto. La fase planificadora puede comenzar durante la fase de Visionamiento, siempre y cuando la información que haya sido recogida sea suficiente para que pueda empezar a organizar y analizar esa información. Durante la fase de *planeamiento,* el ejecutor toma el trabajo que ha hecho durante la fase de Visionamiento y continúa elaborando sobre ella y adicionalmente lo organiza y lo analiza.

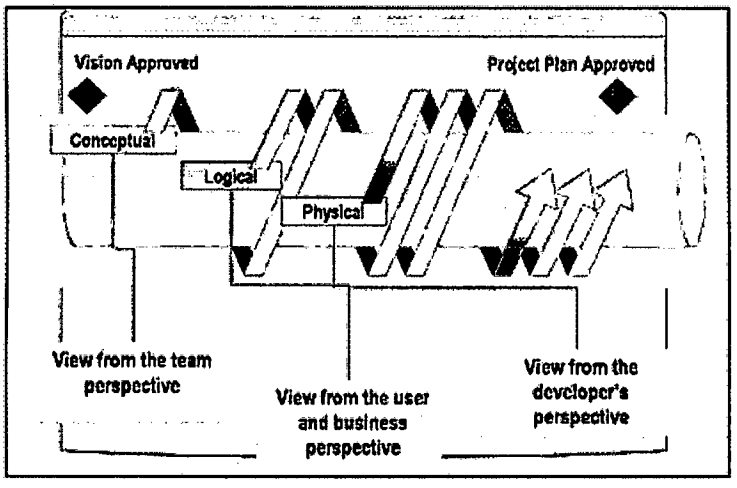



**Figura N° 4.4.2** : Tipo de diseño de procesos
**Fuente** : [01]

#### 5.4.2.1 Creación del diseño conceptual

**i) Definición de requerimientos**

**Requerimientos del negocio**

- Interconectar áreas de la institución
- Automatizar procesos
- Flujo seguro de los datos
- Mejorar la infraestructura

**Requisitos de usuarios**

***De los Administrativos y operativos***

- Acceso mas rápido a la información
- Comunicación más optima entre las áreas de la institución.
- Mantener información en tiempo real.
- Mejorar la utilización de los recursos de hardware.
- Lograr agilidad, flexibilidad y adaptabilidad en el procesamiento de la información.
- Limitar los accesos a la información que cada departamento deba manejar.
- Realizar un mantenimiento general de los equipos de cómputo.

**Requisitos del sistema**

Para poder diseñar la infraestructura de red integrada, basado en Windows 2003 Server es necesario contar con los siguientes servicios:

- Servicio TCP/IP
- Servicio DNS
- Servicio de Active Directory
- Servicio DHCP
- Servicio de archivos
- Servicio de impresión
- Servicio de aplicaciones
- Servicio de correos
- Servicio de mensajería instantánea
- Servicio de Terminal Server
- Servicio de seguridad

**ii) Funcionalidad de los servicios**

Los servicios que son requisitos para el diseño de la infraestructura de red basado en Windows 2003 Server, se describen a continuación.

**Servicio TCP/IP**

**- Transferencia de datos a través de un canal**

Desde el punto de vista de la aplicación, TCP transfiere un flujo continuo de bytes a través de internet. La aplicación no ha de preocuparse de trocear los datos en bloques o en datagramas. TCP

se encarga de esto al agrupar los bytes en segmentos TCP, que se pasan a IP para ser retransmitidos al destino. Además, TCP decide por sí mismo cómo segmentar los datos y puede enviarlos del modo que más le convenga.

A veces, una aplicación necesita estar segura de que todos los datos pasados a TCP han sido transmitidos efectivamente al destino. Por esa razón, se define la función "push". Esta función mandará todos los segmentos que sigan almacenados al host de destino. El cierre normal de la conexión también provoca que se llame a esta función, para evitar que la transmisión quede incompleta.

- **Fiabilidad**

TCP asigna un número de secuencia a cada byte transmitido, y espera un reconocimiento afirmativo (ACK) del TCP receptor. Si el ACK no se recibe dentro de un intervalo de timeout, los datos se retransmiten. Como los datos se transmiten en bloques (segmentos de TCP), al host de destino sólo se le envía el número de secuencia del byte de cada segmento.

El TCP receptor utiliza los números de secuencia para organizar los segmentos cuando llegan fuera de orden, así como para eliminar segmentos duplicados.

- **Control de flujo**

El TCP receptor, al enviar un ACK al emisor, indica también el número de bytes que puede recibir aún, sin que se produzca sobrecarga y desbordamiento de sus buffers internos. Este valor se envía en el ACK en la forma del número de secuencia más elevado que se puede recibir sin problemas. Este mecanismo se conoce también como mecanismo de ventanas.

- **Conexiones lógicas**

La fiabilidad y el control de flujo descritos más arriba requieren que TCP inicialice y mantenga cierta información de estado para cada canal. La combinación de este estado, incluyendo zócalos, números de secuencia y tamaños de ventanas, se denomina conexión lógica. Cada conexión se identifica unívocamente por el par de zócalos del emisor y el receptor.

**Servicios de direccionamiento.**

El servicio de direccionamiento de IP determina rápidamente si una dirección IP dada por la capa de transporte pertenece a la red local o a otra red.

Las direcciones IP son números de 32 bits divididos en 4 octetos. Cada dirección es la combinación del identificador único de la red y el identificador único de la máquina.

El problema inmediato con las direcciones IP es que son difíciles de memorizar. Por esta razón, las computadoras son identificadas con nombres particulares. El DNS fue implementado para facilitar el uso de las direcciones IP a las personas.

**Servicio DNS**

Servicio de Internet que traduce los nombres de los dominios (direcciones por nombre, p. ej. www.proyecto.es) en direcciones IP (direcciones numéricas, p. Ej. 155.210.3.32) y viceversa. Este servicio es imprescindible para poder iniciar cualquier comunicación con otro computador accediendo al mismo por su nombre.

**Servicio de Active Directory**

Es un servicio de directorios de red que identifica todos los recursos en ella y los vuelve accesibles a los usuarios y a las aplicaciones. Active Directory (AD) es el servicio de directorio incluido en todos los W2000, incluido Windows 2003 Server. El elemento principal de AD es el directorio, que almacena información sobre los recursos de la red y los servicios que hacen disponible la información. Los recursos almacenados en el directorio, como los datos del usuario, impresoras, servidores, bases de datos, grupos, computadoras y políticas de sistema, se denominan objetos.

AD los organiza jerárquicamente en dominios. Un dominio (domain) es una agrupación lógica de servidores y otros recursos de red bajo un mismo nombre de dominio.

Cada dominio incluye uno o mas controladores de dominio (domain controllers), que son maquinas que almacenan una replica de un directorio de dominio. Cada vez que se hace algún cambio en alguno de los controladores, el resto se actualiza automáticamente.

**Servicio DHCP**

El servicio DHCP permite acelerar y facilitar la configuración de muchos Hosts en una red evitando en gran medida los posibles errores humanos.

DHCP (Dynamic Host Configuration Protocol) son las siglas que identifican a un protocolo empleado para que los Hosts (clientes) en una red puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS, entre otros.

**Servicio de Archivos**

Proporciona una adecuada administración a los atributo de los archivos definidos por el usuario. Lo más común es encontrar algunos sistemas avanzados que permitan modificarlos después de su creación, pero en algunos sistemas distribuidos las únicas operaciones que pueden realizarse sobre un archivo es CREATE y READ (Crear y Leer). Es decir, una vez creado el archivo no puede modificarse. A este tipo de archivos se les denomina archivos inmutables. Existen dos tipos de servicios de archivos distribuidos: modelo carga/descarga y modelo de acceso remoto.

i. **Modelo Carga/Descarga**

Consiste básicamente en dos operaciones: lectura y escritura., la primera operación consiste en la transferencia de un archivo completo desde el servidor hacia el cliente solicitante; la segunda operación consiste en el envío de un archivo del cliente al servidor, es decir, en sentido contrario. Mientras tanto los archivos pueden ser almacenados en memoria o en un disco local, según sea el caso.

ii. **Modelo de Acceso Remoto**

Este tipo de modelo consiste en que todas las operaciones (abrir y cerrar, leer y escribir, etc.) se realizan en el servidor mas no en los clientes.

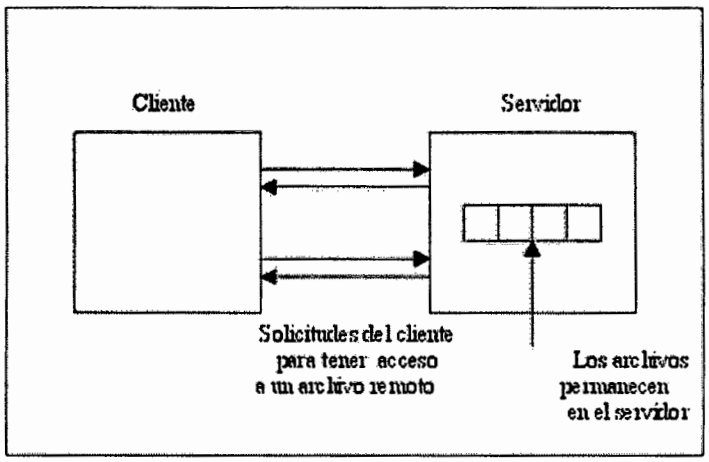



**Figura Nº 4.4.2.1** : El modelo de acceso remoto
**Fuente** : [URL 13]

Estos dos modelos se diferencian en que en el primero se debe transferir el archivo completo del servidor al cliente y viceversa, lo que no es necesario en el modelo de acceso remoto.

