ESCUELA POLITECNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMATICA

BASE DE DATOS DOCUMENTAL PARA EL INTERCAMBIO DE INFORMACIÓN CALIFICADA ENTRE ECUADOR – COLOMBIA "ECORED"

Previa a la obtención del Título de:
Ingeniero de Sistemas e Informática

POR: WILSON GEOVANNI SIMBAÑA LEON

SANGOLQUI, Octubre 8 de 2008

DPTO DE CIENCIAS DE LA COMPUTACION

BASE DE DATOS DOCUMENTAL PARA EL INTERCAMBIO DE INFORMACIÓN CALIFICADA ENTRE ECUADOR – COLOMBIA "ECORED"

ESPE

2008

CERTIFICACION

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. WILSON GEOVANNI SIMBAÑA LEON CANDIDATO A INGENIERO como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMATICA

Sangolquí Octubre 2008

_____

INGENIERO STALIN MALDONADO

DEDICATORIA

El presente trabajo de grado esta dedicado a mis padres quienes me apoyaron incondicionalmente para alcanzar este sueño que parecía se desvanecía mientras pasaba el tiempo.

Nunca podría olvidarme de mi esposa quien con sus palabras de aliento me ayudo ha alcanzar este sueño que se ha hecho realidad.

Wilson Geovanni Simbaña León

AGRADECIMIENTOS

El agradecimiento a mis padres por su ayuda incondicional por saber levantarme cuando desmayaba, quienes siempre han sido fuente de inspiración y sobre todo un ejemplo de vida para mi persona.

Al COMACO quienes nos apoyaron ciento por ciento en el proyecto.

Wilson Geovanni Simbaña León

HOJA DE LEGALIZACION DE FIRMAS

ELABORADO POR
WILSON GEOVANNI SIMBAÑA LEON

_____
Wilson Geovanni Simbaña León

COORDINADOR DE LA CARRERA

_____
Ing. Ramiro Delgado.

Lugar y fecha: Sangolquí 8 Octubre 2008

CAPITULO 1

PRESENTACIÓN E INTRODUCCIÓN DEL PROYECTO BINACIONAL ECUADOR COLOMBIA "ECORED"

CAPITULO 2

ANÁLISIS Y RELEVAMIENTO DE LA SITUACIÓN ACTUAL "ECORED"

CAPITULO 3

ANALISIS DE FACTORES DE RIESGO, DETERMINACION DE AMENAZAS Y MEDIOS DE SEGURIDAD

CAPITULO 4

DISEÑO, CONSTRUCCIÓN E IMPLEMENTACIÓN DE LA BASE DE DATOS DOCUMENTAL PARA INTERCAMBIO DE INFORMACIÓN CALIFICADA ENTRE ECUADOR Y COLOMBIA.

CAPITULO 5

IMPLEMENTACION DE POLITICAS Y ESTRATEGIAS DE SEGURIDAD PARA ECORED.

CAPITULO 6
CONCLUSIONES Y RECOMENDACIONES

Índice de Gráficos

.

Indice de Cuadros

LISTADO DE ANEXOS

LISTADO DE ACRONIMOS Y ABREVIACIONES

COMACO.	Comando Conjunto de las Fuerzas Armadas
1-DE FTC-1	Fuerza de Tarea Conjunta No. 1 de La División de Ejército N°. 1
A2	Inteligencia de la FAE
ACL	Access Control List
ADSL	*Asymmetrix Digital Suscriber Line*,
API	*Application Programmet Interface*
BASJAR	Base Naval de Jaramijó
C.C.	Comando Conjunto
C3I2	Comando control y comunicaciones inteligencia informática
CC.FF.AA	Comando Conjunto de las Fuerzas Armadas
COMBIFRON	Comisión Binacional fronteriza
Cosena	Consejo de Seguridad Nacional
COTOA	Comando de Operaciones del Teatro de Operaciones Aéreo
COTON	Comando de Operaciones del Teatro de Operaciones Naval
COTOT	Comando de Operaciones del teatro de Operaciones Terrestre
D –2.	Departamento de Inteligencia Colombia
DBA	Administrador de Bases de Datos.
DHCP	*Dynamic Host Configuration Protocol*
DIGECO	La red de la dirección de Guerra electrónica y Comunicaciones
DLSw	Data Link Switching.
DLL	*data-link layer*
DNI	Dirección Nacional de Inteligencia
DNS	*Domain Name System*
E2	Inteligencia de la Fuerza Terrestre
ECORED	Red Ecuador Colombia
FAE	Fuerza Aérea del Ecuador
FTC-2	Fuerza de Tarea No. 2
FTP	*File Transfer Protocol*,
G – 2	Departamento de Inteligencia Ecuador
G2	La red de Inteligencia

