

UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA



Análisis y Diseño de Una Intranet Para la Marina de Guerra del Perú

TESIS

Para optar el Grado de Maestro en Ciencia

Mención: Telecomunicaciones

Presentada por:

César Manuel Alvarez Herrera

LIMA – PERU

2000

UNIVERSIDAD NACIONAL DE INGENIERÍA
Facultad de Ingeniería Eléctrica y Electrónica

Análisis y Diseño de una Intranet para la Marina de Guerra del Perú

TESIS

Para optar el grado de Maestro en Ciencias
Mención: Telecomunicaciones

Presentada por:
César Manuel Alvarez Herrera
Lima – Perú

Extracto

La Marina de Guerra del Perú tiene como misión garantizar la independencia, soberanía e integridad territorial, contribuyendo al desarrollo económico y social del país. Dada la naturaleza de sus funciones, esta Institución cuenta con dependencias en Lima, Callao y en provincias.

Un elemento necesario en la toma de decisiones es la obtención de información en el lugar adecuado y tiempo oportuno. Para el cumplimiento de su misión la Marina cuenta con una red de comunicaciones a nivel nacional y una WAN Naval; sin embargo, las máquinas, el software y los sistemas de comunicación que conforman tales redes no necesariamente conversan entre si, por lo que se hace necesario diseñar una Intranet.

Tal Intranet, la que denominaremos Intranet Naval para la Marina de Guerra, será un mecanismo flexible de distribución y de consulta de la información requerida por los miembros de la institución.

Para el diseño de la Intranet Naval se han analizado los procedimientos organizacionales de la institución con el propósito de determinar qué clase de

información se maneja. De este análisis, se han determinado tres categorías de información: administrativa, técnica y operacional, las cuales van a constituir los módulos principales de la Intranet.

Del análisis organizacional de la Marina de Guerra del Perú y teniendo en cuenta los servicios que la Intranet Naval va a proporcionar, se ha determinado que la arquitectura funcional de dicha Intranet tiene que ser distribuida.

La Intranet Naval debe proporcionar un ambiente de comunicación dinámica que permita el intercambio eficaz de información, proporcionando privacidad (no permitiendo accesos no autorizados) a través de firewall y servidores que cumplan dicha función y por medio del desarrollo inicialmente del algoritmo de encriptación PgP en el sistema de mensajería Out Look, para luego dejar en la bandeja de estudio el desarrollo e implementación de la Steganografía, que permitirá esconder mensajes en imágenes, archivos de voz e incluso en archivos de texto. La Intranet así, brindará un servicio en línea, sistematizando las tareas y mejorando el flujo de información.

La Intranet va a permitir también realizar un seguimiento del cumplimiento de la misión de la institución, ya que los niveles superiores de comando pueden tener acceso, de acuerdo a prioridades preestablecidas, a los almacenes de datos. Contar con información oportuna será de gran ayuda en la toma de decisiones.

NATIONAL UNIVERSITY OF ENGINEERING
Faculty of Electrical and Electronic Engineering
Analysis and Design of a Intranet for the Peruvian Navy

THESIS

As a Requirement for the degree of Master of Science

Mention: Telecommunications

by:

César Manuel Alvarez Herrera

Lima – Perú

Abstract

The Peruvian Navy has the mission to guarantee and defend the sovereignty of our country and contribute with its economic and social development. To fulfill its mission, the Peruvian Navy has operative task forces around the country.

The Peruvian Navy possesses a communication system and a Naval WAN. However, the components of such communication systems are not necessarily interconnected in the sense of sharing information. For such a reason, it is necessary to design and implement an Intranet.

A Naval Intranet for the Peruvian Navy can be a flexible way to distribute the required information among their members.

The design of the Intranet requires to analyze the organizational procedures of the institution in order to find out what kind of information needs to be shared and managed. From such an analysis, I have found that the information can be classified into three categories: Managerial, Technical and Operational information.

According to the analysis of the information flow and the objectives of the Intranet, I have determined that a distributed architecture is suitable for the operation of the Intranet.

The Intranet will permit dynamic communications and exchange of information point to point among users, providing access security.

The Intranet is aimed to permit an integral communication in a team work atmosphere, allowing to the users, according to their access priorities, to find the right information at the right time.

Tabla de Contenido

Capítulo 1

Introducción	1
--------------------	---

Capítulo 2

Arquitectura de una Intranet

2.1 Estándares Claves de una Intranet con que cuenta la Institución	6
2.2 Redes y Conectividad en la Marina de Guerra del Perú	9
2.3 Servidores de una Intranet	13
2.3.1 Servidores de Hardware	13
2.3.2 Servidores de Software	13
2.3.3 Servidores de Voz	14
2.3.4 Servidores de Imagen	27

Capítulo 3

Infraestructura de una Intranet

3.1 Procesos a tomar en cuenta en la Intranet	40
3.2 Personal que participa en la Intranet	40
3.3 Políticas de la Institución para con la Intranet	41

Capítulo 4

Diseño de la Intranet Naval

4.1 Metodología de Diseño	42
4.2 Estructura del Diseño de la Intranet Naval	43
4.2.1 La Página Central	43
4.2.2 Mapa de Sitio por Niveles	44
4.2.3 Cartografía del Sitio Web	47
4.3 Diseño de Pantallas	48
4.4 Capacidad de la Intranet	49
4.4.1 Tráfico de Datos	49
4.4.2 Tráfico de Voz	50
4.5 Costos del Desarrollo e Implementación de la Intranet Naval.....	50
4.6 Cronograma de Actividades	53

Capítulo 5

Seguridad de la Intranet Naval

5.1	Modelo General de la Seguridad en Red.....	56
5.2	Seguridad Física de la WAN Naval	58
5.3	Software de Seguridad	61
5.3.1	PgP (Pretty good Privacy).....	61
5.3.2	El Algoritmo RSA	62
5.4	Esteganografía	67
5.4.1	Introducción a la Criptografía	68
5.4.2	Terminología Básica	69
5.4.3	Esteganografía con Gráficos	69
5.4.4	Archivo de Imágenes	73
5.4.5	Formas de Esteganografía en Imágenes	75
5.4.6	Principios: El Modelo RGB	77
5.4.7	Criptografía Icónica	78
5.4.8	Explicación y Evolución del Algoritmo Esteganográfico	80
5.4.9	Pasos a seguir para Ejecutar el Programa de Esteganografía	86

Capítulo 6

Simulación de la Intranet Naval

6.1	Alcance	95
6.2	Metodología y Simulación.....	96

Capítulo 7

Conclusiones	100
---------------------------	-----

Bibliografía	103
---------------------------	-----

Apéndices

Apéndice A: Estándares de Internet	106
---	-----

Apéndice B: Organizaciones de estándares de Intranet	107
Apéndice C: Tipos de servidores	108
Apéndice D: Programa fuente para esconder un texto en una imagen (steganografía)	110
Apéndice E: Terminologías	143

Capítulo 1

Introducción

Las tecnologías de la información, actualmente son elementos fundamentales para la superación de un país. Por eso, los países desarrollados basan su crecimiento en la aplicación y en la programación estratégica de las herramientas computacionales definiendo políticas que los inducirán a su permanencia en el dinamismo mundial de los próximos años.

Ante el nuevo entorno económico mundial los países emergentes están obligados a preparar profesionales en áreas de la informática y las telecomunicaciones, capaces de enfrentar los retos que se tienen hoy en día. Por otra parte, la informática está tan popularizada que es muy difícil que una empresa adquiera una ventaja competitiva por tener computadoras más potentes o una red más extensa. La ventaja competitiva se logra con un uso más eficiente de la tecnología y, por supuesto optimizando la gestión de la empresa.

En definitiva, la tecnología informática define e impulsa la nueva era, rediseña el marco que se utiliza para describir la realidad, por ello los problemas importantes del hombre se pueden convertir en problemas informáticos. Todo está interconectado, es complejo e interdependiente, la efectividad de los sistemas descansa en la seguridad y protección de la comunicación. Es así que los países vecinos no se han mantenido al margen de todos estos adelantos y lo han realizado básicamente con ayuda de otros países, tal es el caso de Brasil que constituye uno de los países importantes para los intereses de EEUU en América del Sur, por tal efecto se vio beneficiada con el asesoramiento tecnológico en la implementación de redes a través de comunicaciones para su fuerza armada, colocándola en la cima en el desarrollo dentro este campo (armamento, apoyo económico, tecnología, etc.). A fines del siglo pasado Chile quiso aprovechar el apoyo que daba EEUU tratando de demostrar a EEUU la necesidad de un gendarme en el Océano Pacífico para complementar el trabajo de Brasil y de esta manera obtener la hegemonía absoluta en Sudamérica, pero los resultados fueron negativos a su gestión. Sin embargo, por tener el país vecino una economía estable hizo posible su desarrollo tecnológico

militar al implementar las comunicaciones con tecnología a través de redes lo cual ha demostrado resultados óptimos en sus fuerzas armadas.

Los países de Argentina, Ecuador, Colombia y Venezuela se han mantenido con un avance hasta cierto punto estacionario, dado que sus prioridades son orientados al campo político y económico. Recién a inicios del Siglo XXI, Argentina y Venezuela han empezado a desarrollar tecnologías que le ponen a un nivel de sus armadas limítrofes, Ecuador y Colombia de acuerdo a su programa de actividades contempla este desarrollo para mediados del 2002.

El Perú no se ha mantenido al margen de esta evolución tanto informático como el de comunicaciones que se ha dado en los países desarrollados como los países limítrofes tal como se menciona en párrafos precedentes, y ha ido haciéndolo en forma considerable. En lo concerniente a la Marina de Guerra del Perú, a pesar de contar con un presupuesto limitado, lo ha realizado por dependencias y de acuerdo a la necesidad institucional.

Inicialmente se vio por conveniente interconectar las dependencias para compartir información, esto se realizó considerando los estudios realizados en el Estado Mayor General de Marina como marco referencial tales como: la Doctrina de Comunicaciones, la Doctrina de Informática y la Política General de Informática, generando así un proyecto de nombre propio llamado WAN Naval a inicios de la década del 90.

La WAN Naval, reflejó el crecimiento y difusión de la informática desde los centros de cómputo tradicionales hasta el uso de computadoras personales (PCs) conectadas en red. Al instalarse las redes con el propósito de modernizar las comunicaciones, se compartió la información con las computadoras centrales que fueron diseñadas para soportar la carga de sistemas tales como el Económico Financiero, Personal, Abastecimiento, entre otros, con un limitado acceso a la información y un lento desarrollo de nuevas aplicaciones. Las unidades y dependencias fueron desarrollando soluciones de diferente magnitud para aplicaciones específicas, con un limitado intercambio de información, acompañado

de una limitada capacidad en la adquisición de equipos de última generación en sus inicios.

Tomando como referencia el Proyecto de la Marina de Guerra, se menciona que la implementación de la WAN Naval de voz y datos permitió considerar un cambio en el paradigma sobre la manera de cómo se crea, administra y se obtiene información. Con la WAN Naval y el Plan de Informática para los próximos años, los sistemas de información de la institución pasan de haber sido herramientas aisladas de soporte a la administración y limitada cobertura operacional, hacia una orientación integrada de sistemas, que puede cambiar los procesos fundamentales mediante los cuales se cumple la misión, mejorando la capacidad del personal naval, incrementando la productividad y asegurando el acceso oportuno a la información disponible para la toma de decisiones en los diferentes niveles de la organización.

Siendo la información un elemento necesario en la toma de decisiones, es que los usuarios se preguntaban sobre dónde, cómo y cuando obtener información necesaria para cumplir su misión. Si bien es cierto que la Marina de Guerra del Perú ha utilizado los adelantos de la tecnología referente a la transmisión de información, para compartir información simultánea entre las fuerzas operativas y el teatro de operaciones, es necesario tomar en cuenta que las máquinas, el software y los sistemas de comunicación que conforman tales redes conversan aisladamente en forma autónoma. De allí la importancia de la Intranet, la cual es una herramienta o mecanismo flexible de distribución de la información requerida por los miembros de la Institución para el cumplimiento de sus funciones logrando conectar a los usuarios sin importar el hardware o software que utilicen; siendo lo más importante, la actualización instantánea y simultáneamente de la información, de modo que todos los usuarios puedan compartirla en tiempo real.

Con los recursos tecnológicos con que cuenta la Marina, una futura implementación de la Intranet diseñada, incrementará la eficiencia en la creación, administración y obtención de la información, permitiendo compartir la infraestructura existente, no sólo para el acceso a la información, sino para el uso efectivo y oportuno de los medios en la toma de decisiones, por lo tanto los objetivos del presente trabajo son:

- Realizar un estudio situacional de la institución para analizar los procesos y el flujo de la información dentro de la organización, así como determinar los recursos tecnológicos con que cuenta actualmente.
- Diseñar una Intranet para la Marina de Guerra del Perú en base a sus requerimientos.
- Validar mediante simulación el diseño propuesto.

Para el desarrollo del presente trabajo se ha visto por conveniente dividirlo en siete capítulos los que describiremos a continuación :

Capítulo 1 Se realiza análisis referencia sobre el uso de la tecnología en un escenario mundial concluyendo con los requerimientos de la Institución.

Capítulo 2 Arquitectura, se explican los estándares claves, tipos de redes, clases de conectividad y servidores utilizados en la red, necesarios para el desarrollo de la Intranet.

Capítulo 3 Infraestructura, se explican los procesos a tomar en cuenta, la capacitación y tipo del personal así como las políticas que deben ser consideradas, para el desarrollo de la Intranet.

Capítulo 4 Diseño, en el cual se detalla la metodología y su estructura del diseño propiamente dicho.

Capítulo 5 Seguridad, se considera la seguridad de hardware y de software, mencionando el algoritmo RSA del PgP utilizado en el sistema de mensajería Outlook, así mismo el desarrollo del algoritmo de la Steganografía, que permitirá esconder textos dentro de otros archivos; este ultimo se adjunta con el programa fuente.

Capítulo 6 Simulación, se comenta acerca del alcance y la metodología.

Capítulo 7 Conclusiones, son las expresiones finales orientadas a servir de marco referencial para asesorar la implementación del presente trabajo.

Capítulo 2

Arquitectura de la Intranet

En este capítulo se describen los elementos relacionados con la arquitectura de una Intranet, tales como estándares, redes, servidores, etc. Esta descripción se desarrolla tanto en forma general como en forma específica cuando la arquitectura está directamente relacionada con la institución.

2.1 Estándares Clave de una Intranet con que cuenta la Marina

Cuando se habla de arquitectura, implica hablar de estándares abiertos, que significa que el software que se utiliza para transformar datos en información útil para la institución puede ejecutarse en cualquier hardware, ello quiere decir que cualquier persona puede desarrollar software sin tener que asegurarse de que sea compatible con cada sistema operativo de la red. Finalmente cualquier PC (Personal Computer) o estación de trabajo que utiliza TCP/IP (Transfer Control Protocol / Internet Protocol) puede desarrollar una aplicación y ponerla disponible en la Intranet. Los estándares de Intranet están conformados por protocolos de Internet, lenguajes de programación y API's (Interfaces para Programación de Aplicaciones).

En la tabla mostrada en el Apéndice A se resumen los estándares clave de internet que facilitan el flujo de información. En el nodo central de la WAN Naval ubicado en La Perla, se emplea los siguientes estándares:

TCP/IP.- La Marina de Guerra del Perú cuenta con una red WAN cuyo nodo principal está ubicada en La Perla. Los nodos de la red WAN hacen uso de este protocolo que en mayor detalle se presenta en la sección 5.2.

HTML.- De sus siglas del inglés Hypertext Mark Up Language, es un lenguaje que permite la publicación de textos, gráficos, videos, audio, etc, empleando el protocolo HTTP (Hypertext Transfer Protocol). El protocolo HTML hace que los archivos

tengan los mismos códigos, de modo que desde cualquier plataforma con un navegador se pueda ver la página Web, tal como se muestra en la figura 2.1.

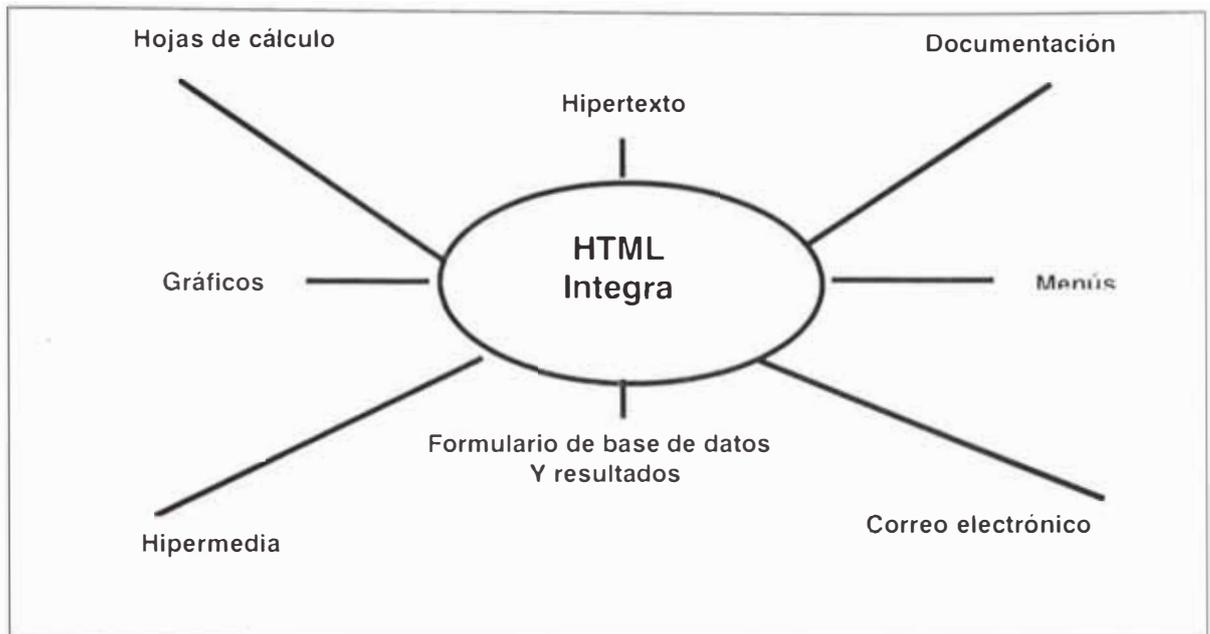


Figura 2.1.1 HTML permite la integración de multimedia.

HTTP.- Este protocolo de transferencia de hipertexto permite el acceso con navegador a las redes globales, enviando y dando seguimiento a los paquetes de información entre clientes y servidores, tal como se muestra en la figura 2.2.

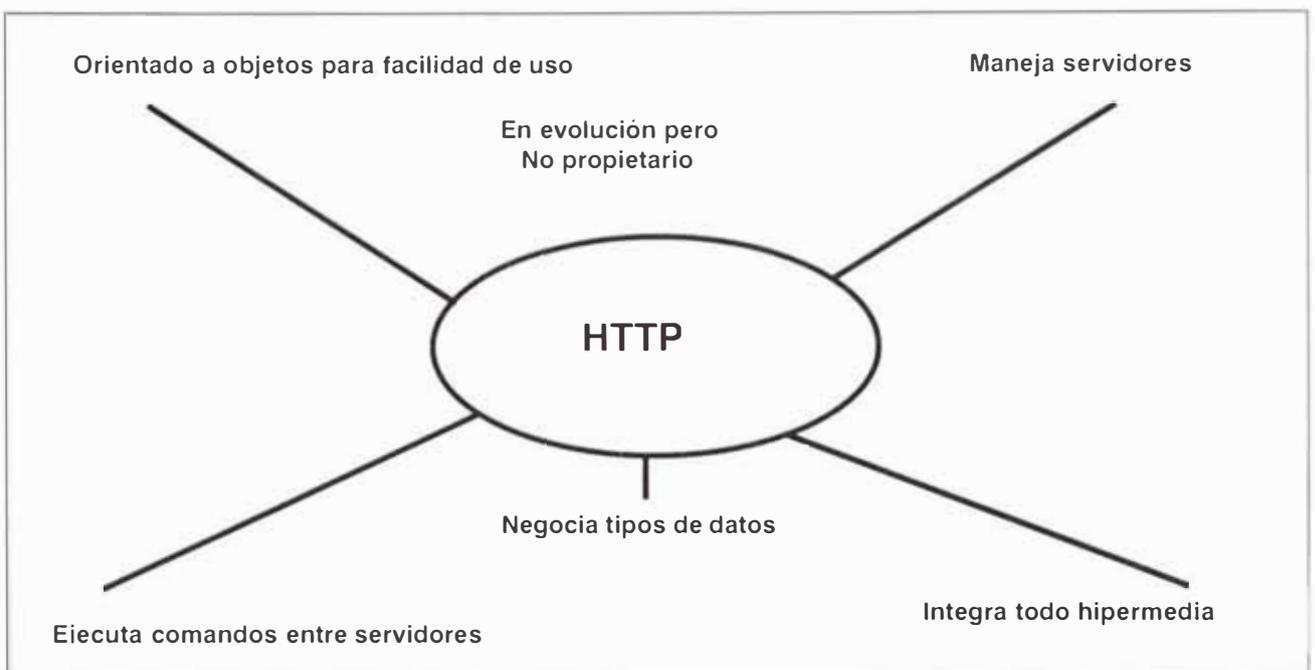


Figura 2.1.2 Panorama de la Funcionalidad de HTTP.

JavaScript.- El JavaScript es un lenguaje basado en el manejo de objetos, los cuales permiten la creación de funciones y procedimientos que pueden incrustarse por completo dentro de documentos HTML. Este lenguaje funciona como un modelo de eventos que proporciona retroalimentación inmediata al usuario cada vez que ocurre una transacción y proporciona una interacción importante entre páginas Web y bases de datos relacionados. La programación con JavaScript es fácilmente asimilable por los programadores de HTML que no tienen experiencia en programación orientada a objetos. La desventaja del lenguaje JavaScript es que no es bueno para manipulación de archivos que necesiten mucha memoria, como las hojas de cálculo.

CGI (Common Gate Interface).- Este interfaz común de puerta de enlace es un estándar para generar una interfaz entre las aplicaciones externas y los servidores de información. Su programación es en tiempo real, de modo que permite generar información dinámica que cambia de acuerdo con la solicitud.

La ventaja de los programas escritos en CGI permiten interactuar con los usuarios, reunir información en un formulario e integrarla con la base de datos, de manera que los usuarios puedan realizar consultas. La desventaja de los programas en CGI es que cada petición cliente significa una conexión al servidor. Para evitar esto, se recomienda que los programas en CGI (Interfaz Común de Puerta de Enlace) residan en un directorio especial.

Java.- Java es un lenguaje de programación orientado a objetos que permite el desarrollo de verdaderas aplicaciones centradas en la red. Se integra directamente en documentos HTML y VRML (Lenguajes de Modelado de Realidad Virtual). Las ventajas que ofrece son: independencia de plataforma, independencia de ubicación, posibilidad de evolucionar, seguridad y aplicación de subprocesos múltiples. La desventaja es que se requiere un aprendizaje y programación especializados.

Con el avance de la tecnología a diario se crean estándares para que el desarrollo de las intranets resulten más sencillas, para mayor información se presenta en el Apéndice B algunas páginas Webs de los comités de estándares de Internet.

2.2 Redes y Conectividad en la Marina de Guerra del Perú

En la última década, las empresas así como las instituciones del estado como la Marina de Guerra del Perú, han invertido tiempo y dinero para conectar en red computadoras personales y estaciones de trabajo, sin embargo, a pesar de ello se presentaban obstáculos para la vinculación de las aplicaciones en plataformas cruzadas, la posibilidad de compartir archivos y sistemas de correo electrónico y el aseguramiento del acceso a información confidencial.

Novell lanzó el NOS (Network Operating System) para resolver los problemas de computación en colaboración. Mediante las actualizaciones de sus sistemas, el NOS de Novell ha obtenido compatibilidad con Intranet, significa esto integrar los protocolos de Internet con sus NOS.

Actualmente se habla de 3 generaciones de Intranet: En la primera generación se ubican intranets básicas empleadas principalmente para publicaciones, la segunda generación de Intranets se diseñaron para colaboración interactiva entre sus componentes y las intranets de tercera generación son las denominadas extranets y está orientada principalmente al comercio electrónico.

El diseño de la Intranet propuesta para la Institución corresponde a una de segunda generación. Los requisitos fundamentales para configurar una red como Intranet de segunda generación son: estándares de Internet (HTML, HTTP), equipos de hardware, elementos estándares de red (red basada en TCP/IP con LAN con varias subredes y como red vertebral una WAN de alta velocidad, etc). En la sección 2.1 se han descrito los estándares de Internet con que cuenta la Institución.

Cabe mencionar que los diferentes componentes que conforman la WAN Naval y la ubicación de cada uno de ellos ha sido diseñado considerando el Modelo OSI (Open System Interconnection). Seguidamente se menciona la tecnología con que cuenta la Institución en cuanto a equipos y estándares de red.

La mayor parte de las dependencias de la Marina cuenta con su propia red LAN (Local Area Network), con equipamiento de diferentes marcas, predominando las computadoras compatibles y equipos de Networking marca 3Com, así como

Routers Cisco e IBM. La mayoría utilizan arquitectura estrella, aunque algunas utilizan una mezcla de arquitectura bus y estrella, debido a consideraciones de distancia, siendo la velocidad promedio de cada red de 100 Mbps.

Las trece redes LAN con que cuenta la Marina se han integrado para conformar una gran red WAN; para ello se han definido siete redes principales: **La Perla** (se refiere a la topología y configuración en el área de La Perla), **Salaverry** (se refiere a la topología y configuración en el área de Salaverry), **Base Naval** y **La Punta** (se refiere a la topología y configuración en el área de La Punta), **Centro Medico Naval**, **Dirección de Capitanías y Guardacostas**, y **Dirección de Inteligencia Naval**. A estas redes principales se suman otras seis redes de menor tamaño, las cuales se encuentran interconectadas mediante el empleo de diferentes tecnologías, tales como Microondas, Satélite, Frame Relay, Bridges Inalámbricos, etc. La red LAN La Perla es considerada como el nodo central de la WAN. Para mayor ilustración ver Figura 2.2.1

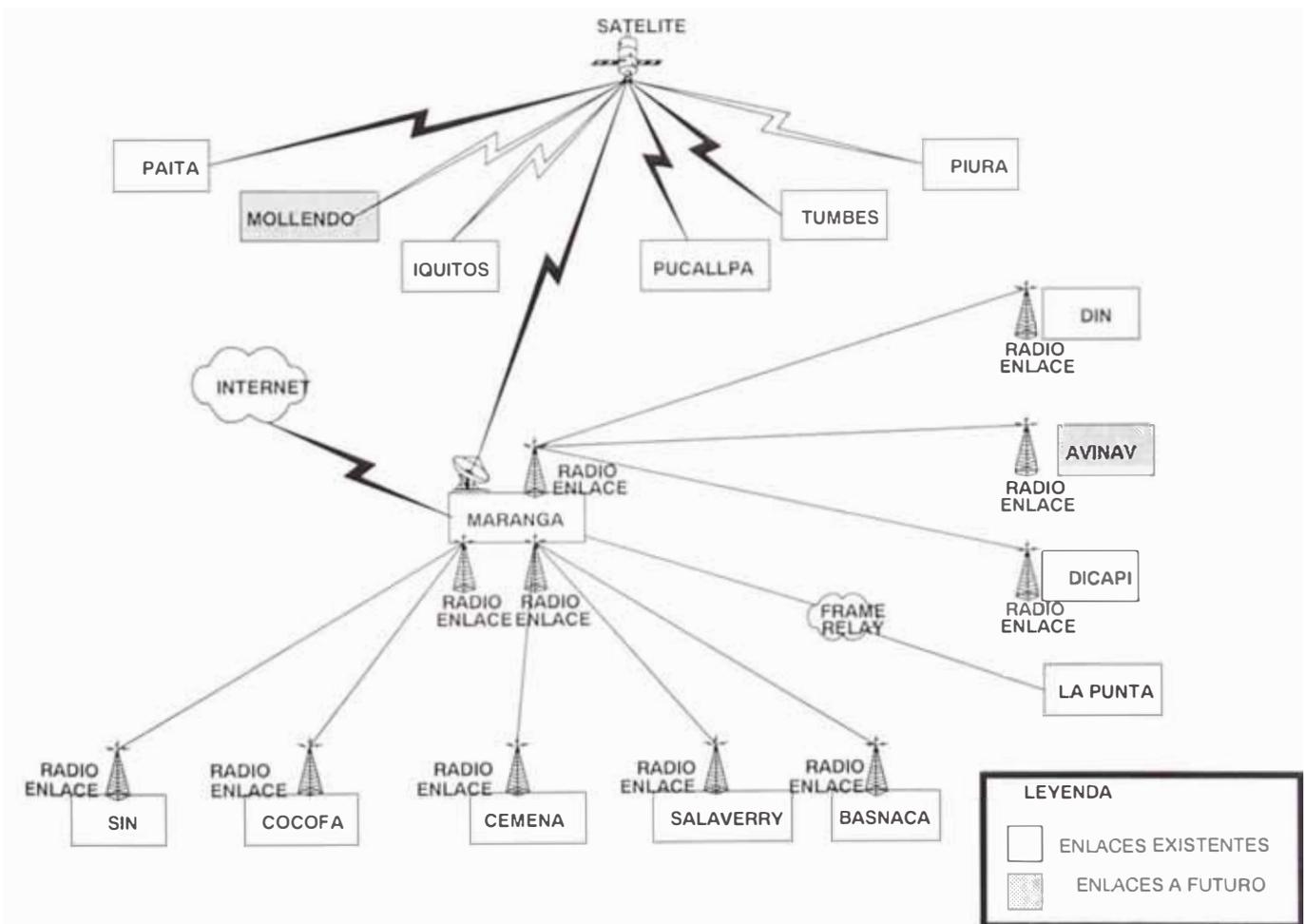


Fig. 2.2.1 Esquema de enlace de las principales redes de la Wan Naval

El esquema básico empleado en cada uno de los diferentes nodos se representa de manera general en el siguiente gráfico de la figura 2.2.2

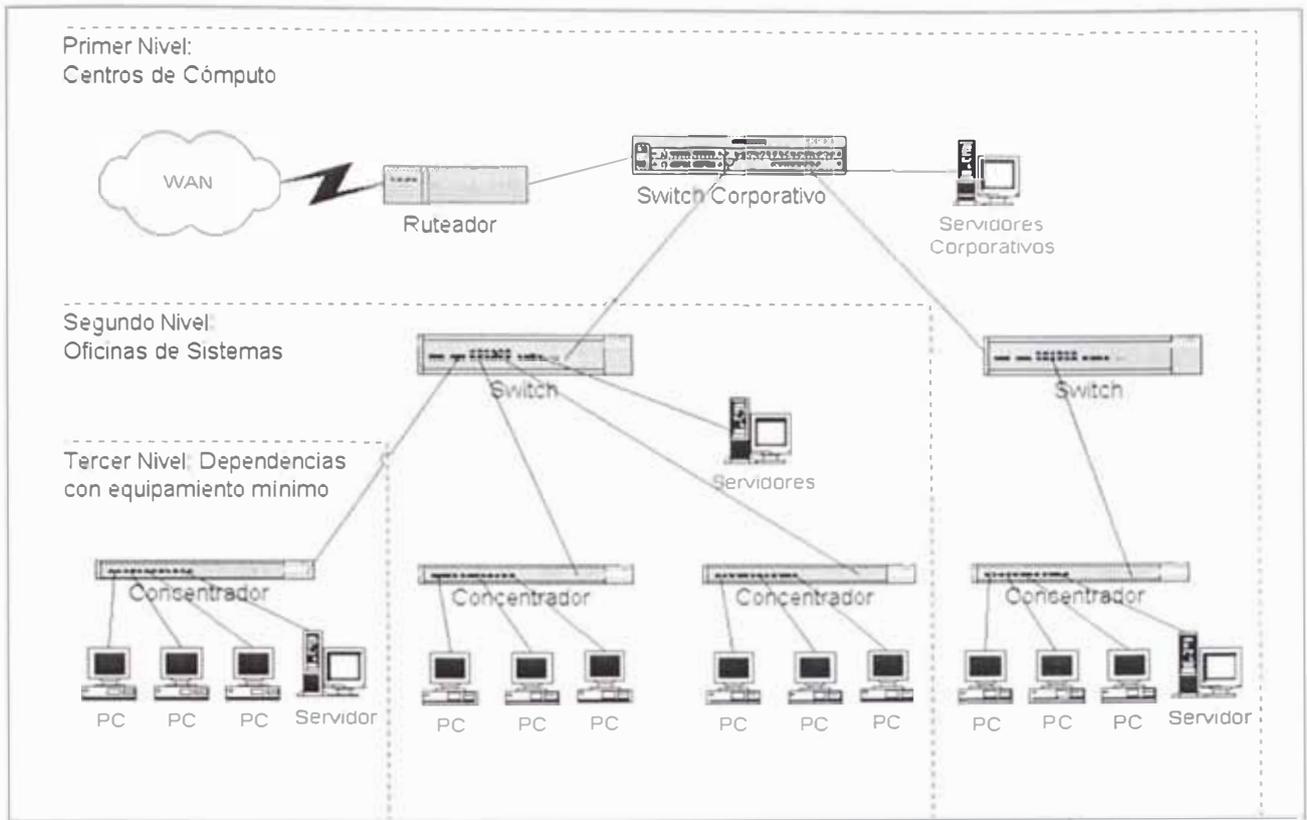


Fig. 2.2.2 Esquema Básico de Enlace a través de las oficinas de la Marina de Guerra del Perú

El backbone principal de la red WAN, ubicado en el nodo La Perla, consiste en una matriz de switches 10/100 Mbps, interconectados por medio de fibra óptica multimodo de seis hilos a una matriz principal de switches con puertos RJ 45 de 100 Mbps. Todos los enlaces empleados entre los diferentes nodos son enlaces privados que se logra mediante el uso de siete radio enlaces de microondas de 04 E1's (cada canal E1 equivale a 2 Mbps), los mismos que tienen fuente de poder redundante, así como transmisor y receptor redundante, lo cual asegura una alta disponibilidad de enlace a través de sistemas UPS (Unit Power Supply). Asimismo, se tiene 05 enlaces con sendos nodos en provincia empleando Tecnología Satelital (Panamsat), permitiendo un ancho de banda de 128 Kbps. Multiplexado Dinámicamente para enlace en Voz y Datos.