**Servicio de Impresión**

Servicio que permite enviar trabajos de impresión a impresoras conectadas localmente a un servidor de impresión que ejecute algún sistema operativo, por Internet o a impresoras conectadas a la red mediante adaptadores de red internos o externos, u otro servidor.

**Servicio de Aplicaciones**

El servidor de aplicaciones ejecuta los programas de negocio en lugar del cliente (navegador, cliente rico), del servidor web o sistemas finales. Se sitúa en el medio entre un cliente y los datos empresariales y otras aplicaciones. Físicamente separa la lógica del negocio del cliente y los datos dentro de una arquitectura conocida como multi-capa. Los servidores de aplicaciones permiten a las empresas desarrollar y desplegar aplicaciones rápida y fácilmente e incrementan la cantidad de sus usuarios sin reprogramación. Pueden hacer esto debido a una capa separada.

**Servicio de Correos**

Nos permite enviar mensajes (correos) de unos usuarios a otros con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

- **SMTP, Simple Mail Transfer Protocol:** Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

- **POP, Post Office Protocol:** Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

- **IMAP, Internet Message Access Protocol:** Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

**Servicio de Mensajería Instantánea**

Permite intercambiar mensajes de texto entre usuarios que previamente han aceptado comunicarse entre sí de esta manera. El procedimiento varía de un sistema a otro pero, en general, funciona así:

1. Un usuario se conecta a un servidor, en el cual está almacenada su lista de contactos, y se establece su estado: disponible, ocupado, ausente, etc.
2. El servidor le envía su lista de contactos y el estado de cada uno de ellos.
3. El servidor, automáticamente, informa de la presencia de este usuario a todos los usuarios de su lista de contactos que estén conectados en ese momento.
4. A partir de este momento, si un usuario quiere comunicarse con alguno de sus contactos, no tiene más que seleccionar el usuario deseado.
5. Para dar de alta un contacto en la lista de contactos, hace falta saber su dirección o álias y que el contacto autorice la inclusión.

6. Cuando el usuario cierra su programa de MI, el programa informa al servidor de la desconexión y éste, a su turno, notifica a todos los contactos.

**Servicio de Terminal Server**

Proporciona acceso remoto a un escritorio de Microsoft Windows a través de software de cliente ligero, con lo que se permite al equipo cliente actuar como emulador de terminal. Servicios de Terminal Server sólo transmite al cliente la interfaz de usuario del programa. El cliente devuelve las pulsaciones de teclado y los clicks del mouse para ser procesados en el servidor. Los usuarios que inician una sesión sólo ven su sesión, administrada de manera transparente por el sistema operativo del servidor e independiente de cualquier otra sesión de cliente.

**Servicio de Seguridad**

Ayuda a impedir el paso a los hackers, virus y gusanos que intenten entrar en su equipo a través de Internet. Si es un usuario doméstico o tiene una pequeña empresa, instalar un servidor de seguridad es el primer paso y el más efectivo para mejorar la protección de su equipo. Es importante tener un servidor de seguridad y un software antivirus activados antes de conectarse a Internet.

# CONCLUSIONES

## Conclusiones generales

El Diseño de la Infraestructura de Servicios de Red Basado en Windows 2003 Server, Integrados mejorara la Gestión Administrativa de la institución pues:

- Con la ejecución del proyecto se logrará el diseño físico de servicios y de la arquitectura de red, para así brindar seguridad tanto en nuestra red local, además seguridad al poner información al exterior (Internet).

- Las características mejoradas del Active Directory permiten realizar tareas fácilmente,entre las que destacan: la habilidad de renombrar dominios, la posibilidad de redefinir el esquema, una replicación más eficiente, la selección de múltiples objetos, arrastrar y soltar para mover objetos, almacenar consultas de usuario y permitir búsquedas basadas en criterios específicos.

- La topología básica en cuanto a la seguridad más fiable es la de crear tres zonas:
  - ✓ Zona Internet
  - ✓ Zona DMZ (Desmilitarized Zone)
  - ✓ Zona de Red Privada
  - ✓ Estas tres Zonas son creadas por el firewall

- El firewall nos permite poner seguridad para nuestro acceso a Internet, y para la publicación de información de ciertos servicios hacia el exterior; como servidor Web, servidor ftp, servidor de correo, etc. Brindando así una seguridad a nuestra red ante cualquier ataque del exterior; gracias a esta implementación de nuestro firewall y de las zonas de seguridad planteadas.

**Conclusiones específicas**

- La infraestructura de Servicios de Red, Basado en Windows 2003 server, quedará apta para el levantamiento de sistemas informáticos, sistemas web y acceso a Internet.

- En el diseño de la red se contempla el posible crecimiento de la red, en una planificación a mediano y largo plazo, además de implementar los servicios de seguridad para el Internet.

## RECOMENDACIONES

Se recomienda a la Comision Portal Web - UNAP lo siguiente:

- El presente trabajo debe constituir la base del desarrollo de los sistemas transaccionales y web que se desarrollen mas adelante para la institución, pues quedara el diseño de la infraestructura de Servicios de Red integrados la cual servirá para mejorar la comunicación entre las distintas áreas de la institución.

- Integrar en el más breve plazo las aplicaciones existentes en la institución para un mejor funcionamiento de los procesos que se llevan a cabo en el mismo.

- Contando con este diseño de infraestructura de Servicios de Red integrados, sirve como base para la posterior implementación de otros servicios de red que por el momento no están configurados ya que no es necesario hacer uso de ellos.

- Capacitar al personal para obtener un mayor aprovechamiento de las ventajas que tiene una Infraestructura de Servicios de Red Integrados.

# BIBLIOGRAFÍA

## Libros

[01] EVANS, Tim. "Construya su propia Intranet", Editorial Pegasus. Mexico D.F. Mexico. 1997.

[02] Lefebvre, A., Intranet: client-serveur universel. Editions Eyrolles, París, 1997.

[03] MICROSOFT, *"Analyzing Requirements and Defining Microsoft .NET Solution Architectures"*. Workbook Course Number 2710B

[04] Tittel, E., Stewart, J.M., La biblia de Intranet. Anaya Multimedia, 1997.

[05] Tittel, E., Megabyte, Windows Server 2003. Maribel Sabana Mendoza, 2005.

## Web Sites

[URL 01] Autor: Rodrigo Fuentes
http://www.monografias.com/trabajos12/intrants/intrants.shtml

[URL 02] Autor: Softdownload.com.ar
http://www.wikilearning.com/intranet-wkccp-8418-22.htm

[URL 03] Autor: Miguel Alejandro Soto
http://usuarios.lycos.es/janjo/janjo1.html

[URL 04] Autor: M. A. Redondo, C. Bravo, J. Bravo, M. Ortega
http://chico.inf-cr.uclm.es:8080/adie/revista/r11/11art6.pdf

[URL 05] Autor: Matías Palomec
http://www.nnss.d7.be/zope/pub/servicios/varios/HomeMadeWebServer/index_html/c211.html

[URL 06] Autor: Softdownload.com.ar
http://www.wikilearning.com/servicios_de_acceso_remoto_ras-wkccp-8418-21.htm

[URL 07] Autor: Microsoft Corp
http://www.microsoft.com/latam/windows.netserver/evaluacion/resumen/default.asp

[URL 08] Autor: Alex Torres
http://orbita.starmedia.com/~alex-torres/glossary.htm

[URL 09] Autor: Microsoft Corp
http://www.microsoft.com/latam/msdn

[URL 10] Autor: Microsoft Corp
http://www.microsoft.com/latam/technet/fases/default.mspx

[URL 11] Autor: Learn the Net
http://www.learnthenet.com/english/html/41intra.htm

[URL 12] Autor: Willy Marroquin
http://www.willydev.net/

[URL 13] Autor: José Walter Fernández Sánchez

http://www.elrinconcito.com/articulos/ArchivosDist/ArchDist.htm

## Glosario de Términos

*A*

**Accesibilidad**
Cualidad de un sistema que incorpora hardware o software para ofrecer una interfaz de usuario personalizable, métodos de entrada y salida alternativos, así como mayor exposición de los elementos de pantalla con el fin de lograr que el equipo pueda ser utilizado por personas con discapacidades cognitivas, auditivas, físicas o visuales.

**Activa/activa**
Configuración de clúster de una aplicación, en la que la aplicación se ejecuta en todos los nodos al mismo tiempo.

**Activa/pasiva**
Configuración de clúster de una aplicación, en la que la aplicación se ejecuta sólo en un nodo cada vez.