II-DE	División de Ejército No. 2
III-DE FTC-3	Fuerza de Tarea No. 3 de la División de Ejército No. 3
IP	Internet Protocol
IPX	InterNetwork Packet Exchange
ISDN	Integrate Service Digital Network
ISP	Internet Service Provider
IV-DE FTC-4	Fuerza de Tarea No. 4 de la División de Ejército No. 4
LCP	Enlace (*Link Control Protocol*,
M.D.N.	Ministerio de Defensa Nacional
M2	Inteligencia de la Marina
NAS	*Network Access Server*,
NAT	Traductor de direcciones de red
PGP	Pretty Good Privacy,
POP3	Post Office Protocol 3
POV	Procedimientos operacionales vigentes
	ECORED
PPP	*Point-to-Point Protocol*
PPTP	*Protocolo de Túnel punto a punto" (Point-to-Point Tunneling*
	Protocol)
RAM	Randon Acces Momory
RRAS	*Routing and Remote Access Service*
SNMP	Simple Mail Transfer Protocol
SPX	Sequence Packet Exchange
SSL	Secure Socket Layer
TCP	Transmision Control Protocol
VPN	*virtual private network*
WINS	*Windows Internet Name Service*,

RESUMEN

La meta del presente proyecto fue realizar una base de datos no tradicional, es decir una base de datos documental, que nos sirviera para poder manejar, controlar, verificar la información generada por los diferentes departamentos de inteligencia de los países involucrados en el proyecto binacional denominado ECORED.

La base de datos documental ha sido creada la versión 5.0 de Lotus Notes que fue utilizado como Server, Dominio Mail, Dominio Aplication, y para los clientes tengo Notes, Designer y admin, tomando en cuenta que no sigue los métodos tradicionales de programación y de creación de B.D.

Al no ser una programación tradicional primero no tenemos modelador de base de datos no requerimos de herramientas CASE, para su modelo ya que cada documento se lo maneja como worflow, como Web y como B.D., permitiendo para su conectividad protocolos TCP/IP, SPX, Netbios, XPC.

Con estas características se logro tener cualidades al la BD para un manejo muy amigable con el usuario, seguimiento de la documentación, y el manejo de perfiles de creación, modificaron, lectura, y de administración, con esto podemos tener un seguimiento de la información hasta su publicación final del documento todo esto de forma Web o vía correo electrónico según el perfil del creador.

CAPITULO 1

PRESENTACIÓN E INTRODUCCIÓN DEL PROYECTO BINACIONAL ECUADOR COLOMBIA "ECORED".

1.1 Introducción

El proyecto tiene como finalidad el intercambio de la información calificada entre Ecuador y Colombia por medio de una Base de Datos Documental que será desarrollada en Lotus Notes, y se utilizará el medio el Internet como medio comunicación, los cuales accesarán a su Base de Datos Documental localmente desde los usuarios debidamente autorizados y validados por las Direcciones de Inteligencia de los respectivos países.

La seguridad de la información será tomada en cuenta por el encriptamiento tanto físico, que será conectado a la salida del servidor, y lógico, además se tomará en cuenta en este proyecto la seguridad a nivel de puertos, codificación de campos y de usuarios.

1.2 Nombre del proyecto

ECORED "RED PROTEGIDA DE DATOS ECUADOR – COLOMBIA", Este nombre fue escogido por los departamentos de inteligencia tanto de Ecuador como de Colombia.