Las agregadurías Navales que se encuentran en el extranjero, así como las Capitanías de Puerto ubicadas en provincia y otras Dependencias que no tienen posibilidad de Conexión Física directa con la WAN, se enlazan a la WAN Naval

mediante el empleo de esquemas de Redes Privadas Virtuales (VPN's), de encriptación con algoritmo privado y de firewalls que utilizan la Internet como medio, lo cual provee un canal punto a punto seguro entre las diferentes Agregadurías y/o Capitanías con la WAN Naval.

Para permitir redundancia se ha dotado con líneas RDSI de 128 Kbps ; como es el caso de las capitanías de puerto que se encuentran conectados por satélite las cuales se comportan como enlaces alternos en el caso de que se produzca una caída de los enlaces principales.

La WAN Naval mantiene una conexión con INFOVIA para soportar cierta aplicación particular de carácter reservado. El único protocolo de tráfico que se esta utilizando como protocolo WAN es el TCP-IP, siendo este tráfico el único permitido de enrutar por los diferentes Routers entre Nodos. En lo concerniente a la salida a Internet, la WAN mantiene un enlace de salida a INTERNET para enrutar el trafico de los usuarios (ver Figura 2.2.3). Uno principal en el Nodo de La Perla por medio de Fibra Optica con un ancho de Banda de 2 Mbps que se comporta como salida principal y primaria.

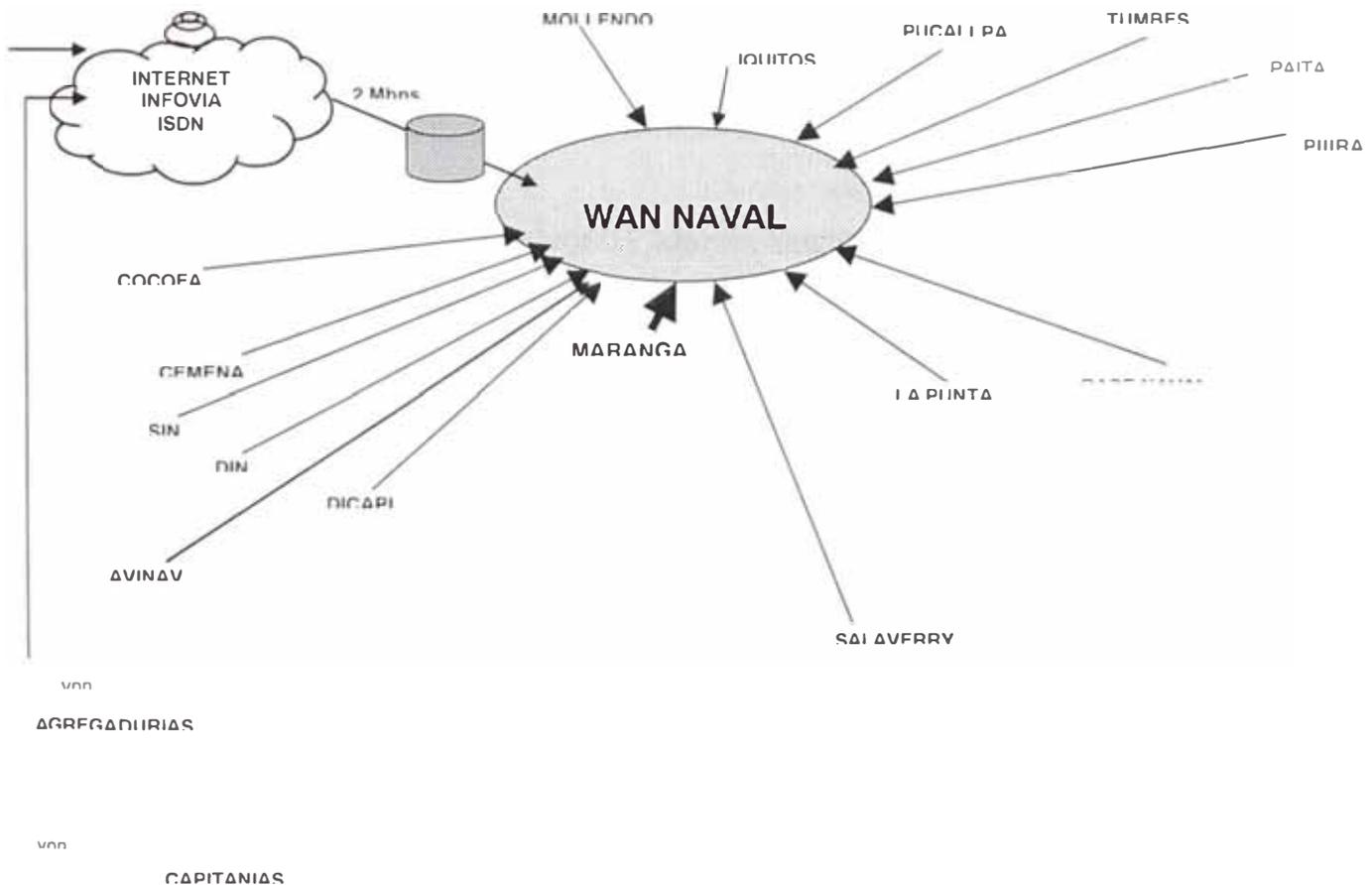


Fig. 2.2.3 Esquema Básico de comunicación en los nodos de la Wan Naval

2.3 Servidores de la Intranet

Las intranets están integradas por dos tipos de servidores: de hardware y de software, en el Apéndice C se brinda mayor información al respecto.

El servidor de correo y el servidor de administración están ubicados en el nodo central de la WAN Naval La Perla, la Marina cuenta con los siguientes tipos de servidores:

2.3.1 Servidores de Hardware.- Son computadoras, estaciones de trabajo y a veces mainframes que operan usando estándares de Internet. Cualquier computadora puede configurarse como servidor, utilizando cualquier sistema operativo. Lo recomendable es iniciar por lo menos con una máquina 486 de 66 Mz, con 16 Mb de RAM y un módem de 28.8 Kbps (para salir a internet)

2.3.2 Servidores de Software.- El componente clave de cualquier intranet es el software del servidor, pues este software se ejecuta en una computadora central y actúa como distribuidor de todos los datos disponibles sin importar su origen, estos datos pueden ser por ejemplo: solicitud de documentos, correo electrónico, consultas de base de datos, servicios de noticias, páginas de inicio, transacciones, etc. todo debe pasar por el servidor web antes de enviarlo al usuario.

Como sistemas operativos la Marina cuenta con Microsoft Windows NT y Novell Netware, para base de datos con el Oracle Server, el Informix y Microsoft SQL Server, para mensajes navales con Novell GroupWise y Microsoft Exchange y finalmente para servidores Web se cuenta con Internet Information Server (Option Pack4) y NetScape Enterprise Server.

Cada nodo de la WAN Naval cuenta con un servidor Proxy que sirve como servidor Caché, así como con un firewall en cada punto de conexión a internet (La Perla y Salaverry) como Servidor Espejo que es un enlace alternativo en el caso que se produzca una caída de los enlaces principales. En el sistema de correo la Marina cuenta con un Servidor Principal y con un Servidor Stand By como servidor Espejo, ambos poseen una capacidad de almacenamiento de 8 Gigabits con un arreglo de discos para preservar la información.

De acuerdo a lo que se explicó en la parte de infraestructura del diseño de la Intranet para la Marina se detallaron los requerimientos básicos para la implementación de ésta, pero sin embargo los avances tecnológicos son bastantes rápidos que traen como consecuencia mejores equipos con aplicaciones superiores que satisfacen mayores necesidades.

Este es el caso de los Servidores, la Institución proyectada a un corto plazo va a necesitar de servicios que tengan mayor soporte en Voz e Imagen, ya que se tiene previsto la implementación de una central totalmente digitalizada sin asistencia de operadores, que pueda brindar un enrutamiento total de la comunicación hacia la dependencia que se requiere; así mismo se espera contar con un servicio de envío de información satelital de fotos de los viajes de investigación a la Antártida, que se realizan anualmente así como información meteorológica para la Dirección de Hidrografía que se empleará para fines de navegación para navegantes y pescadores en nuestro litoral.

Pero esta tecnología aún no está disponible, ya que se encuentra en la fase final de desarrollo del mismo. Lo que se pretende es dar una visión de cómo se podría implementar un Servidor de Voz y uno de Imagen, para ello es necesario tener claro en que consiste y cuales son sus aplicaciones, sus ventajas , conocer algunos próximos servicios, concluyendo con las características de diseño; pero esta implementación se pretende efectuar con los medios disponibles con que cuenta la Institución, que muchas veces por razones políticas y económicas de gobierno en las partidas de Defensa, hacen posible que sean insuficiente los recursos para poderlas llevar a cabo.

2.3.3 Servidores De Voz

Siempre que hemos necesitado conseguir información de nuestra situación académica o bien sobre las fechas y plazos de alguna convocatoria, o simplemente el tratar de comunicarnos con alguna persona que posee un anexo dentro de una Institución, hemos echado de menos algún sistema cómodo y rápido para evitar tener que desplazarnos a la Secretaría o módulo de información correspondiente, o de lo contrario soportar ese teléfono que continuamente comunica. Nos preguntamos cómo es posible que tengamos que invertir tanto tiempo en realizar

nuestra consulta y al final, aunque hayamos conseguido resolver nuestra duda, nos queda la sensación de “haber perdido la mañana”.

Existen épocas dentro del año académico en que el volumen de consultas, bien por teléfono o en persona, aumenta considerablemente. Como media, se puede recibir aproximadamente 5000 llamadas diarias, y en épocas que se pueden considerar como de máximo tráfico aumentan a 8000, por lo que no nos debe extrañar que se produzca colapsos en la centralita. Además, las personas dedicadas a la atención al público, aún dedicándose exclusivamente a esta labor, no podrían absorber todas las peticiones, con lo que el tiempo dedicado a la consulta y la calidad de la información aportada se vería seriamente mermada.

Actualmente se está recurriendo a todas las ventajas que ofrece la red para poner a disposición una extensa y variada información. El uso de la red nos posibilita conseguirla de una forma rápida y relativamente sencilla, pero también existe información personal y privada que precisamos conocer. Por ejemplo, nos gustaría conocer por la red nuestra calificación en una asignatura; lo que no nos convencería tanto, sería que todo el mundo pudiese conocerla también, sobre todo si es que esta es desaprobatória.

Posibles Soluciones

Algunas veces las consultas realizadas tienen un carácter genérico, otras en cambio, el usuario necesita un trato personalizado, ya que su pregunta no puede ser resuelta mediante ningún sistema automatizado.

La existencia de contestadores automáticos, que ofrecen servicio las 24 horas del día, permiten aportar una primera respuesta a la persona que lo solicita. Sin embargo, si no se desea que el mensaje grabado se haga eterno para quien lo escucha, la información incluida en el mensaje deberá ser limitada.

La utilización de los Servidores Web, dedicados a ofrecer información variada, ha resultado ser un gran avance en la calidad del servicio de atención al usuario. Pero para ello se necesita tener acceso a un ordenador que este conectado a la red, con un navegador como el Netscape o el Internet Explorer y por supuesto, que la información solicitada haya sido volcada en algún servidor.

Aunque cada vez el número de computadoras personales conectados a Internet es mayor, numerosas personas carecen de dicha infraestructura. Por otro lado, se necesita invertir tiempo y esfuerzo en depositar toda la información en la red y, por supuesto, actualizarla con frecuencia para ofrecer un servicio de calidad, fiable y útil.

Desde hace dos años, está en marcha un nuevo servicio de atención al usuario, el Servidor de Voz, con el que se pretende facilitar el acceso a la información, descongestionando la central de conmutación tradicional. La principal ventaja de este servicio es que no precisamos más que de un teléfono para poder utilizarlo.

Estado Actual de la tecnología

En los últimos años, las tecnologías del habla han constituido un campo importante de investigación, pasando de ser un objetivo meramente científico a ser un objetivo claramente comercial. En la comercialización de estas tecnologías tiene protagonismo relevante los Servidores Vocales Interactivos (SVIs). Un SVI no es más que un sistema capaz de proporcionar un servicio de adquisición o difusión de información a través de la línea telefónica, utilizando síntesis y reconocimiento de voz. Tradicionalmente, los operadores de telefonía han venido dando este tipo de servicios a través de operadores que atendían personalmente las llamadas. La automatización que se puede conseguir mediante la introducción de las tecnologías del habla, y la reducción de costos asociada, está despertando un gran interés comercial.

La utilización de esta tecnología fue implementándose en los EEUU aproximadamente a partir de los 90, "Demostel" fue el servidor vocal que podía generar y recibir llamadas telefónicas en el mismo tiempo o automáticamente a números ausentes u ocupados, conduciendo cuestionarios y registrando respuestas con la ayuda de los botones del teléfono. Actualmente, existen millares de entrevistas por teléfono sin ninguna intervención a nombre de los encuestadores.

Actualmente EEUU y Europa con España a la cabeza tienen desarrollo exponencial en lo referente a comunicaciones a través de red, los servidores vocales

cada vez se van perfeccionando más, brindando mayor bondad a los usuarios. Compañías como CISCO, 3com, etc. presentan plataformas que incluyen procesadores que extienden el alto rendimiento en la ejecución de aplicaciones.

La disponibilidad o el porcentaje del tiempo que un sistema está disponible para proporcionar servicio era un supuesto en las redes tradicionales. En las redes del nuevo mundo, la disponibilidad es un requisito clave, la cual ofrecerá plataformas robustas para aplicaciones críticas (alimentación redundante, disco duro redundante, etc).

Qué es un Servidor de Voz

Es un servicio automático de atención al usuario, pero no debemos confundirlo con un contestador automático normal y corriente.

El Servidor de Voz está formado por una PC conectado, por un lado al ordenador central de la Institución o empresa, y por el otro a 24 líneas inicialmente, y se encargará de proporcionar información Las 24 horas del día. Por lo tanto, podría decirse que sirve de puente entre el usuario y el ordenador central, donde se encuentra la base de datos de la Oficina de ordenación, por lo que el servidor de voz tiene acceso a la misma información que poseen las secretarías de los centros, cuya actualización es constante y automática.

Este servicio puede aportar tanto información general (Modalidades de acceso, Titulaciones, Planes de estudio) como información individual y actualizada de cada usuario (Admisiones de cursos, Calificaciones de Asignaturas Universitarias, etc).

Además se encarga de comunicarse con la persona que llama. Según los códigos que ésta le aporte (los números que marcamos en el teclado del teléfono o los que decimos mediante la voz), el ordenador ejecuta la acción correspondiente y consulta en el ordenador central el dato solicitado. Para conversar con el oyente, en esta PC se encuentran grabadas un conjunto de frases y palabras sueltas, que combinará para que se produzca una respuesta coherente y acorde con la pregunta realizada.

Unos cuantos Números

Las unidades de atención al público reciben diariamente unas 5000 llamadas telefónicas solicitando información y en los meses de mayor flujo se pueden llegar a recibir más de 8000 llamadas. Esto supone al mes entre 30000 y 40000 consultas.

La mayor parte de ellas se realizan en horario de trabajo o de atención al público pero, aproximadamente un 10 por ciento, se hacen fuera de este horario e incluso en días no laborables.

Se sabe que el tiempo dedicado a cada llamada es variable, dependiendo del tipo de información solicitada. Suponiendo que se invierte 90 segundos a cada una de ellas, para atender a todas ellas se necesitarían entre 12 y 22 personas trabajando al 100 por ciento en atención telefónica.

El Servidor de Voz es capaz de atender en horas punta hasta 390 llamadas cada hora y el servicio está operativo las 24 horas del día, con lo que se consigue dar respuesta a unas 3100 personas que solicitan el servicio diariamente. Desde luego puede que ciertas preguntas no encuentren en este servicio la respuesta adecuada, por lo que habrá que solicitar un servicio más personalizado en la secretaría correspondiente, pero un número nada despreciable de llamadas habrán resuelto su duda sin haber esperado a que el teléfono deje de comunicar o haber tenido que desplazarse al centro correspondiente.

Cómo utilizar este servicio

La forma de acceder a este servicio no puede ser más fácil. Debemos marcar el número de teléfono, el costo de la llamada se pagará en partes iguales entre las personas que efectúan la comunicación.

Antes de comenzar a “navegar” por este servidor, nos preguntarán si nuestro teléfono tiene una tecla con un asterisco. Si es así es una ventaja, puesto que a partir de ese momento todas las opciones a elegir las podemos realizar desde el teclado de nuestro aparato. En caso contrario, no pasa nada. El sistema reconocerá la opción elegida si la solicitamos mediante la voz, aunque deberemos haber el

esfuerzo de decir los números de forma clara. Todo ello, por supuesto, después de oír la señal pero atención con ella, por que es más bien corta.

Con el servidor, podemos obtener información personal como la situación de un trámite documentario o de la preinscripción de algún curso o de las calificaciones en las asignaturas del año en curso si es que se tratase de una Institución que imparte educación. Al elegir este tipo de opciones, se nos solicitará que digamos, o pulsemos, los números de nuestro DNI. Solo así accederemos a esa información, cabe mencionar que el número o código que se solicite será designado por la política de la empresa donde se instale el servidor. La mejor forma de conocer la capacidad del servidor es probándolo.

Actualmente, la Universidad Politécnica de España está desarrollando una implementación de este servicio, en donde toda la información se encuentra dividida en cuatro bloques, los cuales son:

- 1) Información General: Al elegir esta opción podremos conseguir una primera información sobre becas, precios públicos, colegios mayores y residencias y transportes universitarios.
- 2) Titulaciones y Planes de Estudio: Donde se podrá conocer los estudios que pueden realizarse en la universidad, junto con las direcciones y teléfonos en donde podemos conseguir más información.
- 3) Modalidad Ingreso: Se comunicará los lugares a los que acudir para formalizar el ingreso y los plazos para realizarlo, en función de nuestra situación personal. Es decir si se tiene un grado académico anterior. Información Personal: la información aportada ya no es genérica. Si se opta por esta opción se podrá saber la situación en la que se encuentra nuestra preinscripción, o bien las calificaciones obtenidas hasta el momento en las asignaturas del año en curso. En este caso, para realizar las consultas necesitaremos decirle al servidor el número de nuestro DNI, o algún código que nos identifique como tales.

Ventajas

El servidor de voz se pone en marcha como un sistema que puede ayudar a mejorar el servicio de atención al público. Aunque determinadas consultas necesitan

una atención personalizada, y el servidor no conseguirá resolverlas, aporta una información que es solicitada como una mayoría de consultas.

Existen dos características que lo hacen interesante. Por un lado el servicio Universal, es decir, la conexión entre el usuario y la información que se consigue mediante el teléfono, un instrumento totalmente extendido.

Por otro lado, la información se recoge directamente de la base de datos del departamento u oficina de Ordenación de Datos, que se debe encontrar actualizándose constantemente. Además, el servidor ha aportado mejoras inmediatas en el servicio de atención al público:

La central telefónica se bloqueaba, puesto que las llamadas no atendidas, retornaban a ésta. El servidor ha rebajado la presión telefónica.

Se consigue ampliar y flexibilizar el horario de atención a las 24 horas del día.

El número de llamadas solicitando atención individualizada disminuye, aumentando con ello la calidad en la atención tanto de llamadas genéricas como concretas.

Es un servicio abierto a modificaciones en la información aportada y, lo más importante, con posibilidades de poder incrementarla de forma rápida y sencilla. De hecho, se espera aumentar sus prestaciones añadiendo nuevos apartados a los ya existentes.

Tecnología de los Servidores de Voz

A continuación se describen algunos de los tipos de Servidores desarrollados para las diferentes aplicaciones a través de sus diferentes módulos, los cuales son: Marshal Server (MS).- Es una implementación, del Protocolo de Iniciación de la Sesión (SIP) del servidor proxy y actúa como el punto inicial de contacto para todas las señales del SIP que incorporen el sistema Vocal. El MS, proporciona funciones de autenticación, expedición y facturación.

Redirect Server (RS).- Es la implementación, combinada del SIP con los servidores redireccionados de registro, y, de localización. Los almacenes de RS entra en

contacto con los datos de las características registrados, y, en el momento de marcar permite el encaminamiento para las llamadas fuera de la red.

Call Detail Record Server (CDR).- Es aquel, que recibe datos de la llamada desde el servidor Marshal, y, tiene un formato que puede ser transmitido a los sistemas de facturación de terceros.

Network Manager.- Es el encargado, de red que provee al administrador la capacidad de supervisar el sistema con el Protocolo SNMP (Simple Network Management Protocol).

Voice Mail Server.- Proporciona mensajería unificada, para que los mensajes del correo de voz puedan ser distribuidos.

Feature Server.- Es otra implementación, del SIP del servidor proxy. Estos servidores, son transcritos en el lenguaje del proceso de llamada (CPL), y, proporcionan características del sistema básico tales como llamadas en espera, y, bloqueo de llamadas.

Provisioning Server (PS).- El servidor, del aprovisionamiento almacena expedientes de datos sobre cada módulo del usuario, y, del servidor del sistema, y, distribuye esta información a través del sistema vía un modelo de suscripción-notificación. El PS, proporciona al usuario un interfaz entre el gráfico y la web-capacitada (GUI) que permite a los técnicos y administradores del sistema manejar el sistema.

Policy Server.- La política del servidor, ha sido diseñado para utilizar el servicio común de política abierta, para proporcionar la calidad de servicio (QoS), reservando el ancho de banda para llamadas o para segmentos de llamadas que son transmitidas sobre Internet. La política del servidor, también es capaz de usar Protocolo de Establecimiento Abierto (OSP) para interactuar con las cámaras de compensación para reservar el ancho de banda, y, autorizar el uso de una red para llamadas de la red interna.

Heartbeat Server:- Este servidor, supervisa el flujo de las señales de pulsación emitidas por los otros servidores. Esta información, ayuda al administrador del sistema a conocer si los módulos del servidor están por encima o por debajo.

Aplicaciones de la Tecnología y Empresas Proveedoras

En cuanto a la aplicación se puede definir como un conjunto de instrucciones que se irán ejecutando en forma secuencial. El lenguaje diseñado, ofrece sentencias de gestión de la línea telefónica (como colgar, descolgar, marcar o esperar llamada),

sentencias de voz (reconocimiento, síntesis en español, reproducción y grabación), de acceso de base de datos (abrir/cerrar bases de datos y ejecutar consultas), correo electrónico (enviar e-mail), de gestión de directorios, y, archivos, de manejo de cadenas, y, operaciones aritméticas básicas.

Seguidamente se brinda algunas aplicaciones con sus respectivas empresas proveedoras.

1. Reconocedor de Voz ND-URVI – NewData Real Time, la librería ND-URVI ha sido desarrollada como un servicio para el entorno CT Access de Natural Microsystems. ND-URVI, permite el desarrollo de aplicaciones avanzadas de integración de la telefonía, y, los ordenadores mediante la utilización de sistemas reconocimiento de voz, y, conversión texto-a-voz en castellano y catalán.
2. El centro del vocal servidor, el servicio vocal permite entregar la información exacta que se desea comunicar a los clientes anticipados por teléfono o por fax de una manera eficiente y de uso fácil. TELL ME, tiene una sociedad estratégica con FCR, France Telecom. And Ring.
3. Vox Populi, (Servidor Vocal Interactivo) es el minorista aprobado en Lyon del Software de CT-Studio Envox. CT-Studio, es un software americano que es simplemente, el de más alcance, el de uso más fácil, y, las más económicas para la interconexión de la telefonía/computador (CTI). Con una PC con multimedia, el servidor vocal interactivo de VoxPhone ofrece un número de ventajas tales como: estar disponible 24 horas al día, inmediato acceso, posibilidad de hablar en varios idiomas, posibilidad de enviar en forma automática fax y E-mail, reducción de costo de personal, y, brindar un mejor servicio al cliente.
4. VoicePhone: servidor vocal interactivo para números telefónicos, es un sistema de diálogo, diseñado para reconocer números de teléfono sobre la red de teléfono público. La primera, versión se ha utilizado en el IDIAP (Institut Dalle Molle d' Intelligence Artificielle Perceptive).
5. Cisco Media Convergence Server 7835 (MCS-7835), es una plataforma de servidor de alta disponibilidad para la arquitectura para voz, vídeo y datos integrados (Architecture for Óbice, Video and Integrated Dart, AVVID) de Cisco. Cisco Call Manager, (CCM) es el software de procesamiento de llamadas que forma de la red Cisco y el software Cisco uOne se comunica a

través de varias LAN y WAN haciendo uso de voz a través de IP (VoIP). La industria de los mensajes de voz, a pasado de ser una infraestructura propia, cerrada, y, de elevado costo, a convertirse en un sistema abierto, distribuido y basado en estándares, con una relación precio rendimiento superior. Cisco Systems y la aplicación Cisco uOne constituyen la vanguardia de esta evolución. La distribución de mensajes de voz a través de IP reduce los gastos generales en infraestructuras, reduce los costos de capital y funcionamiento, abriendo el entorno a espectaculares innovaciones en las aplicaciones de telefonía.

Características de Diseño

Entre los diferentes tipos de servidores desarrollados y de acuerdo a las investigaciones efectuadas de acuerdo a las empresas proveedoras de estos servicios podremos mencionar algunas características de diseño que se podrían implementar con productos CISCO:

Servidor

Procesador Intel Pentium III a 733 Mhz.

256 Kb de memoria caché secundaria.

512 MB de memoria SDRAM registrada de ECC a 133Mhz.

Tarjeta de Interfaz de voz Fast Ethernet 10/100 Tx.

Controlador Ultra Wide SCSI-3 de doble canal integrado.

Dispositivos duales Ultra2 SCSI conectables en activida de 18,2 GB.

Disquetera de 1,44 MB.

CD ROM IDE de alta velocidad preinstalado.

Fuente de Alimentación de 275 vatios redundante conectable en actividad.

Requisitos de Alimentación

Rango de Tensión de Línea	de 90 a 132 VCA, de 180 a 265 VCA
Tensión de línea nominal	de 100 a 120 VCA, de 220 a 240 VCA
Tensión de entrada	432 W
Frecuencia de línea	de 50 a 60 Hz
Dimensiones	13,1 x 48,3 x 62,5 cm
Peso	25 Kg sin discos duros

Disquetera de 1,44 MB

Tamaño de discos	3,5 pulgadas
------------------	--------------

Capacidad de lectura y escritura	1,44 MB/ 720KB (Alta/Baja densidad)
Unidad compatible	Una
Velocidad de Transferencia (alta/baja)	500/ 250 Kbps
Bytes/ Sector	512
Sectores/ Pistas (alto/bajo)	18/ 9

Tiempo de Acceso

Pista a pista (alto/bajo)	3/ 6 ms
Promedio (alta/baja)	94/ 169 ms
Tiempo de asentamiento	15 ms
Promedio de latencia	100 ms
Cabezas de lectura y escritura	Dos

Discos Duros Ultra2 Wide SCSI conectables en actividad

Capacidad	18.209,3 MB
Interfaz	Ultra2 Wide SCSI
Velocidad de Transferencia síncrona	80 MBps.

Tiempo de Búsqueda

Pista individual	0,8 ms
Promedio	7 ms
Full Stroke	15 ms

Unidad de CD ROM IDE 24X

Discos Utilizables	CD ROM (modos 1 y 2) CD-DA, CD-XA modo 2, format 1,2
Capacidad	550 MB (modo 1, 12 cm) 640 MB (modo 2, 12 cm)
Tiempo de Acceso	menor de 140 ms
Full Stroke	menor de 300 ms
Velocidad de Transferencia	150 KBps sostenida
Ráfaga	de 2.100 a 4.800 KBps
Tiempo de arranque	menor de 10 seg.
Tiempo de parada	menor de 5 seg.

Adaptador Dual Channel Ultra Wide SCSI-3 integrado

Unidades Compatibles	Hasta 6 Discos Duros SCSI
Método de Transferencia de Datos	Bus maestro PCI de 32 bits
Velocidad de Transferencia	80 MBps por canal SCSI

Velocidad de Transferencia por PCI	133 MBps
Terminación SCSI	Terminación activa
Conectores SCSI	1 externo, 2 internos (68 pines)

Controlador UTP PCI 10/100 (integrado)

Interfaz de Red	10 Base T /100 Base TX
Método de Transferencia de Datos	Bus maestro PCI de 32 bits

Velocidad de Transferencia de Red

10 Base T (semiduplex)	10 Mbps
10 Base T (duplex completo)	20 Mbps
100 Base TX (semiduplex)	100 Mbps
100 Base TX (duplex completo)	200 Mbps
Conector	RJ-45

Soporte para cable

10 Base T	UTP Categorías 3,4 o 5 hasta 100 m
100 Base TX	UTP Categoría 5 hasta 100 m.

A continuación se desarrolla un diagrama del diseño del servidor de voz con tecnología "CISCO". Como se puede apreciar, el esquema representa a un servidor que va a recibir simultáneamente 24 líneas a la vez, que serán atendidas por una central con su contestadora electrónica, la cual procederá a pasar la comunicación al servidor quien tendrá como misión analizar el contenido de acuerdo a su base de datos y procesarlo, para luego derivar la comunicación a quien corresponda a la brevedad posible (ver Figura 2.3.3.1).

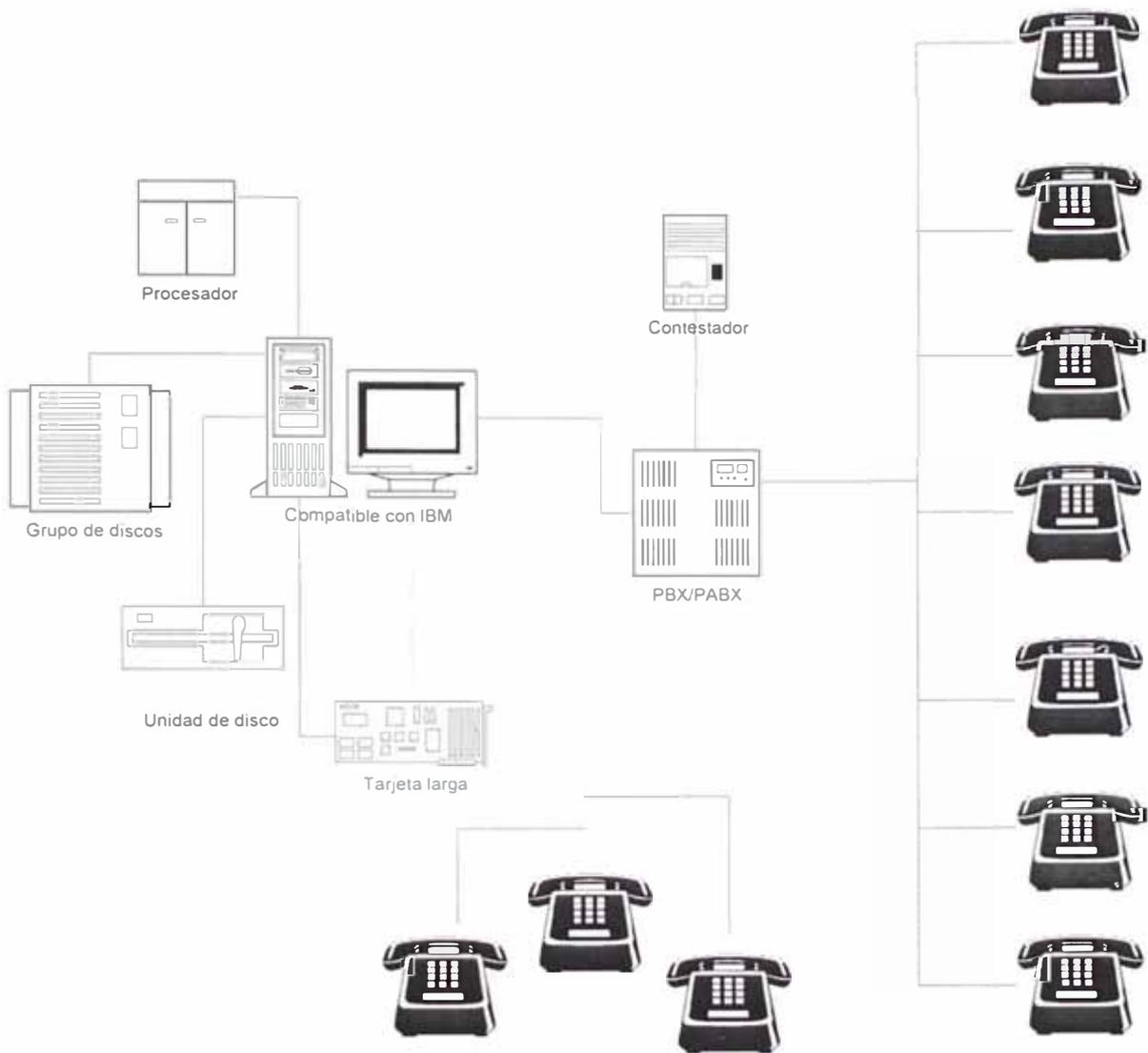


Figura 2.3.3.1 Diagrama de diseño de un Servidor Vocal con tecnología "CISCO"

2.3.4 Servidores De Imagen

Imagen

Las imágenes que aparecen normalmente en los programas de computador suelen ser dibujos o imágenes reales digitalizadas. Las primeras han sido realizadas utilizando alguna técnica de diseño por computadora, como son los programas de diseño, los cuales se denominan creaciones, dado que no se ha partido de algo ya existente para plasmarlas a la computadora. Esto no ocurre con las imágenes digitalizadas, pues se trata de una imagen real ya existente que es transformada a un formato comprensible por la computadora.

Una forma técnica de explicar de lo que es una imagen digital es imaginando cómo se digitaliza una imagen convencional, una diapositiva en blanco y negro. Para ello supongamos que a la diapositiva se le superpone una retícula cuadrículada y que, con un aparato, denominado fotómetro, se mide la cantidad de luz que pasa a través de la cuadrícula; se mide utilizando una escala de intensidad tal que estas medidas sean números enteros (8 bits en la mayoría de los casos). Estos números ordenados de igual forma que las cuadrículas, constituyen una matriz que es la imagen en forma digital. Esto es lo que básicamente realiza un digitalizador o escaner.