**Active Directory**
Servicio de directorio incluido en Windows Server 2003. Almacena información acerca de objetos de una red y la pone a disposición de los usuarios y administradores de la red.

**Actualización de dominios**
Proceso que consiste en sustituir una versión anterior de un sistema operativo en los equipos de un dominio con una versión posterior.

**Actualización dinámica**
Especificación actualizada del estándar Sistema de nombres de dominio (DNS) que permite que los hosts que almacenan información de nombres en DNS registren y actualicen sus registros dinámicamente en zonas mantenidas por servidores DNS que puedan aceptar y procesar mensajes de actualización dinámica.

**Actualización dinámica segura**
Proceso mediante el que un cliente de actualización dinámica segura envía una solicitud de actualización dinámica a un servidor DNS y el servidor intenta la actualización sólo si el cliente puede demostrar su identidad y tiene las credenciales apropiadas para realizarla.

**Adaptador de red**
Tarjeta complementaria de software o hardware que conecta un nodo o host a una red de área local. Si el nodo es miembro de un clúster de servidores, el adaptador de red es un objeto de clúster de servidores (el objeto de interfaz de red).

**Administrador de DHCP**
Principal herramienta utilizada para administrar servidores DHCP. El Administrador de DHCP es una herramienta de Microsoft Management Console (MMC) que se agrega al menú Herramientas administrativas cuando se instala el servicio DHCP.

**Administrador de red**
Persona responsable de instalar y administrar controladores de dominio o equipos locales, y sus cuentas de usuario y grupo, asignar contraseñas y permisos, así como ayudar a los usuarios con los problemas de red. Los administradores son miembros del grupo Administradores y tienen control total del dominio o el equipo.

**Administrador de seguridad**
Usuario al que se ha asignado el derecho de administrar la auditoria y el registro de seguridad. De forma predeterminada, este derecho de usuario se concede al grupo Administradores.

**Algoritmo**
Regla o procedimiento para solucionar un problema. La seguridad de Protocolo Internet utiliza algoritmos basados en cifrado para cifrar los datos.

**Almacén de información**
Almacenamiento físico de las réplicas de particiones de directorio de Active Directory en un controlador de dominio determinado. El almacén se implementa mediante el Motor de almacenamiento extensible.

**Almacenamiento remoto**
En Windows Server 2003, cintas extraíbles de una biblioteca utilizadas para el almacenamiento secundario de los datos. Las cintas especificadas que se utilizan para el almacenamiento secundario de los datos las administra Almacenamiento remoto y contienen datos que están almacenados localmente o se han quitado del almacenamiento local para liberar espacio de disco.

**Alta disponibilidad**
Capacidad de mantener una aplicación o un servicio en funcionamiento y en uso para los clientes la mayor parte del tiempo.

**Ámbito (scope)** es el rango de direcciones IP.

**Ancho de banda**
En comunicaciones, diferencia entre las frecuencias más alta y más baja en un intervalo determinado. Por ejemplo, una línea de teléfono permite un ancho de banda de 3000 Hz, la diferencia entre la frecuencia más baja (300 Hz) y la más alta (3300 Hz) que puede transportar. En redes informáticas, un ancho de banda mayor indica una capacidad de transferencia de datos más rápida y se expresa en bits por segundo (bps).

**Árbol de dependencias**
Un conjunto de diferentes recursos que están conectados entre sí mediante relaciones de dependencia. Todos los recursos de un árbol de dependencias determinado deben ser miembros de un sólo grupo.

**Árbol de directorio**
Jerarquía de objetos y contenedores de un directorio que se puede ver gráficamente como un árbol al revés, con la raíz en la parte superior. Los extremos del árbol son normalmente objetos únicos (hojas) y los nodos del árbol, o ramas, son objetos contenedores. Un árbol muestra cómo están conectados los objetos en cuanto a la ruta de acceso entre un objeto y otro. Un árbol sencillo es un sólo contenedor y sus objetos. Un subárbol contiguo es cualquier ruta ininterrumpida del árbol, lo cual incluye a todos los miembros de todos los contenedores de esa ruta.

**Árbol de dominio**
En DNS, estructura jerárquica en forma de árbol invertido que se utiliza para indizar nombres de dominio. El propósito y el concepto de los árboles de dominio son similares a los de los árboles de directorios utilizados por los sistemas de organización de archivos de los equipos para el almacenamiento en disco.

**Archivo hosts**
Este archivo asigna nombres de host a direcciones IP. En Windows Server 2003, este archivo se encuentra en la carpeta C:\WINDOWS\system32\drivers\etc.

**Archivos de sistema**
Archivos utilizados por Windows para cargar, configurar y ejecutar el sistema operativo. En general, nunca se debe eliminar ni mover archivos del sistema.

**Atributo (objeto)**
En Active Directory, una propiedad única de un objeto. Un objeto se describe mediante los valores de sus atributos. Para cada clase de objeto, el esquema define qué atributos debe poseer una instancia de la clase y los atributos adicionales que puede tener.

**Autenticación**
En el acceso de red, proceso mediante el que el sistema valida la información de inicio de sesión del usuario. El nombre de usuario y la contraseña se comparan con una lista autorizada. Si el sistema detecta una coincidencia, concede acceso hasta el grado especificado en la lista de permisos del usuario. Cuando un usuario inicia una sesión en una cuenta de un equipo que ejecuta Windows 2000 Professional, la autenticación la realiza el cliente. Cuando lo hace en una cuenta de un dominio de Windows Server 2003, la autenticación la puede realizar cualquier servidor de ese dominio.

## *B*

**Base de datos WINS**
Base de datos utilizada para registrar y convertir nombres de equipos a direcciones IP en redes basadas en Windows. El contenido de esta base de datos se replica a intervalos regulares en toda la red.

**Binario**
Sistema de numeración en base 2 en el que los valores se expresan como combinaciones de dos dígitos, 0 y 1.

**Bit**
Unidad mínima de información utilizada por un equipo. Un bit expresa un 1 o un 0 en un numeral binario, o una condición lógica verdadera o falsa. Un grupo de 8 bits forma un byte, que puede representar muchos tipos de información, como una letra del alfabeto, un dígito decimal o un carácter. El bit se llama también dígito binario.

**Bloquear**
Hacer que un archivo sea inaccesible. Si varios usuarios pueden tratar un archivo, ese archivo se bloquea cuando un usuario tiene acceso al mismo con el fin de evitar que otro usuario pueda modificar el archivo simultáneamente.

**Bosque**

Colección de uno o varios árboles de Active Directory de Windows Server 2003, organizados como iguales y conectados mediante relaciones de confianza transitiva bidireccionales entre los dominios raíz de cada árbol. Todos los árboles de un bosque comparten un esquema, una configuración y un catálogo global comunes. Cuando un bosque contiene múltiples árboles, éstos no forman un espacio de nombres contiguo.

**Búfer**

Área de la memoria que se utiliza para el almacenamiento intermedio de datos hasta que se puedan utilizar.

**Bus**

Línea de comunicación utilizada para la transferencia de datos entre los componentes de un sistema informático. Un bus es básicamente una vía de comunicación que permite que distintas partes del sistema compartan datos.

**Búsqueda inversa**

Consulta en la que la dirección IP se utiliza para determinar el nombre DNS del equipo.

## *C*

**Caché**

En DNS y WINS, almacén de información local de registros de recursos para los nombres de host remotos resueltos recientemente. Por lo general, la caché se crea dinámicamente cuando el equipo consulta y resuelve nombres. Ayuda a mejorar el tiempo necesario para resolver los nombres consultados.

**Centro de distribución de claves (KDC, Key Distribution Center)**

Servicio de red que proporciona vales de sesión y claves de sesión temporales, utilizado en el protocolo de autenticación Kerberos. En Windows Server 2003, KDC funciona como un proceso privilegiado en todos los controladores de dominio. KDC utiliza Active Directory para administrar información confidencial de cuentas, como las contraseñas de las cuentas de usuario.

**Certificado**

Archivo utilizado para la autenticación y el intercambio seguro de datos en redes no protegidas, como Internet. Un certificado enlaza de forma segura una clave de cifrado pública con la entidad que guarda la clave de cifrado privada correspondiente. Los

certificados están firmados digitalmente por la entidad emisora de certificados y se pueden administrar para un usuario, un equipo o un servicio.

**Cifrado**

Método de creación de un mensaje oculto. El cifrado se utiliza para transformar un mensaje legible llamado texto sin formato en un mensaje ilegible, codificado u oculto, llamado texto cifrado. Sólo alguien con una clave secreta decodificadora puede convertir el texto cifrado de nuevo al texto sin formato original.

**Cifrado**

El proceso de camuflar un mensaje o datos de forma que se oculte su contenido.

**Clave**

Código o número secreto requerido para leer, modificar o comprobar datos protegidos. Las cla ves se utilizan en combinación con los algoritmos para proteger los datos. Windows Server 2003 controla automáticamente la generación de claves. En el Registro, una clave es una entrada que puede contener tanto subclaves como entradas. En la estructura del Registro, las claves son similares a las carpetas y las entradas son similares a los archivos. En la ventana del Editor del Registro, una clave aparece como una carpeta de archivos en el panel de la izquierda. En un archivo de respuesta, las claves son cadenas de caracteres que especifican los parámetros de los que el programa de instalación obtiene los datos necesarios para la instalación desatendida del sistema operativo.