1.3 Unidades responsables del proyecto

Ecuador:

Dirección General de Inteligencia del Comando Conjunto de las Fuerzas Armadas y Dirección General de Inteligencia de la Policía Nacional

Colombia

Jefatura del Departamento D-2 del Comando General de las Fuerzas Militares y la Dirección de la Policía Judicial de Colombia

1.4 Información a intercambiar

- Tráfico de armas, municiones y explosivos.
- Subversión, y Terrorismo

1.5 Colaboradores usuarios de inteligencia

- Jefe Grupo de Inteligencia
- Jefe Grupo Técnico, delegado de C3I2
- Jefe Sección Técnica de Inteligencia
- Encargado del Centro de Cómputo de Inteligencia

1. 6 Localización geográfica

Centro de Cómputo de la Dirección General de Inteligencia ubicada en Quito, provincia de Pichincha.

1.7 Área de Influencia

Internacional (Ecuador – Colombia)

1.8 Antecedentes

La Red Protegida para el intercambio de Información, tiene su origen en la voluntad expresada mediante resolución de la II Reunión Plenaria de la COMBIFRON celebrada en Bogotá, en el mes de Febrero de 1999 bajo el nominativo de Base Binacional de Datos.

En este sentido, en el Acta de la II Reunión de la COMBIFRON, en el Anexo "A" al Manual de Procedimientos Operativos Vigentes (POV) (BANCO BINACIONAL DE DATOS), se establece la conveniencia de crear formas de comunicación eficientes entre las Agencias de Inteligencia de las Policías Nacionales de Ecuador y Colombia; y en el Acta de la Comisión Técnica reunida en Ipiales el 04 y 05 de Noviembre de 1999, igualmente se establece la conveniencia de crear una Base de Datos paralela entre las Fuerzas Militares de Colombia y las Fuerzas Armadas de Ecuador sobre:

- Tráfico de armas, municiones y explosivos
- Subversión, y Terrorismo.

En la reunión de la COMBIFRON realizada en Colombia – Bogotá, se toma la decisión de constituir un grupo de trabajo para estudiar su viabilidad y las alternativas disponibles en cuanto a formas y modalidades que podrían asumirse, estableciendo un cronograma primario de actividades para estructurar el mencionado proyecto. En ésta Reunión Técnica realizada en Ipiales, se decidió continuar con los estudios necesarios para desarrollar una aplicación para el intercambio de Información calificada, siendo considerada en primera instancia la elaboración de páginas WEB con interfaces a Bases de Datos, utilizando como medio de comunicación Internet. Tomando como base las reuniones de Bogotá e Ipiales, en la III Reunión de la COMBIFRON realizada en Quito–Ecuador en el mes de Noviembre de 1.999, se procede a cambiar la nominación del proyecto por “ECORED” y se elaboró los Estatutos

correspondientes en forma separada, tanto de la PN “Policía nacional” y de FF.AA. Los mismos que fueron estudiados y analizados; Estableciéndose en estos Estatutos que se realice la reunión del Grupo de Inteligencia del 10 al 12 de Enero del 2.000 en Ipiales y la del Grupo Técnico del 24 al 29 de Enero del 2.000 en Santa Fe de Bogotá.

1.9 Importancia

Este Proyecto es importante ya que ofrecerá rapidez y seguridad durante el intercambio de información calificada a través de Internet periódicamente, en forma confiable, veraz y segura, con el fin de mantener las Bases de Datos actualizadas tanto en Ecuador como en Colombia.

1.10 Objetivos

1.10.1 Objetivos Generales

Implementar una base de datos documental, para el intercambio de información calificada entre la Dirección General de Inteligencia del COMACO de Ecuador y el Departamento D-2 de las Fuerzas Militares de Colombia, para, prevenir, combatir, controlar el narcotráfico, terrorismo, subversión y trafico ilegal de armas.

1.10.1 Objetivos Específicos

- Establecer los procesos adecuados para la comunicación entre las Direcciones de Inteligencia de Ecuador y Colombia utilizando una base de datos documental.
- Facilitar a los recintos militares involucrados el flujo de información de manera ágil, oportuna y veraz.
- Establecer normas y procedimientos de seguridad para el manejo de la información.
- Replica de la información de las Bases de Datos de Ecuador y Colombia

- Diseño de la infraestructura física de la red de datos y comunicaciones para prestar los servicios de información.
- Establecer un plan de contingencia para la comunicación.