En el caso de que la diapositiva fuese en color, realizaría la anterior operación tres veces, colocando respectivamente un filtro rojo, uno verde y otro azul. Se obtienen así tres matrices, que son las componentes roja, verde y azul de la imagen digital, la cual es en este caso una imagen multiespectral. Cada punto de una imagen digital, es decir la intensidad de cada una de las cuadrículas en que se ha dividido la imagen original se denomina píxel o pel (apócope de picture element).

Una imagen digital, por tanto, es una matriz de puntos o píxeles que vienen caracterizados por su resolución espacial y su profundidad espectral.

Por consiguiente, una imagen digital es el conjunto discreto y organizado de todos los valores numéricos de intensidad lumínica posicionados en un plano de referencia. Existen dos tipos de imágenes digitales:

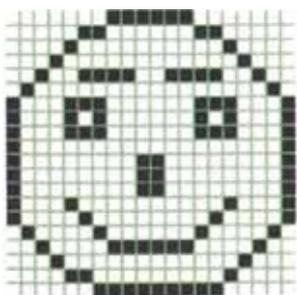
- Imagen raster o bitmap: los datos están organizados según sus coordenadas (x,y).
- Imagen vectorial: están construidas a partir de líneas, arcos y círculos, y soportadas por una fórmula matemática.

Las imágenes del primer tipo son más utilizadas en el tratamiento de imágenes aplicado a documentación; las de segundo tipo se utilizan fundamentalmente en el proceso de imágenes de radares, aplicaciones gráficas (CAD), planos y visualización de datos arquitectónicos.

Los mapas de bits se muestran en pantalla de manera mas rápida que las imágenes vectoriales al no tener que dibujarse en pantalla; sin embargo, necesitan mayor espacio en disco. Existen programas que transforman las imágenes de mapa de bits en imágenes vectoriales (proceso de vectorización); aunque la tecnología actual considera el tema de estos conversores como un problema abierto con soluciones parciales que deben personalizarse para cada caso en particular.

Las imágenes de mapa de bits

Las imágenes se pueden representar, mediante retículas de celdillas a las que se asigna valores. Este modo de "pintar", es la base de todas las imágenes impresas y de buena parte de las digitales (ver figura 2.3.4.1).



Una imagen de 20 × 20 píxeles (400). Podría medir 2 cm. o un campo de futbol.

1	1	1	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0	0	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	0	0	0	0	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	1	0	1	1	1	1	0	1	1
1	0	0	0	1	1	0	0	0	1
1	1	1	1	1	1	1	1	1	1

Como se exhibe en esta imagen bitonal, a cada píxel se le asigna un valor tonal, en este ejemplo 0 para el negro y 1 para el blanco

Figura 2.3.4.1 Imágenes de mapa de bits

Las imágenes digitales en dos dimensiones se realizan creando una retícula de cuatro lados, iguales de dos a dos (ancho y alto, siempre en ese orden, rectángulo, cuadrado). Hoy día no se puede hacer de otra manera (las siluetas o formas desiguales son siempre un enmascaramiento de imágenes rectangulares o cuadradas).

Cada una de las celdillas de dicha retícula se llama **píxel**, a pesar de ser una unidad de medida, es un concepto inmaterial que no tiene una medida concreta. No podemos decir si un píxel mide 1 cm. o 1 km. En principio, es solamente una medida de división en celdillas. De este modo, se puede hablar de una imagen que tenga 200×100 píxeles sin saber que tamaño real y físico tiene. Lo único que se sabe es que se ha dividido en 20.000 celdillas. Sin embargo, cuando se le asigna a esa imagen una resolución, entonces sí se sabe qué tamaño tiene esa imagen. Por ejemplo, si se dice que una imagen tiene 100 píxeles por pulgada, querrá decir que en cada 2,54 cm. habrá 100 celdillas, con lo que cada píxel equivaldrá a 2,54 mm. Si se dijera que esa imagen tiene una resolución de 1 píxel por pulgada, lo que se sabría es que ahora esa celdilla tomaría el valor de 2,54 cm.

Todo ello significa, que el píxel es sólo una unidad de división sin un tamaño real concreto. Sólo cuando se asigna una resolución a la imagen de la que se habla se está dando un tamaño concreto al píxel.

Existen imágenes de resolución alta e imágenes de resolución baja. A mayor resolución mayor nitidez del dibujo y mejor se reflejo de los detalles. Sin embargo, se debe tener presente que cualquier resolución que supere a la que el dispositivo de salida tenga (pantalla, impresora, etc...), no hace más que sobrecargar el sistema y hacer mas lento el trabajo.

Tipos de imágenes de mapa de bits

De lo anteriormente mencionado, cabe indicar que una forma de clasificar las imágenes de mapa de bits es saber cuánta información se asigna a cada píxel. Un píxel puede cobrar muchos valores (blanco y negro, grises, color, etc...), por lo que es necesario tomar en cuenta para la clasificación de las imágenes de mapa de bits.

1. **Imágenes de 1 bit por píxel** . En este tipo de imágenes cada celdilla (píxel) sólo puede tener uno de dos valores: Uno o cero. Como basta 1 bit para definir esa alternativa, se les llama "imágenes de 1 bit" (también se les llama "imágenes de mapa de bits, de alto contraste, o de línea") ver figura 2.3.4.2.



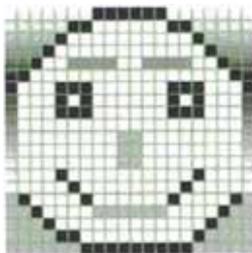
Una imagen de 20 × 20 píxeles (400). Podría medir 2 cm. o ser del tamaño de una cancha de fútbol. Los píxeles son sólo una división de la información que contiene.

Una imagen de 200 × 200 píxeles en este modo. La información es muy escasa para reproducir bien este tipo de imagen.



Figura 2.3.4.2 Imágenes de un bit por píxel

2. **Imágenes de escala de grises (8 bits por píxel)** . Cada píxel puede tener 256 valores diferentes (las 256 posibilidades combinatorias de un byte u octeto 2^8). Este es la forma de las imágenes digitales de blanco y negro "normales", aunque parezca increíble, en ellas sólo se distinguen hasta 256 tonos diferentes de gris (y no suelen aparecer todos a la vez), ver fig. 2.3.4.3.



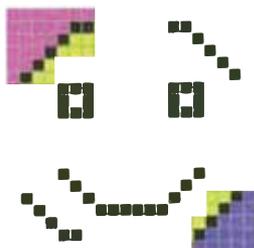
Una imagen de 20 × 20 píxeles (400) con 1 byte (8 bits) por píxel. Pesará 400 × 8 bits, es decir: 3.200 bits.

La imagen de 200 × 200 píxeles en escala de grises. La información es suficiente para reproducir fotografías en blanco y negro.



Figura 2.3.4.3 Imágenes de escala de grises

3. **Imágenes RGB o Lab (24 bits por píxel)** . Si se toma un píxel y se le asigna tres bytes, entonces se dispone de 24 bits en tres grupos de ocho, se puede "colorear" siguiendo el sistema de color de los monitores de televisión, que se basan en tres "canales" de luz de color (Rojo, Azul y Verde). De este modo se distingue hasta 16.777.216 millones de tonos de color (256 Rojo × 256 Azul × 256 Verde). En realidad, lo que se hace es superponer tres canales de luz, uno rojo, otro verde y otro azul cada uno con 256 posibilidades de tono, ver figura 2.3.4.4.



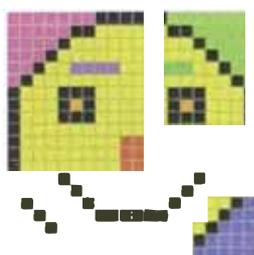
Una imagen de 20 × 20 píxeles (400) con 3 bytes (8 bits) por cada píxel. Pesará 400 × 8 × 3 bits, es decir: 9.600 bits.

La imagen de 200 × 200 píxeles en modo RGB, el tipo de color de las televisiones.



Figura 2.3.4.4 Imágenes RGB o Lab

4. **Imágenes CMYK (32 bits por píxel)** . Si a cada píxel se le asigna 4 bytes, entonces se puede representar, teóricamente, porque la representación máxima del color que la pantalla de una computadora puede hacer es la de imágenes RGB, ya que ese es el modo de reproducir el color de los monitores., los valores CMYK propios de la cuatricromía profesional (1 byte para el cian, otro para el magenta, otro para el amarillo y un cuarto para el negro), ver figura 2.3.4.5.



Una imagen de 20 × 20 píxeles (400) con 4 bytes (8 bits) por cada píxel. Pesará 400 × 8 × 4 bits, es decir: 12.800 bits.

La imagen de 200 × 200 píxeles en modo CMYK. Lo que ves es una representación RGB, no hay monitores CMYK.



Figura 2.3.4.5 Imágenes CMYK

5. **Imágenes en color de 8 bits o menos.** Es lo que se llama color indexado, lo que se hace es crear una tabla o índice de 256 colores y a cada uno de los posibles valores de un píxel se le asigna uno de ellos. Si la tabla se construye con menos posibilidades (16, por ejemplo), esa imagen no será un color indexado de 256 tonos sino uno de 16.

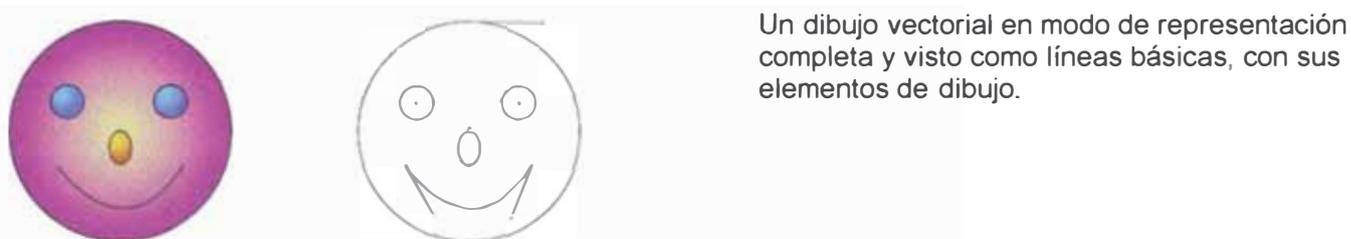
Las imágenes vectoriales

Una manera distinta de formar una imagen es la de hacerlo mediante operaciones matemáticas. Es decir, en lugar de trazar una retícula con miles o millones de puntos para trazar una línea, se da a la máquina unas coordenadas x_1 e y_1 se le ordena que trace una línea hasta otras coordenadas x_2 e y_2 . De esta manera se puede dibujar círculos, cuadrados, triángulos y miles de formas, sin entrar en detalles, se dice que esa es la base de los llamados dibujos vectoriales. Los programas de dibujo vectorial los suelen representar de dos maneras: Mediante representación completa (es decir, tal cual se imprimirán) y como líneas (es decir, sólo el esqueleto de las formas básicas, mucho menos pesado para el ordenador).

Los trazados (líneas curvas o rectas propias de un dibujo vectorial) se pueden modificar fácilmente, se almacenan en muy poco espacio y además son independientes de la resolución, ya que no dependen de una retícula dada,

basándose en que cualquier operación geométrica es multiplicable o divisible en su conjunto sin que eso afecte al aspecto del resultado, sino sólo a su tamaño final.

Las imágenes vectoriales de dos dimensiones suelen tener varias partes, sólo el contorno y el relleno serán visibles al imprimir lo demás son instrumentos de trabajo. La base de estas operaciones son las llamadas "Curvas Bezier", para mayor ilustración ver figura 2.3.4.6.

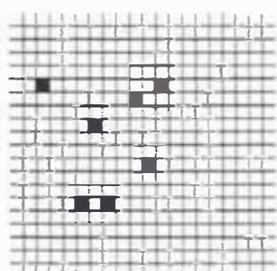


Un dibujo vectorial en modo de representación completa y visto como líneas básicas, con sus elementos de dibujo.

Figura 2.3.4.6 Imágenes vectoriales

Qué es la resolución

En la actualidad, las máquinas electrónicas destinadas a la impresión sólo tienen un sistema de imprimir: Dividen el espacio imprimible en una retícula de diminutas celdillas e imprimen unas sí y otras no, ver figura 2.3.4.7.



Siete puntos de impresión dentro de una retícula de 20 × 20 puntos de impresión. Si esta retícula tuviera 1 pulgada de lado, la resolución del aparato sería de 20 puntos por pulgada.

Figura 2.3.4.7 Resolución de imágenes

Al espacio mínimo imprimible de cada una de las celdillas de la retícula en las que las máquinas dividen el espacio se le denomina "**punto (de impresión)**", también llevan la misma denominación los fluidos que se aplican y los medios sobre los que se aplica, pero lo que no varía, por lo menos a comienzos del siglo XXI, es el hecho de que las máquinas sólo pueden imprimir un punto o no imprimirlo, pero no pueden "imprimirlo un poco", como sí lo haría un pincel o un lápiz manejado por un artista.

Se debe destacar que los aparatos a los que aquí se hace referencia son básicamente aparatos Post-Script, que es el sistema para la realización de documentos digitales predominante hoy día en las artes gráficas. Una máquina capaz de dividir un espacio dado en más celdillas que otra, hará que estas celdillas sean más pequeñas. El resultado de esto será que el dibujo que trace imprimiendo unas celdillas sí y otras no, será mucho más detallado.

El número de celdillas o unidades mínimas de impresión que una máquina es capaz de realizar como máximo en un espacio dado es lo que se llama " **resolución**". A mayor número de resolución, mayor nitidez de dibujo, ver figura 2.3.4.8



Figura 2.3.4.8 Resolución versus nitidez

Es importante resaltar que la resolución se suele medir en puntos por pulgadas (abreviado ppp) y que estas son **siempre** lineales, es decir, que están formadas por una fila de puntos de impresión colocados en línea, uno detrás de otro. Así, hablamos de una impresora con 300 puntos por pulgada (una pulgada equivale a unos 2,54 centímetros).

De hecho la resolución en puntos de impresión por pulgada cúbica de una filmadora de 2.400 ppp es de 5.760.000 puntos, la resolución por pulgada cúbica de una impresora de 600 ppp es de sólo 360.000 puntos, la diferencia es notable (por eso los fabricantes de impresoras han logrado imponer la medida lineal sin resaltar la palabra "lineal"). A cualquier sistema que se base en la división del espacio en una retícula, se le puede aplicar este concepto de "resolución". De hecho, los monitores tienen una resolución de 72 píxeles por pulgada en los aparatos Macintosh y 96 píxeles por pulgada en las PCs del sistema Windows.

Profundidad de Bits

La Profundidad de Bits es determinada por la cantidad de bits utilizados para definir cada píxel. Cuanto mayor sea la profundidad de bits, tanto mayor será la cantidad de tonos (escala de grises o color) que puedan ser representados. Las imágenes digitales se pueden producir en blanco y negro (en forma bitonal), a escala de grises o a color.

Una imagen bitonal está representada por píxeles que constan de 1 bit cada uno, que pueden representar dos tonos, utilizando los valores 0 para el negro y 1 para el blanco.

Una imagen a escala de grises está compuesta por píxeles representados por múltiples bits de información, que típicamente varían entre 2 a 8 bits o más.

Ejemplo: En una imagen de 2 bits, existen cuatro combinaciones posibles: 00, 01, 10 y 11. Si "00" representa el negro, y "11" representa el blanco, entonces "01" es igual a gris oscuro y "10" es igual a gris claro. La profundidad de bits es dos, pero la cantidad de tonos que pueden representarse es 2^2 ó 4. A 8 bits, pueden asignarse 256 (2^8) tonos diferentes a cada píxel.

Una imagen a color está típicamente representada por una profundidad de bits entre 8 y 24 o superior a ésta. En una imagen de 24 bits, los bits por lo general están divididos en tres grupos: 8 para el rojo, 8 para el verde, y 8 para el azul. Para representar otros colores se utilizan combinaciones de esos bits. Una imagen de 24 bits ofrece 16,7 millones (2^{24}) de valores de color. Cada vez más, los escáneres están capturando 10 bits o más por canal de color y por lo general imprimen a 8 bits para compensar el "ruido" del escáner y para presentar una imagen que se acerque en el mayor grado posible a la percepción humana.

Cálculos binarios para la cantidad de tonos representados por profundidades de bits comunes:

1 bit (2^1) = 2 tonos

2 bits (2^2) = 4 tonos

3 bits (2^3) = 8 tonos

4 bits (2^4) = 16 tonos

8 bits (2^8) = 256 tonos

16 bits (2¹⁶) = 65.536 tonos

24 bits (2²⁴) = 16,7 millones de tonos

Tipos de imagen

Atendiendo al conjunto de valores que puede tomar cada uno de los píxeles la imagen puede ser uno de los tipos siguientes:

- Binaria, de blanco y negro o monobanda. Su profundidad espectral es de 1 bit: blanco, representado por el 1 y negro, por el 0.
- De niveles de gris. Su profundidad espectral es de n bits que representan sucesivas gradaciones de intensidad luminosa que van del negro (valor 0) al blanco (valor máximo, que frecuentemente es 255 al venir cada píxel representado por un Byte). Es lo que en fotografía se denomina blanco y negro. Ejemplo: imágenes digitalizadas procedentes de placas de Rayos X con un elevado contenido de niveles de grises.
- Multiespectrales o multibanda. Corresponden a diferentes intervalos de radiación electromagnética. Las imágenes de color son un caso concreto de este tipo, es decir, imágenes de tres bandas que se corresponden con los colores primarios (rojo, verde y azul o RGB). Por ejemplo, las imágenes tomadas por cámaras y escáneres multiespectrales a bordo de satélites y aviones generan imágenes formadas por gran número de bandas (doce o más).

Formatos de ficheros de imágenes

Una vez que se ha generado una imagen se tiene que guardar de alguna manera, para poder utilizarla más tarde. La manera de guardar una imagen es grabarla en un archivo y posteriormente, cuando sea necesaria su utilización, se podrá volver a recuperar leyendo el contenido del archivo.

Esto, explicado así puede parecer sencillo, pero se complica ya que no existe un único formato para grabar imágenes, sino que existen infinidad de ellos debido principalmente a que cada casa comercial crea su propio formato totalmente diferente de los demás. La principal dificultad que engendra esta diversidad de formatos se produce a la hora de intentar comunicar dos sistemas diferentes, ya que

al usar formatos diferentes esta comunicación no se puede establecer; este problema se ha solventado incluyendo en los programas que utilizan imágenes un abanico de formatos, permitiendo la comunicación entre programas.

Pero no solamente la existencia de diversas casas de generación de software ha motivado la aparición de diversos formatos, sino que algunos de ellos han aparecido debido a su utilidad para hacer determinadas cosas que con los formatos existentes no se podían conseguir.

En general, un formato genérico de imagen contendrá la siguiente información:

- Cabecera: información del tamaño de la imagen, el número de bits por píxel, así como el tipo de compresión si existiese, el orden de los datos, etc.
- Paleta: si no contiene los colores directamente, deberá contener los índices sobre una paleta para permitir reconstruirla.
- Bitmap: los valores de los píxeles específicamente.

Aplicaciones de la Tecnología y Empresas Proveedoras.- Podemos mencionar las siguientes:

1. Servidor Geográfico del Mapa de Imagen de Iowa. Iowa State University, USDA – NRCS (Natural Resources Conservation Service).

El propósito de este, sitio, es evaluar métodos de distribuir datos digitales geográficamente referidos vía el World Wide Web, para el uso en sistemas de información geográficos, y, otros usos. Este sitio, permite que el usuario revise los datos, generando mosaicos de la imagen, permitiendo, que se pueda visualizar en tamaño, y, resolución que el usuario desee.

2. Interoperatividad para los servicios de imágenes digitales del orthophoto. Publicación, en la ingeniería photogrametric y la detección alejada. Juan D. Evans, M.I.T. Departamento de estudios urbanos y del planeamiento, 1999.

La diseminación de imágenes geoespacial digital vía un servicio en línea hace accesible a usuarios en el que se requiera banda ancha, en el que se automatiza las tareas de selección de imagen, extracción, georeferencia, etc. Este servicio, ofrece una arquitectura aerodinámica, modular, con un interfaz simple de pregunta que facilita su integración en un contexto de ámbito grande. Este prototipo, ilustra cómo la interfaz interoperables pueden ligar

- servicios en línea en una infraestructura global, que proporcione ortho-imágenes y la información geoespacial relacionada al pedido de cualquier cliente.
3. Servidor de Imagen de Borealis. Eric A. Meyer y Peter Murray. Universidad Occidental de De La Reserva del Caso.
Se desarrolla, en base a la necesidad, de crear un lugar central para almacenar, una gran cantidad de imágenes. Un servidor de Borealis, puede adquirir una imagen de cualquier servidor, y, entregar una imagen, que ha sido marcada por el agua. Se afirma, que este watermarking, es, para afirmar la propiedad de la imagen en una manera discreta.
 4. Servidor de Imagen SDK, se puede utilizar, con eficacia en los servidores de imagen, y, aplicaciones E-comercio, base de datos, multimedias, etc., como motor de gran alcance para la compresión de imagen, optimización de la gama de colores en las imágenes, conversiones de formato de imagen, exportación de web y otras funciones. Con el servidor SDK, de imagen, se puede agregar rápidamente funcionalidad superior de la optimización de la imagen, sus usos, del servidor web, y modificar el proceso de imagen de acuerdo a los requisitos particulares de internet orientado.

Diseño para un Servidor de Imágenes

Por experiencia propia en imágenes digitales, puedo decir que hay que tener en cuenta el tipo de imágenes que vamos a utilizar, hacia donde esta dirigido, etc.

Por ejemplo:

Si la imágenes que vamos a utilizar son imágenes de ropa, calzado, etc. Para una empresa que se dedica a la venta de ropa en Internet, pues tenemos que tener en cuenta la calidad de la foto que según el diseño podemos utilizar archivos con extensión JPG (JPEG), que es un formato de mucha calidad (existen de 256 colores, 24 bits, 32 bits) para poder exhibir el detalle del producto a vender, pero también podemos utilizar el formato GIF (existe en 256 colores, 24 bits, soporta colores indexados y transparencias) el cual tiene un formato especial llamado GIF animado. Y como está dirigido a ser mostrado en una página web, debemos de tener en cuenta que la resolución máxima en la web es 72 ppp (pixels por pulgada o ppi) si le

damos una resolución mayor no se vería la diferencia y lo obtendríamos sería una imagen mucho mas pesada y mas difícil de procesar.

Pero si se utiliza un Servidor de Imágenes dirigido hacia imágenes satelitales, estamos hablando de imágenes muy grandes en tamaño, de calidad de resolución alta y por ende muy pesadas, en este caso utilizaríamos el formato JPG.

Entonces si se desea tener especificaciones de hardware para un servidor web (dirigido a imágenes satelitales) tendríamos que tener en cuenta lo siguiente:

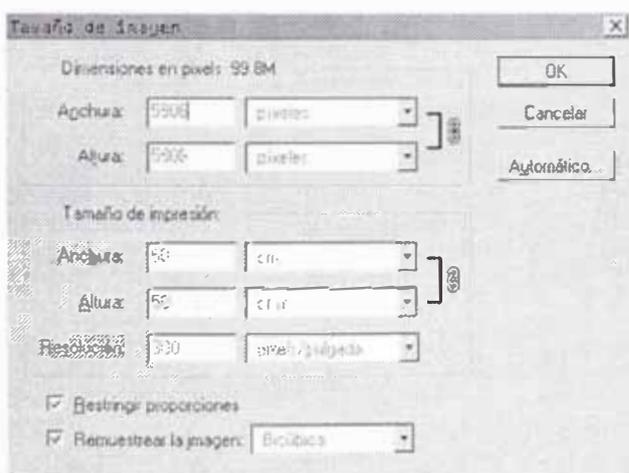
No solo maneja imágenes, sino, que también maneja texto (para la descripción de cada fotografía como: lugar, la hora, fecha, descripción del lugar, etc.)

Que se catalogan los tipo de imágenes satelitales como imágenes visibles, infrarrojas que a su vez pueden ser fotos climatologicas, geograficas, etc.

Las imágenes son de 50 cm² como mínimo (según Universidad Estatal de San Francisco (SFSU).

La resolución es de 300 ppp como mínimo.

Teniendo en cuenta lo antes mencionado tendríamos los siguientes resultados, como que el tamaño de una imagen satelital con requerimientos mínimos pesa 99.8 Mb, el alto y el ancho de dicha imagen es de 5906 pixeles.



Suponiendo que su tamaño o peso final de la imagen con su respectiva descripción y clasificación llegue a ser 101 Mb, podríamos deducir que en un disco de 1 Gb. Solo se podrán almacenar 10 imágenes como el de la figura 2.3.4.9, así que tendríamos tener en cuenta la cantidad de imágenes con la que trabajaríamos.

Figura 2.3.4.9 Tamaño de imagen

Por lo tanto se necesita una capacidad de disco duro que se acerque al orden del TeraByte, Por información obtenida en las revistas "Computer Shopper" y "Inform" de Compaq, podríamos tener un servidor con:

Servidor Proliant Compaq

10 Discos duros de 100 Gb. 15000RPM Ultra 160 SCSI

Procesador Pentium IV 2Ghz

4 Gb DDR SDRAM (PC-2100) memoria RAM

Es interesante tomar en cuenta lo siguiente:

Nota1: Los servidores de la serie PROLIANT de Compaq, son servidores web, que actualmente se están actualizando para soportar Pentium IV, también se podría utilizar la serie TaskSmart N-Series de Compaq

Nota2: Sobre la posibilidad de utilizar herramientas de tratamiento de imágenes como el Macromedia Freehand 9 o el Corel Draw 10, los cuales pueden vectorizar imágenes, no sería recomendable para este tipo de trabajos (imágenes satelitales) ya que se pierde mucha resolución. El diagrama de un servidor de imagen se muestra en la Figura 2.3.4.10.

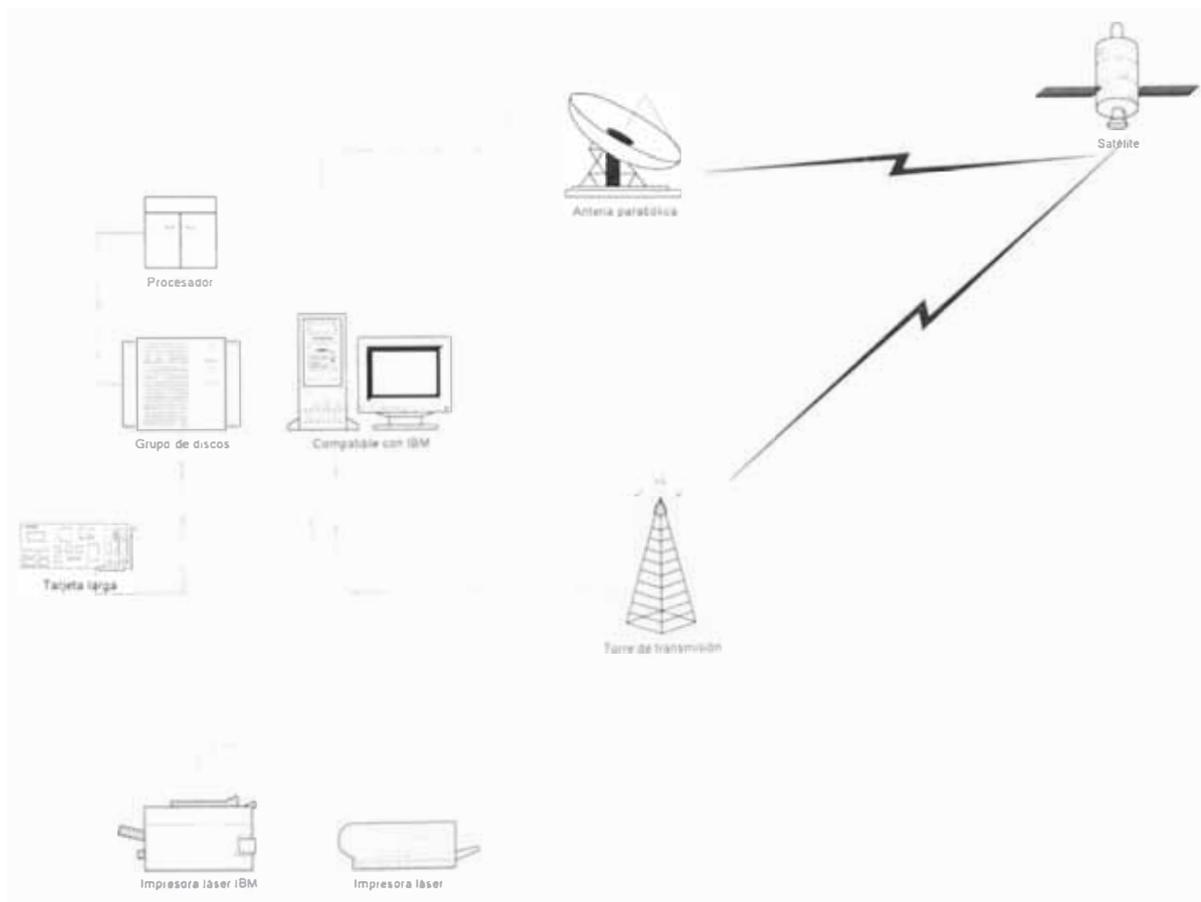


Figura 2.3.4.10 Diagrama de un Servidor de Imagen

Capítulo 3

Infraestructura de una Intranet

En este capítulo se describen algunos escenarios de infraestructura de Intranet, entendiéndose por infraestructura a la determinación de los procesos, las personas y las políticas de la institución que tienen que ver con la Intranet, tal como se detalla en los párrafos siguientes.

3.1 Procesos a Tomar en Cuenta en una Intranet

Cuando una organización determina desarrollar una Intranet debe de considerar dos procesos fundamentales: el proceso de convencimiento a la alta dirección y el proceso de planeación.

Para el proceso de convencimiento al alto mando de La Marina de Guerra del Perú para adquirir la tecnología de Intranet, se propone cuál es el objetivo y cómo funcionaría al implementarse ésta, utilizando para ello la tecnología existente mediante el uso racional de los equipos, de manera que no se incurra en mayores costos para la institución. Como resultado de su implementación la Intranet Naval va a mejorar el flujo de información entre las diferentes dependencias integrándolos y obteniendo información en tiempo real para la toma de decisiones beneficiando al cumplimiento de la misión en forma más eficiente.

El proceso de planeación de la intranet requiere analizar la organización de la institución así como las funciones que se realizan dentro de ella. La figura 3.1 muestra la estructura organizacional de la Marina. Es necesario mencionar que dicha estructura se presenta en forma general y no en forma detallada por su carácter reservado.

3.2 Recursos Humanos de la Intranet

Una vez que se define ciertos procesos o tareas, es necesario tomar en cuenta qué aptitudes son necesarias para crear una intranet, de manera que permita seleccionar el personal idóneo para el desarrollo de una Intranet. Este personal debe

ser aquel que conceptualice la Intranet más allá de cables, páginas web estáticas y la sobrecarga de información, tal vez sea una persona o un grupo de personas quienes la desarrollen, pero es necesario que en cualquiera de los dos casos el personal posea un mínimo de habilidades tales como: creación de archivos HTML, Scripts CGI, JavaScript o VBScript, tenga experiencia en configuración de Base de datos externas, desarrollo de interfaces de usuario, prueba de facilidad de uso, etc.

Cuando es un equipo grande quien desarrolle una Intranet, es importante obtener una cuidadosa mezcla de habilidades, aptitudes y experiencia para asegurar el éxito. Felizmente la Marina de Guerra del Perú cuenta con personal especializado por contar con experiencia en el manejo de la WAN Naval y que laboran en el centro de informática de los principales nodos de la WAN, por lo que en principio no habría mayor problema excepto para los casos que se requieran mayor especialización.

3.3 Políticas de la Institución para con la Intranet

En el diseño propuesto se ha tomado en cuenta las políticas que la institución debe considerar, estas políticas de contenido, diseño y seguridad son las que a continuación se detallan.

La política de contenido se refiere a las normas relacionadas a la cantidad, calidad y tipo de información que debe contener la Intranet Naval. Así mismo, tal política debe contemplar las futuras aplicaciones y necesidades de los usuarios manteniendo una retroalimentación dinámica. En base al resultado del análisis de las funciones y requerimientos de la institución se propone la información que va a contener el Diseño de la Intranet propuesta para la institución, en mayor detalle se presenta el Capítulo 4 del presente trabajo.

La Política de diseño esta referido en la apariencia común para facilitar el acceso a la información y agrupando conceptos similares, de manera que se brinde una consistencia y facilidad de navegación.

La Política de seguridad y de uso esta orientada a la responsabilidad, en este caso la responsabilidad directa recae a la Dirección de Telemática en lo referente a ejecución y verificación, este órgano se encuentra ubicado en el nodo central de la WAN Naval.