**Clave de cifrado**

Valor utilizado por un algoritmo para cifrar y descifrar un mensaje.

**Clave de sesión**

Clave utilizada principalmente para cifrado y descifrado. Por lo general, las claves de sesión se utilizan con algoritmos de cifrado simétrico donde se utiliza la misma clave para el cifrado que para el descifrado. Por este motivo, las claves de sesión y simétricas normalmente se refieren al mismo tipo de clave.

**Cliente**

Cualquier equipo o programa que se conecte con otro equipo o programa, o solicite sus servicios.

**Clúster**

Conjunto de equipos que trabajan juntos para proporcionar un servicio. El uso de un clúster mejora la disponibilidad del servicio y la escalabilidad del sistema operativo que suministra el servicio.

**Cola**

Lista de programas o tareas pendientes de ejecución. En la terminología de impresión de Windows Server 2003, una cola hace referencia a un grupo de documentos que esperan para imprimirse.

**Compartir impresoras**

Capacidad de un equipo para compartir una impresora en la red. Esto se consigue al hacer doble clic en Impresoras en el Panel de control o introducir el comando net share en el símbolo del sistema.

**Conectividad abierta de bases de datos (ODBC, Open Database Connectivity)**

Interfaz de programación de aplicaciones (API) que permite a las aplicaciones de base de datos tener acceso a los datos de una serie de orígenes de datos existentes.

**Conexión de red privada virtual**

Vínculo en el que los datos privados se encapsulan y se cifran.

**Confidencialidad**

Servicio de seguridad de Protocolo de Internet que garantiza que un mensaje se revela sólo a los destinatarios a los que va dirigido mediante el cifrado de los datos.
Configuración avanzada e interfaz de energía (ACPI, Advanced Configuration and Power Interface).

**Conjunto de direcciones**

Grupo de direcciones IP en un ámbito. El conjunto de direcciones está disponible para asignación dinámica mediante un servidor DHCP a los clientes DHCP.

**Consolidación de dominios**

Proceso que consiste en combinar varios dominios en un dominio mayor.

**Contexto de seguridad**

Atributos o reglas de seguridad que están en vigor actualmente. Por ejemplo, las reglas que regulan lo que un usuario puede hacer con un objeto protegido se determinan mediante información de seguridad en el testigo de acceso del usuario y en el descriptor

de seguridad del objeto. Conjuntamente, el testigo de acceso y el descriptor de seguridad forman un contexto de seguridad para las acciones del usuario sobre el objeto.

**Control de acceso**
Mecanismo de seguridad que determina qué objetos puede utilizar un principal de seguridad y cómo puede usarlos.

**Controlador de dominio**
Servidor que autentica los inicios de sesión en el dominio y mantiene la política de seguridad y la base de datos principal de un dominio. Tanto los servidores como los controladores de dominio son capaces de validar el inicio de sesión de un usuario, pero para cambiar las contraseñas se debe entrar en contacto con el controlador de dominio.

**Controlador IPSec**
Mecanismo de seguridad de Protocolo Internet que se activa cuando se configura la seguridad de Protocolo Internet para un equipo y que controla si los paquetes coinciden con algún filtro IP de la política de seguridad de Protocolo Internet activa en el equipo. El controlador IPSec también realiza el cifrado y descifrado reales de los datos.

**Criptografía**
Ciencia que estudia la seguridad de la información. Proporciona cuatro funciones básicas de seguridad de la información: confidencialidad, integridad, autenticación y sin repudio

## *D*

**Datagrama**
Paquete de datos no reconocido enviado a otro destino de red. El destino puede ser otro dispositivo al que se puede llegar directamente en la red de área local (LAN) o un destino remoto al que se llega mediante entrega enrutada a través de una red de conmutación de paquetes.

**Derechos de usuario**
Credencial expedida a un usuario por el Centro de distribución de claves (KDC) cuando el usuario inicia una sesión. El usuario debe presentar el TGT al KDC cuando solicita

vales de sesión para los servicios. Como un TGT normalmente es válido durante todo el tiempo que dure la sesión de inicio del usuario, a veces se denomina vale de usuario.

**Descifrado**

Proceso que consiste en hacer que los datos cifrados sean legibles de nuevo mediante la conversión de texto cifrado en texto sin formato.

**Desfragmentación**

Proceso de reescritura de componentes de un archivo en sectores contiguos de un disco duro para aumentar la velocidad de acceso y de obtención de datos. Al actualizar los archivos, el equipo suele guardar estas actualizaciones en el espacio contiguo más grande del disco duro, que suele estar en un sector distinto al de las otras partes del archivo. Cuando los archivos se fragmentan de esta manera, el equipo debe buscar en todo el disco duro cada vez que se abre el archivo para encontrar todas las partes del archivo, lo que reduce el tiempo de respuesta. En Active Directory, la desfragmentación reorganiza el modo en que están escritos los datos en el archivo de la base de datos del directorio para compactarlos.

**Deshabilitar**

Hacer que un dispositivo deje de estar operativo. Por ejemplo, si se deshabilita un dispositivo de un perfil de hardware, ese dispositivo no se podrá utilizar cuando se utilice ese perfil de hardware. Al deshabilitar un dispositivo se liberará los recursos asignados al mismo.

**Detección de errores**

Técnica para detectar la pérdida de datos durante la transmisión. Esto permite que el software solicite que el equipo transmisor vuelva a transmitir los datos para recuperar los que se hayan perdido.

**DHCP de multidifusión (MDHCP, Multicast DHCP)**

Extensión del estándar del protocolo DHCP que permite la asignación y configuración dinámica de direcciones de multidifusión IP en redes basadas en TCP/IP.

**DHCP distribuido**

Caso de DHCP en que las direcciones IP se distribuyen en un límite de sitios.

**Difusión**

Dirección destinada a todos los hosts de una red determinada.

**Dirección**

En Systems Management Server, las direcciones se utilizan para conectar sitios y sistemas de sitios. Los remitentes utilizan las direcciones para enviar instrucciones y datos a otros sitios.

.

**Dirección IP**

Dirección de 32 bits que se utiliza para identificar un nodo en un conjunto de redes IP Interconectadas. A cada nodo de las redes IP interconectadas se le debe asignar una dirección IP única, que se compone del identificador de la red más un identificador de host único.

**Direcciones privadas**

Direcciones IP dentro del espacio de direcciones privadas que están designadas para ser usadas por las organizaciones para el direccionamiento de intranets privadas. Una dirección IP privada pertenece a uno de los siguientes bloques de direcciones: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

**Direcciones públicas**

Direcciones IP asignadas por el Centro de información de red de Internet (InterNIC, Internet Network Information Center) con la garantía de que son únicas globalmente y de que se pueden encontrar en Internet.

**Directorio**

En un sistema de archivos, un directorio almacena información acerca de archivos. En un entorno informático distribuido, el directorio almacena información acerca de objetos como las impresoras, las aplicaciones, las bases de datos y otros usuarios.

**Disponibilidad**

Medida de la tolerancia a errores de un equipo y sus programas. Un equipo altamente disponible se ejecuta las 24 horas del día, los 7 días de la semana.

**Dispositivo**

Cualquier equipo que se pueda conectar a una red o a un equipo; por ejemplo, un equipo, impresora, joystick, adaptador o tarjeta de módem, o cualquier otro periférico.

**Distribución de paquetes**

En Systems Management Server, proceso que consiste en colocar una imagen de paquete descomprimida en puntos de distribución, compartirla y hacerla accesible para

los clientes. Este proceso ocurre cuando se especifican puntos de distribución para un paquete.

**División en subredes**
Acción que consiste en subdividir el espacio de direcciones de un identificador de red TCP/IP en segmentos de red más pequeños, cada uno con su propio identificador de red de la subred.

**Dominio**
Conjunto de equipos interconectados que comparten una base de datos de Administrador de cuentas de seguridad (SAM) y que se pueden administrar como un grupo. Un usuario con una cuenta en un dominio en particular puede iniciar una sesión y tener acceso a su cuenta desde cualquier equipo del dominio.

**Drainstop**
En Equilibrio de la carga en la red, herramienta que deshabilita el control de todo el tráfico nuevo en los hosts especificados. Luego, los hosts entran en el modo de agotamiento para finalizar las conexiones existentes. Durante el agotamiento, los hosts permanecen en el clúster y detienen sus operaciones de clúster cuando ya no hay más conexiones activas. Se puede terminar el modo de agotamiento si se detiene explícitamente el modo de clúster con el comando stop o se reinicia el control de nuevo tráfico con el comando start. Para agotar las conexiones de un puerto específico, utilice el comando drain.

**DMZ** (Demilitarized Zone):
Término utilizado comúnmente para designar una zona de la red donde las medidas de seguridad perimetral son menos estrictas. En el caso de la red de la UCLM coincide con la zona de servidores públicos.