CAPITULO 2

ANÁLISIS Y RELEVAMIENTO DE LA SITUACIÓN ACTUAL "ECORED"

2.1. Situación Actual

2.1.1. Relevamiento de la Información

En la reunión del Grupo Técnico realizada en Ipiales el 04 y 05-NOV-99, se estableció la utilización de páginas WEB con interfaces a Bases de Datos a través de Internet, La Dirección General de Inteligencia del COMACO, previa investigación y análisis, propone reestructurar el proyecto en "tres fases", a fin de aumentar la seguridad de la información que se va a intercambiar.

- Fases del proyecto ECORED

Fase 1: E-mail con seguridad

- Aplicación: E-Mail
- Medio: Internet
- Enlace: punto a punto
- Seguridad: Software PGP

Fase 2: Diseño de la Base de Datos Documental

- Aplicación: B.D. Documental(Lotus)
- Medio: Internet
- Enlace: Servidor – Cliente
- Seguridad: Software PGP, aplicación Lotus y protocolo SSL

Fase 3: Implementación de la Base de Datos Documental

- Aplicación: B.D. Documental (Lotus)
- Medio: Internet y establecer medios alternativos.
- Enlace: Servidor – Servidor.
- Seguridad: Software PGP, aplicación Lotus con seguridad en campos, y usuarios y protocolo SSL,

Para esta propuesta es necesario realizar una reunión del Grupo de Inteligencia en los sectores fronterizos, a fin de establecer en forma definitiva los formatos de intercambio de información, y de igual manera realizar una reunión del Grupo Técnico en Santa Fe de Bogotá, en vista de que Colombia ya dispone de una gran Base de Datos, en la misma que se utilizará una parte de ésta para la Implementación definitiva de la aplicación; en esta reunión del Grupo Técnico se coordinará en forma conjunta los términos técnicos en hardware, software, aplicaciones y seguridad para el mencionado proyecto.

En referencia con el manual de procedimiento operativo vigente, obtenido previo a reuniones realizadas conjuntamente con la **D2 de las Fuerzas Militares de Colombia** (“Inteligencia Militar Colombia”) y la **Dirección General de Inteligencia del Ecuador**, se determino los campos que debe contener la base de datos Binacional Ecuador / Colombia para el flujo de información y que se detallara en este capitulo posteriormente.

2.1.2. Comunicaciones ECORED

En la reunión Técnica realizada en Ipiales, se estableció utilizar Internet como medio de comunicación para el intercambio de información, se utilizará un software de correo y para seguridad el PGP (Pretty Good Privacy), en cada país se dispondrá de una cuenta de Internet con E-Mail, en donde se instalará el PGP para encriptar los mensajes. Para que entre en funcionamiento el intercambio de información segura, será necesario utilizar los principios de encriptación asimétrica (se fundamenta en claves públicas y privadas), ver gráfico 2.2:

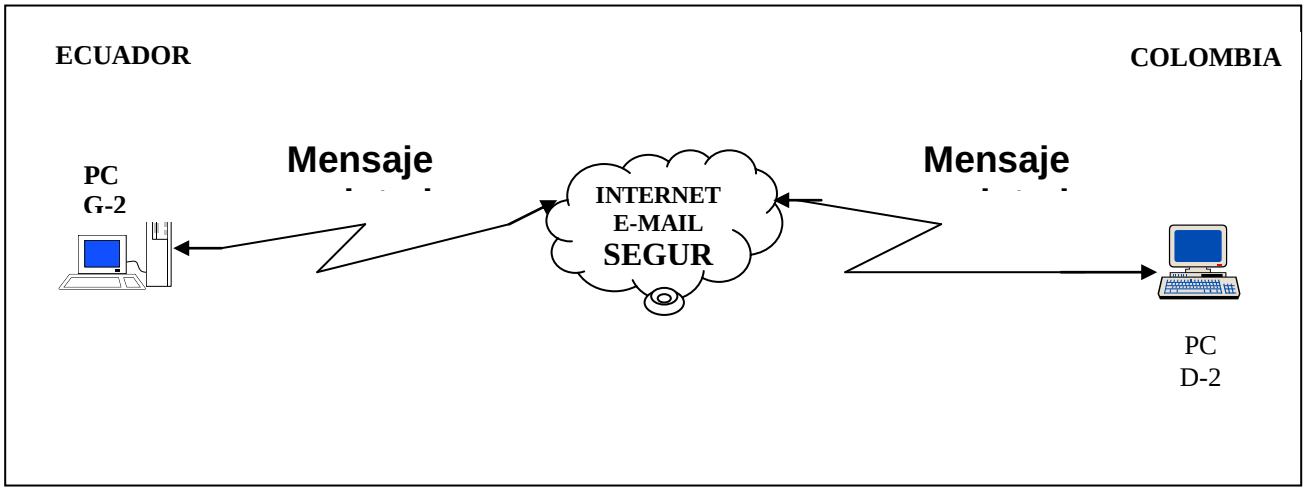


Gráfico 2.1: (E-mail con seguridad)

2.1.3. Análisis y descripción de la Intranet del CC.FF.AA.

2.1.3.1. La Intranet del CC.FF.AA.

La Intranet del Comando Conjunto ha sido desarrollada para manejar toda la información relativa a una crisis en el nivel estratégico operacional.

Cuando se habla de manejar toda la información relativa a una crisis, se está aludiendo estrictamente a la información que permite satisfacer los requerimientos operacionales del COMACO.

La Intranet del Comando Conjunto es un conjunto de hardware, software, personal y procedimientos que busca procesar información para diferentes destacamentos militares y civiles que coadyuvan al cumplimiento de su misión, agrupados en cuatro redes fundamentales:

Tabla 2.1: (Redes, ubicación, servidores y usuarios del COMACO)

REDES	UBICACIÓN	N° SERVIDORES	N° USUARIOS
DIGECO	COMACO	2	20
G2	COMACO	2	50
Centro informático	COMACO	2	10
C^3I^2	COMACO	2	60

DIGECO "La red de la dirección de Guerra electrónica y Comunicaciones"

G2 "La red de Inteligencia"

La red Administrativa (Centro de Informática),

La Red de Comando C^3I^2 "Control, Comunicaciones, inteligencia Informática"

El departamento de la DIGECO, está encargado de canalizar los proyectos de comunicación, la red de la dirección de Guerra electrónica y Comunicaciones que fue la encargada por algunos años atrás del correo estratégico.

La red de inteligencia, es la encargada de filtrar la información y clasificarla para direccionarla en forma correcta a los diferentes usuarios con la finalidad de evitar que cierta documentación calificada sea tomada en forma indiscriminada por usuarios no calificados.

La red administrativa, es la encargada de enviar mensajes al exterior por diferentes roles internacionales que se ejecutan en la Institución y para el conocimiento externo.

La red del C3I2, permite mantener datos permanentes como mapas, elementos de cartografía, bases documentales, instalaciones, sitios, etc, así como también datos de crisis como observaciones, acontecimientos, situaciones particulares, etc.; es decir, manejar la situación operacional de una crisis determinada con datos estructurados representados en el modelo de datos del sistema, los cuales son replicados automáticamente a los puntos remotos.

Permite la visualización de los datos en forma:

- **Gráfica, selectiva y georeferenciada**
- **Alfanumérica visualizada en tablas (texto, cifras)**

Ambas con capacidad de hacer anotaciones o comentarios sobre la situación presentada, seleccionando datos para la transmisión a otros escalones

El sistema maneja la gestión de la documentación operacional constituida por Memorándums, Planes, Apreciaciones, Anexos, etc.

El sistema es extensible, es decir, permite el crecimiento y/o adaptación del esquema de los datos.

Dispone de explotación del sistema amigable (ambiente Windows), tanto para el ingreso, consulta, visualización gráfica de la información referente a un teatro de operaciones o zona de defensa; elementos de cartografía, infraestructuras, organismos y organizaciones, Fuerzas y sus dotaciones, terroristas, subversivos, personalidades; lugares particulares, operaciones, acontecimientos. En resumen, aproximadamente 150 tipos de datos diferentes según encargado del C^3I^2 .