Capítulo 4

Diseño de la Intranet Naval

4.1 Metodología de Diseño

Para iniciar el diseño de la Intranet, es importante definir el tipo de modelo a emplear. El modelo de una Intranet puede ser centralizado o descentralizado [4]. En un modelo centralizado cada organización individual tiene su propia intranet, y se suscribe a la página principal de la intranet donde se proporciona información y herramientas comunes desde un grupo central. El modelo descentralizado proporciona más flexibilidad y acceso a la información de los expertos desde la fuente. En este modelo descentralizado, las Intranets separadas pueden operar mejor manejando su flujo de trabajo y sus procesos de negocios a su propio nivel. Se debe recalcar que lo que se centraliza es la arquitectura, tal como se muestra en la figura 4.1:

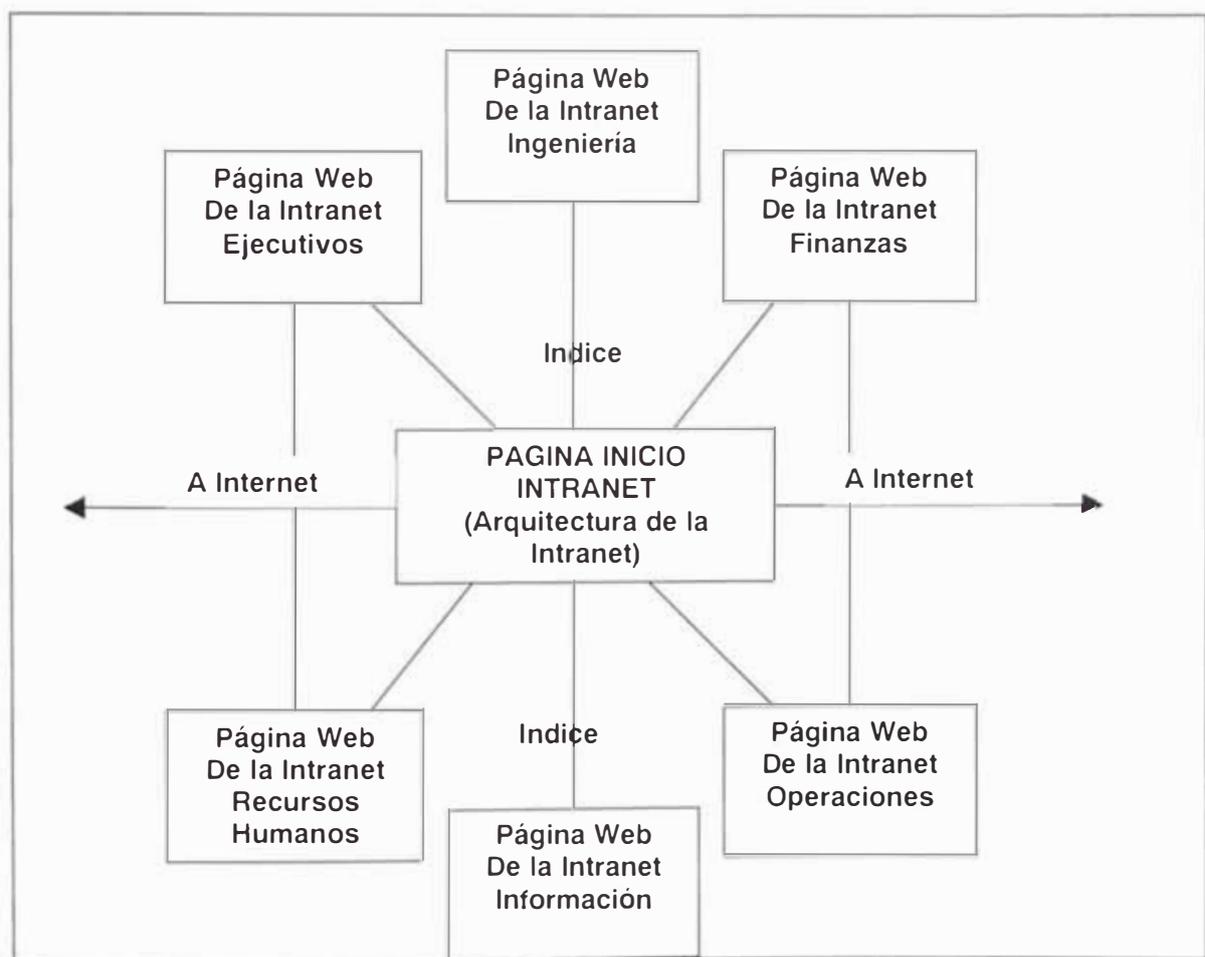


Figura 4.1: Modelo descentralizado, con arquitectura y página web central de Intranet.

En el diseño propuesto se conceptualiza a la Intranet orgánica, esto significa pensar en un modelo descentralizado y distribuido, donde cada función, cada grupo y cada parte única de la Intranet se desarrolla en su propio servidor y es mantenido por el personal encargado de elaborar el contenido. Esto incluye operaciones financieras, legales, administrativas, etc. las cuales se encuentran almacenadas en un servidor único. Incluso, la administración de la seguridad y el acceso de conexión están dedicadas a un solo servidor. Todos los demás componentes se interconectan con tecnología Web en red.

Como el desarrollo del contenido es descentralizado, significa que cada grupo es responsable de la cantidad y calidad de su información; de su creación, administración y mantenimiento y de su envío a la Web centralizada para su ubicación dentro de la institución.

4.2 Estructura del Diseño de la Intranet Naval

Para iniciar el diseño de la Intranet Naval se toma en cuenta un elemento importante que es el analizar los procedimientos organizacionales de la Institución, con el propósito de determinar el/los tipo(s) de información que se maneja en la institución. De este análisis, se determina que se manejan diferentes tipos de información, por lo que se cree conveniente clasificarlas en tres categorías: Técnico, Administrativo y Operacional. Esta categorización se realiza con la finalidad de estandarizar el manejo de la información dentro de la página principal a diseñarse, para que sirva como fuente de información fundamental para los usuarios.

Para el diseño de la Intranet Naval se ha considerado tres estructuras básicas que son la Página Inicial o Central, el Mapa de sitio por niveles y Cartografía del sitio web [1], tal como se describe a continuación.

4.2.1 La página Central

Contiene la máxima información disponible en forma ordenada y accesible, permitiendo mostrar información importante, en su presentación se toma en cuenta los colores que caracterizan al tipo de información que maneja la institución.

Esta página contiene las siguientes partes: menú de barras, pantalla de mensajes, descripción de accesos y páginas auxiliares (para mayor detalle ver la figura 4.1.1)

Menú de Barras.- este menú de barras está conformada por íconos en el que se detalla la clasificación o agrupación de la información, siendo estas Administrativas, Técnicas y Operacionales. Al presionar alguno de los íconos, debe aparecer en el margen izquierdo el tipo de información por clasificación o agrupación, tales como: noticias, servicios, grupos de trabajo, asuntos, dependencias, documentos publicaciones, entre otros.

Pantalla de mensajes.- Es una pequeña ventana dinámica en la cual se brinda noticias diarias de interés general tales como aniversarios, ceremonias, efemérides, etc.

Descripción de accesos.- En esta ventana se detalla el contenido de la información de cada agrupación o clasificación de la información.

Páginas auxiliares.- Diseñadas para información de orientación general, en las cuales se incluyen las salidas tanto a Internet, al correo electrónico a través de la WAN Naval, y hacia algunos directorios. También presenta información de interés general, como por ejemplo actividades en dependencias, novedades, etc.

4.2.2 Mapa de Sitio por Niveles

El Mapa de Sitio por niveles está conformada por los siguientes niveles: el nivel de la página de inicio de la intranet, el nivel de los índices o de navegación, el nivel de contenido y el nivel de almacén de datos (ver figura 4.2.2.1).

Página de inicio Intranet:- La página de inicio de la Intranet representa el centro comunitario de la institución, es el espacio principal para dar énfasis a la información importante y a la navegación para la Intranet. Su estructura se diseñó en el punto 4.2.1.

Índices y Navegación.- Los índices y navegación alberga a todas las páginas de índices y define lógicamente la estructura de las diversas funciones de la institución

Nivel de Contenido.- El nivel de contenido es un sitio Web especializado que brinda información específica. En este nivel interactúan los componentes de la página principal descritos en el punto 4.2.1. Es en este nivel de contenido que la información al ser compartida por las diferentes oficinas cambia de acuerdo al uso;

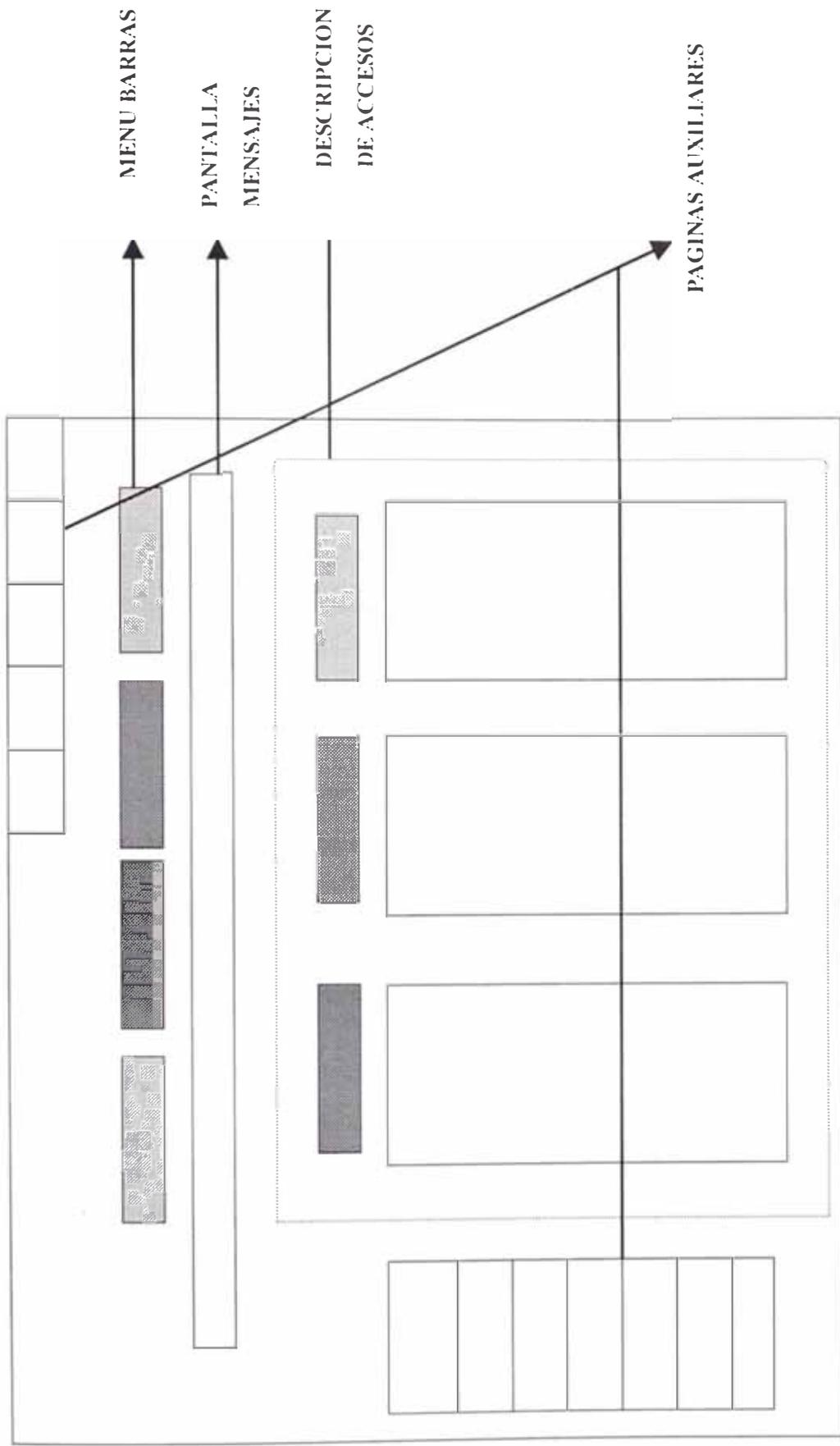


Figura 4.1.1 Estructura de la Página Central de la Intranet

PAGINA PRINCIPAL

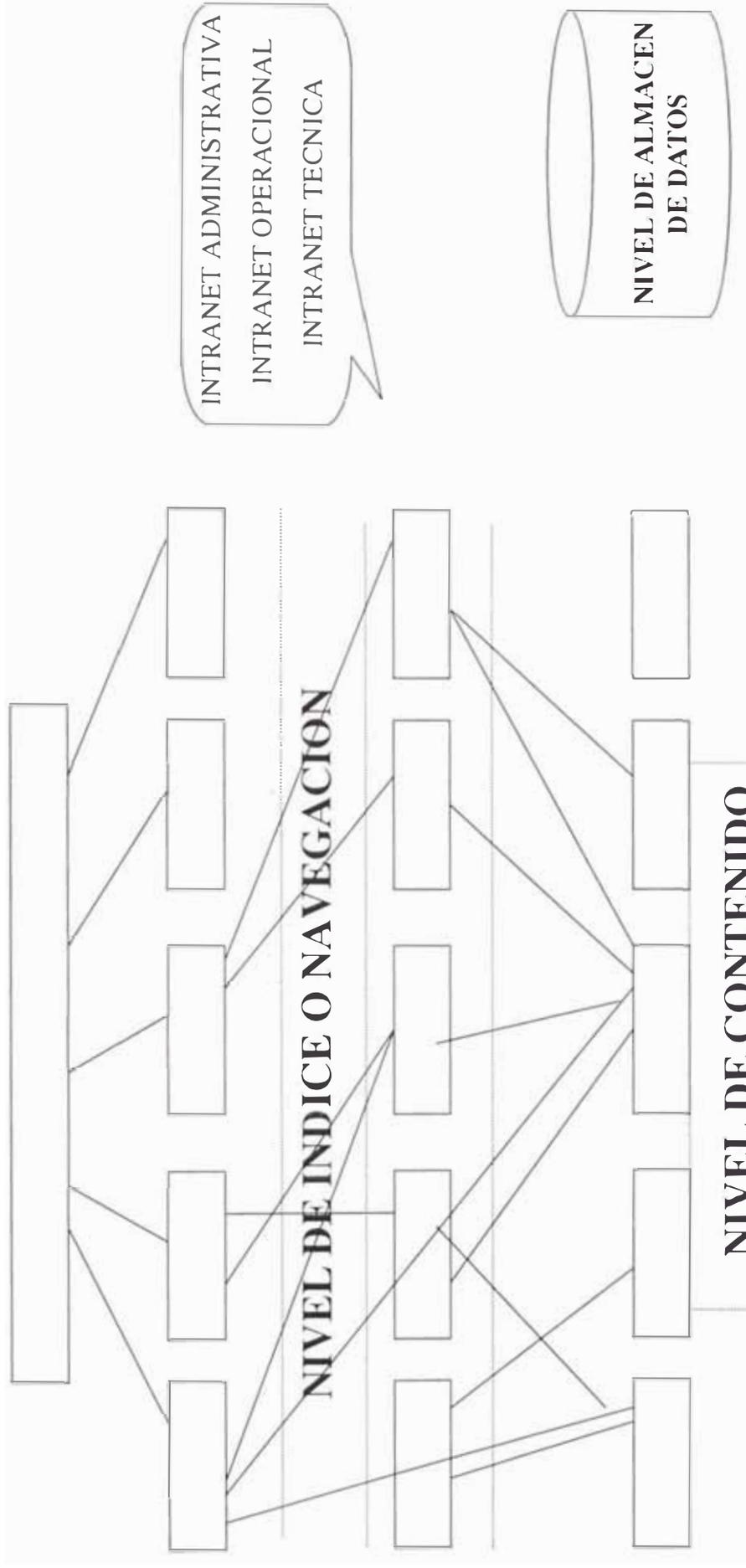


Figura 4.2.2.1 Mapa de Sitio por niveles de la Intranet Naval

es decir, una información técnica una vez procesada pasa a ser una información operacional o administrativa. Seguidamente, se detalla el contenido de los accesos de información a los tres niveles: Administrativo, Técnico y Operacional

Nivel Administrativo.- Está integrada por información que va a ser proporcionada por todas las oficinas.

El nivel administrativo, esta clasificada en seis subniveles que son los siguientes:

Noticias: integrado por información de interés general tales como mensajes circulares, órdenes generales (permanentes y/o transitorias).

- Servicios: integrado por información que se proporciona al usuario sobre los procedimientos en casos específicos tales como defunciones, pago de beneficios, bienestar.
- Grupos de Trabajo: contiene información de la relación de personal encargado de efectuar el estudio sobre diferentes temas de interés, para la toma de decisiones.
- Asuntos Administrativos: es el conjunto de información base para tomar decisiones técnicas y operacionales, estos incluyen registro de proveedores, registro de repuestos, partidas presupuestarias.
- Dependencias: integrada por todas las oficinas cuya misión está principalmente relacionada al área administrativa.
- Documentos y Publicaciones: contiene información periódica o permanente que norma los procedimientos administrativos, tales como formatos, leyes, reglamentos, directivas.

Nivel Técnico.- Procesa información proporcionada por las oficinas que tienen a su cargo el mantenimiento y reparación de equipos y el desarrollo de sistemas que procesan datos (tales como software). Esta información contempla desde la identificación del número de serie de microprocesadores hasta las especificaciones de uso, así como los componentes que puedan suplir el trabajo de otros en casos de emergencia, como soluciones alternas.

Este nivel esta integrado por siete subniveles, que son los siguientes:

- Noticias Técnicas: contiene información técnica nacional o internacional que sirve de apoyo para el mejor funcionamiento de las áreas técnicas. En ella se incluye lo siguiente: boletines, artículos, notas de información.

- Informática: En este subnivel se incluye información del área de desarrollo tales como manuales, cursos en línea, servicios de PgP (sistema de cifrado encriptado).
- Grupos de Trabajo: contiene información con la relación de personal encargado de efectuar el estudio sobre diferentes temas de interés para la toma de decisiones.
- Biblioteca Institucional: incluye la relación de todas las publicaciones existentes en la institución, tales como publicaciones de hemeroteca, biblioteca y videoteca.
- Servicios: se brinda información de todo lo relacionado al sistema de control de equipos.
- Dependencias: integrada por todas las oficinas cuya misión está principalmente relacionada al área técnica.
- Documentos y publicaciones: en este subnivel se almacena información brindada por las áreas técnicas de la institución.

Nivel Operacional.- Está integrada por información proporcionada por oficinas netamente operacionales (fuerzas operacionales). Contiene información sobre el estado actual del funcionamiento de los equipos y sistemas que tengan bajo su responsabilidad, así como también la programación y resultado de pruebas que se puedan realizar. Este nivel esta integrado por los siguientes seis subniveles:

- Noticias Operacionales: integrada por información que sirve para tomar decisiones en la parte operativa, tales como mensajes, órdenes, mensajes pendientes.
- Sistema de Correo: Es aquel subnivel donde se almacena todo el sistema de correo para lograr una comunicación inmediata.
- Grupos de Trabajo: contiene información proporcionada de la relación de personal encargado de efectuar el estudio sobre diferentes temas de interés para la toma de decisiones.
- Asuntos Operacionales: Es aquel subnivel donde se almacena información que detalla los procedimientos, programación, resultados de ejercicios que se programan en las diferentes fuerzas operativas, tales como ejercicios antisuperficie, fuego naval de apoyo, etc.
- Dependencias: integrada por todas las oficinas cuya misión está principalmente relacionada con el área operacional.

- Documentos y Publicaciones: Es aquella donde se almacena información necesaria para ejecutar un plan operativo. Para ello se cuenta con publicaciones, manuales de procedimientos, publicaciones conjuntas, publicaciones combinadas.

Nivel de almacén de datos.- Abarca todos los niveles, porque une todos los datos de la red. Está disponible para el apoyo en la toma de decisiones y en el análisis histórico de la institución, de sus procesos y de sus logros. Este es el nivel de la intranet que administra todos los datos de la institución.

4.2.3 Cartografía de Sitio Web

Permite distribuir la información estratégica a través de ella se presenta el sitio en una disposición genealógica o “vista de árbol”, proporcionando una guía visual de las relaciones estructurales entre los recursos. (Ver figuras, 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4).

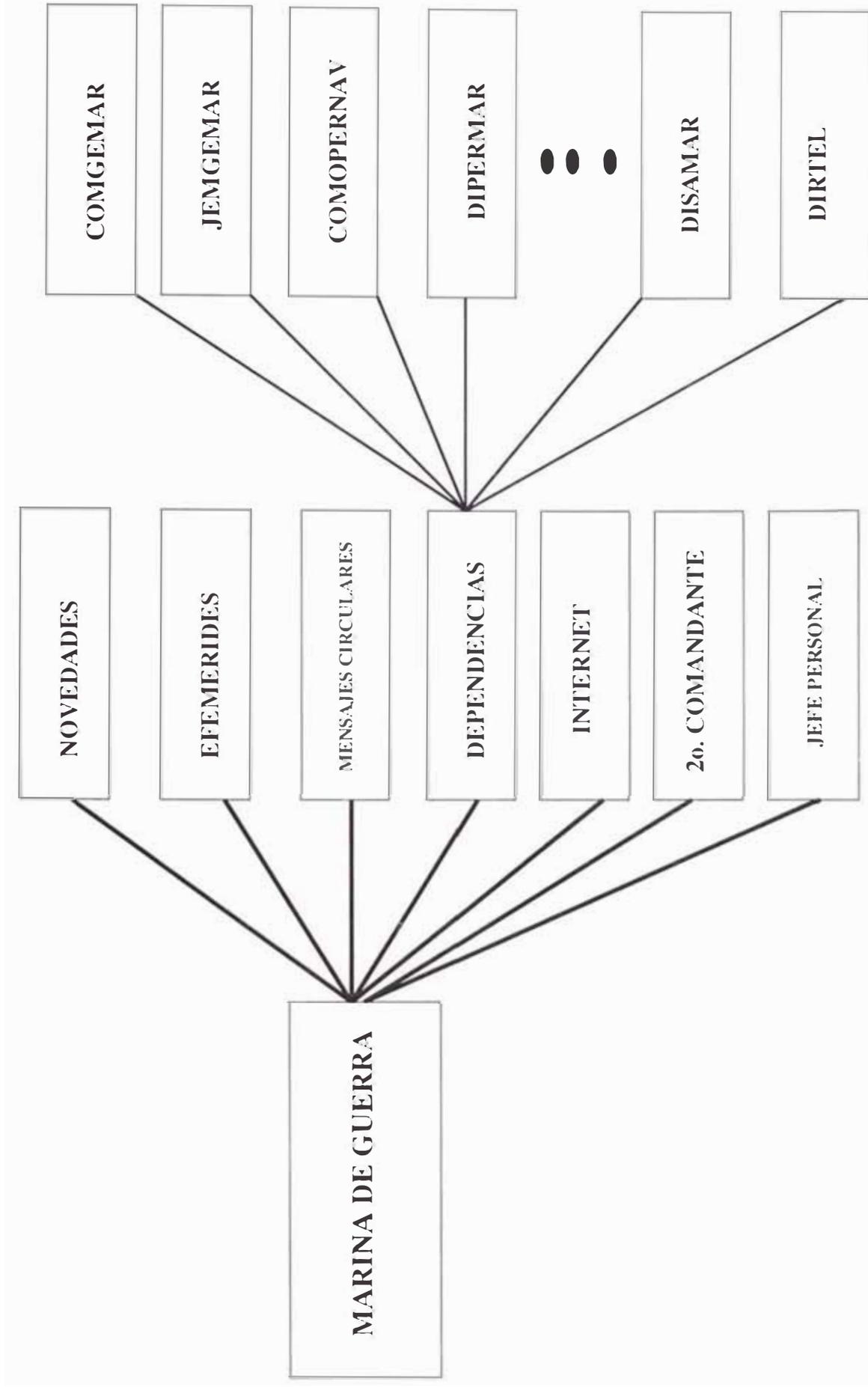


Figura 4.2.3.1 Cartografía del Sitio Web Página Principal

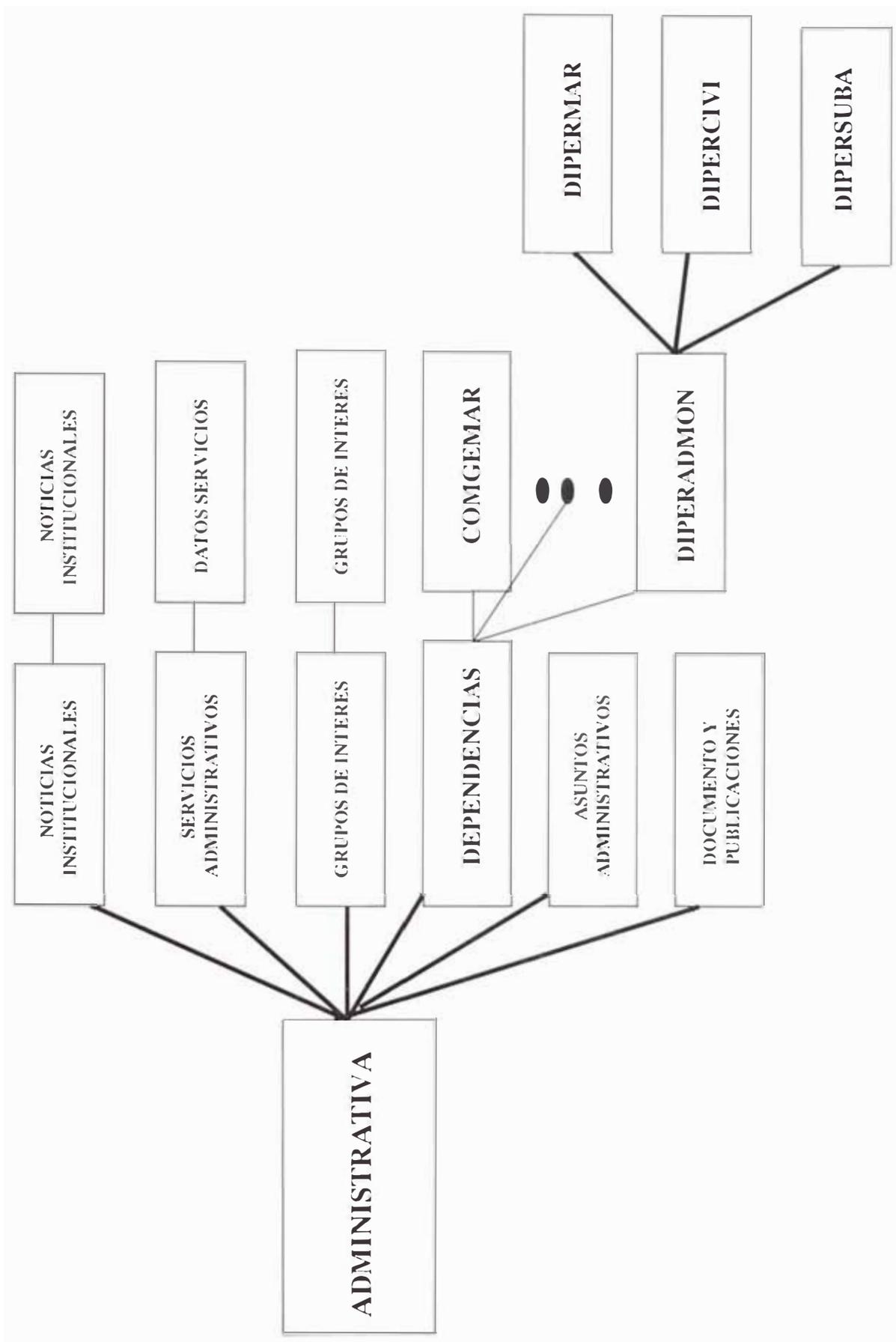


Figura 4.2.3.2 Cartografía del Sitio Web del Area Administrativa

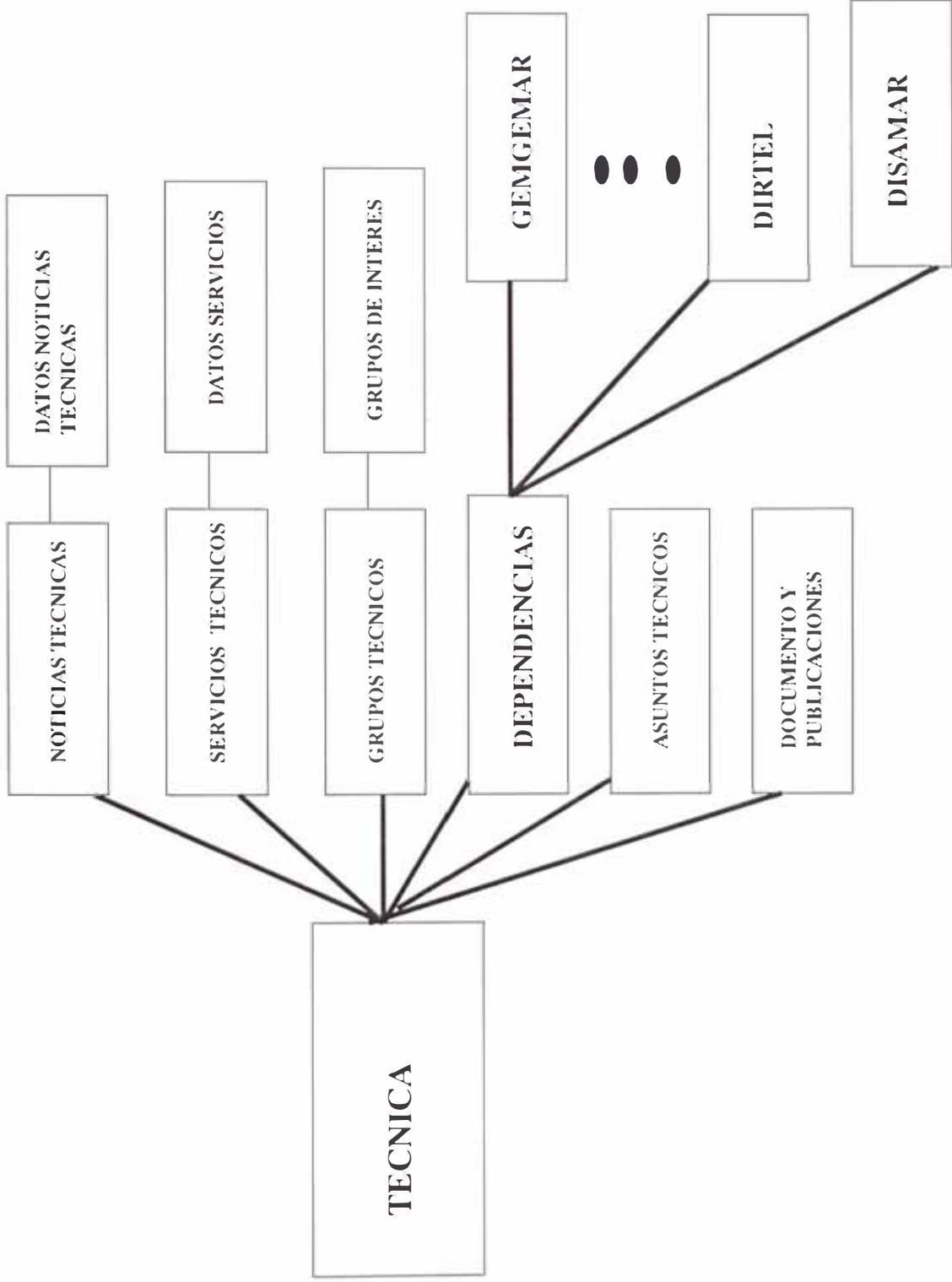


Figura 4.2.3.3 Cartografía del Sitio Web del Area Técnica

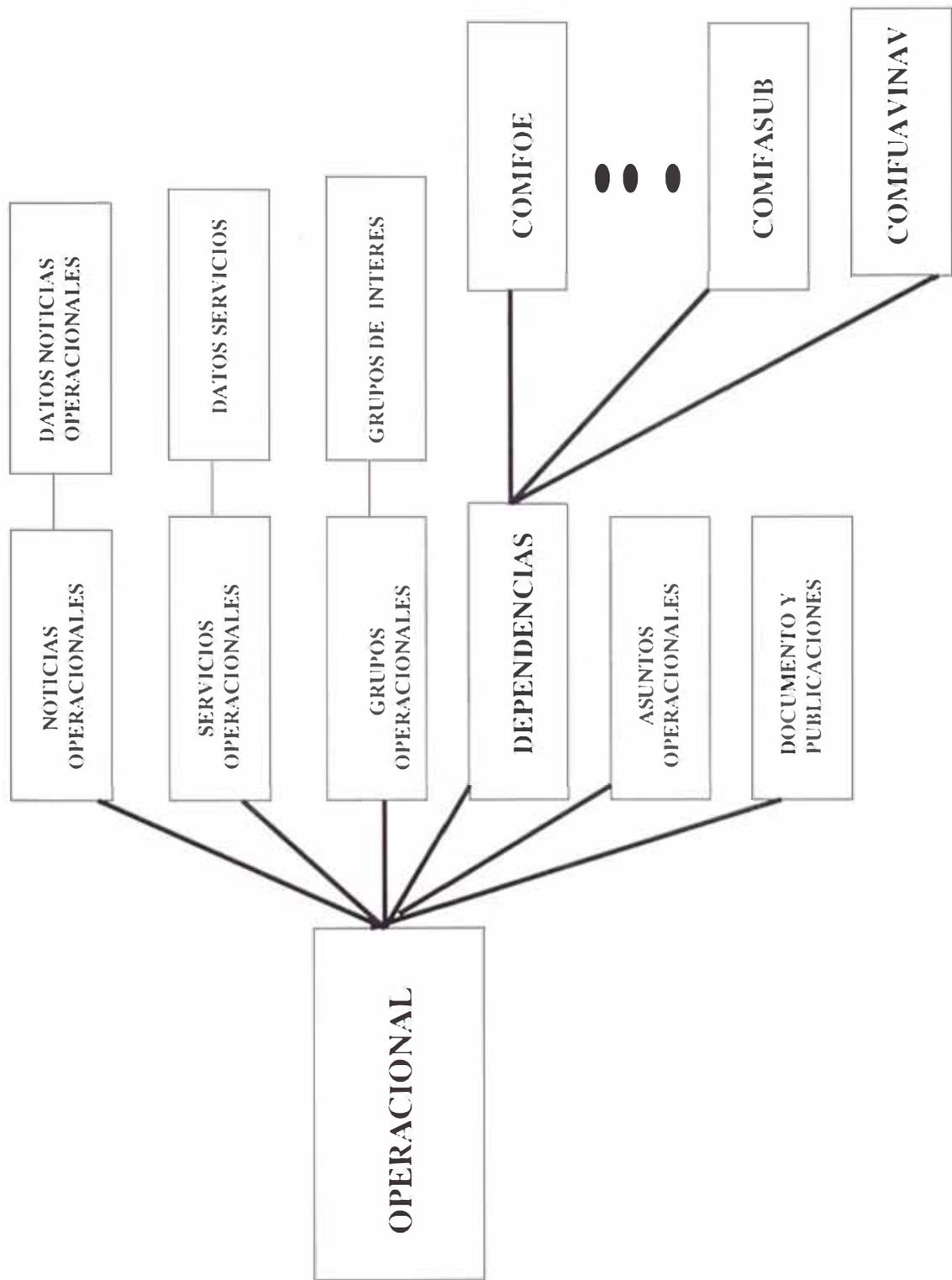


Figura 4.2.3.4 Cartografía del Sitio Web del Area Operacional

4.3 Diseño de Pantallas de la Intranet Naval

Todas las pantallas que se muestran a continuación tiene un acceso de seguridad a nivel de usuario. Es decir, pueden ser sólo de modo consulta o de adición y modificación. También las opciones de cada pantalla de menú serán mostradas según el tipo de usuario. Entiéndase usuario a la persona que manipula información, no el que utiliza el sistema. La figura 4.3.1 que se muestra, es la pantalla que aparece en el momento de ingresar a la Intranet.