## *E*

**Equilibrio de la carga**
Ajustar el rendimiento de un programa basado en servidor (como un servidor Web) al distribuir las solicitudes de los clientes entre múltiples servidores dentro del clúster mediante Organización por clústeres de Windows. Cada host puede especificar el porcentaje de carga que controlará o la carga puede distribuirse uniformemente entre todos los hosts. Si se produce un error en un host, Organización por clústeres de Windows redistribuye dinámicamente la carga entre el resto de los hosts.

**Equilibrio de la carga en la red**
Componente de Organización por clústeres de Windows que distribuye las solicitudes Web entrantes entre su clúster de servidores IIS.

**Equipo local**
Equipo en el que un usuario ha iniciado una sesión. Más concretamente, un equipo local es aquel al que se puede tener acceso directamente sin utilizar una línea de comunicación ni un dispositivo de comunicaciones, como un adaptador de red o un módem. Igualmente, ejecutar un programa local significa ejecutar el programa en el equipo, en contraposición a ejecutarlo desde un servidor.

**Equipo remoto**
Equipo al que sólo se puede tener acceso mediante una línea de comunicación o un dispositivo de comunicaciones, como un adaptador de red o un módem.

**Emisor**
Componente de subproceso de Systems Management Server que utiliza un sistema de conectividad existente para comunicarse entre sitios. Un emisor administra la conexión, garantiza la integridad de los datos transferidos, se recupera de los errores y cierra las conexiones cuando ya no se necesitan.

**Enrutador**
Servidor de red que contribuye a conseguir interoperabilidad y conectividad de redes LAN y WAN, y que puede vincular redes LAN que tienen topologías de red diferentes, como Ethernet y Token Ring.

**Enrutamiento**
Proceso que consiste en reenviar un paquete en función de la dirección IP de destino.

**Escalabilidad**
Medida de la capacidad de un equipo, un servicio o una aplicación para poder expandirse con el fin de satisfacer el aumento de las demandas de rendimiento. En los clústeres de servidores, capacidad de agregar gradualmente uno o varios sistemas a un clúster existente cuando la carga global del clúster supera su capacidad.

**Escalar**
Proceso que consiste en agregar procesadores a un sistema para lograr mayor rendimiento.

**Escritorio**
Área de trabajo en pantalla en la que aparecen ventanas, iconos, menús y cuadros de diálogo.

**Explorador**
Herramienta cliente para explorar y tener acceso a la información en Internet o en una intranet. En el contexto de las redes de Windows, "explorador" también puede significar el servicio

**Extranet**
Subconjunto limitado de equipos o usuarios en una red pública, por lo general Internet, que pueden tener acceso a una red interna de una organización. Normalmente, los equipos o usuarios pertenecen a organizaciones asociadas.

***F***

**FAT32**
Derivado del sistema de archivos tabla de asignación de archivos. FAT32 admite tamaños de clúster más pequeños que FAT, lo que permite una asignación más eficaz del espacio en las unidades FAT32.

**Filtro**
En IPSec, regla que proporciona la capacidad de desencadenar negociaciones de seguridad para una comunicación en función del origen, el destino y el tipo de tráfico IP.

**Finalizar una sesión**
Dejar de utilizar una red, lo que quita el nombre de usuario del uso activo hasta que el usuario inicia una sesión de nuevo.

**Firma de código**
Firma digital de código de software para asegurar su integridad y ofrecer garantía de su origen.

**Fragmentación**
Dispersión de las partes de un mismo archivo por distintas áreas de un disco. La fragmentación se produce a medida que se eliminan los archivos de un disco y se

agregan otros nuevos. Ralentiza el acceso al disco y degrada el rendimiento general de las operaciones de disco, aunque no de forma grave.

## *G*

**Gigabit Ethernet**
Estándar de Ethernet que transmite datos a mil millones de bits por segundo o más.

**Grupo**
Colección de usuarios, equipos, contactos y otros grupos. Los grupos se pueden utilizar como conjuntos de distribución de correo electrónico o de seguridad. Los grupos de distribución sólo se utilizan para correo electrónico. Los grupos de seguridad se utilizan como listas de distribución de correo electrónico y para permitir el acceso a los recursos.

## *H*

**Herencia**
Capacidad de crear nuevas clases de objetos a partir de clases de objetos existentes. El objeto nuevo se define como una subclase del objeto original. El objeto original se convierte en una superclase del objeto nuevo. Una subclase hereda los atributos de la superclase, incluidas las reglas de estructura y de contenido.

**Hexadecimal**
Sistema numérico de base 16 cuyos números se representan por los dígitos 0 a 9 y las letras A (equivalente a 10 en decimal) a F (equivalente a 15 en decimal).

**Host**
Equipo que ejecuta un programa de servidor o servicio que utilizan redes o clientes remotos. En Equilibrio de la carga en la red, un clúster se compone de múltiples host conectados mediante una red de área local.

## *I*

**Identificador**
En la interfaz de usuario, una interfaz agregada a un objeto que facilita el movimiento, el cambio de tamaño, el cambio de forma u otras funciones propias de un objeto. En

programación, un puntero a otro puntero, es decir, un identificador que permite que un programa tenga acceso a un recurso identificado.

**Identificador de host**
Número utilizado para identificar una interfaz en una red física limitada por enrutadores. El identificador de host debe ser único en la red.

**Identificador de red**
Número utilizado para identificar los sistemas que se encuentran en la misma red física limitada por enrutadores. El identificador de red debe ser único en el conjunto de redes interconectadas.

**Identificador de seguridad (SID, Security Identifier)**
Nombre único que identifica a un usuario que ha iniciado una sesión en un sistema de seguridad de Windows 2000 o Windows Server 2003. Un identificador de seguridad puede representar un usuario individual, un grupo de usuarios o un equipo.

**Infraestructura de enrutamiento**
Estructura y topología de las redes interconectadas.

**Interconexión de red**
Dos o más segmentos de red conectados mediante enrutadores.

**Interfaz**
En redes, dispositivo lógico sobre el que se pueden enviar y recibir paquetes. En la herramienta administrativa Acceso remoto y enrutamiento, representación visual del segmento de red al que se puede llegar a través de los adaptadores LAN o WAN. Cada interfaz tiene un nombre único.

**Internet**
Miles de redes públicas TCP/IP interconectadas en todo el mundo que vinculan servicios de investigación, universidades, bibliotecas y organizaciones privadas.

**Intranet**
Red interna de una organización que utiliza tecnologías y protocolos de Internet, pero que está disponible sólo para ciertos usuarios, como los empleados de una organización. Una intranet también se denomina red privada.

*J*

**Jerarquía de certificados**
Modelo de confianza para los certificados en que las rutas de acceso de certificación se crean mediante el establecimiento de relaciones principal-secundario entre las entidades emisoras de certificados.

*N*

**KDC. {Key Distribution Center}.** Servicio de red que proporciona credenciales de sesión usado por el protocolo de autenticación Kerberos.

**Kerberos V5.** Protocolo de autenticación usado para verificar la identidad de un usuario o host. Us ado como protocolo de autenticación predeterminado en Windows 2003 Server.

*L*

**Latencia de replicación**
En la replicación de Active Directory, el retardo entre el momento en que se aplica una actualización a una réplica dada de una partición de directorio y el momento en que se aplica a otra réplica de la misma partición de directorio. La latencia hace referencia algunas veces a un retardo en la propagación.

**Longitud mínima de contraseña**
El número mínimo de caracteres que puede contener una contraseña.

*M*

**Máscara de subred**
Valor de 32 bits expresado como cuatro números decimales entre 0 y 255 separados por puntos (por ejemplo, 255.255.0.0.). Este número permite que TCP/IP distinga la parte del identificador de red de la dirección IP de la parte del identificador de host.
El identificador de host identifica equipos individuales de la red. Los hosts TCP/IP utilizan la máscara de subred para determinar si un host de destino se encuentra en una red local o remota.

**Medios de red**

Tipo de cableado físico y protocolos de nivel inferior utilizados para transmitir y recibir tramas. Por ejemplo, Ethernet, FDDI y Token Ring.

**Memoria virtual**
Espacio del disco duro que Windows Server 2003 utiliza como memoria. Gracias a la memoria virtual, la cantidad de memoria ocupada desde el punto de vista de un proceso puede ser mucho mayor que la memoria física real del equipo. El sistema operativo lleva a cabo esto de forma transparente para la aplicación, mediante la paginación de los datos que no caben en la memoria física a y desde el disco en un momento dado.

**Método de seguridad**
Proceso que determina los servicios de seguridad de Protocolo Internet, la configuración de claves y los algoritmos que se utilizarán para proteger los datos durante la comunicación.

**Migración**
Proceso que consiste en copiar un objeto desde el almacenamiento local a un almacenamiento remoto.

**Migración de dominios**
Proceso que consiste en mover cuentas, recursos y los objetos de seguridad asociados de una estructura de dominios a otra.

**Migrar**
Proceso que consiste en pasar archivos o programas de un formato de archivo o protocolo antiguo a un formato o protocolo más reciente. Por ejemplo, las entradas de base de datos WINS se pueden migrar de entradas de base de datos WINS estáticas a entradas DHCP de registro dinámico.