El sistema permite sintetizar, buscar y navegar en la información basados en su estructura específica, permitiendo la emisión de documentos recapitulativos.

Es un sistema distribuido, organización multisitios con protocolos estándar de intercambio de datos.

2.1.3.2. Beneficios de la Intranet en el CC.FF.AA.

Del análisis de esta Intranet se deducen los siguientes beneficios de la misma:

- **Fácil acceso a la información almacenada en la misma**
- **Mejores comunicaciones entre todos los elementos del C.C.**
- **Mejor aprovechamiento de la información y otros recursos**
- **Reducción de costos**

La conexión a la Intranet del M.D.N. tiene como propósito fundamental el flujo de información sobre la gerencia y coordinación de las estrategias y políticas Nacionales de Defensa.

La conexión a las Intranet de las Fuerzas tiene como propósito fundamental la gerencia y coordinación de la ejecución de misiones asignadas.

La conexión a la Intranet de la Honorable Junta de Defensa Nacional tiene como propósito establecer las condiciones de Defensa en el campo económico.

La conexión a INTERNET global tiene como propósito establecer conexión con las Agregadurías Militares en Alemania, Argentina, Bolivia, Brasil. Chile, Colombia, Estados Unidos, Francia, Inglaterra, Israel, Italia, Perú y Venezuela y a todo el mundo.

La conexión a Andinatel tiene como propósito establecer conexión con: La Presidencia de la República, Consejo de Seguridad Nacional (COSENA), Dirección Nacional de Inteligencia (DNI), Cancillería, Instituto Geográfico Militar, Dirección de Movilización e Inteligencia de la Policía Nacional

La conexión de nube X-25 tiene como propósito establecer conexión con estaciones remotas de elementos operativos como:

- **1-DE FTC-1 – Fuerza de Tarea Conjunta No. 1 de La División de Ejército N°. 1**
- **II-DE – División de Ejército No. 2**
- **FTC-2 – Fuerza de Tarea No. 2**

- **III-DE FTC-3 – Fuerza de Tarea No. 3 de la División de Ejército No. 3**
- **IV-DE FTC-4 – Fuerza de Tarea No. 4 de la División de Ejército No. 4**
- **COTOT - Comando de Operaciones del teatro de Operaciones Terrestre**
- **COTON – Comando de Operaciones del Teatro de Operaciones Naval**
- **COTOA – Comando de Operaciones del Teatro de Operaciones Aéreo**
- **BASJAR – Base Naval de Jaramijó**

De lo anterior se deduce la amplitud geográfica que cubre la Intranet del Comando Conjunto y la importancia de la información que en ella se administra, de ahí que sea importante realizar una evaluación de las consecuencias y el impacto de potenciales brechas de seguridad dentro del sistema, considerando la confiabilidad, la integridad y la disponibilidad de la información para todos los usuarios del sistema.