M.G.P	INTRANET NAVAL	DD-MM-AA
		
USUARIO: _____		
PASSWORD _____		

Figura 4.3.1 Pantalla Física del Software

4.4 Capacidad de la Intranet Naval

4.4.1 Tráfico de Datos

Los futuros usuarios de la Intranet son los mismos usuarios de la red naval. Por ello, la capacidad de la Intranet está referida a la red naval actual que posee una capacidad de 10 Mbps con proyección hasta 100 Mbps.

Para el cálculo del tráfico de datos en la red se tomó como muestra una jornada de trabajo de 8 horas de un usuario que emplea una PC para trámites administrativos internos. Vamos a considerar generosamente que la PC va a ser empleada realmente el 50 % de la jornada de trabajo (4 horas). En este tiempo de 4 horas asumiremos que se transmite el equivalente a 10 páginas WEB estáticas que pueden contener archivos pdf, archivos ps, fotos, logotipo, imágenes, íconos, mapas de imagen, etc. . Consideraremos que cada página ocupa aproximadamente 531 KB.

Para realizar los cálculos siguientes se debe tomar en consideración que a la red de la Institución se conectan aproximadamente 350 PC's, las cuales ejecutan transacciones de base de datos, transferencia de archivos, e-mail, etc. Por consiguiente, 350 PC's trabajando 4 horas por jornada, ocupan

$$(350 \text{ PC's}/4 \text{ horas}) \times (10 \text{ pág.} / \text{PC}) \times (531 \text{ Kbytes} / \text{pág.})$$
$$= 1\,858\,500 \text{ Kbytes}/4 \text{ horas.}$$

Por tanto, en una hora se ocupa 464 625 Kbytes. De las 4 horas de trabajo, una de ellas se considera como hora punta, en la que asumiremos una recarga de trabajo del 100 % con respecto al tráfico normal, este dato es producto de experiencias ocurridas en organizaciones con similares cargas de trabajo. Esta recarga significa

$$464\,625 \text{ Kbytes/hora} \times 1 = 464\,625 \text{ Kbytes/hora}$$

La ocupación total del tráfico de información en la hora punta es de:

$$464\,625 \text{ Kbytes/hora} + 464\,625 \text{ Kbytes/hora} = 929\,250 \text{ Kbytes/hora punta}$$

La capacidad total (sin considerar futuras ampliaciones) resulta:

464 625 Kbytes/hora x 3 horas + 929 250 Kbytes/hora punta = 2 323 125 Kbytes por jornada de trabajo de 4 horas.

Se considera también el factor de capacidad instalada de la red para futuras ampliaciones, en este caso se asume un factor de 2 tomando como base estadísticas de trabajos realizados. Entonces la capacidad total afectado por este factor sería de la siguiente manera:

$2 \times 2\,323\,125 \text{ Kbytes} = 4\,646\,250 \text{ Kbytes}$ por jornada de trabajo de 4 horas.
Realizando conversiones para convertir a Mbps tenemos:

$(4\,646\,250 \text{ Kbytes}/4 \text{ horas}) \times (1 \text{ hora}/3600 \text{ seg}) \times (1 \text{ Mbyte}/1024 \text{ Kbytes}) (8 \text{ bit}/1 \text{ byte})$
 $= (37\,170\,000 \text{ Megabit}/14\,745\,600 \text{ seg.}) = 2.52 \text{ Mbps}$

Actualmente la capacidad empleada de la red por la institución es de 1.5 Mbps, por lo tanto la capacidad total empleada al ser implementada la Intranet sería de 2.52 Mbps + 1.5 Mbps = 4.02 Mbps

Por lo tanto se concluye que aproximadamente el 40 % de la capacidad de la WAN Naval estará ocupada por la Intranet, teniendo un 60% de capacidad para realizar futuras aplicaciones.

4.4.2 Tráfico de Voz

Actualmente se tiene la instalación de RDSI (Tráfico voz a través de IP conocida como Vo IP) solamente en las Capitanías de Puerto para los casos de emergencia en que se caiga los enlaces principales. Para tráfico de voz se utiliza los radio enlaces y centrales telefónicas por lo que es innecesario usar a través de redes, dado que no existe requerimiento institucional.

4.5 Costos del Proyecto

Los factores de costo más importantes que afectan el desarrollo de una Intranet en una organización son: opciones de conectividad (capacidad de la red), plataforma de servidor Web, seguridad de la red, costo total anual de operación para un cliente de intranet, construcción de aplicaciones interactivas, mantenimiento, actualización de contenidos y diseño de la intranet. Al respecto, el costo en que

incurrir el instituto se reduce tremendamente, dado que cuenta con plataformas existentes tales como: capacidad disponible, servidor Web, seguridad de red, etc. También cuenta con personal experimentado en tareas de mantenimiento y administración de red, incluso se cuenta con personal para actualización de contenido de la Intranet. Sin embargo, es necesario que el personal sea capacitado en la programación en Java, dado que este lenguaje permite integrar bases de datos y adquirir experiencia en interfaces de aplicaciones de Netscape y Microsoft que apoyarían en rediseños posteriores de la intranet. Esta capacitación es necesaria, para que haya un personal que se encargue básicamente del desarrollo de la Intranet a tiempo completo y pueda enseñar al personal que posteriormente se encuentre al frente, de manera que se evite la paralización del desarrollo o mantenimiento por falta de algún personal.

El Cuadro 4.5.1 muestra una estructura de costos en que incurriría la Marina de Guerra del Perú al aprobar la implementación de la Intranet, como se detalla la Marina sólo incurriría en un gasto de \$US 8,500.00, en el que el mayor costo es el de capacitación que tiene un costo de \$US 5,000.00, sin embargo, es necesario mencionar que esto permitiría que la Institución ahorre en contratar a terceros que se dedican al desarrollo de aplicaciones para Intranet y que tienen tarifas de aproximadamente \$US 50,000.00 [4], y por supuesto también es necesario mencionar que se cuenta con capacidad instalada y tecnología que permite implementar la Intranet, costos que tampoco la institución incurriría.

CUADRO 4.5.1

CUADRO DE COSTOS DEL DESARROLLO E IMPLEMENTACION DE LA INTRANET NAVAL

ETAPAS	COSTO MENSUAL (\$)	TIEMPO MESES	COSTO TOTAL (\$)
Análisis	700.00	2	1,400.00
Diseño	700.00	3	2,100.00
Capacitación (desarrollo de aplicaciones) para 5 programadores		6	5,000.00
TOTAL			8,500.00

4.6 Cronograma de Actividades del Desarrollo e Implementación de la .Intranet

Para desarrollar el diseño de la Intranet se requiere del cronograma de actividades que se muestra en el cuadro 4.6.1, cuyas tareas se describen a continuación.

Capacitación.- En esta actividad el personal de la Dirección de Telemática debe ser capacitado para desarrollar aplicaciones en la Intranet.

Análisis.- Esta tarea se refiere al análisis y procesamiento en detalle de la información necesaria para diseñar la Intranet. De este análisis se determinó que los tipos de información utilizados en la institución pueden ser clasificados en administrativo, técnico y operacional.

Diseño.- En base al análisis se pasa al diseño en detalle de la Intranet, de modo tal que satisfaga las necesidades de la institución. Básicamente el diseño consiste en definir la estructura de la página principal y las especificaciones de su contenido. También se propone la infraestructura mínima necesaria para dar soporte a esta Intranet en cuanto a software y hardware.

Elaboración de Programas.- En esta etapa se procede a programar la estructura lógica de la página principal del diseño propuesto. Se requiere programación especializada para la construcciones de aplicaciones interactivas, Java y programas de interfaces de aplicaciones Netscape y Microsoft.

Simulación.- Antes de realizar la implementación es necesario realizar una simulación con datos ficticios.

Implementación.- Definido el hardware y software se tiene que realizar las conexiones con las diferentes dependencias.

Pruebas de Operación.- Una vez realizada las conexiones con las dependencias, es en esta etapa la puesta en funcionamiento.

Elaboración de Manuales.- Descripción de la Intranet su forma de empleo, acceso y resolución de problemas.

CUADRO 4.6.1

CRONOGRAMA DE ACTIVIDADES DEL DESARROLLO E IMPLEMENTACION DE LA INTRANET

ACTIVIDAD	DURACION (MESES)																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ANALISIS	■	■																
DISEÑO		■	■	■	■													
CAPACITACION	■	■	■	■	■													
ELABORACION DE PROGRAMAS						■	■	■	■	■								
SIMULACION										■	■							
IMPLEMENTACION											■	■	■	■	■	■	■	■
PRUEBAS DE OPERACION													■	■	■	■	■	■
ELABORACION DE MANUALES							■	■	■	■	■	■	■	■	■	■	■	■

Capítulo 5

Seguridad de la Intranet Naval

5.1 Modelo General de Seguridad de una Red

La seguridad en la transmisión de información es una preocupación permanente de las organizaciones cuyos activos son controlados por sistemas de computo. Con la introducción de la computadora, la necesidad de herramientas automatizadas para proteger los archivos y cualquier otra información almacenada es evidente, particularmente en el caso de sistemas compartidos. La necesidad de seguridad es aún más crítica en sistemas en los cuales se puede tener acceso empleando la red telefónica o una red de datos.

El uso del término seguridad en la red está muy extendido, y se refiere a las medidas a tomar para asegurar la transmisión de datos entre el usuario y la computadora, o entre computadoras, dentro de una red distribuida.

La figura 5.1.1 muestra un modelo general de seguridad red descrito en [9].

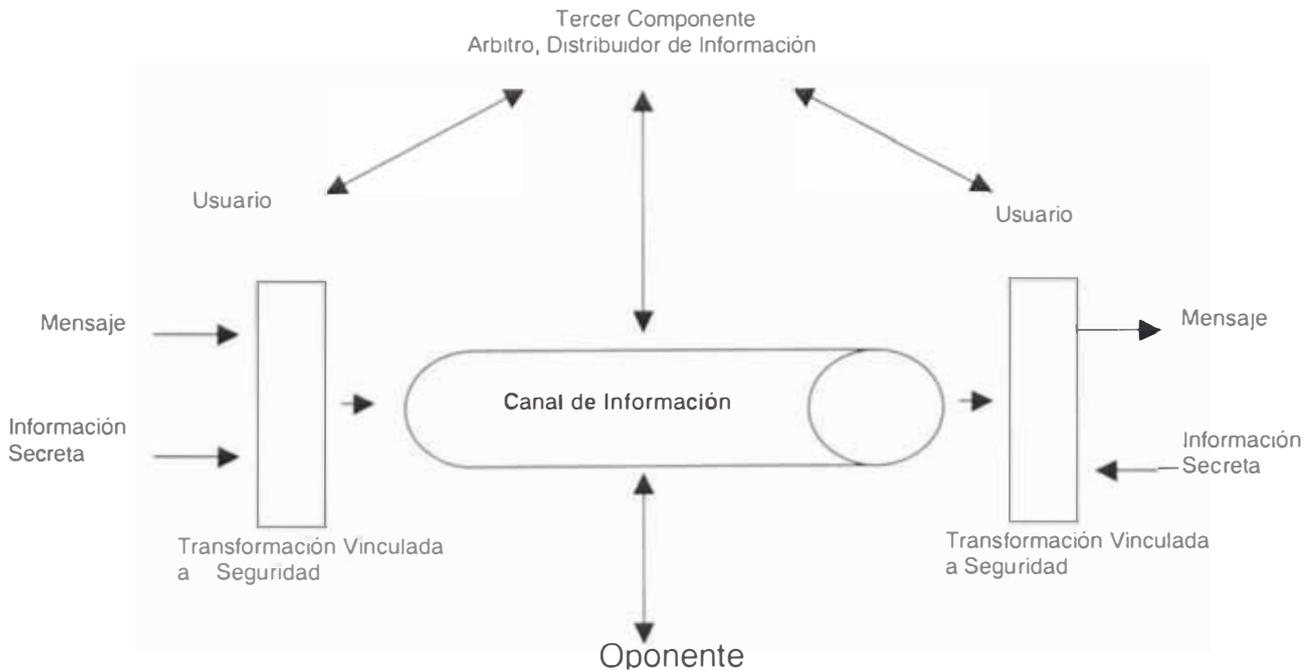


Figura 5.1.1 Modelo de Seguridad para trabajo en Red

En este modelo se observa que, un mensaje es transferido de una parte a otra a través de una red. Las dos partes que son las principales en esta transacción, deben cooperar para que realice el intercambio. El canal lógico de información se establece definiendo una ruta a través de la red, desde la fuente al destino y por el uso corporativo de dos principales protocolos de la comunicación (ejemplo TCP/IP).

Los aspectos de seguridad intervienen cuando es necesario o deseable proteger la transmisión de un oponente que puede representar una amenaza para la confidencialidad, autenticidad, etc. Todas las técnicas que proveen seguridad tiene dos componentes:

1. Una transformación vinculada con seguridad en la información a ser enviada, como por ejemplo codificación de mensajes, que hace ilegible para el oponente además de un código basado en el contenido del mensaje que puede utilizarse para identificar la identidad del transmisor.
2. Alguna información secreta compartida por dos usuarios y desconocida por el oponente.

Una tercera parte puede ser requerida para lograr una transmisión segura. Por ejemplo, puede ser responsable de distribuir una información secreta a los dos usuarios y desconocida por el oponente, considerando un árbitro de distribución secreta. Este modelo general muestra cuatro tareas básicas en el diseño de un servicio particular de seguridad:

1. Diseñar un algoritmo para actuar en una transformación relativa a seguridad. El algoritmo debe ser tal que el oponente no pueda lograr su propósito.
2. Generar la información secreta a ser usada con el algoritmo.
3. Desarrollar métodos para distribuir y compartir la información.
4. Especificar el protocolo de seguridad a usarse por los dos usuarios.

Sin embargo, existen otras situaciones de seguridad que no se visualiza en el modelo anterior que también se debe tomar en cuenta, como es el modelo que se detalla en [9] y se muestra en la figura 5.1.2, el cual refleja el interés por proteger un sistema de información de un acceso no deseado.

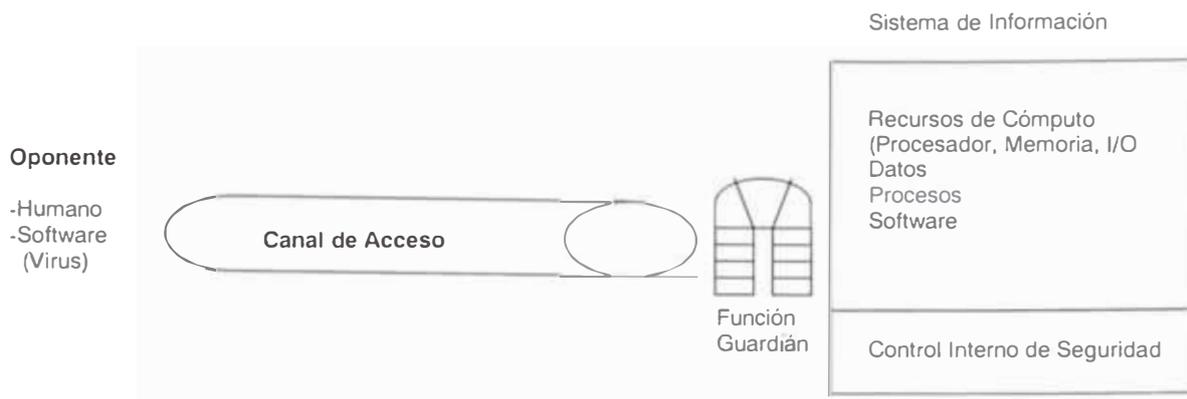


Figura 5.1.2 Modelo de Seguridad de Acceso a la Red

Los mecanismos de seguridad para enfrentar accesos no deseados, como por ejemplo, obtener el número de una tarjeta de crédito, realizar transferencias ilegales de dinero, virus de software, etc., están en dos categorías. La primera categoría es una función de guardián, la cual incluye procedimientos de claves que se diseñan para negar el acceso a usuarios no autorizados y una lógica diseñada para rechazar virus y otros ataques similares. Una vez que se obtiene el acceso por un software o usuario no deseado, la segunda categoría, consiste en una variedad de controles internos que monitorean la actividad y analizan la información almacenada en un intento por detectar la presencia de intrusos.

La herramienta más importante para la seguridad en comunicaciones y en red es la encriptación. Dos formas de encriptación son de uso común: la convencional o simétrica, y la encriptación llave pública o asimétrica [9].

5.2 Seguridad Física en la WAN Naval

La Dirección de Telemática garantiza la seguridad en la WAN Naval a través el cifrado de los enlaces, mediante la evaluación de redes locales antes de su incorporación a la WAN Naval y el control permanente de posibles brechas de seguridad en las redes locales, ocasionadas por implementación de enlaces a Internet u otros accesos físicos al exterior de la WAN Naval que no pasen por sistemas de protección (firewalls) controlados.

La Dirección de Telemática cuenta con una Oficina de Seguridad de la WAN Naval con personal especializado en la administración de enlaces, protocolos y puertas de acceso a la WAN Naval, como protección al uso indebido desde el interior y al ataque externo por intrusos o saboteadores (hackers) que intenten ingresar a la WAN Naval. El empleo de herramientas de control en el tráfico de la WAN Naval es parte de ese esquema.

En adición a la seguridad del canal, para la seguridad de contenido (dentro de la WAN Naval físicamente segura), se emplean técnicas de limitación de acceso y autenticación de la información mediante software de cifrado.

El problema de seguridad es el tema más importante, tanto en el tráfico interno como en lo concerniente al servicio de Internet. Para prevenir y neutralizar cualquier intento de penetración no deseada a la Red WAN Naval desde el exterior, se ha implementado un firewall del tipo Application Gateway en cada punto de conexión a Internet (La Perla y Salaverry), que se encarga de proporcionar las facilidades de filtrado de paquetes y filtrado de los protocolos no autorizados, tanto a la entrada a la WAN Naval como a su salida hacia el exterior. Así también se cuenta con la encriptación para todos los acceso remotos (VPN's). A fin de complementar y apoyar las características de seguridad del firewall, se ha implementado un Proxy en cada Nodo de la WAN el cual se encarga de restringir en su respectivo nodo el tráfico de salida de dicho nodo hacia la Internet, así como servir de caché para los requerimientos Web, lo cual se traduce en una respuesta sensiblemente mas rápida a los usuarios de las paginas que deseen visitar en Internet. De manera adicional, en el router de conexión a Internet se efectuó la inclusión de listas de control de acceso, a fin de filtrar los paquetes IP (tanto en el tráfico Inbound como el Outbound). En lo referente a la seguridad que se debe tener en el tráfico interno, el tráfico de cada enlace entre Nodos que se realiza de manera encriptada.

En resumen, se tiene el siguiente equipamiento en el área de seguridad:

Firewall: Equipo encargado de la seguridad de accesos externos y salidas desde la WAN Naval.

Servidores Proxy: Equipos encargados de hacer más eficiente el acceso a Internet, mediante el manejo de caché de memoria, y control de usuarios autorizados a salir a Internet.

Filtrado de paquetes a nivel ruteador (Router).

Cifrado de Radio Enlaces (Encriptadores-Decriptadores).

Una vez contemplados los aspectos de seguridad física de la WAN Naval, el aprovechamiento de la tecnología para la distribución de correspondencia naval y el trabajo en grupo en las redes locales, en las redes a nivel cuarteles y en la WAN Naval, se debe considerar la seguridad del acceso por el usuario (conexión a la red) y los derechos de acceso a servicios, directorios y aplicaciones que normalmente son función del administrador de cada red. Las regulaciones al respecto son emitidas en directivas y procedimientos de responsabilidad de la Dirección de Telemática.

Por el hecho de ser la WAN Naval una red de carácter militar, los servicios permitidos desde y hacia Internet o, mejor dicho, el tráfico autorizado entre la WAN e internet ha sido restringido a los siguientes servicios:

Entrante a la WAN desde Internet:

HTTP (Navegación Web)

SMTP (Correo)

POP3 (Correo)

FTP (Transferencia de Archivos)

Saliente a Internet desde la WAN:

SMTP (Correo)

HTTP (Web), para permitir a Internet visitar las páginas Web de marina alojadas en servidores al interior de la WAN.

La Dirección de Telemática, es quien implementa apropiadamente los servicios de administración, control técnico y de seguridad, así como los sistemas informáticos navales. Este control incluye el monitoreo continuo de los accesos externos a la red Naval, técnicas contra intrusos y administración del ancho de banda de los enlaces con priorización por aplicaciones (Quality of Service).

Las direcciones, a través de las Oficinas de Informática, tienen la autoridad de controlar o limitar el uso de los sistemas de información navales con propósitos de seguridad, moral, buena conducta, disciplina y la promoción de la eficiencia de su comando. Esta autoridad puede ser delegada a los administradores de los sistemas, como por ejemplo, para limitar las horas de acceso al sistema, accesos a Internet, revocar autorizaciones a los sistemas, limitar el tamaño y volumen de archivos a ser transferidos por la Red Naval para evitar su congestión.

El desarrollo de nuevos sistemas administrativos considera la obtención de información de otros sistemas a través de la Red Naval. Mientras que en el establecimiento Naval Terrestre es posible instalar enlaces digitales de alta velocidad para voz y datos, los enlaces de la Red Naval con las Unidades Navales son, por su naturaleza, de baja velocidad, por lo que su explotación está enmarcada dentro de los Sistemas de Comando y Control de alcance estratégico y táctico, como el SIRIUS y el OLIMPO. Otros sistemas informáticos de apoyo a las operaciones emplean dichos sistemas como medio de enlace (gateway) hacia las Unidades Operativas.

5.3 Software de Seguridad

Virtualmente en todos los medios de distribución, el correo electrónico es el más usado en la aplicación basada en la red. Es también la única aplicación que se usa en todas las plataformas y arquitecturas. Los usuarios esperan ser capaces de enviar correspondencia a otros que están conectados a internet en forma directa o indirecta. La Marina de Guerra del Perú no se ha mantenido al margen y emplea la encriptación PGP (Pretty Good Privacy) .

5.3.1 Software de Seguridad PGP

PGP es un programa de encriptación por llave pública escrito por Philip Zimmermann, que en la actualidad se utiliza para disponer de un correo electrónico seguro. PGP resulta mucho más fácil de utilizar. Esto se debe a que PGP está basado en una potente nueva tecnología llamada criptografía de "llave pública".

PGP combina la comodidad del criptosistema de llave pública de Rivest-Shamir-Adleman (RSA) con la velocidad de la criptografía convencional, con resúmenes de mensajes para firmas digitales, con compresión de datos antes de

encriptar, con un buen diseño ergonómico y con una completa gestión de claves. Por otra parte, PGP realiza las funciones de llave pública con más rapidez que la mayoría de las demás implementaciones informáticas. La siguiente tabla muestra los servicios que presta el PGP, de acuerdo a la referencia [9].

TABLA DE SERVICIOS DE PGP

FUNCION	ALGORITMOS USADOS	DESCRIPCIÓN
Encriptación del mensaje	IDEA, RSA	Encripta un mensaje usando IDEA con una llave sesión. Encripta esta llave usando RSA con la llave pública del receptor e incluido el mensaje.
Firma digital	RSA, MD5	Crea un código de un mensaje usando MD5. El mensaje es encriptado usando RSA con la llave privada del transmisor.
Compresión	ZIP	Puede comprimir un mensaje para almacenarlo o transmitirlo usando ZIP.
Compatibilidad E-mail	Conversión Radix 64	Convierte el mensaje encriptado a ASCII para dar transparencia a las aplicaciones E-mail, usando la conversión Radix 64.
Segmentación	-----	Acomoda al máximo los límites del tamaño del mensaje, PGP lleva a cabo segmentación y el reagrupamiento.

De todos los servicios que brinda el PGP, la Marina ha visto por conveniente utilizar el algoritmo RSA para la encriptación de mensajes, por que este algoritmo presenta características de tecnología de encriptación fuerte, diseñado para responder a las expectativas de la institución.

5.3.2 El Algoritmo RSA

RSA es un criptosistema de llave pública diseñado tanto para encriptación como para identificación que fue inventado en 1977 por Ron Rivest, Adi Shamir, y Leonard Adleman. El esquema desarrollado emplea una expresión exponencial. El texto lineal se encripta en bloques donde cada bloque tiene un valor binario menor que un número n . El procedimiento de encriptación y desencriptación se formula en

la forma siguiente. Para algún bloque de texto simple M y un bloque de texto cifrado C se cumple:

$$C = M^e \text{ mod } n \quad (5.1)$$

$$M = C^d \text{ mod } n \equiv (M^e)^d \text{ mod } n \equiv M^{ed} \text{ mod } n$$

Ambos, el que envía y el que recibe deben conocer el valor de n . El que envía debe saber el valor de e , y el que recibe solamente el valor de d . Por tanto, este algoritmo de encriptación es de llave pública con llave pública $KU = \{e, n\}$ y con llave privada $KR = \{d, n\}$. Según ecuación (5.1), se necesita encontrar una relación de la forma: $M = M^{ed} \text{ mod } n$. Para ello usaremos el corolario del teorema de Euler que se describe en el Apéndice 4A de [9], el cual indica que dado dos números primos p y q y dos enteros n y m , con $n = pq$ y $0 < m < n$ y un entero aleatorio k , la siguiente relación estima que:

$$m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \text{ mod } n$$

En el Apéndice 4A de [9] se demuestra que para dos números primos p, q , se tiene que $\phi(pq) = (p-1)(q-1)$. Por consiguiente: $ed = k\phi(n)+1$, lo cual es equivalente a decir que:

$$ed \equiv 1 \text{ mod } \phi(n) \quad (5.2)$$

$$e \equiv d^{-1} \text{ mod } \phi(n)$$

De la ecuación (5.2) podemos notar que e y d son inversos multiplicativos de $\text{mod } \phi(n)$. Cabe anotar que de acuerdo a las reglas de aritmética modular, la ecuación anterior es válida solamente si d (y por lo tanto e) es primo relativo a $\phi(n)$, lo que equivale a decir que $\text{gcd}(\phi(n), d) = 1$, donde gcd significa el máximo común divisor de $\phi(n)$ y d .

El esquema de encriptamiento RSA necesita lo siguientes datos:

p, q , dos números primos	(privado, escogido)
$n = pq$	(público, calculado)
d , con $\text{gcd}(\phi(n), d) = 1$; $1 < d < \phi(n)$	(privado, calculado)
$e \equiv d^{-1} \text{ mod } \phi(n)$	público, escogido)

La llave privada consiste en el par $\{d, n\}$ mientras que la llave pública consiste en el conjunto $\{e, n\}$. Si suponemos que el usuario A ha revelado su llave pública y el usuario B desea enviar un mensaje C de M a A, entonces el usuario B calcula $C = M^e \pmod{n}$ y lo transmite. El usuario A recibe este texto y lo descripta usando $M = C^d \pmod{n}$.

De acuerdo a la ecuación (5.2), ed es de la forma $K\phi(n)+1$. Por aplicación del corolario del Teorema de Euler, para dos números primos p y q dados, se cumple que $n = pq$ para $0 < M < n$. Luego, la ecuación (5.1) toma la forma:

$$M^{k\phi(n)+1} = M^{k(p-1)(q-1)+1} \equiv M \pmod{n}$$

Como $M^{ed} \equiv M \pmod{n}$. Entonces se tiene:

$$C = M^e \pmod{n}$$

$$M = C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n} \equiv M \pmod{n}$$

Seguidamente se detalla un resumen del algoritmo RSA que incluye la generación de llaves y el proceso de encriptación y descriptación.

Generación de Llaves

Seleccione p,q	p, q primos
Calcular $pxq = n$	
Seleccionar un entero d	$cd (\phi(n), d) = 1 ; 1 < d < \phi(n)$
Calcular e	$e = d^{-1} \pmod{\phi(n)}$
Llave Pública	$KU = \{e, n\}$
Llave Privada	$KR = \{d, n\}$

Encriptación

Texto Lineal : $M < n$

Texto Cifrado: $C = C^e \pmod{n}$

Desencriptación

Texto Cifrado: C

Texto Lineal: $M = C^d \pmod{n}$

A continuación se realiza una aplicación del algoritmo RSA, iniciando con la generación de llaves pública y privada para luego proceder a encriptar y desencriptar para valores hipotéticos

Generación de llaves:

1. Se selecciona 2 números primos $p = 7$ y $q = 17$
2. Se calcula $n = pq = 7 \times 17 = 119$
3. Se calcula $\phi(n) = (p-1)(q-1) = 96$
4. Se selecciona e de manera que e sea un primo relativo a $\phi(n) = 96$ y menor que $\phi(n)$ en este caso $e = 7$.
5. Se determina $ed \equiv 1 \pmod{96}$ aplicando la ecuación (5.2), como se sabe el valor de $e = 7$, reemplazando se tiene $7d \equiv 1 \pmod{96}$. Para el cálculo de d se utiliza el concepto de congruencia de módulo y se halla un valor que multiplicado por 7 y dividido entre 96 de cómo resultado un resto de 1, este valor es $d = 77$, porque $77 \times 7 = 539$ y este valor cumple la condición de que al dividir este valor entre 96 da como resto 1, es decir: $539 \equiv 1 \pmod{96}$

Las llaves resultantes son: llave pública $KU = \{7, 119\}$ y llave privada $KR = \{77, 119\}$.

Encriptación y Desencriptación:

El texto lineal queda codificado en un número M , la condición es que $M < 119$, en este caso $M = 15$, se cifra M en C aplicando la fórmula $C = 15^7 \pmod{119}$, igualmente aplicando el concepto de congruencia de módulos se obtiene que el texto cifrado es de 67 por que $15^7 \equiv 67 \pmod{119}$.

Para desencriptar, se toma el bloque C aplicando la fórmula $M = 67^{77} \pmod{119}$ aplicando el mismo concepto de congruencia se tiene que $67^{77} \equiv 15 \pmod{119}$, significa esto que se desencripta el mismo tamaño de bloque que ingreso para cifrar que es 15.

Para mayor ilustración, este cálculo de valores hipotéticos se representa en forma gráfica en la figura 5.3.1

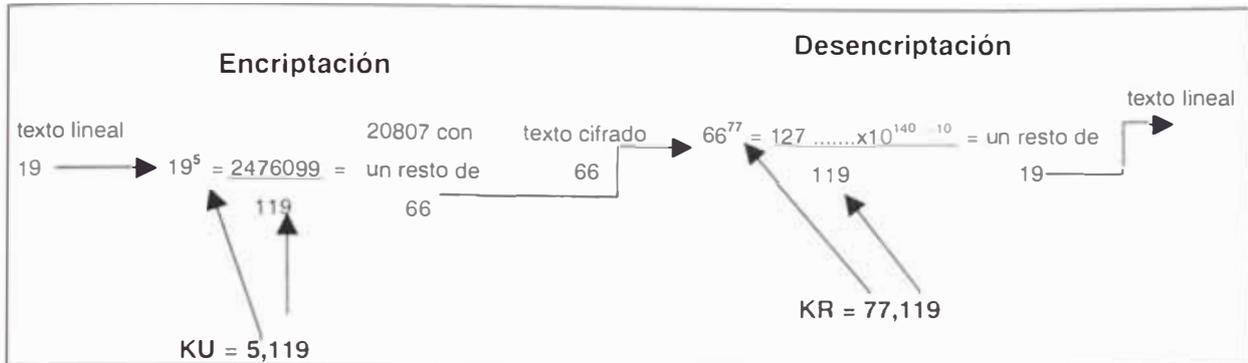


Figura 5.3.1 Aplicación El Algoritmo RSA

Es necesario mencionar que la selección de valores tanto para e como para M , se realizan en forma aleatoria y esta incluido en el software del algoritmo RSA.

Como se ha visto, en el capítulo que versa sobre la Seguridad, éste es un elemento de suma importancia para cualquier institución, en especial para aquellas que pertenecen a la Fuerza Armada, como es el caso de la Marina de Guerra del Perú. Desde que la Marina concibió la idea de mantenerse a la vanguardia de las comunicaciones, tuvo como énfasis principal la seguridad en el envío y recepción de mensajes.

La tecnología electrónica digital desde la década de los 60 ha tenido un avance vertiginoso; en países con limitados recursos económicos como el nuestro, éste ha sido un factor decisivo para el desarrollo de sistemas que puedan mantener cierta ventaja sobre los países vecinos.

Antes de empezar a diseñar las diferentes redes, para luego convertirse en la Wan Naval que actualmente se conoce, la Institución ya había contemplado la necesidad de encriptar su información para ser enviada a las diferentes embajadas alrededor del mundo. La información se encriptaba empleando equipos telefónicos, correo humano, pintura invisible, entre otros. Uno de los principales proveedores de

la tecnología de la encriptación ha sido Suecia a través del criptofax , con diferentes claves para cada usuario.

La seguridad en el envío de información a través de mensajes por medio del sistema de mensajería outlook se reforzó en un inicio con la implementación del PGP, el cual ha sido objeto de un estudio anterior. Pero como todo algoritmo criptográfico se puede desencriptar, esta es una de las razones para el desarrollo de la Steganografía, tecnología de última generación de los inicios de este siglo XXI, la cual permite esconder un mensaje dentro de una imagen, haciendo imposible detectarlo a través del ojo humano. Está probado que esta tecnología ha sido utilizada por terroristas afganos en los EE.UU, logrando vulnerar el complejo sistema de seguridad del país más fuerte del mundo. El desarrollo de esta tecnología nos mantendrá en ventaja con respecto a nuestros potenciales enemigos, los cuales no podrán descifrar nuestros mensajes, ya que como se verá los mensajes de texto pueden ser insertados en archivos de imagen, voz y hasta dentro de otro texto.