**Multitarjeta**
Equipo que tiene instalados múltiples adaptadores de red.

## *N*

**NetBIOS sobre TCP/IP (NetBT)**
Característica que proporciona la interfaz de programación NetBIOS sobre el protocolo TCP/IP. Se utiliza para supervisar los servidores enrutados que utilizan la resolución de nombres

**Nivel de red**

Nivel que dirige los mensajes y traduce direcciones y nombres lógicos a direcciones físicas. También determina la ruta desde el origen al equipo de destino y administra problemas de tráfico, como la conmutación, el enrutamiento y el control de la congestión de los paquetes de datos.

**Nodo**

En estructuras de árboles, ubicación en el árbol que puede tener vínculos a uno o varios elementos por debajo. En redes de área local (LAN), dispositivo conectado a la red y que es capaz de comunicarse con otros dispositivos de red. En un clúster de servidores, servidor que tiene instalado software de Servicio de Cluster Server y es miembro de un clúster.

**Nombre de dominio**

El nombre que un administrador asigna a un grupo de equipos de red que comparten un directorio común. En DNS, los nombres de dominio son nombres de nodo específicos del árbol de espacio de nombres DNS. Los nombres de dominio DNS utilizan nombres de nodo singulares, conocidos como "etiquetas", unidos por puntos (.) que indican cada nivel de nodo en el espacio de nombres.

**Nombre de host**

Nombre de un equipo de una red. El nombre de host se utiliza para referirse a la primera etiqueta de un nombre de dominio completo.

**Nombre de red**

En clústeres de servidores, nombre mediante el que los clientes tienen acceso a los recursos de los clústeres de servidores. Un nombre de red es similar a un nombre de equipo y, cuando se combina en un grupo de recursos con una dirección IP y los clientes de aplicaciones tienen acceso, presenta un servidor virtual a los clientes.

**Nombre de usuario**

Nombre único que identifica una cuenta de usuario en Windows Server 2003. El nombre de usuario de una cuenta debe ser único entre los demás nombres de grupo y nombres de usuario pertenecientes a su propio dominio o grupo de trabajo.

**Nombre del equipo**

Nombre único de un máximo de 15 caracteres en mayúsculas que identifica un equipo en la red. Este nombre no puede coincidir con el de ningún otro equipo o dominio de la red.

## *O*

**Objeto**
Entidad, como un archivo, una carpeta, una carpeta compartida, una impresora o un objeto de Active Directory, descrito mediante un conjunto de atributos diferenciados con nombre.

## *P*

**Paquete**
Unidad de transmisión de tamaño máximo fijo que se compone de información binaria. Esta información representa tanto datos como un encabezado que contiene un número de identificación, las direcciones de origen y de destino, y datos para el control de errores.

**Partición**
División lógica de un disco duro. Las particiones facilitan la organización de la información. Cada partición se puede formatear para un sistema de archivos diferente. Una partición debe estar contenida completamente en un disco físico y la tabla de particiones del registro de inicio maestro de un disco físico puede contener hasta cuatro entradas de particiones.

**Perfil de usuario**
Archivo que contiene información de configuración para un usuario específico, como configuración de escritorio, conexiones de red persistentes y configuración de aplicaciones. Las preferencias de cada usuario se guardan en un perfil de usuario que Windows NT y Windows 2003 utilizan para configurar el escritorio cada vez que un usuario inicia una sesión.

**Permisos**
Regla asociada a un objeto para regular los usuarios que pueden tener acceso al mismo y de qué forma. En Windows Server 2003 los objetos incluyen archivos, carpetas, recursos compartidos, impresoras y objetos de Active Directory.

**Ping**

Herramienta que comprueba conexiones a uno o varios hosts remotos. El comando ping utiliza la solicitud de eco ICMP y los paquetes de respuesta de eco para determinar si un sistema IP determinado de una red está en funcionamiento. Ping es útil para diagnosticar errores de redes IP o enrutadores.

**Plug and Play**

Conjunto de especificaciones desarrolladas por Intel que permiten a un equipo detectar y configurar automáticamente un dispositivo, e instalar los controladores de dispositivo correspondientes.

**Política de acceso remoto**

Conjunto de condiciones y parámetros de conexión que definen las características de la conexión entrante y el conjunto de restricciones impuestas sobre ella. Las políticas de acceso remoto determinan si un intento de conexión específico tiene autorización para ser aceptado.

**Privilegio**

Derecho de un usuario a realizar una tarea específica, que normalmente afecta a un sistema informático completo y no a un objeto concreto. Los privilegios los asignan los administradores a usuarios individuales y grupos de usuarios como parte de la configuración de seguridad del equipo.

**Proceso**

Objeto del sistema operativo que consta de un programa ejecutable, un conjunto de direcciones de memoria virtual y uno o varios subprocesos.

**Protocolo**

Conjunto de reglas y convenciones mediante las que dos equipos se intercambian mensajes a través de una red. Normalmente, el software de red implementa múltiples niveles de protocolos distribuidos en capas superpuestas.

**Protocolo Internet (IP)**

Protocolo enrutable del conjunto de protocolos TCP/IP que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reorganización de los paquetes IP.

**Proveedor de servicios Internet (ISP, Internet Service Provider)**

Empresa que proporciona acceso a Internet y a World Wide Web. Un ISP proporciona un número de teléfono, un nombre de usuario, una contraseña y otro tipo de información de conexión para que los usuarios puedan conectar sus equipos a los equipos del ISP. Por lo general, un ISP cobra una tarifa de conexión mensual y por horas.

**Puerto**

Mecanismo que permite múltiples sesiones. Refinamiento de una dirección IP. En el Administrador de dispositivos, punto de conexión de un equipo donde se pueden conectar dispositivos por los que atraviesan datos. Por ejemplo, la impresora se conecta normalmente a un puerto paralelo (conocido también como puerto LPT) y un módem suele conectarse a un puerto serie (conocido también como puerto COM).

**Puerta de enlace (o gateway) de red**

Dispositivo que conecta redes con diferentes protocolos de comunicaciones de forma que la información pueda pasar de una red a la otra. Una puerta de enlace transfiere información y la convierte a un formato compatible con los protocolos que se estén utilizando en la red de destino.

**Puerta de enlace predeterminada (gateway)**

Elemento de configuración para el protocolo TCP/IP que es la dirección IP de un enrutador IP al que se puede llegar directamente. La configuración de una puerta de enlace predeterminada crea una ruta de acceso predeterminada en la tabla de enrutamiento IP.

***R***

**Raíz**

El nivel más alto o nivel superior en un conjunto de información organizado jerárquicamente. La raíz es el punto a partir del que se bifurcan subconjuntos adicionales en una secuencia lógica que se mueve desde enfoques amplios o generales a perspectivas más limitadas.

**Recuperación**

Proceso que consiste en utilizar un archivo de registro para restaurar una base de datos a un estado coherente después de un error de sistema y para restaurar una base de datos desde una copia de seguridad al estado más reciente registrado en el archivo de registro después de un error de los medios.

**Red de área extensa (WAN, Wide Area Network)**
Red de comunicaciones que conecta equipos, impresoras y demás dispositivos separados geográficamente. Una WAN permite que cualquier dispositivo conectado interactúe con cualquier otro de la red.

**Red de área local (LAN, Local Area Network)**
Red de comunicaciones que conecta un grupo de equipos, impresoras y otros dispositivos que se encuentran dentro de un área relativamente limitada (por ejemplo, un edificio).

**Red privada virtual (VPN, Virtual Private Network)**
Extensión de una red privada que abarca vínculos entre redes compartidas o públicas, como Internet.

**Red virtual**
Red lógica existente en servidores y enrutadores Novell NetWare o compatibles con NetWare que no está asociada a un adaptador físico. El usuario ve la red virtual como una red independiente. En un equipo que ejecuta Windows Server 2003, los programas anuncian su ubicación en una red virtual, no una red física. El número de red interna identifica una red virtual dentro de un equipo.

**Redes interconectadas**
Al menos dos segmentos de red conectados mediante enrutadores.

**Registro**
En Windows Server 2003, Windows 2000, Windows NT y Windows 98, base de datos de información de la configuración de un equipo. El Registro está organizado en una estructura jerárquica y consta de subárboles y sus claves, secciones y entradas.

**Rendimiento**
Referido a discos, la capacidad de transferencia del sistema de disco.

**Réplica**
En la replicación de Active Directory, copia de una partición lógica de Active Directory que se sincroniza mediante la replicación entre los controladores de dominio que contienen copias de la misma partición de directorio. Réplica también puede referirse al

conjunto compuesto de particiones de directorio contenido en cualquiera de los controladores de dominio.

**Replicación**

Proceso que consiste en copiar datos de un almacén de datos o sistema de archivos en múltiples equipos que almacenan los mismos datos con el fin de sincronizarlos. En Windows Server 2003, la replicación de Active Directory se produce mediante el servicio replicador de directorios y la replicación del sistema de archivos se produce mediante la replicación DFS.