2.1.3.3. Esquema físico de la Intranet / Internet del CC.FF.AA.

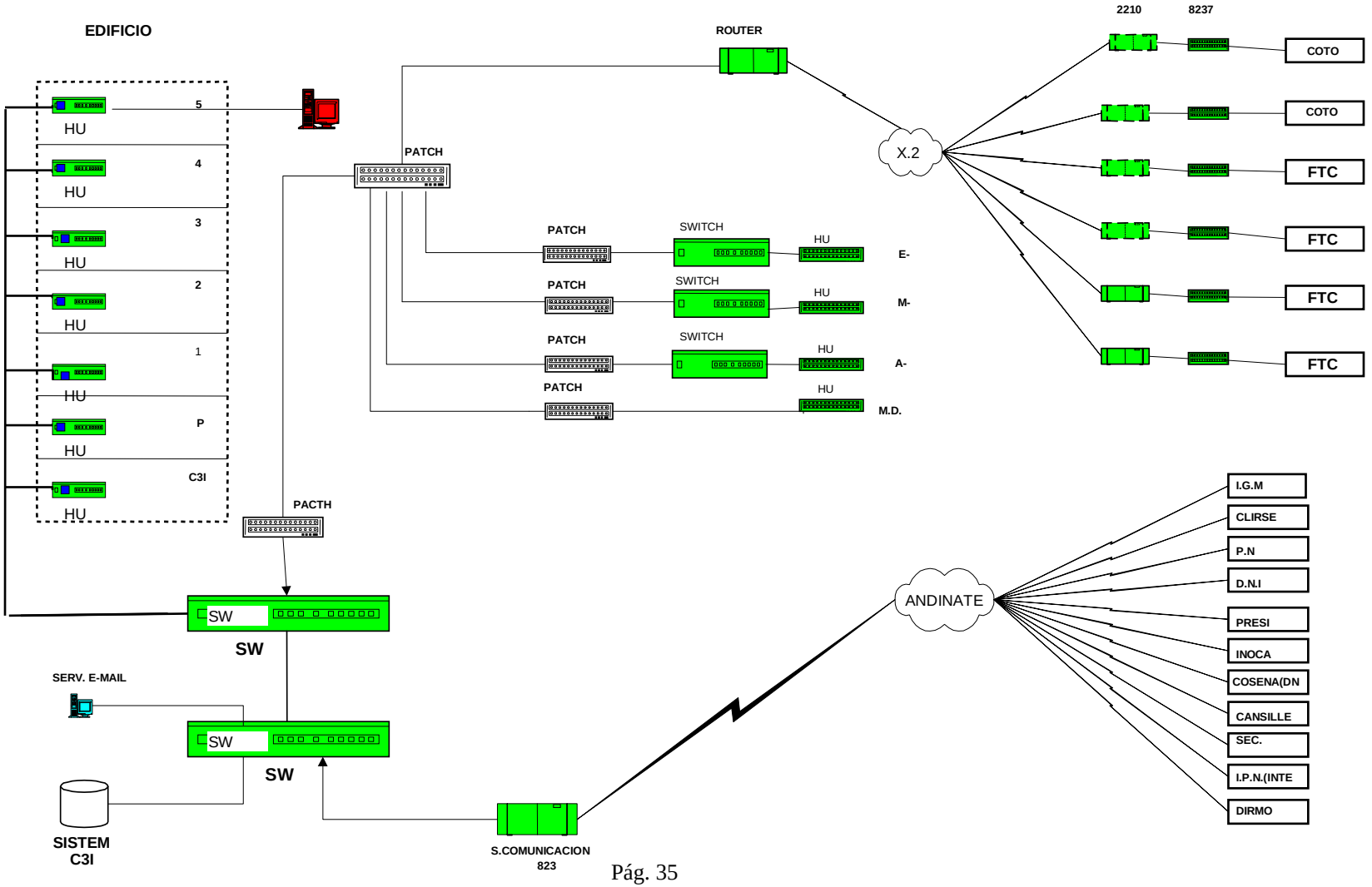


Figura 2.2: (Esquema Físico de la Intranet / Internet para Fuerzas Armadas y sus Unidades)

2.1.3.4. Descripción de hardware, software, base de datos y el servicio de Internet

2.1.3.4.1. Hardware

2.1.3.4.1.1. Server

- Arquitectura abierta
- Tecnología RISC
- Procesador de 32 bits
- 332 Mhz.
- RAM 128 MB exp. 1GB
- Memoria cache 512 MB
- HD 9 GB
- Tape Backup 4 GB 4 mm. Expandible a 8 GB
- Soporte Arreglo de discos
- Unidad de diskette 1.44 MB compatible DOS
- Puertos paralelos 1 Centronics compatible (DB-25)
- No. De slots disponibles luego de la configuración requerida mínima 2
- No. Puertos seriales mínimo 2
- Controlador de disco Fast Wide SCSI-2
- Tarjeta de red Ethernet/Fast Ethernet, TP (10/100)
- Monitor Color de alta resolución de 17"
- Teclado tipo UNIX
- CD-ROM de última tecnología SCSI-2, 20 X mínimo

2.1.3.4.1.2. Estación De Trabajo

- Procesador Pentium, Velocidad 266 Mhz.
- Memoria RAM instalado 64 MB
- Crecimiento de RAM mínimo 256 MB