5.4 Esteganografía

La esteganografía es una técnica que permite información dentro de otra información diferente. Se puede "esconder" mensajes o ficheros dentro de imágenes gráficas, archivos de sonido, documentos de texto, etc. En los últimos tiempos ha tenido un verdadero impulso que ahora es considerado como una de las opciones con más futuro para proteger la confidencialidad de la información. Es evidente que un mensaje cifrado en la red, es identificado rápidamente como tal; en cambio, si se pone ese mismo mensaje dentro de una imagen, un sonido, u otro texto, se garantiza que los datos cifrados no se vayan paseando por el mundo con un letrero "de encriptado".

Esta técnica también se está usando en la autenticación de imágenes para cuestiones de derechos de imagen mediante el llamado **watermarking**. En ella se puede introducir información en una imagen gráfica para que permita saber quién es el autor, o por lo menos si es una copia no autorizada. Con archivos de sonido se procede de forma parecida a lo descrito anteriormente y también se puede enviar un texto dentro de otro texto de manera invisible.

La esteganografía, es un campo aún por explotar con detenimiento; en cualquier caso, es interesante hacer alguna aplicación de manejo sencillo y que además recoge los formatos más populares de imágenes, sonido y texto.

La palabra esteganografía literalmente significa escritura encubierta. Esto incluye una vasta colección de métodos para comunicaciones secretas que ocultan la existencia de un mensaje.

Esteganografía es el arte o la ciencia de comunicar de manera oculta un mensaje; en contraste con la criptografía, donde el enemigo permite ser detectado, interceptado, logrando modificar sus mensajes siempre que se logre violar el sistema de seguridad de la encriptación de dicho mensaje.

El acierto de la Esteganografía radica justamente en ocultar los mensajes dentro de otros mensajes, de manera que no exista enemigo que detecte que hay un segundo mensaje, o que se halla oculto.

En la siguiente tabla están definidos los métodos de “seguridad” como de “protección” y donde inteligencia es definida como método de “recuperación”.

Signal security	Signal intelligence
<ul style="list-style-type: none"> • Esteganografía (Tintas invisibles, Códigos Abiertos). • Criptografía (códigos y ciphers) • Traffic-security (radio silence, call-sign, changes, dummy messages) 	<ul style="list-style-type: none"> • Interceptar y dirección-hallamiento • Criptoanálisis • Traffic análisis

5.4.1 Introducción a la criptografía

La gente usualmente se refiere a diferentes cosas cuando habla de la criptografía. Hasta los niños juegan con lenguajes secretos. Pero, esto no tiene nada que ver con la criptografía real, la cual debe difícil de descifrar para así poder ser usado en la protección de información de diversa índole (información en organizaciones criminales, en corporaciones multinacionales, de gobierno). Este tipo

de criptografía va a ser denominada “fuerte” y generalmente es usada por instituciones militares como La Marina de Guerra, en donde se ha desarrollado con mayor intensidad en estos últimos años. En este sentido, la Marina cuenta actualmente con equipos sumamente sofisticados y capaces de romper claves y enviar mensajes indescifrables para el enemigo. Igualmente, la criptografía es una de las primeras herramientas para la privacidad, confianza, control de acceso y otros campos.

La criptografía no es solamente para uso militar. Esta técnica puede proveer para nuestra sociedad moderna herramientas necesarias para dar privacidad en un mundo donde toda la información, por lo general, esta a la vista y al acceso de todos.

5.4.2 Terminología Básica

En la terminología de la criptografía el mensaje es llamado plaintext o cleartext. La codificación del contenido del mensaje de manera que la información esté oculta a los demás es la criptografía. El mensaje encriptado es llamado ciphertext.

El proceso de convertir al plaintext del ciphertext es decriptación o desencriptamiento. La criptografía y la decriptación solo puede ser realizadas si se conoce dicha clave.

5.4.3 Esteganografía con Gráficos

La tecnología digital nos brinda nuevas formas de aplicar las técnicas esteganográficas, siendo una de las mas usadas la de esconder información en imágenes digitales. Existen varios formatos gráficos de imágenes y técnicas para esconder información dentro de ellas, tales como:

- **BMP:** los archivos BMP (Windows Bitmap) son utilizados por Windows como el formato estándar de imagen; incluso todas las imágenes que gestionan de forma interna están en este formato. Los archivos BMP se pueden encontrar comprimidos o descomprimidos. El método de compresión que utiliza es RLE (Run Length Encoding), que funciona comprimiendo cadenas secuenciales iguales cambiándolas

por el símbolo repetido y el número de veces que se repite. Los ficheros almacenados con este formato tienen extensión .BMP.

- **PCX:** los archivos PCX fueron creados para ser utilizados en paquetes de dibujo. Es uno de los formatos con mayor estandarización que existen, ya que puede ser utilizado por la gran mayoría de los programas de manejo de imágenes para existentes en el mercado, en especial para imágenes de 256 colores. Los archivos con este formato tienen la extensión .PCX.
- **TIFF:** el formato TIFF (Tagged Interchange File Format) fue diseñado para ser un formato universal de imagen. Debido a su nivel de estandarización (PC, estaciones de trabajo) el formato TIFF es el más popular entre los usuarios de computadoras; sobre todo, en el mundo del diseño publicitario y de la autoedición, ya que es utilizado como formato de transferencia para programas.

El formato TIFF tiene una especificación muy amplia, lo que quiere decir que no tiene un formato único, sino que está compuesto por multitud de especificaciones diferentes. Esta diversificación en subconjuntos puede provocar que una imagen en formato TIFF generada por un determinado paquete no pueda ser utilizada por otro diferente.

Los archivos TIFF suelen grabarse de forma comprimida; son varios los métodos de compresión que utilizan, aunque generalmente se suele usar el método LZW (Lempel-Ziv-Welch). Esta forma de compresión es totalmente reversible y mucho más eficaz que la RLE. Otras formas de compresión utilizados con el formato TIFF son PackBits, CCITT Grupo III y Grupo IV y RLE. Los archivos de imagen almacenadas en este formato tienen la extensión .TIF.

- **GIF** (Graphic Interchange Format) : El formato GIF fue creado como un formato de imagen totalmente independiente del ordenador, de modo que pudiera ser visualizada la imagen mientras que el ordenador estaba en conexión. Esta era originalmente su misión, pero rápidamente fue aceptado como formato gráfico por los usuarios. El formato GIF es el más utilizado para almacenar imágenes de 8 bits digitalizadas.

El método de compresión que utiliza es LZW; actualmente está dividido en dos variantes. La primera es el formato GIF87a, que es el formato base; el segundo es el formato GIF89a que permite almacenar información no gráfica junto con la imagen, como pueden ser comentarios, texto, etc. Los archivos almacenados con las especificaciones de este formato tienen la extensión .GIF.

- **TARGA:** El formato de archivos de imagen Targa fue creado como soporte a las tarjetas gráficas del mismo nombre. El formato se hizo rápidamente popular gracias a la calidad gráfica que suministraba, ya que era capaz de transferir archivos de 24 bits cuando prácticamente ningún formato lo hacía. Motivado por esta gran calidad, alcanzó mucho éxito entre los usuarios de programas de digitalización y diseño gráfico de alta calidad. Con el tiempo la mayoría de los formatos han adquirido la posibilidad de almacenar imágenes de 24 bits; esto unido a que genera archivos de gran tamaño ha provocado que este formato haya perdido muchos adeptos. El método de compresión es el RLE y las imágenes almacenadas en este formato tienen la extensión .TGA.
- **EPS:** los archivos EPS son un subconjunto del lenguaje llamado PostScript encapsulado. Fue diseñado para poder imprimir fácilmente desde programas profesionales de autoedición, en impresoras que soportaran este lenguaje. Una ventaja importante es su capacidad para especificar tonos de grises utilizando patrones de puntos, lo cual resulta muy beneficioso a la hora de imprimir imágenes en escala de grises o de colores si se está utilizando una impresora que sólo sea capaz de imprimir en blanco y negro. Las imágenes en formato EPS pueden ser incluidas como tales en algunos procesadores de textos y programas de imágenes y llevan la extensión .EPS.
- **JPEG** (Joint Photographic Experts Group): el formato JPEG fue diseñado para realizar trabajos de fotografía digital. Es un formato que depende básicamente de dos parámetros:
 - nivel de codificación: marca el nivel de codificación óptimo del archivo
 - nivel de calidad: indica la calidad de la imagen para esa codificación

La virtud más importante de estos archivos es que ambos parámetros pueden ser controlados por el usuario, permitiendo así definir el nivel de calidad y

codificación que desea en cada momento. Por contra es un formato que siempre sufre pérdidas en el proceso de compresión, por lo que la imagen original nunca coincide con la imagen comprimida, aunque cuanto mayor sea el factor de calidad menor será la pérdida que se produce. Las imágenes creadas bajo este formato llevan la extensión .JPG.

A continuación se describen otros formatos de menor importancia, pero que pueden encontrarse alguna vez:

- PIC: utilizado principalmente en el paquete de animación gráfica GRASP.
- RAW: utilizado fundamentalmente por expertos en tratamiento de imágenes que desean manipular directamente la imagen y tener un control total de cada uno de los colores.
- WPG: formato de las imágenes que tiene el editor de textos WordPerfect.
- IFF, LBM e ILBM: formatos generados por los ordenadores AMIGA.
- MAC: formato utilizado por los programas MacPaint.
- IMG y GEM: formatos utilizados por Ventura Publisher.
- MSP: imágenes generadas por Microsoft Paint
- ART: formato utilizado por PFS Publisher.
- RLE: formato utilizado por Windows.

De todos los Formatos Gráficos de Imágenes, el que se usa en este estudio es el **GIF** (Graphic Interchange Format), diseñado como un formato de imagen totalmente independiente del ordenador, de modo que pueda ser visualizada cuando el computador está conectado. El formato GIF es el más utilizado para almacenar imágenes de 8 bits digitalizadas, lo cual permite ocupar menos espacio de almacenamiento de información de los mensajes que se quieren ocultar. En el formato GIF se utilizan las 256 primeras combinaciones de colores básicos del modelo RGB (RED, GREEN, BLUE), tal como se detalla más adelante .

5.4.4 Archivos de imágenes

Para la computadora una imagen es una matriz de números que representan intensidades de colores en varios puntos (píxeles). (ver figura 5.4.4.1).

Una imagen típica es de 640x480 píxeles y 256 colores (ú 8 bits por píxel). El tamaño de esta imagen es de unos 300 Kb. Las imágenes digitales normalmente se almacenan en una calidad de 24 bits (16.0000.000 de colores). Una imagen de 24 bits es lo ideal para esconder información, pero estas imágenes pueden llegar a ser bastante grande en tamaño. (ver figura 5.4.4.2)



Figura 5.4.4.1 Archivo de Imágenes

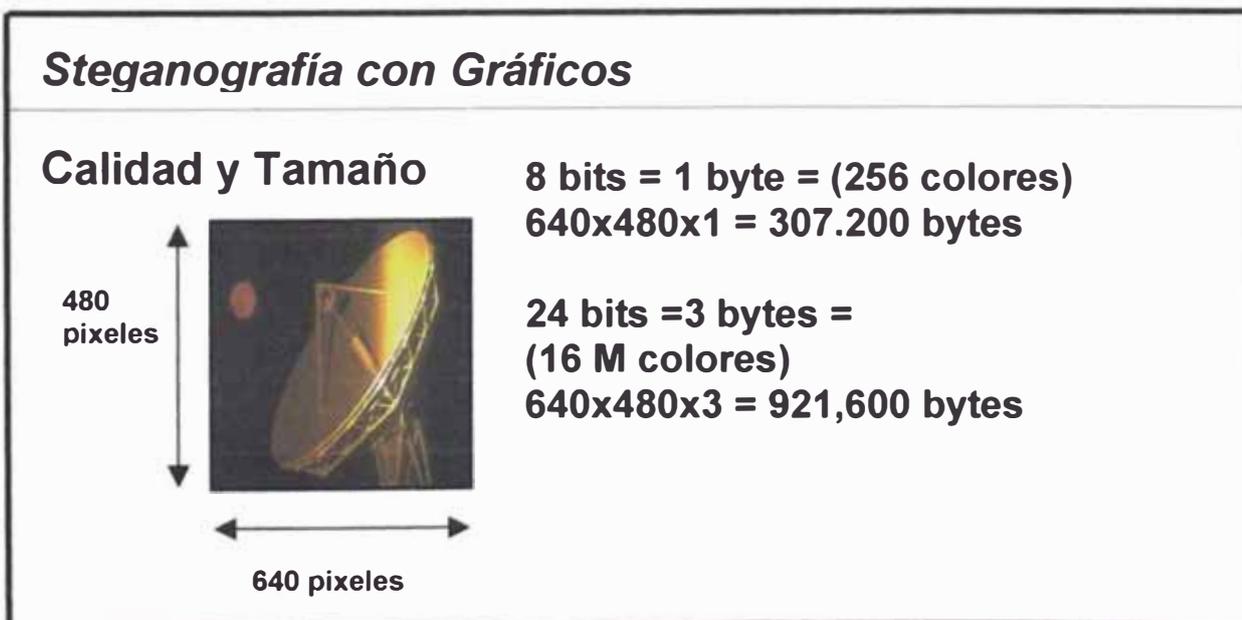


Figura 5.4.4.2 Imagen Típica grande en tamaño

Las imágenes de 24 bits utilizan 3 bytes por cada píxel para representar un valor de color. Estos bytes podrían ser representados en decimal; los valores que podrían tomar cada uno de estos bytes va desde 0 a 255. Cada uno de estos bytes representa un color como: rojo, verde y azul. Por ejemplo, un píxel en blanco tendría 255 de rojo, 255 de verde y 255 de azul.

Cabe mencionar que las imágenes de 24 bits ocupan mucho tamaño; sin embargo, la compresión de archivos puede ayudar. La compresión de archivos es de dos tipos: GIF y JPEG. Un archivo con extensión GIF guarda la estructura original del archivo, mientras que uno con extensión JPEG ahorra espacio pero no mantiene la integridad del archivo original. Para trabajos de esteganografía es necesario utilizar el del primer tipo.

Para almacenar la información que va a ser escondida en una imagen, se requiere de dos archivos. El primero es la imagen "inocente" que será la cubierta y alojará la información que se desea esconder; este archivo se llama imagen de cubierta. El segundo archivo es el mensaje: la información a esconder. Un mensaje puede ser texto plano, texto encriptado, otra imagen o cualquier cosa que puede ser llevado a bits. (Ver Figura 5.4.4.3)



Figura 5.4.4.3 Información a Esconder

El estándar en esteganografía dicta utilizar el formato BMP o GIF, evitando de no utilizar el formato JPEG. Cuando se tiene que esconder información dentro de una imagen, el primer paso es seleccionar la imagen en donde esconder la información. Se debe elegir una imagen que no posea grandes áreas de colores sólidos. Una vez que la imagen está seleccionada se debe pasar al paso de seleccionar la técnica que se va a utilizar para esconder la información.

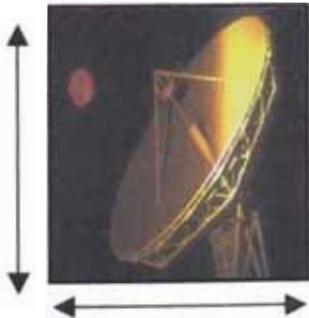
5.4.5 Esteganografía con Gráficos

La información puede ser escondida en imágenes en diferentes formas. Para esconder la información el programa puede codificar cada bit de la información a lo largo de la imagen, robando un bit de cada píxel de la imagen, o selectivamente, colocando el mensaje en áreas "ruidosas" de la imagen para que no atraigan la atención (por ejemplo el cielo). Para esconder la imagen se emplea el método clásico denominado inserción del último bit significativo. Si por ejemplo tenemos un archivo GIF con la información escondida y se convierte a.JPG, el archivo gráfico permanecerá igual, pero toda la información escondida se perderá.

Para esconder información en una imagen de 24 bits utilizando el método de inserción del último bit significante, se puede almacenar tres bits en cada píxel.

Steganografía con Gráficos

Inserción del último bit significante



24 bits = 3bytes por píxel
1024x768x3 = 2359296 bytes
Se utiliza el último bit de cada byte de la imagen y queda un espacio de 294912 bytes.

Figura 5.4.5.1 Utilización del último bit

Una imagen de alta resolución de 1024x768 en 24 bits en tamaño real ocupa: 2.359.296 Kb (ver figura 5.4.4.4), si se utiliza el último bit de cada byte de la imagen de cubierta para almacenar la información, quedaría unos 294.912 Kb para almacenar información, si a su vez esta información esta compactada, por ejemplo se podría esconder un documento de word de 300 hojas sin que haya ninguna variación en la imagen para el ojo humano.

Un ejemplo:

Si por ejemplo se tuviera una imagen que posee los siguientes valores:

00100111	}	3 bytes = 1 pixel
11101001		
11001000		

00100111	}	3 bytes = 1 pixel
11001000		
11101001		

11001000	}	3 bytes = 1 pixel
00100111		
11101001		

Suponga que se desea almacenar la letra A, cuyo código ASCII es 65 y su valor binario es: 10000011.

Si se coloca estos valores en el último píxel de cada byte quedará de la siguiente forma:

00100111	}	3 bytes = 1 pixel
11101000		
11001000		

00100110	}	3 bytes = 1 pixel
11001000		
11101000		

11001001	}	3 bytes = 1 pixel
0010011 <u>1</u>		
11101001		

Los valores subrayados son los que han sido cambiados. El color de la imagen casi no varió en nada, pero para el ojo humano es imposible distinguir esta diferencia de colores. Las imágenes de 8 bits (256 colores) no son muy utilizadas en el método de inserción del último bit significativo. Software que permite cumplir esta función son Steganos y S-Tools.

Como ya se ha mencionado anteriormente El esconder un mensaje dentro de una imagen se llama "esteganografía"., que es un sistema conocido desde hace mucho tiempo, pero actualmente mucho más refinado gracias a la computación. En las líneas siguientes se hace una descripción de cómo funciona el modelo RGB que es la base de colores que se usa en una plantilla a través de píxeles que son necesariamente usados en las imágenes. Así mismo, se debe tener en cuenta la posición o ubicación del mensaje a ocultar, dado que algunos lugares dentro de una imagen pueden ser más adecuados que otros, por la claridad de los contrastes, en donde se puede almacenar la información o texto a enviar.

5.4.6 Principios del Modelo RGB

En el modelo de colores RGB ("red, green, blue": rojo, verde y azul), que se utiliza para las imágenes en formato GIF, los colores se describen mediante tres valores cuyo rango va de 0 a 255. El primer valor es para el rojo, el segundo para el verde y el tercero para el azul. Mientras más alto sea el número, más fuerte será el color, tal como se muestra en la tabla 5.4.6.1.

Color	R	G	B
Rojo	255	0	0
Verde	0	255	0
Azul	0	0	255
Amarillo	255	255	0
Blanco	255	255	255
Negro	0	0	0

En el modelo RGB hay un total de:
 $256 \times 256 \times 256 = 16.777.216$ posibles colores



Tabla 5.4.6.1 Algunos Colores Primarios en RGB

El pintado con números se realiza con una paleta que es la lista de los colores RGB usados en una imagen. La mayor parte de los documentos GIF en web utilizan una palette de 8 dígitos binarios, lo cual quiere decir que de los 16.777.216 posibles colores se admite solamente 256, porque una cifra de 8 bits sólo puede tomar 256 distintos valores. La imagen ha de ser concebida como una rejilla u hoja cuadrículada con una cifra de la paleta en cada celda de la rejilla. Esa cifra o “índice” tiene la forma de un número binario de 8 dígitos, es decir, una serie de ocho ‘1’ y ‘0’ que corresponde a un número .espués entre 0 y 256. Cada celdilla es un punto de color llamado .espu.

Recordar que el bit ubicado en el extremo derecho de una serie binaria se designa como el menos significativo, por cuanto su cambio es el que menos afecta el valor del número. Al cambiarlo en la imagen, será por lo tanto casi indetectable.

5.4.7 Criptografía icónica

Sabiendo lo anterior, se puede ahora pensar en un sistema que utilice estas características para esconder mensajes en una imagen GIF. Para que no sea detectable a primera vista, la técnica consiste en utilizar el bit menos significativo de cada píxel, cambiándolo en función del mensaje a esconder. Veamos cómo hacerlo. Para codificar la imagen en formato binario, primero ordenar la paleta como sigue:

2. Para empezar se recoge la paleta de todos los colores que aparecen en la imagen (esta es la “paleta original”). Se emplea el comando Put píxel.
2. Luego se reordena esta paleta de tal modo que los colores cercanos en la realidad sean igualmente cercanos en la paleta digital (Es la “paleta reordenada”).

La figura 5.4.7.1, ilustra cómo se verán los 9 primeros colores de la paleta para la imagen GIF anexa, antes y después del reordenamiento:



Figura 5.4.7.1 Colores de la imagen antes y después del reordenamiento

Luego, para poder introducir el mensaje, se debe cambiar un bit a la vez como sigue:

1. Se toma el primer bit del mensaje.
2. Se busca el índice del primer píxel en la paleta reordenada y se lo cambia por el primer bit del mensaje a esconder.
3. Se busca el nuevo color RGB al cual corresponde este nuevo número en la paleta original.
4. Se cambia el píxel original por este nuevo color.

Ejemplo:

17 231 31 es el color 00100101 en la paleta reordenada.

El índice de valor 00100101 es cambiado a 00100100.

El color 00100100 en la paleta reordenada es 179 233 36.

179 233 36 es el color 11101110 en la paleta original.

El valor del píxel se cambia a 11101110.

Para recuperar el mensaje original, proceder de la forma siguiente:

1. Buscar el índice del color de cada píxel RGB en la paleta reordenada.
2. El bit menos significativo de este índice proviene del mensaje original, así que se copia al archivo de salida. (out.gif)
3. Terminado el proceso con todos los píxeles, se lee el nuevo documento con una aplicación normal de lectura (o el mismo programa de decodificación, si lo permite).

Ejemplo:

179 233 36 es el color 00100100 en la paleta reordenada.

El bit menos significativo es 0.

Se escribe 0 en el archivo de salida.

5.4.8 Explicación y Evolución del Algoritmo Esteganográfico.

Los códigos RGB hacen posible la unión de muchas tonalidades de colores críticos para formar una pieza formal gráfica adecuada.

Mapa de Bits

Un mapa de bits (bitmap en inglés), es un conjunto de bytes (un byte es un conjunto de 8 dígitos binarios como por ejemplo 10111011 que representan algo), ubicados en alguna zona de la memoria de la computadora. Ahora nos debemos de plantear la interrogante siguiente: ¿En que se diferencia un mapa de bits de otro conjunto ordenado de bytes? La respuesta es en la forma en cómo son interpretados por la computadora. Un mapa de bits se relaciona normalmente con la salida hacia una impresora o pantalla. Estos interpretan el código de cada byte como un color. Puesto que tenemos 8 posiciones distintas para un byte, la cantidad de colores que se puede almacenar se explica a continuación:

Potencias de 2

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
0	0	0	0	0	0	0	0	= 0 hasta
1	1	1	1	1	1	1	1	= 255

Esto significa que existen 256 posiciones distintas donde se podrían almacenar hasta 256 colores por trama. Cada parte de la gráfica es tratada como una cuadrícula (ver figura 5.4.8.1), la cual tiene una representación en un byte que es traducido a un código hexadecimal. Cada cuadradito de la cuadrícula o rejilla (es decir cada celda en que se parte la gráfica) viene a ser un píxel. Entonces la trama de bits, 00101101 puede expresarse de la siguiente manera: 0010 1100 = 2C, esto de acuerdo a los códigos binarios. Luego, 1 byte es igual a 2 dígitos hexadecimales, para mayor ilustración tabla 5.4.8.1.

Código Binario	Código Hexadec.
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7

Código Binario	Código Hexadec
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Tabla 5.4.8.1 Equivalencias de Códigos Binarios a Hexadecimales

Profundidad del color

Se denomina profundidad del color a la cantidad de bits que se destinan a representar un código de color. Por ejemplo, si se tuviera una profundidad de color de un bit únicamente podríamos tener imágenes en blanco (1) y negro (0), dado que éstos serían los únicos valores posibles para almacenar un bit. Una profundidad de dos bits, daría lugar a cuando mucho 4 colores por píxel. Entonces, la fórmula para hallar el número de colores es:

$$N^{\circ} \text{ de colores} = 2^{(\text{profundidad de color})}$$

Teniendo entonces los códigos RGB, éstos representan una trama de 24 bits por ello, el mapa de bits se le suele llamar color de 24 bits, dado que tenemos 8 bits (1 byte) por cada código RGB. Para el rojo (Red) hay 8 bits, para el verde (Green) hay otros 8 bits y para el azul (Blue) hay también 8 bits. Luego todas las combinaciones por cada byte serán:

Por Rojo = 8 bits = 1 byte = puede almacenar hasta 256 tonalidades de rojo.

Por Verde = 8 bits = 1 byte = puede almacenar hasta 256 tonalidades de verde.

Por Azul = 8 bits = 1 byte = puede almacenar hasta 256 tonalidades de azul.

En la figura 5.4.8.1, se observa, que cada píxel de la gráfica representa un número de dos dígitos pero hexadecimal: es decir, 1 byte por cada píxel. Esto es lo que puede almacenar un formato BMP (o bitmap o mapa de bits por cada punto de color). Por ello el formato BMP ocupa más espacio que el GIF, que sólo almacena 1

byte; es decir, los primeros 256 colores de toda la paleta RGB. El algoritmo esteganográfico trabaja con GIF.

$$256 \times 256 \times 256 = 2^{24} = 16\,777\,216$$

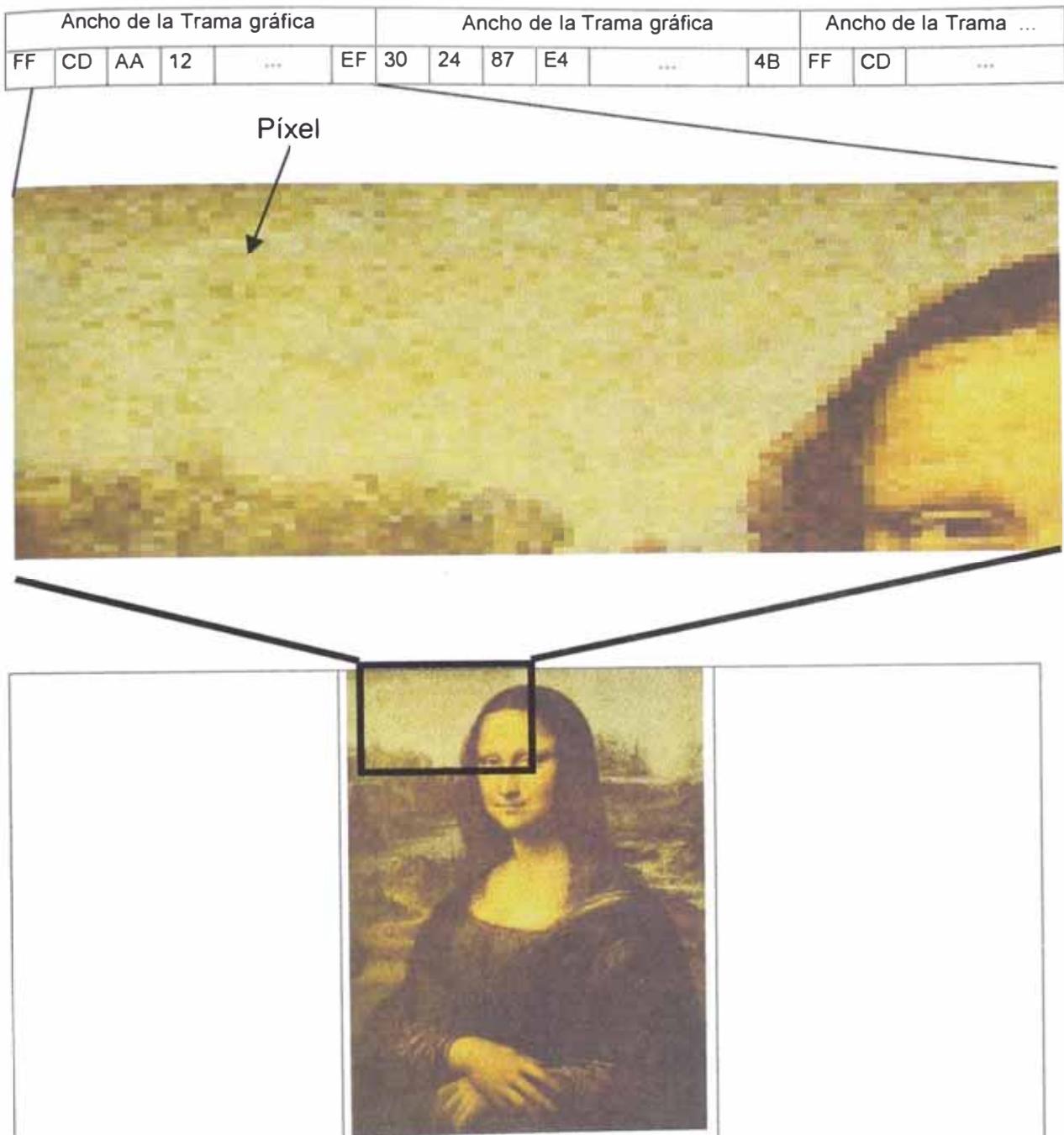


Figura 5.4.8.1 Trama de bits en forma de rejilla o cuadrícula.

Algoritmo

Para una mejor explicación del algoritmo se emplean dos ejemplos.

Ejemplo 1:

1. Se lee cada trama de cada bit, por ejemplo tomando el caso de la figura 5.4.8.1 se tiene:

Ancho de la Trama gráfica					
FF	CD	AA	12	...	EF

El primer Byte es: FF = 1111 1111. El bit menos significativo es el de la menor potencia de dos: 1111 111 **1** → Bit menos significativo.

2. En dicho bit se inserta cada bit del mensaje. Por ejemplo si se inserta la letra **A**, se utilizará su código ASCII = 65 = 41 en hexadecimal. Ahora 41 en hexadecimal es en binario 0100 0001. Luego necesitaríamos 8 píxeles para insertar dicha información:

Trama de bits originales		Trama de bits insertando la letra A
1111 111 1		1111 111 0
1100 110 1		1100 110 1
1010 101 0		1010 101 0
0100 110 1		0100 110 0
1010 100 0		1010 100 0
1000 010 0		1000 010 0
1001 011 0		1001 011 0
0011 110 1		0011 110 1

0100 0001 = Código ASCII de la letra **A**.

Esto variará un poco el color pero será poco perceptible.

- Se procede a insertar todas las letras hasta que se acabe la trama de caracteres. Cuando se acaba. Se pone un carácter de finalización para la hora de la descryptación.

Ejemplo 2:

Se tiene la siguiente trama de bits:



Cada código numérico de 8 bits de los colores es:

11110001	10001010	10101010	10000110	11111101
11110001	10001010	10101010	10000110	11111101
11110001	10001010	10101010	10000110	11111101
11110001	10001010	10101010	10000110	11111101
11110001	10001010	10101010	10000110	11111101
11110001	10001010	10101010	10000110	11111101
11110001	10001010	10101010	10000110	11111101

Se desea guardar el mensaje **ABC** como ejemplo didáctico. Para ello se separan los últimos bits menos significativos por cada fila:

```

1111000 1
1000101 0
1010101 0
1000001 1
1111110 1

```

Como tenemos una trama de 35 bytes, podemos guardar $35 / 8$ aproximadamente 4 caracteres, es decir ABC más un carácter de finalización de trama. ABC~. El carácter ~ (Código ASCII 126) indica la finalización de la trama, y el algoritmo sólo lee hasta encontrar el carácter ~. Los códigos de A, B y C son los siguientes:

A = 01000001 = 41 hexadecimal

B = 01000010 = 42 hexadecimal

C = 01000011 = 43 hexadecimal

Por ello insertaremos los bits de la siguiente manera (ver figura 5.4.8.2)

1111000 0	1000101 1	1010101 0	1000011 0	1111110 0
1111000 0	1000101 0	1010101 1	1000011 0	1111110 1
1111000 0	1000101 0	1010101 0	1000011 0	1111110 1
1111000 0	1000101 0	1010101 1	1000011 0	1111110 0
1111000 0	1000101 0	1010101 0	1000011 1	1111110 0
1111000 1	1000101 1	1010101 1	1000011 1	1111110 1
1111000 1	1000101 0	1010101 0	1000011 0	1111110 1

Figura 5.4.8.2 Inserción de bits

El carácter ~ en binario es: 0111 1110 = 7E h. para la mejor visualización del ejemplo anterior se puede apreciar la figura 5.4.8.3.