**Ruta de acceso**

Secuencia de nombres de directorios (o carpetas) que especifica la ubicación de un directorio, un archivo o una carpeta dentro del árbol de directorios de Windows. Cada nombre de directorio y nombre de archivo dentro de la ruta de acceso debe ir precedido por una barra diagonal inversa (\).

## *S*

**Seguridad de Protocolo Internet (IPSec)**

Conjunto de servicios y protocolos estándar de protección basados en la criptografía. IPSec protege todos los protocolos del conjunto de protocolos TCP/IP y las comunicaciones a través de Internet mediante L2TP.

**Servicio de acceso remoto (RAS, Remote Access Service)**

Servicio que proporciona acceso a redes para los tele trabajadores, los trabajadores móviles y los administradores de sistemas que supervisan y administran servidores en múltiples oficinas.

**Servicio de nombres**

Servicio, como el proporcionado por WINS o DNS, que permite convertir nombres descriptivos en direcciones u otros datos de recursos especialmente definidos que se utilizan para encontrar recursos de red de diversos tipos y con varios fines.

**Servicio de Replicación de archivos**

Servicio utilizado por el Sistema de archivos distribuido (DFS) para sincronizar el contenido entre las réplicas asignadas y también utilizado por Sitios y servicios de Active Directory para replicar información de catálogo topológico y global entre los controladores de dominio.

**Servicio DHCP**

Servicio que permite que un equipo funcione como servidor DHCP y configure los equipos c liente habilitados para DHCP en una red. DHCP funciona en un equipo servidor, permitiendo la administración automática y centralizada de direcciones IP y otras opciones de configuración de TCP/IP para los equipos cliente de una red.

**Servicios de Internet Information Server (IIS)**

Servicios de software que admiten la creación, configuración y administración de sitios Web, además de otras funciones de Internet. Servicios de Internet Information Server incluye Protocolo de transferencia de noticias a través de la red (NNTP), Protocolo de transferencia de archivos (FTP) y Protocolo simple de transferencia de correo (SMTP).

**Servidor**

Equipo que proporciona recursos compartidos a usuarios de red.

**Servidor de acceso remoto**

Equipo basado en Windows Server 2003 que ejecuta el Servicio de Acceso remoto y enrutamiento y que está configurado para proporcionar acceso remoto.

**Servidor de archivos**

Servidor que proporciona acceso en toda la organización a archivos, programas y aplicaciones.

**Servidor de impresión**

Equipo dedicado a administrar las impresoras de una red. El servidor de impresión puede ser cualquier equipo de la red.

**Servidor de nombres**

En el modelo cliente-servidor de DNS, servidor con autoridad para una parte de la base de datos DNS. El servidor hace que los nombres de equipos y demás información estén disponibles para los clientes que consulten la resolución de nombres a través de Internet o de una intranet.

**Servidor de seguridad**

Combinación de hardware y software que proporciona un sistema de seguridad, generalmente para impedir el acceso no autorizado del exterior a una red interna o intranet. Un servidor de seguridad impide la comunicación directa entre equipos externos y de la red mediante el enrutamiento de la comunicación a través de un servidor Proxy que se encuentra fuera de la red.

**Servidor DNS**

Equipo que ejecuta programas de servidor DNS que contiene asignaciones de nombres a direcciones IP, asignaciones de direcciones IP a nombres, información acerca de la estructura del árbol de dominios y otra información. Los servidores DNS también intentan resolver las consultas de los clientes.

**Servidor principal**

Servidor DNS con autoridad para una zona que puede utilizarse como punto de actualización para esa zona. Sólo los servidores maestros principales tienen la capacidad de actualizarse directamente para procesar las actualizaciones de zona, lo que incluye agregar, quitar o modificar registros de recursos almacenados como datos de zona. Los servidores maestros principales se utilizan también como los primeros orígenes para replicar la zona en otros servidores DNS.

**Servidor Web**

Servidor que proporciona la capacidad de desarrollar aplicaciones basadas en COM y crear sitios grandes para Internet y para intranets corporativas.

**Sesiones**

Múltiples paquetes enviados con confirmación entre dos extremos.

**Sistema de archivos NTFS**

Sistema de archivos recuperable diseñado para usarse específicamente con Windows NT, Windows 2000 y Windows Server 2003. NTFS utiliza bases de datos, procesamiento de transacciones y paradigmas de objetos para proporcionar seguridad a la información, confiabilidad del sistema de archivos y demás características avanzadas. Admite recuperación del sistema de archivos, medios de gran almacenamiento y diversas características del subsistema POSIX. También admite la aplicación orientada a objetos mediante el tratamiento de todos los archivos como objetos con atributos definidos por el usuario y definidos por el sistema.

**Sistema de nombres de dominio (DNS, Domain Name System)**
Sistema jerárquico de nomenclatura utilizado para encontrar nombres de dominio en Internet y en redes TCP/IP privadas. DNS proporciona un servicio para asignar nombres de dominio DNS a direcciones IP y viceversa. Esto permite que los usuarios, los equipos y las aplicaciones consulten el DNS para especificar sistemas remotos mediante nombres de dominio completos en lugar de direcciones IP.

**Subdominio**
Dominio DNS que se encuentra directamente bajo otro nombre de dominio (el dominio principal) en el árbol de espacio de nombres. Por ejemplo, "eu.reskit.com" es un subdominio del dominio "reskit.com".

**Subproceso**
Tipo de objeto dentro de un proceso que ejecuta instrucciones de programa. El uso de múltiples subprocesos permite operaciones simultáneas dentro de un proceso y posibilita que un proceso ejecute diferentes partes del programa en distintos procesadores simultáneamente. Un subproceso tiene su propio conjunto de registros, su propia pila de núcleo, un bloque de entorno de subprocesos y una pila de usuario en el espacio de direcciones del proceso.

**Subred**
Subdivisión de una red IP. Cada subred tiene su propio identificador de red único de la subred.

## *T*

**Tabla de enrutamiento**
Base de datos de rutas que contiene información acerca de los identificadores de red, las direcciones de reenvío y la métrica de los segmentos a los que se puede tener acceso en redes interconectadas.

**Telnet**
Protocolo de emulación de Terminal que se utiliza ampliamente en Internet para iniciar una sesión en equipos de red. Telnet también se refiere a la aplicación que utiliza el protocolo Telnet para los usuarios que inician una sesión desde ubicaciones remotas.

**Terminal**

Dispositivo consistente en una pantalla de presentación y un teclado que se utiliza para comunicarse con un equipo.

**Texto cifrado**

Texto que ha sido cifrado mediante una clave de cifrado. El texto cifrado es ininteligible para quien no tenga la clave para descifrarlo.

**Tiempo de búsqueda**

Cantidad de tiempo requerido para que una cabeza de disco se coloque en el cilindro de disco correcto para tener acceso a los datos solicitados.

**Tiempo de respuesta**

Cantidad de tiempo requerida para hacer un trabajo desde el principio hasta el final. En un entorno cliente-servidor, por lo general se mide en el cliente.

**Token Ring**

Tipo de medio de red que conecta clientes en un anillo cerrado y utiliza el paso de un testigo para permitir que los clientes utilicen la red.

**Topología**

En los sistemas operativos Windows, las relaciones entre un conjunto de componentes de red. En el contexto de la replicación de Active Directory, topología hace referencia al conjunto de conexiones que utilizan los controladores de dominio para replicar información entre sí.

## *U*

**Unidades organizativas**

Objeto contenedor de Active Directory que se utiliza en los dominios. Las unidades organizativas son contenedores lógicos en los que se colocan los usuarios, los grupos, los equipos y demás unidades organizativas. Sólo pueden contener objetos de su dominio principal. Una unidad organizativa es el ámbito más pequeño al que se puede aplicar una Política de grupo o entidad delegada.

**Usuarios**

Grupo especial que contiene todos los usuarios con permisos de usuario en el servidor. Cuando un usuario asigna permisos a todos, esos permisos se dan a los usuarios e invitados de los grupos.

## *V*

**Vale de sesión**

Credencial presentada por un cliente a un servicio de protocolo de autenticación Kerberos. Como los vales de sesión se utilizan para obtener conexiones autenticadas a los servicios, a veces se denominan vales de servicio.

**Variable de entorno**

Cadena que consta de información de entorno, como una unidad, una ruta de acceso o un nombre de archivo, asociada con un nombre simbólico que puede ser utilizada para definir variables de entorno se utiliza la opción Sistema del Panel de control o el comando set en el símbolo del sistema.

**Volumen**

Parte de un disco físico que funciona como si fuera un disco físicamente independiente. En Mi PC y el Explorador de Windows, los volúmenes aparecen como discos locales, como C: o D:

## *Z*

**Zona de seguridad:**

Conjunto de nodos de una red que comparten finalidad, condiciones de conectividad, medidas de seguridad y modelo de asignación de ancho de banda.