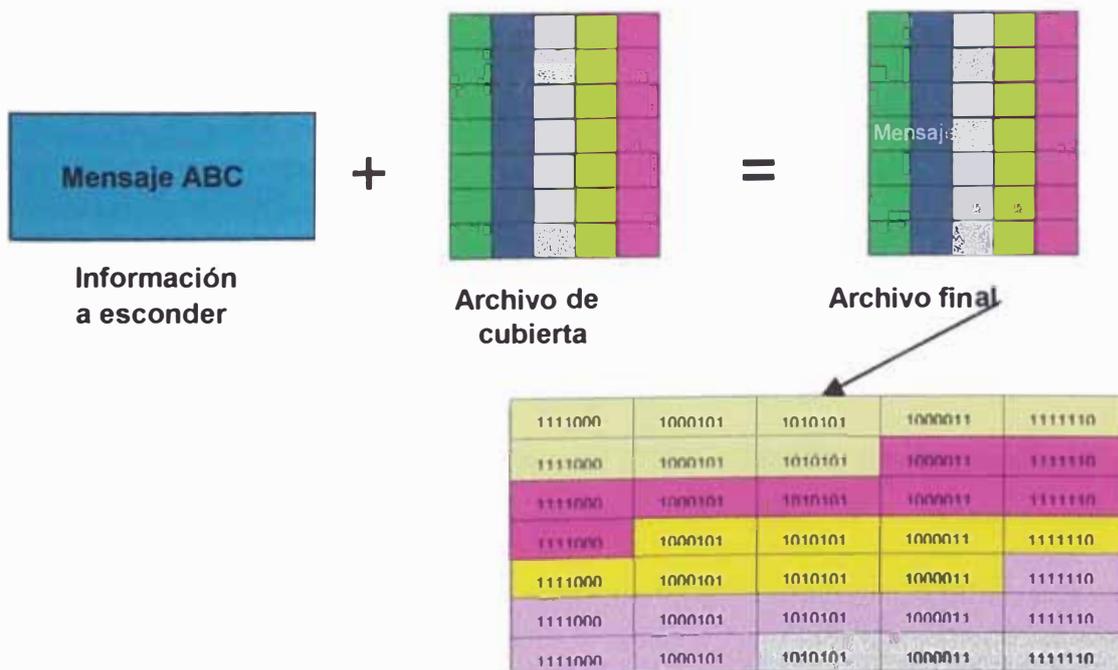


Figura 5.4.8.3 Almacenamiento de Información

El programa fuente para simular este algoritmo se ha elaborado en Java y se anexa en la presente investigación.

5.4.9 Pasos a seguir para Ejecutar el Programa de Esconder (Esteganografía) un Texto dentro de una Imagen

Los pasos siguientes se pueden verificar en cualquier PC compatible que tenga instalado el programa JAVA versión 1.1.8.

- 1 Se ingresa al disco duro donde se ha guardado el programa fuente. En nuestro caso particular, el "C". Ingresar la siguiente dirección: C:\jdk1.1.8\lib> (ver figura 5.4.9.1).

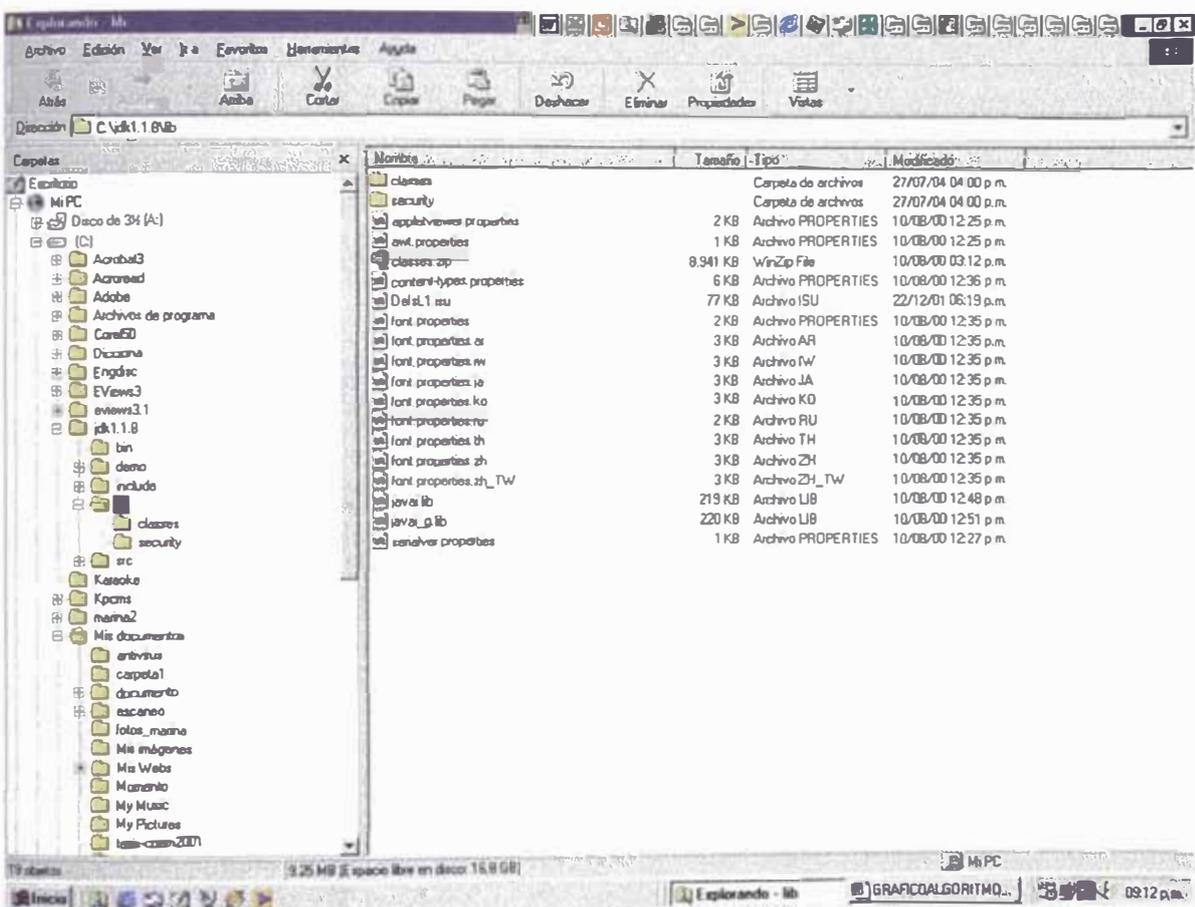


Figura 5.4.9.1 Pantalla de inicio para Ejecutar el Programa

2. Se va al icono inicio y se ingresa al icono ejecutar, apareciendo la ventana ejecutar con el comando command.com, tal como se muestra en las figuras 5.4.9.2 y 5.4.9.3.

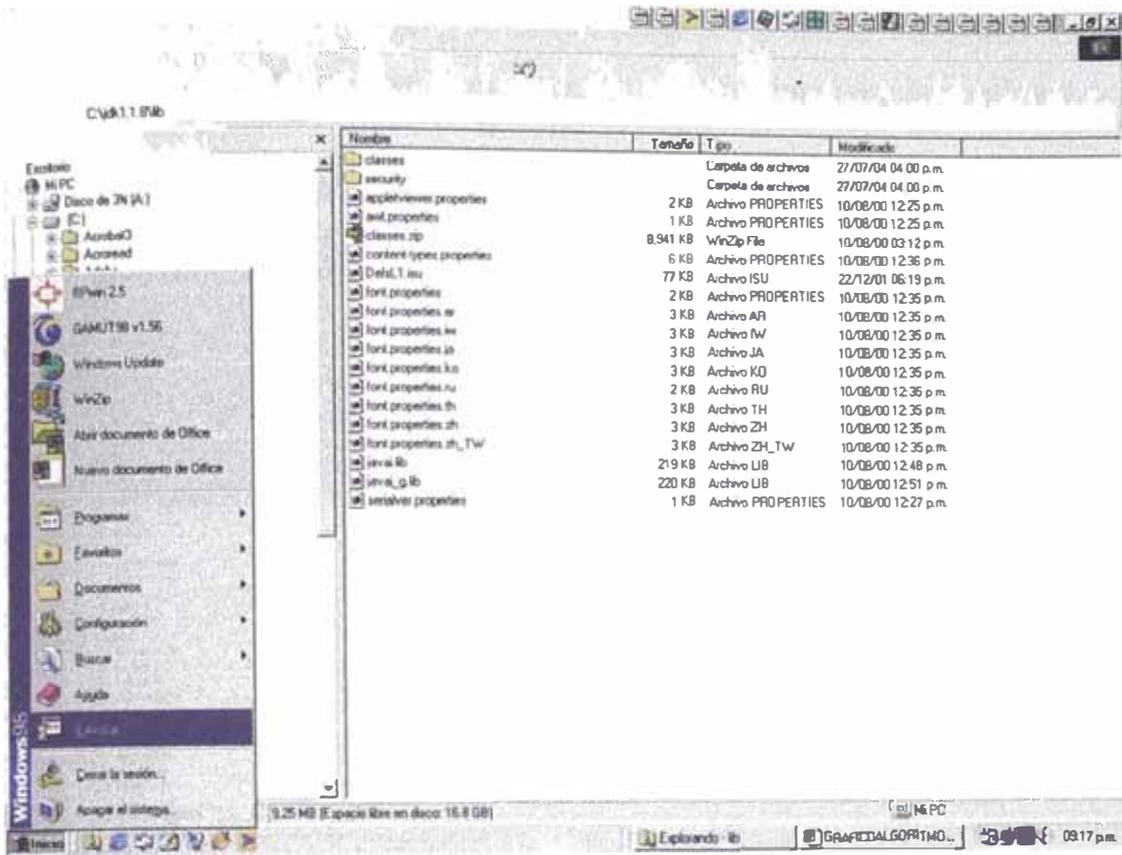


Figura 5.4.9.2 Pantalla muestra el icono Ejecutar

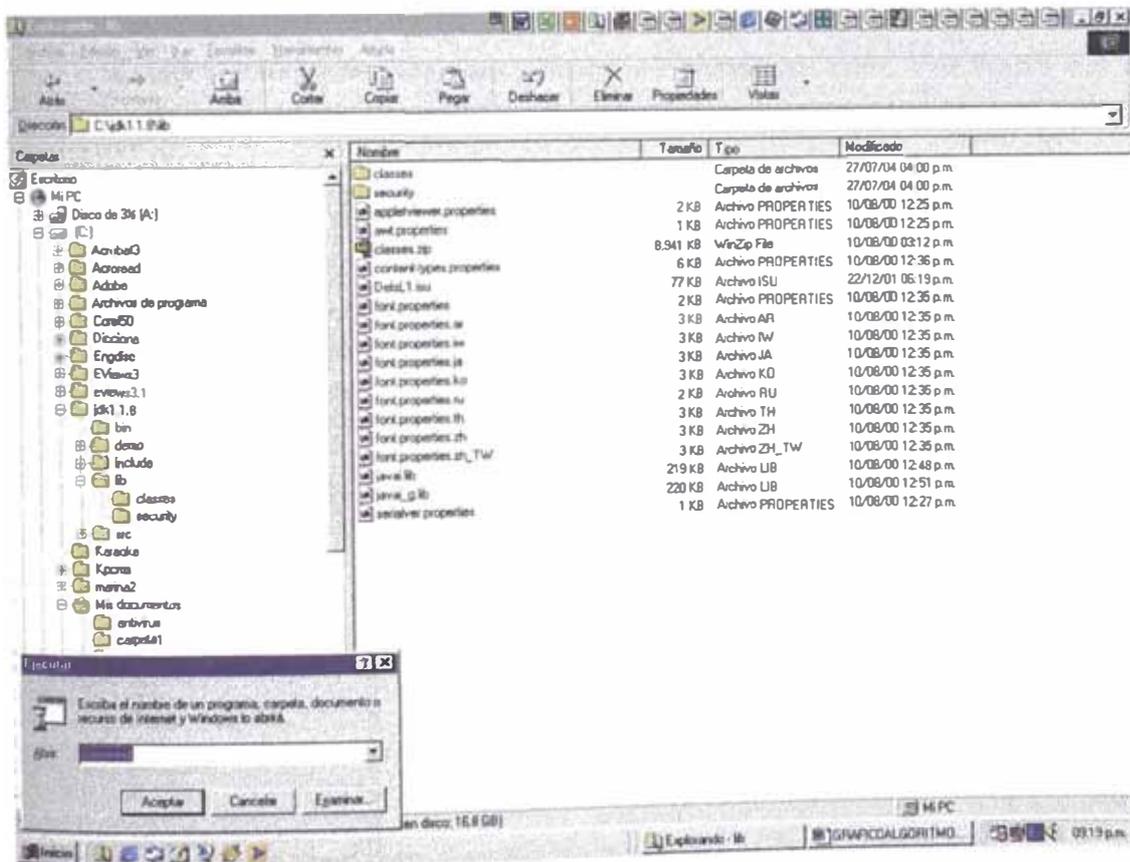


Figura 5.4.9.3 Pantalla que muestra el comando Command.com

3. En la ventana Ejecutar presionar Aceptar. Entonces aparece la ventana del sistema operativo sobre el que correrá el programa. Ver figura 5.4.9.4.

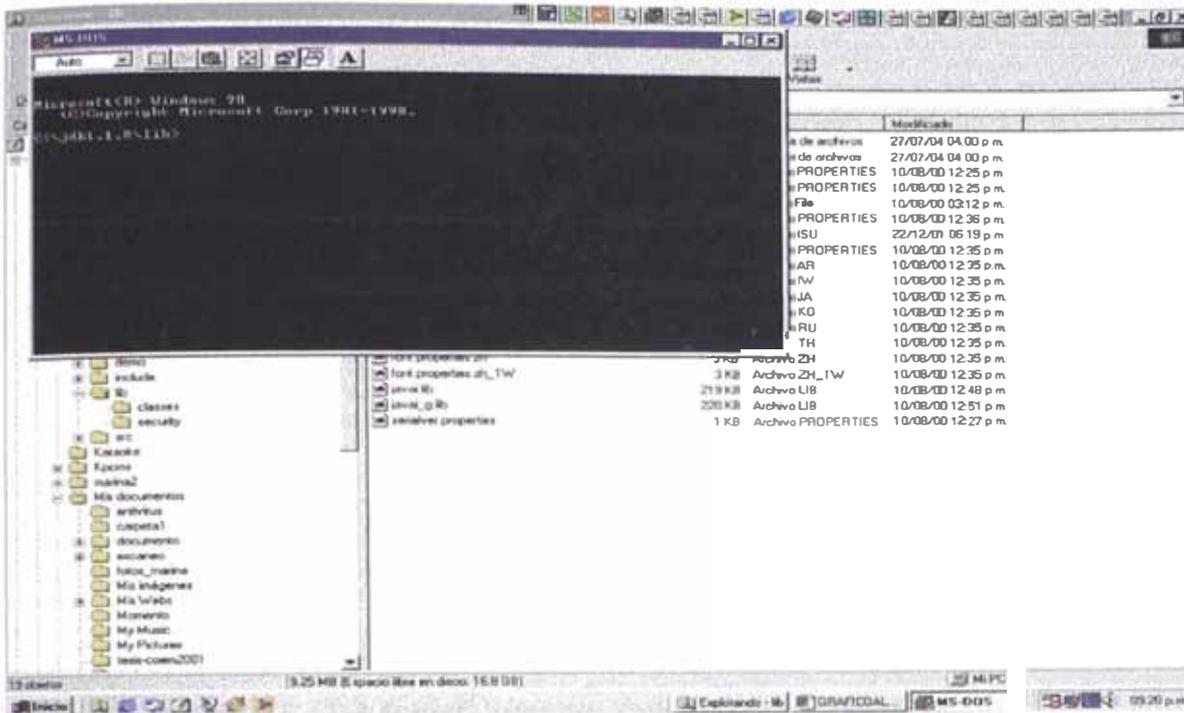


Figura 5.4.9.4 Pantalla que muestra el DOS sobre el que va a correr el Programa

4. En la ventana del sistema operativo escribir el siguiente comando:
`C:\jdk1.1.8\lib\classes>java SteganoGifPaletteOrder.` Ver figura 5.4.9.5.

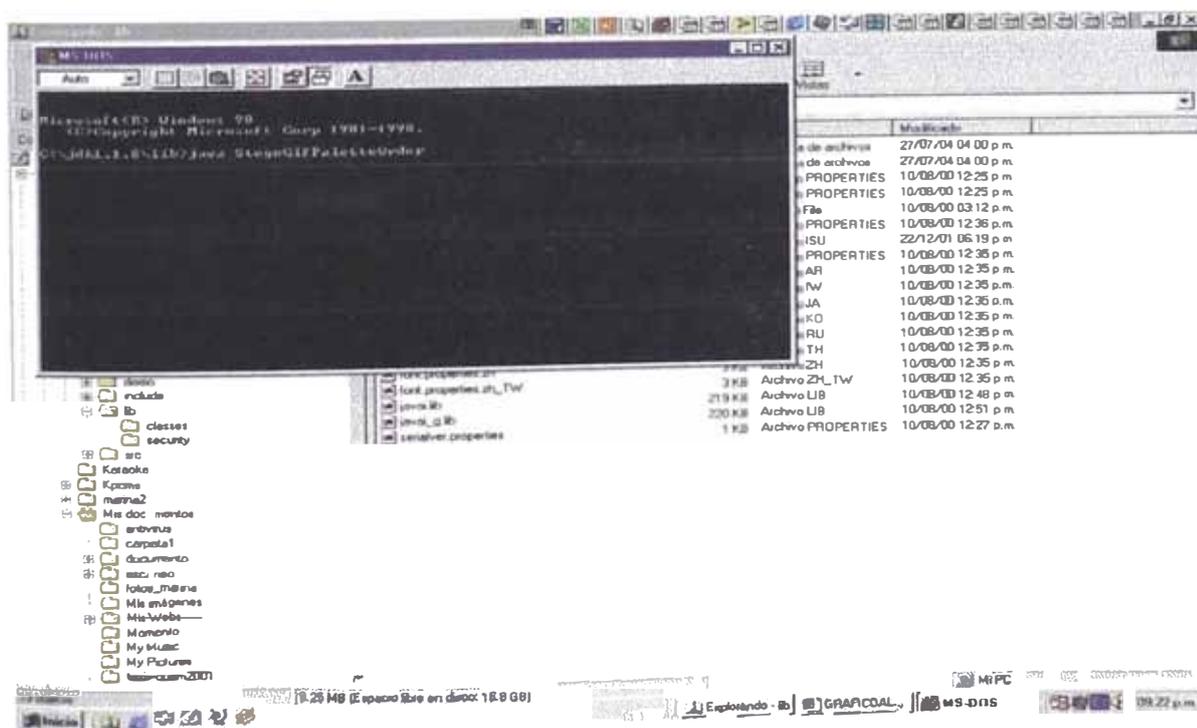


Figura 5.4.9.5 Pantalla para escribir el Comando para correr el Programa

- Una vez que el programa reconoce el comando aparece una nueva ventana donde escribiremos el mensaje a esconder (ver figura 5.4.9.6).

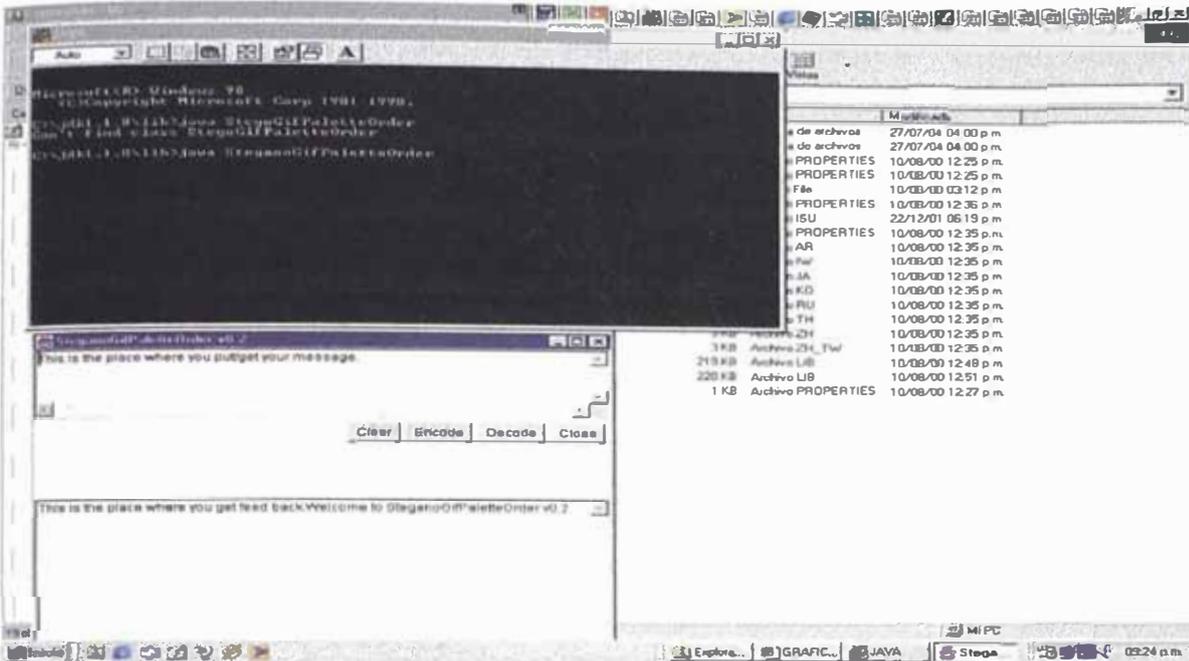


Figura 5.4.9.6 Pantalla para escribir el mensaje a esconder

- Seguidamente se escribe el mensaje a esconder presionando el icono ENCODE, apareciendo la ventana GIF for encoding requiriendo el archivo de la figura GIF que se utilizará (ver figura 5.4.9.7).

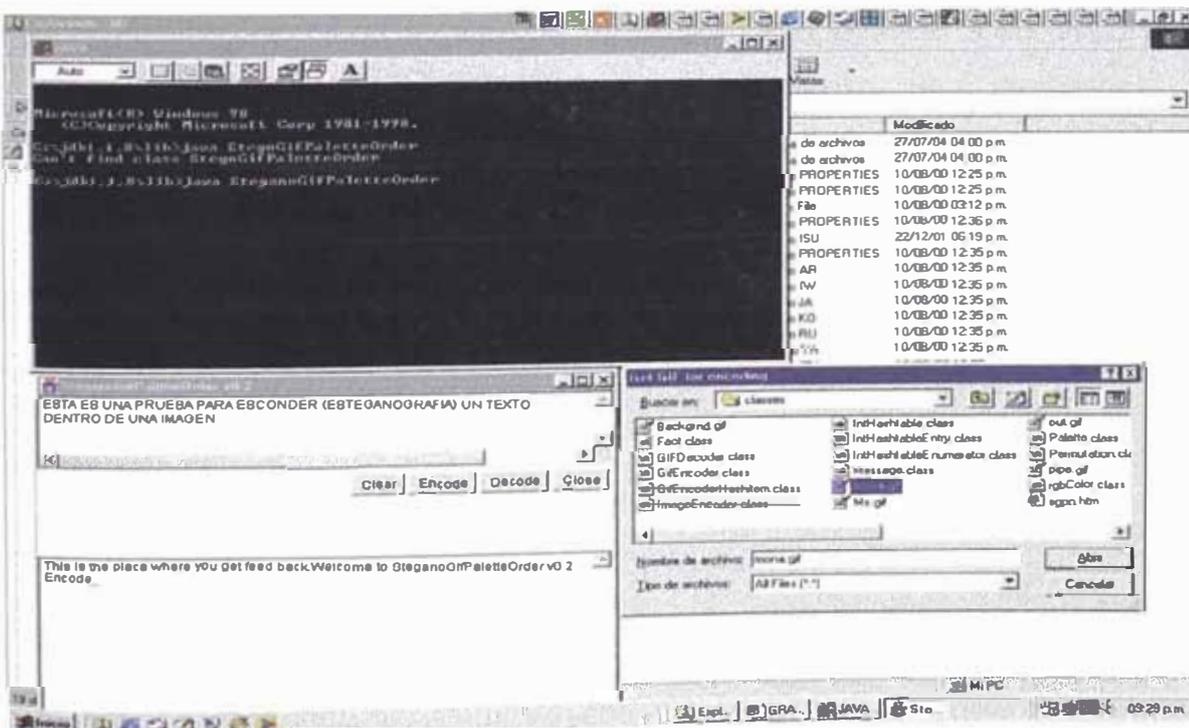


Figura 5.4.9.7 Pantalla que muestra la figura sobre el que se escondera el mensaje

7. Una vez que se dá el comando Abrir en la ventana GIF for encoding de la imagen GIF seleccionada, aparecerá la imagen seleccionada en la pantalla, y la ventana SteganoGifPaletteOrder. En la parte inferior de esta ventana debe aparecer la palabra DONE, lo que significa que el texto ha sido escondido (ver figura 5.4.9.8)

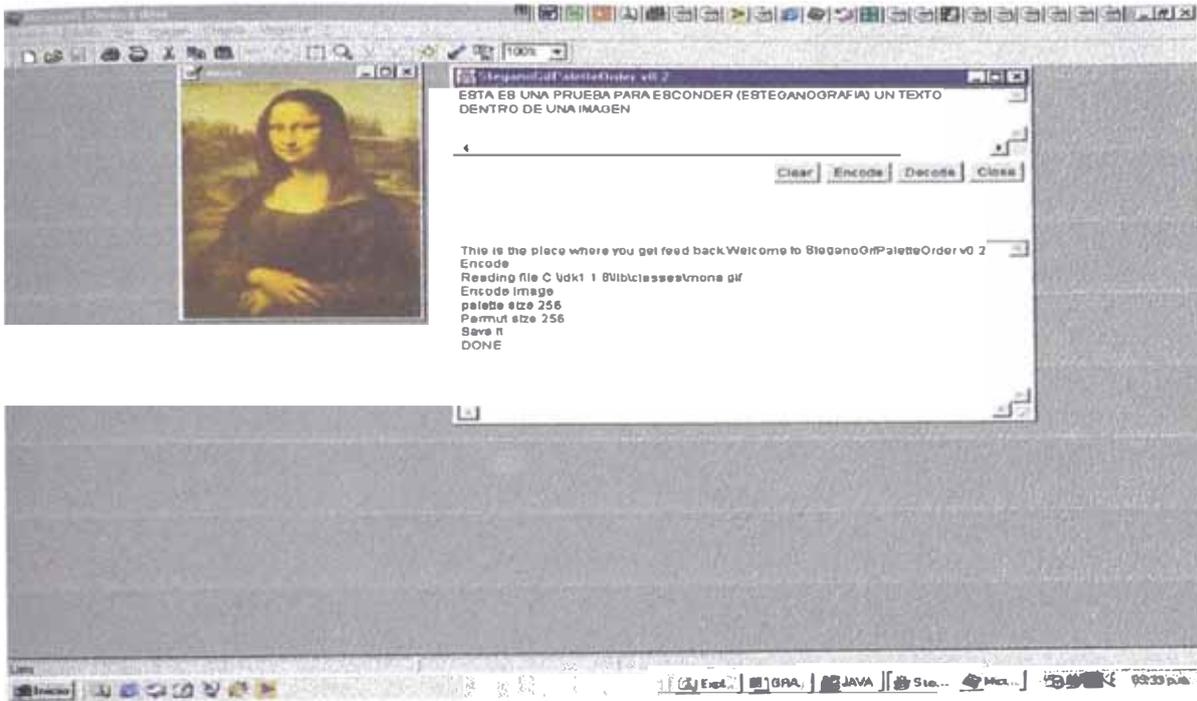


Figura 5.4.9.8 Pantalla que muestra que se ha escondido el mensaje (DONE)

8. Una vez escondido el mensaje, este mensaje es enviado al destinatario, quién debe también tener instalado los mismos programas que el remitente. Cuando el destinatario recibe el mensaje, aparece la imagen y la ventana SteganoGifPaletteOrder, donde se procede a hacer clic en Decode, después de lo cual aparecerá la ventana Get GIF for decoding. En esta ventana seleccionar out.gif y presionar Abrir (ver figura 5.4.9.9.)

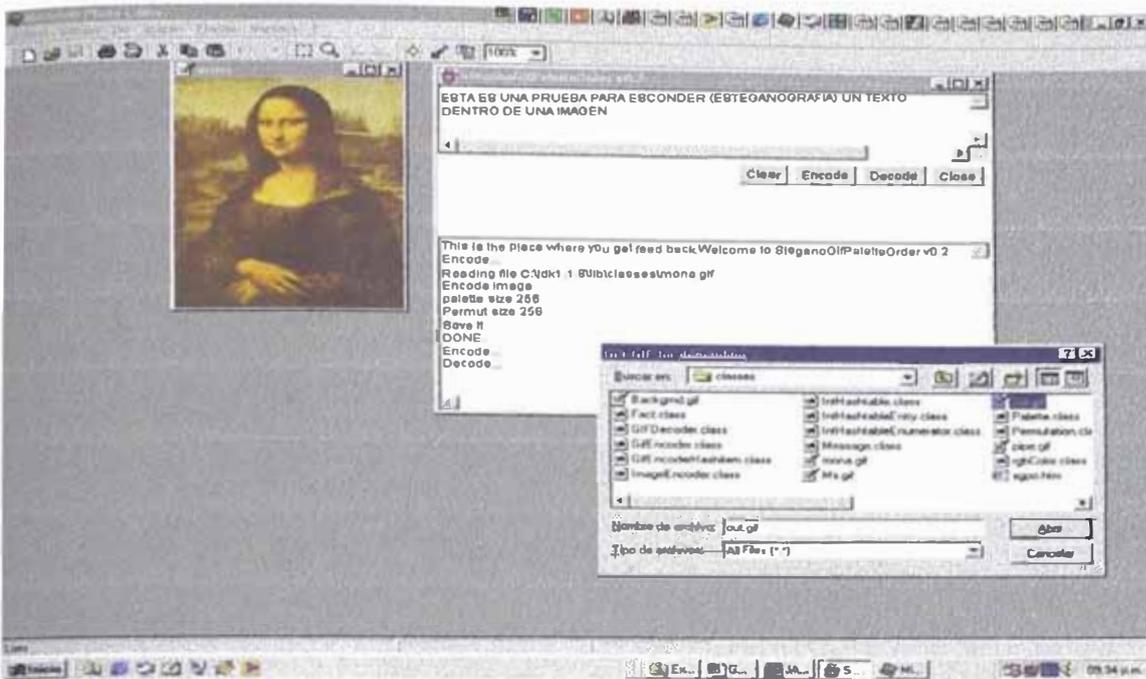


Figura 5.4.9.9 Pantalla que muestra el mensaje enviado (out.gif)

9. Una vez que se abre el archivo out.gif, aparecerá la imagen y una ventana mostrando el mensaje que había escondido para su envío (ver figura 5.4.9.10)

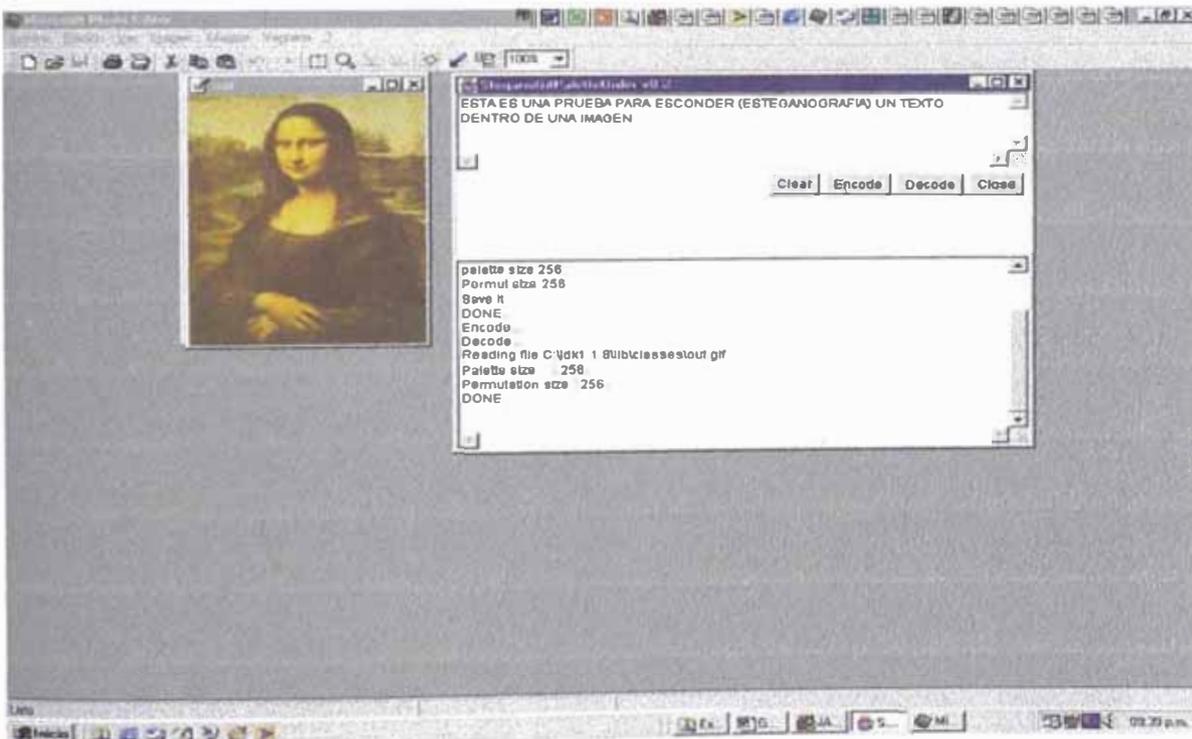


Figura 5.4.9.10 Pantalla que muestra el mensaje enviado y la imagen

10. En la siguiente pantalla se muestra las dos imágenes, la que se utiliza para esconder y enviar el mensaje y la que se recepciona con el mensaje (ver figura 5.4.9.11).