# ANEXOS

# ANEXOS DE GRAFICOS Y TABLAS

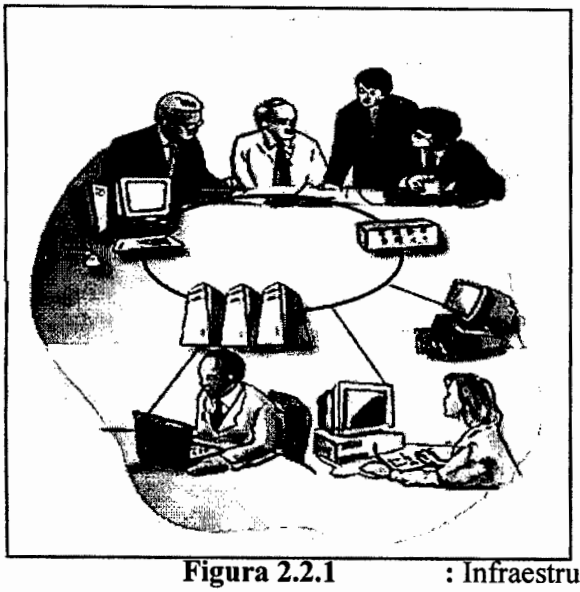


**Figura 2.2.1** : Infraestructura de Servicios de Red
**Fuente** : [URL 11]

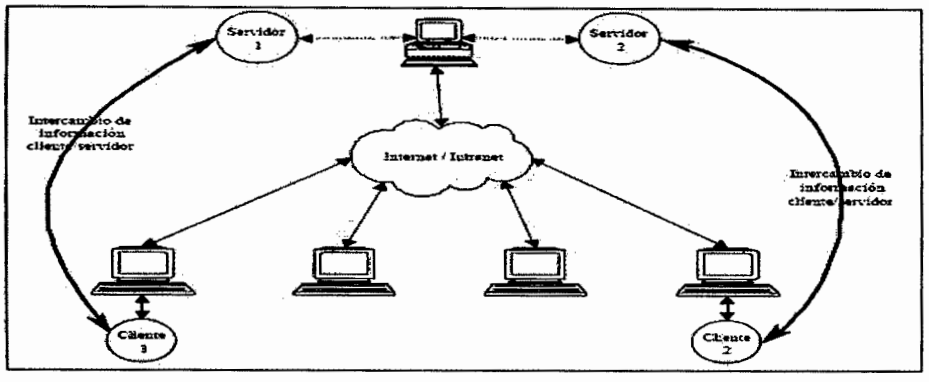



**Figura 2.2.2** : Arquitectura Cliente/Servidor
**Fuente** : [URL 04]

| | Standard Edition | Enterprise Edition | Datacenter Edition | Web Edition |
|---|---|---|---|---|
| **Velocidad CPU** | 550 MHz | 733 MHz | 733 MHz | 550 MHz |
| **RAM** | 256 MB | 256 MB | 1 GB | 256 MB |
| **Espacio de Disco** | 1.5 GB | 1.5 GB (x86)<br>2.0 GB (Itanium) | 1.5 GB (x86)<br>2.0 GB (Itanium) | 1.5 GB |

**FIGURA 2.2.3 : Requerimiento de Hardware**
**FUENTE** : [05]

| Usuario | Perfil | Requerimientos |
|---|---|---|
| Directivos | - Administración de la Universidad.<br>- Usuario de toma de decisiones.<br>- Acceso a toda la información. | - Obtención de reportes de manera oportuna.<br>- Comunicación rápida con las demás áreas para agilizar la toma de decisiones |
| Operativos | - Encargados de la parte transaccional (generación de reportes).<br>- Acceso a casi toda la información. | - Consultas rápidas de la información.<br>- Realizar transacciones seguras, fáciles y rápidas con los datos. |
| Docentes | - Generación de evaluaciones<br>- Generación de material didáctico<br>- Evaluación de los alumnos. | - Proceso de evaluación eficiente y sencillo<br>- Obtención de listado de alumnos en forma oportuna. |
| Estudiantes | - Acceso a cursos dictados<br>- Horarios<br>- Acceso a notas de los cursos<br>- Servicio de aplicaciones. | - Reporte de notas a tiempo<br>- Informe de horarios<br>- Acceder a programas e información necesaria para el desarrollo de los cursos. |

**Cuadro N° 01** : Perfiles de Usuario
**Fuente** : Elaboración propia

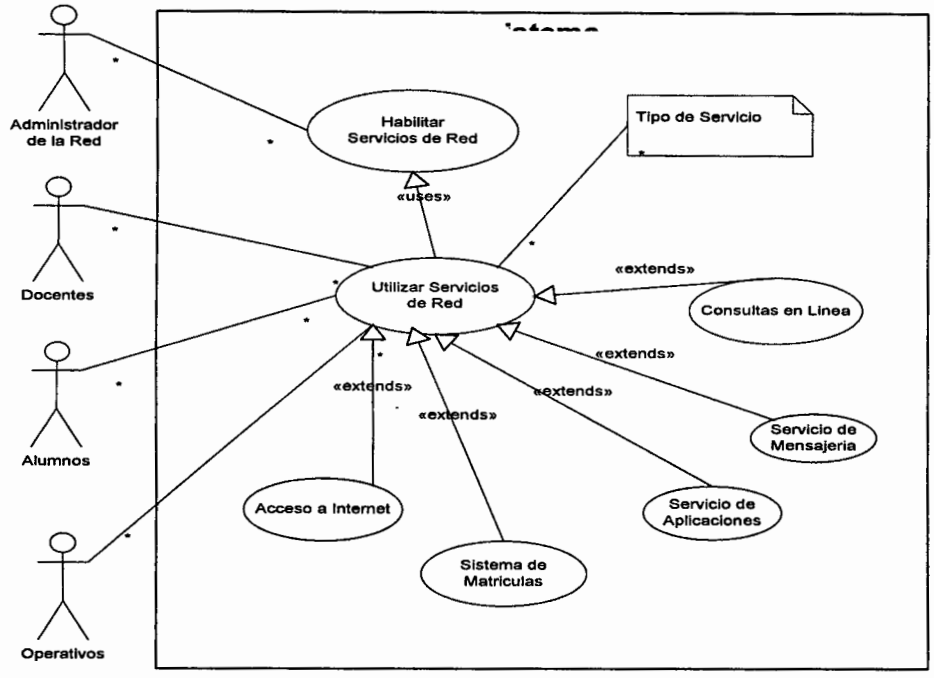



**Diagrama N°01** : Caso de Uso del Alcance del Proyecto

**Fuente** : Elaboración Propia

| Nombre | Rol |
|---|---|
| Alan Alberto García Panduro (Responsable) | Encargados del levantamiento de la información.<br>Análisis de la información<br>Implementación del Sistema de Servicios de Red, basado en Windows 2003 server.<br>Responsabilidad<br>Monitorear el correcto desarrollo del proyecto |
| Administrador Comision Portal Web - UNAP | Facilitar el acceso a la información y las instalaciones de la Empresa<br>Responsabilidad<br>Brindar apoyo y acceso oportuno. |

**Cuadro N° 02** : Roles y responsabilidades del Responsable y de Cliente.

**Fuente** : Elaboración propia

| Condición/ Descripción | Consecuencia | Probabilidad | Impacto | Prioridad | Mitigación |
|---|---|---|---|---|---|
| No se tiene un acceso oportuno a la información que necesita hacer uso el ejecutor del proyecto. | Retraso en la implementación de la Infraestructura de Servicios de Red, basado en Windows 2003 Server | 1 (Bajo) | 3 (Alto) | 0 | El ejecutor del proyecto debe identificar a la(s) personas encargadas de proveer esta información y solicitar su pronta atención. |
| Falta de implementación de un plan para asegurar información sensible de la institución. | Acceso a información confidencial de la institución | 1 | 3 | 1 | El equipo debe implementar ni veles de seguridad y autenticación de usuarios |

**Cuadro N°03** : Valoración de Riesgos
**Fuente** : Elaboración propia

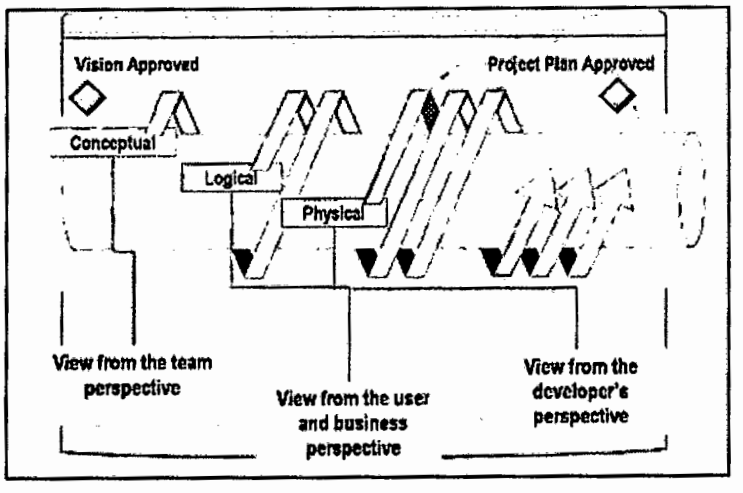



**Figura N° 4.4.2.1** : El modelo de acceso remoto
**Fuente** : [URL 13]