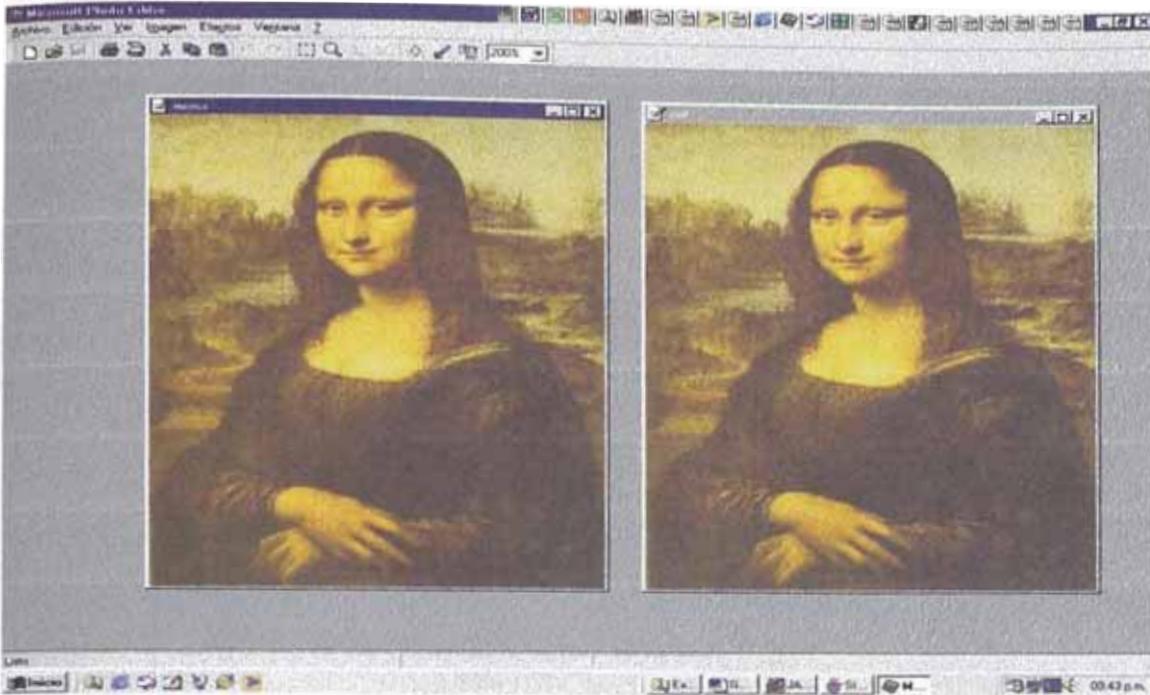


Figura 5.4.9.11 Pantalla muestra imagen con mensaje y sin mensaje

11. Como se puede apreciar la diferencia entre las dos imágenes en la pantalla anterior, es imperceptible a la vista humana, para dar mayor evidencia a lo indicado, se muestran las mismas figuras a una escala de 1,600. Es de notar que a esta escala se aprecia con mejor claridad los píxeles, los cuales no muestran diferencia alguna (ver figura 5.4.9.12).

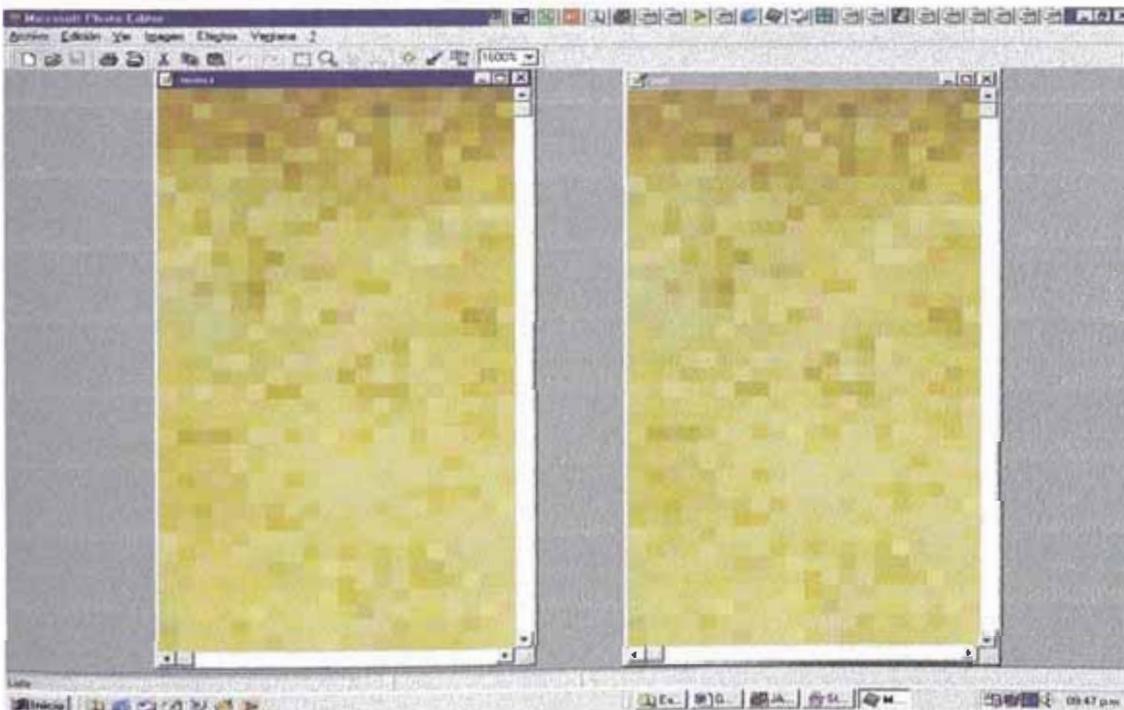


Figura 5.4.9.12 Pantalla muestra los píxeles de una imagen a escala de 1,600 antes y después del envío de mensaje

La programación de los programas de codificación y decodificación se basan en los diagramas de flujo adjuntos. Los programas fuentes correspondientes se encuentran en el anexo D.

DIAGRAMA DE FLUJO PARA EL PROGRAMA CODIFICADOR

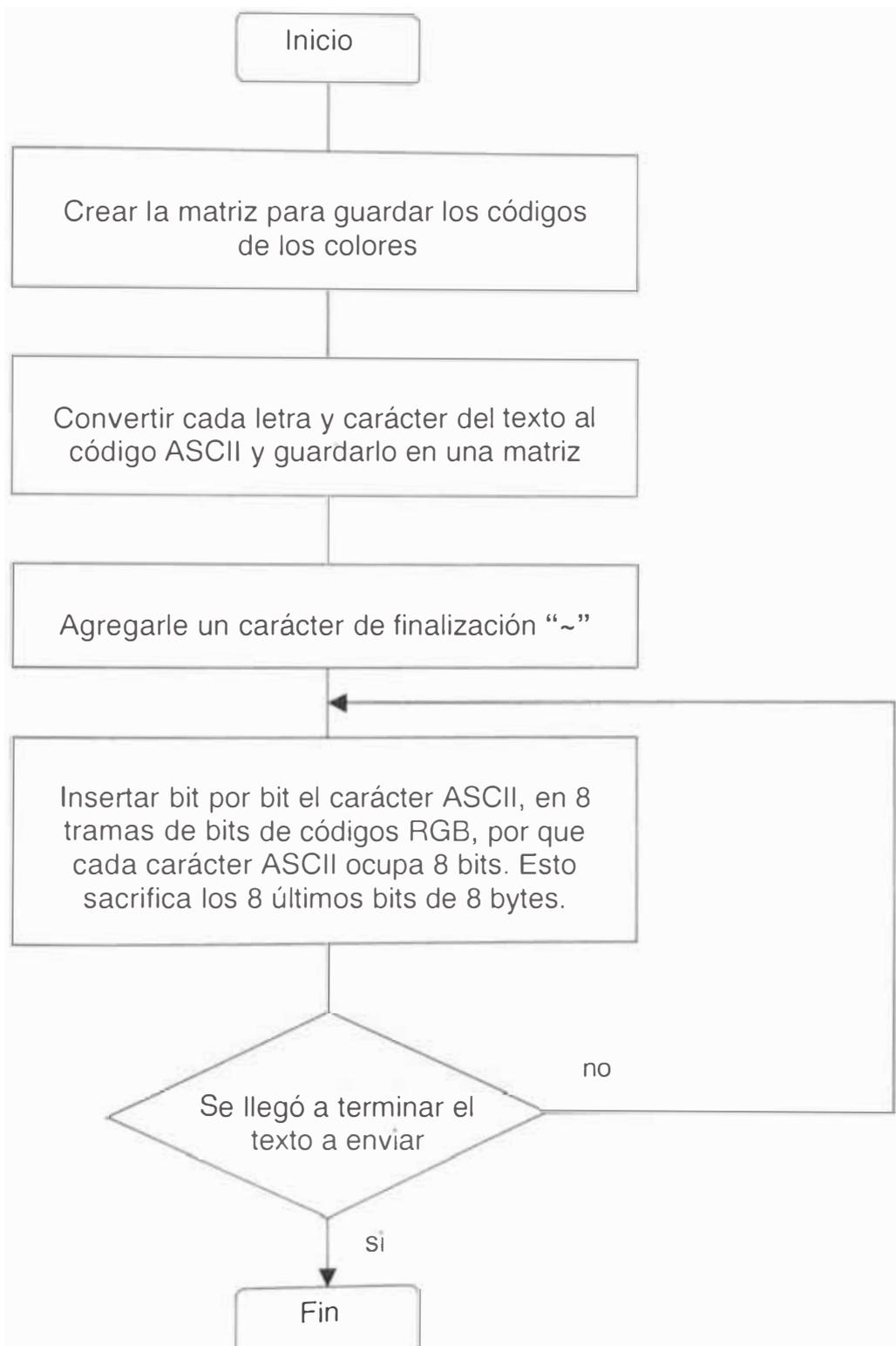
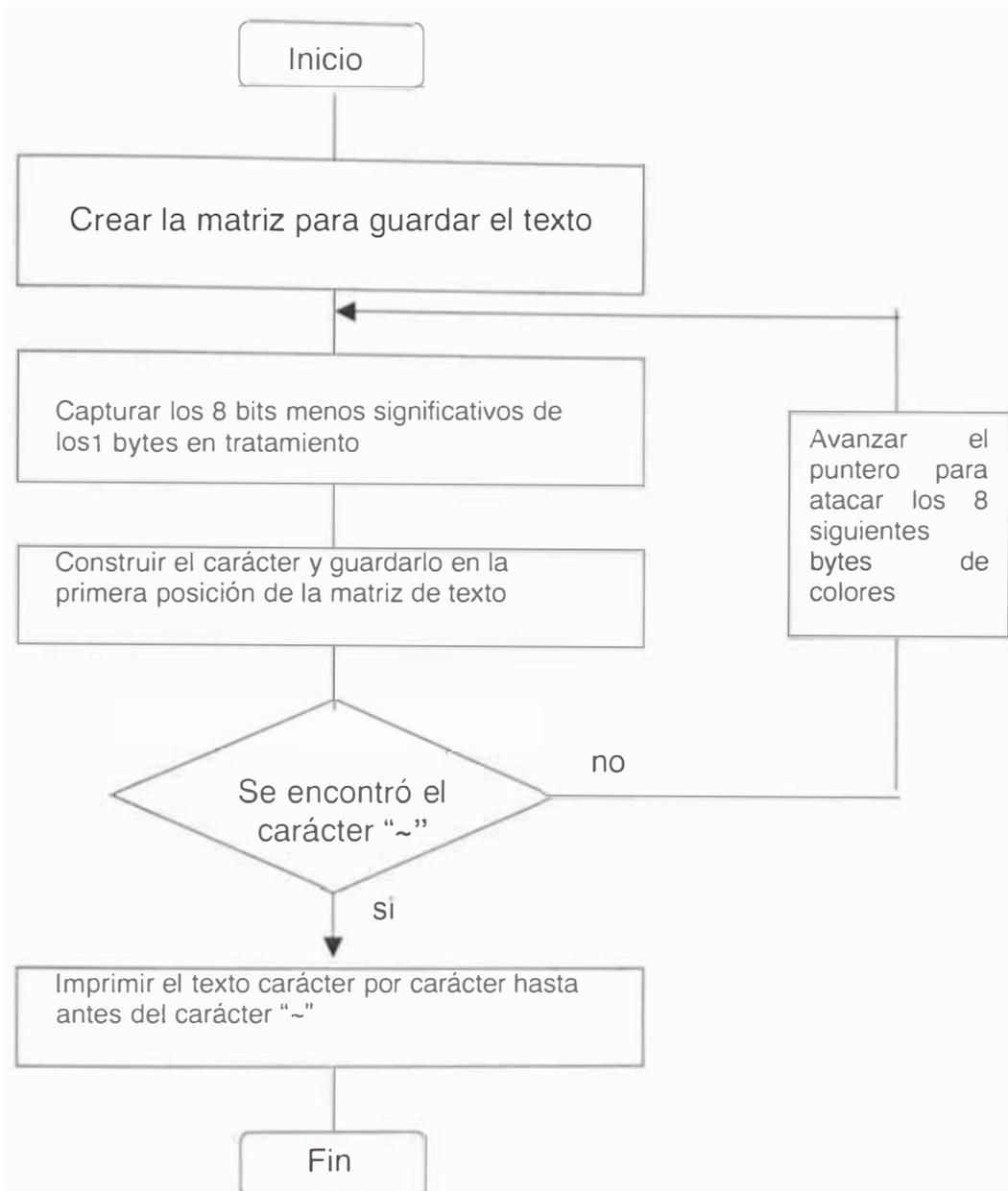


DIAGRAMA DE FLUJO PARA EL PROGRAMA DECODIFICADOR



Capítulo 6

Simulación de la Intranet

6.1 Alcance

La simulación del diseño propuesto tiene como objetivo presentar la estructura básica de la Intranet para la Marina de Guerra, así como brindar los lineamientos básicos para que exista una estandarización de contenido, de manera que de ser implementada, permita que cada dependencia al momento de iniciar el desarrollo de su propia Intranet lo realice bajo un mismo patrón.

En la simulación se presenta la Página Central de la Intranet, en el que se visualiza la interrelación de la estructura básica desarrollada en el punto 4.2. , esta estructura está representada por diferentes íconos, por ejemplo, dependencias, datos administrativos, etc., siendo éstos dinámicos y listos para introducir información.

En mayor detalle, se ha desarrollado la Intranet del CEMENA, dado que se contaba con información de las necesidades y requerimientos de esta dependencia.

Debe mencionarse que la Intranet desarrollada es solamente una propuesta, de ser posible su implementación, esta sujeta a muchos cambios de acuerdo al uso y a las necesidades que se presenten en el uso continuo, de manera que se logre llegar a la satisfacción de los usuarios.

Para validar el diseño de la Intranet propuesta en este trabajo de tesis, se simuló en mayor detalle la Intranet del CEMENA, dado que se contaba con información de las necesidades y requerimientos de dicha dependencia.

Finalmente, debe tomarse en consideración que la presente simulación no contempla intercambio de información de base de datos, dado que las interfaces para intercambio de información con base de datos se realiza una vez implementada.

6.2 Metodología

Una vez que se ha realizado el análisis y el diseño, se ha procedido a realizar el desarrollo de la Intranet, para lo cual se presenta una simulación orientada a mostrar la interrelación de los íconos de la Página Central descrita en el punto 4.2, esta demostración se realizó utilizando como herramienta de programación el Front Page 2000 por ser de fácil manejo.

A continuación se va a proceder a describir en forma breve el funcionamiento de esta simulación, dando énfasis al ícono correspondiente a DISAMAR.

Por ejemplo, si se ingresa por el menú de barras o por descripción de accesos, en ambos casos se obtiene información en el nivel administrativo, técnico u operacional, y el contenido de cada nivel nos brinda información relacionada a noticias, servicios, grupos de trabajo, dependencias, etc., también se puede observar que en la página auxiliar que se encuentra en la parte izquierda de la página se ha considerado como uno de los íconos dependencias. Si se ingresa por este ícono, aparecerá todas las dependencias de Marina sin tomar en cuenta a que área pertenece si es administrativa, técnica u operacional, a diferencia que si uno ingresa por la ventana de descripción de accesos tendría uno que saber a que área pertenece, finalmente se puede observar que el aviso de área de interés es dinámico, significa esto que tiene que estar en constante actualización.

Cada ventana ó icono de la página principal esta lista para almacenar información.

Como parte de la simulación se ha desarrollado la Web del Centro Médico Naval en forma mas detallada por contar con información de los requerimientos.

Para una mayor ilustración se ha realizado la cartografía del sitio correspondiente, ello se muestra en las figuras 6.2.1 y 6.2.2.

Para ingresar a la ventana correspondiente a DISAMAR se puede ingresar por dos vías en la página principal, uno por páginas auxiliares y entrar a dependencias y por otro lado por la parte de accesos en el nivel técnico y dependencias, por cualquiera de ellas se obtiene la siguiente información:

Se ingresa a DISAMAR y aparece una foto del Hospital Naval una vez que se realiza un enter, automáticamente aparece la página principal y en la columna de la derecha se visualiza los siguientes vínculos

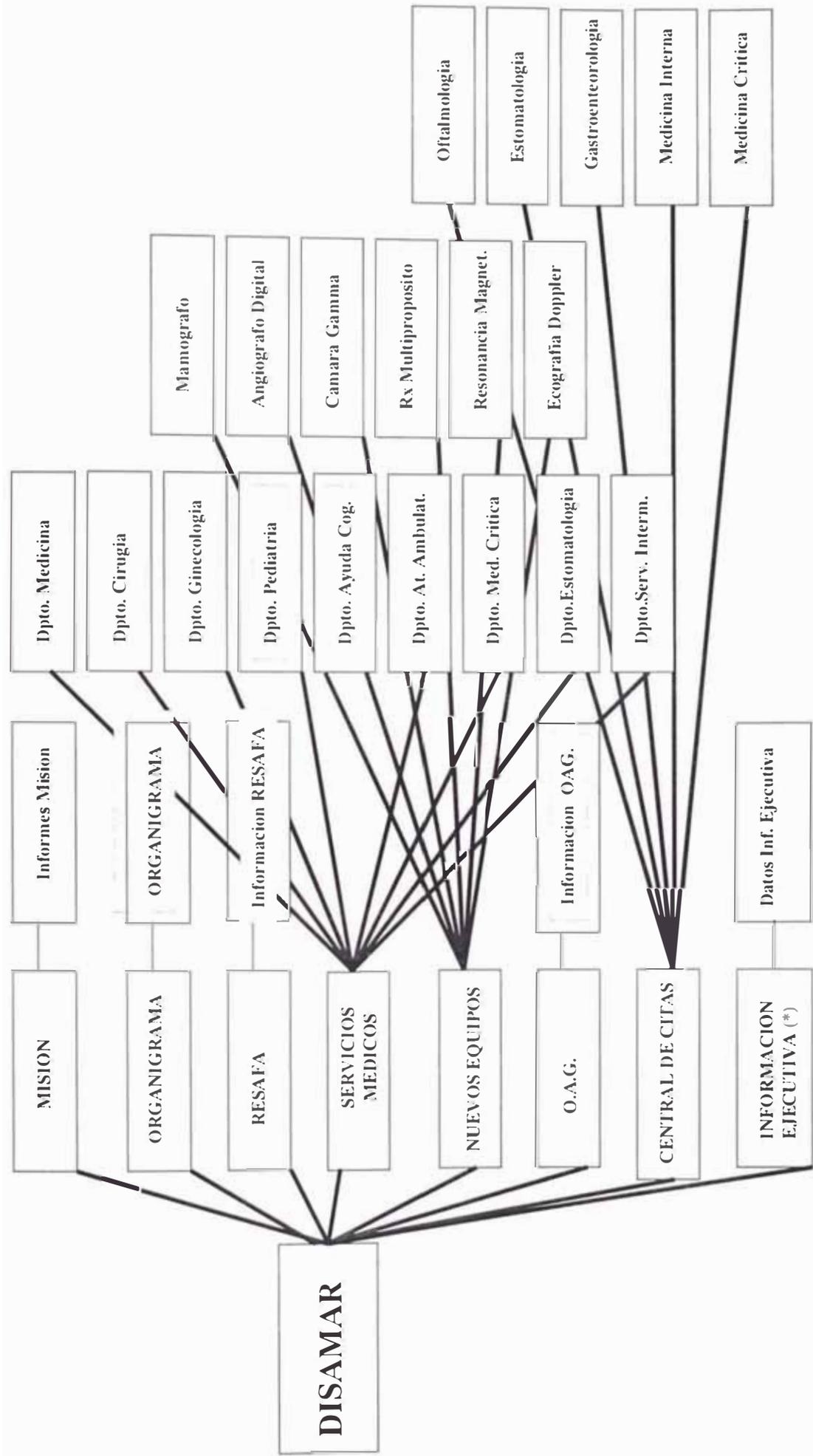


Figura 6.2.1 Cartografía del Sitio Web de DISAMAR

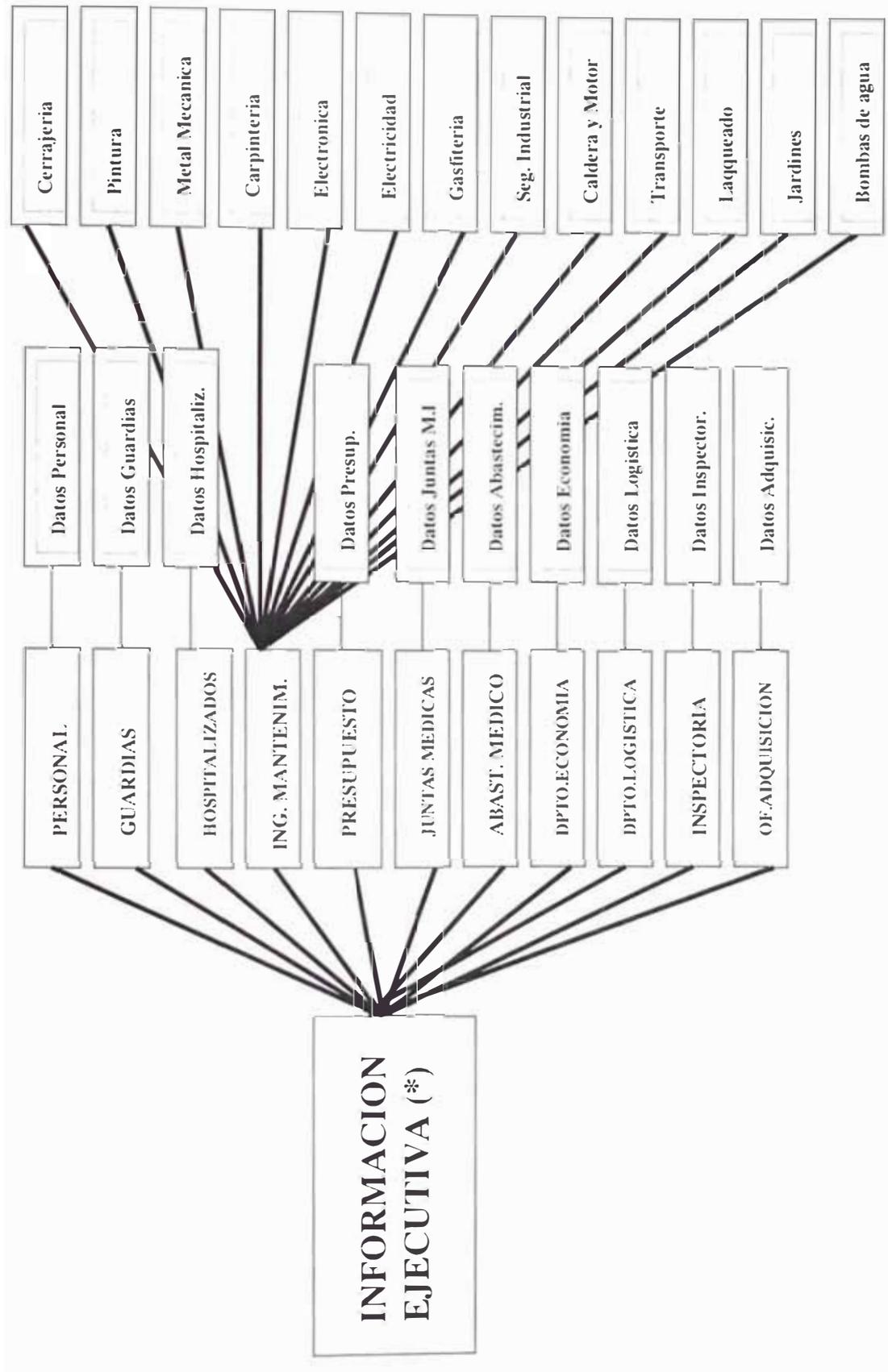


Figura 6.2.2 Cartografía del Sitio Web de Información Ejecutiva

sión (en esta ventana se da a conocer la misión que tiene el Hospital Naval)

Organigrama (se muestra la organización del Hospital)

RESAFA (en el se describe el reglamento de la salud de las fuerzas armadas en lo concerniente a uso, beneficios, etc.)

Servicios Médicos (se detalla los departamentos médicos con que cuenta el Centro Médico representados por íconos y cada icono contiene un listado de los Jefes y encargados de cada departamento. A continuación se detalla los íconos que conforman esta ventana ó icono).

- Departamento Medicina
- Departamento de Cirugía
- Departamento de Cirugía y Obstetricia
- etc.

Nuevos Equipos (se detalla la relación de los equipos de última generación, adquiridos en el presente año que obedece a un plan de actualización médica. Cada equipo está representado por un icono y en cada una de ellas se describe en forma detallada las características y bondades de cada una de ellas con la finalidad de que los usuarios del hospital se encuentren informados).

- Mamógrafo
- Angiógrafo Digital
- Cámara Gama Topográfica (SPECT)
- Rx Multipropósito
- Resonancia Magnética
- Ecografía:DOPPLER – Color con Harmonic

O.A.G. (Oficina de Actividades Generadoras, en el se describe la visión, objetivo, alcance funcional entre otros de esta oficina)

Central de Citas (en el se detalla los servicios que presta el Centro Médico, cada servicio esta representado por un icono y cada icono brinda información sobre el estado de las citas en los pacientes)

- Oftalmología
- Estomatología
- Gastroenterología
- Medicina Interna
- Medicina Crítica
- etc.

Información Ejecutiva (este icono de la página principal de DISAMAR solo está disponible para el personal del Centro Médico, mas no para el público usuario del hospital como es en el caso de los íconos anteriores. Para esto, se tendrá una clave de acceso, significa esto que solamente las personas que el Director del centro Médico designe tendrá acceso a la información que se brinda en este icono. Como se observa al ingresar a información ejecutiva se pide una clave de ingreso, una vez que se introduzca la clave de acceso se ingresará a los siguientes íconos y cada icono esta preparado para ingresar el contenido correspondiente):

- Personal
- Guardias
- Ingeniería y Mantenimiento
- Cerrajería
- Pintura
- Metal Mecánica
- Carpintería
- Electrónica
- Electricidad
- Gasfitería
- Seguridad Industrial
- Calderas y Motores
- Transporte
- Laqueado

- Jardines
- Bombas de Agua
- Aire Acondicionado
- Presupuesto
- Juntas Médicas
- Abastecimiento Médico
- Departamento de Economía
- Departamento de Logística
- Inspectoría
- Oficina de adquisiciones

Capítulo 7

Conclusiones

1. La Marina de Guerra del Perú cuenta con una red de comunicaciones a nivel nacional y una WAN Naval; sin embargo, el hardware, el software y los sistemas de comunicación no conversan entre si; por consiguiente, no actualizan información instantánea y simultánea, de modo que los usuarios compartan dicha información en tiempo real, por lo que se hace necesario diseñar una Intranet. La implementación de la Intranet Naval permitirá que los integrantes de la Institución y en especial el Comando de cada unidad pueda contar con información oportuna extraída de una base de datos, con la finalidad de apoyar la toma de decisiones..
2. La metodología empleada en el diseño de la Intranet es el modelo descentralizado distribuido en donde cada función, cada grupo y cada parte única de la intranet se desarrolla en su propio servidor y es mantenido por el personal encargado de elaborar este contenido. Significa esto, centralizar la arquitectura y descentralizar el contenido (El servidor de cada centro cómputo de las dependencias se encuentran conectados a la WAN Naval). De la simulación realizada (capítulo 3), se puede concluir que el modelo aplicado en el diseño es el correcto.
3. El diseño de la Intranet requiere del manejo de la información en niveles adecuados, tal como se desarrollo en el Capítulo 4. Del análisis de los procedimientos organizacionales de la institución, se ha determinado que principalmente se manejan tres categorías de información: Técnico, Administrativo y Operacional, siendo éstos los campos de la Página Principal. Esta clasificación es la base de la estructura de la Intranet Naval diseñada. Sin embargo, tal estructura es susceptible a cambios por disposición de los comandos superiores.

4. La red actual de la Marina de Guerra del Perú posee una capacidad de 10/100 Mbps de los cuales sólo el 40% de la capacidad de la WAN Naval es ocupado por el tráfico de datos normales, quedando una capacidad disponible del 60% para soportar otras aplicaciones tales como la Intranet. Entonces, la implementación de la Intranet se puede realizar empleando la infraestructura existente, reduciéndose de esta manera los costos de infraestructura a cero.
5. Por otro lado, la Marina cuenta en la actualidad con recursos humanos y tecnología adecuada para implementar la Intranet diseñada. Este hecho hace posible que los costos de implementación de la disminuyan notablemente. Solo se requiere invertir un monto aproximado de US \$ 5000.00 para la capacitación del personal que se va a dedicar al desarrollo de aplicaciones en Intranet, evitando de esta forma depender de terceros, siendo éste un factor importante que justifica su implementación.
6. Para validar el diseño de la intranet propuesta, se realizó una simulación en los ambientes de la Sección de Post-grado de la Facultad de Ingeniería Eléctrica y Electrónica utilizando estaciones de trabajo como si fueran dos dependencias. Se comprobó que se logra compartir información en tiempo real. No se pudo llevar a cabo esta simulación en los ambientes de la Dirección de Telemática de la Marina por que se necesita la autorización correspondiente del alto Mando Naval.
7. La seguridad en la red utilizada para la transmisión de información, empleada por la Marina de Guerra del Perú fue contemplada para impedir el acceso de agentes externos que quieran ingresar a nuestra base de datos para extraer información o para introducir virus, así como para evitar la fuga de información desde nuestras propias instalaciones. Para tal efecto, se vió por conveniente la instalación de hardware de seguridad a través de firewalls en el nodo central, Servidores Proxy y ruteadores en cada nodo; y como software de seguridad el encriptador de mensajes PgP descrito en el Capítulo 5, el cual ha demostrado ser confiable.

8. El algoritmo PGP actualmente en uso se puede complementar con la esteganografía, que es una tecnología de última generación, la cual permite esconder mensajes dentro de archivos de imagen, voz y de texto, siendo imperceptibles a la vista humana y difíciles de detectar. A diferencia de otras técnicas criptográficas, en donde el empleo de mensajes encriptados resulta evidente, en la esteganografía es difícil de detectar si se está empleando encriptamiento. En esta tesis se ha verificado el potencial del algoritmo esteganográfico de encriptamiento.

9. Con el propósito de que este trabajo de tesis sea enriquecido y ampliado, se adjunta un CD que contiene el programa fuente del algoritmo esteganográfico con su respectivo Readme en el que se detalla como se instala para el funcionamiento del programa, páginas web referentes a los servidores de voz e imágenes, información acerca del avance de la esteganografía en el mundo, así como las páginas del diseño de la Intranet.

Bibliografía

- [1] Naval Virtual Intranet (NVI)--Functional Architecture and Concept of Operations., Departament of the Navy Chief Information Officer.USA. Diciembre 1997. Este documento se encuentra en el Archivo general de la Dirección de Telemática de la Marina de Guerra del Perú.

- [2] “Política General de Informática de la Marina de Guerra del Perú”, 1998. Este documento se encuentra en el Archivo general de la Dirección de Telemática de la Marina de Guerra del Perú.

- [3] Andrew S. Tanenbaum, *Redes de Computadoras*, Prentice-Hall Hispanoamericana S.A., 1977, México

- [4] J. Hinrichs Randy. *Intranets -- Usos y Aplicaciones*. Prentice-Hall Hispanoamericana, S.A., 1977, México.

- [5] J. C. Palais, *Fiber Optic*, Third Edition, Prentice Hall, Englewood Cliffs, NJ,1992

- [6] Douglas. E. Comer, *Internetworking with TCP/IP*, Vol I, Third Edition, Prentice Hall Englewood Cliffs, NJ 07632, 1995

- [7] James A. Senn, *Análisis y Diseño de Sistemas de Información*, McGraw Hill – Interamericana de México, 1992.

- [8] Armando Aramayo, “*Planeamiento Estratégico de Tecnologías de Información*”, Biblioteca para Estudios de Especialización Gerencial de la Universidad Peruana de Ciencias Aplicadas, 1999.

- [9] William Stallings, *Network and Interwork Security--Principles and Practice*, Prentice Hall, Englewood Cliffs, NJ 07632,, 1995

- 10] A. Casas Guijarro, *Sistema Telefónico Multilínea con recocimiento de voz y acceso a base de datos remoto*, Grupo de tecnología del Habla. DIE. UPM. Madrid, 1997
- [11] J. Colás, J.M. Montero, R. Córdova. *Servidores Vocales Interactivos: Desarrollo de un Servicio de Páginas Blancas por Teléfono con Reconocimiento de Voz*, Proyecto IDAS,. Grupo de Tecnología del Habla. DIE. UPM. E.T.S.I. Telecomunicación. Madrid, 1999.
- [12] www.cd.sc.ehu.es/DOCS/UPV-EHU/revista/n11.html
- [13] Información sobre tecnologías de servidores vocales o de voz
www.vovida.org/document/Vocal_Technology_Overview/Technology_Overview3a.html
- [14] Información sobre tecnología de servidores vocales traducción al español.
www.translate.google.com/tran.../search%3Fq%3Vocal%2Bserver%26hl%3Des%26sa%3D
- [15] WWW.cisco.com/warp/public/cc/pd/mxsv/mxcvsr/prodlit/_sp_mc783_ds.htm – Información sobre tecnología de servidores de voz
- [16] www.tellme.net/en/onlineLabPage.html. Información sobre servidores de voz e imagen.
- [17] www.asturnet.es/adsl_3.htm. Tecnología de servidores
- [18] www.sc.ehu.es/scwceinf/paginas/Gestion/Serv.voz.html. Servidores de voz
- [19] www.idiap.ch/publications/hans-com-96-04.bib.abs.html
Información sobre servidores de imagen
- [20] <http://centros5.pntic.mec.es/cpr.de.hortaleza/Cursofoto/generalidades.htm>. Información sobre servidores de imagen

- [21] Información sobre servidores de imagen. www.gusgsm.com/html/imagen.html
- [22] http://www.earthetc.com/iws/about_text.htm. Image Web Server
Información sobre servidores de imagen, para paginas web
- [23] [www.lowa](http://www.lowa.gov) Geographic Image Map Server. Información sobre servidores de imagen
- [24] www.EarthEtc.com, The Home of Image Web Server. Información sobre servidores de imagen
- [25] [www.Borealis](http://www.Borealis.com) Image Server. Información sobre servidores de imagen.
- [26] [www.Oddl](http://www.Oddl.com) Image Server. Información sobre servidores de imagen.