- Puertos seriales 2, paralelo 1
- Tipo de controlador de vídeo SVGA
- 3 slots disponibles, 3 bahías disponibles
- Memoria cache 512 KB
- Memoria de vídeo 2 MB
- Disco duro 4.1 GB mínimo
- Unidad de Floppy 3.5 , 1.44 MB
- Tarjeta Fax / módem 56 kbps
- Kit de multimedia, CD ROM 32X
- Monitor color 15" SVGA, .28
- Teclado en español
- Mouse
- Windows 95 última versión en español
- 45 Estaciones

2.1.3.4.1.3. Router Switch Principal

- 1 puerto de consola
- 1 puerto RS-232 para administración vía módem
- 4 Puerto’s de Switch Full-Duplex Ethernet 10 Base-T (RJ-45)
- 4 Puerto’s de Switch Full-Duplex Ethernet 10 Base-FL (ST)
- 1 Puerto Fast-Ethernet 100Base-TX(RJ-45)
- 1 Slot para crecimiento:
- Explicación del crecimiento
- Soporta 4 puertos WAN de Switch FRAME-RELAY, soporta 2 puertos ATM de 155 Mbps
- Soporta 2 puertos FDDI/CDDI
- Incluye tres puertos Fast-Ethernet 100 Base-T libres

- Protocolos de comunicaciones como TCP/IP
- Guías de usuario de todos los módulos
- Características incluidas en el Switch:, IEEE 802, ID Spanning Tree
- Transparent Bridging, Traslation Bridging
- Sorce Route, Sorce Route Transparent
- Optimised Device Switching, Virtual Ring Extensions, IP e IPX outing, IP Fragmentation
- Configuración por FTP, SLIP, TELNET, Zmodem
- Redes virtuales por políticas de seguridad
- Redes por puerto y entre puertos
- Redes virtuales por dirección Física
- Redes virtuales por dirección de protocolo de Nivel 3
- Fuentes de poder y módulos Hot Swap

2.1.3.4.1.4. Hub

- 16 puertos + 1 slot para expansión
- Administración vìa SNMP
- Connectors for stack link cables
- MDI port, Stackable
- 4 Unidades

2.1.3.4.1.5. Ras (Servidor de Comunicaciones)

- 8 Modems

2.1.3.4.1.6. Laptop

- Velocidad 233 Mhz

- RAM 64 MB
- HD 4.3 GB
- CD ROM 32 X
- Tarjeta Fax/Módem
- Tarjeta de Red 10/100
- Con maletín
- Tarjeta de Red Ethernet PC CARD / PCMCIA
- Tarjeta Fax Módem de 33.6 Kbps
- Tiempo de duración de la batería, mínimo 4 horas
- Unidades

2.1.3.4.1.7. Tarjetas de Red

- Fast Ethernet 10/100
- PCI

2.1.3.4.1.8. Impresoras de Red

- B/N
- 12 ppm
- 4 MB
- Tarjeta de red Fast Ethernet PCI 10/100
- 3 Unidades

2.1.3.4.1.9. Servidor Internet

- Pentium II 333 Mhz.
- Memoria caché 512 KB por cada actualización de procesador
- Memoria RAM 128 MB expandible a 1 GB

- Arquitectura del Bus: Dual PCI de 132 Mbps
- Controlador de disco EIDE
- CD-ROM 24X
- S.O LINUX. Server última versión (7.0)
- Coprocesador matemático: Incorporado
- Disco duro:9.4 GB expandible a 109. GB
- Memoria de vídeo est./máx.: 2 MB
- Monitor de 15 pulg.
- Fax/módem: Procesador Advanced System Management
- Interfaz de red: Ethernet (integrada), 10/100 Mbps.
- Funciones de redes: Puerto para 10Base-T/100Base-TX, conector RJ-45
- 1 Unidad

2.1.3.4.2.1. Software y Accesorios

2.1.3.4.2.2. Sistema Operativo

- Windows NT Server 4.0
- Usuarios ilimitados
- Interfaz gráfica
- Protocolo TCP/IP incluido en el S.O.

2.1.3.4.2.3. Office 97 en Español

- Edición profesional
- Español
- Licencia corporativa

2.1.3.4.2.4. Lotus Notes Server E-Mail 4.0

- Transferencia de archivos
- Seguimiento de información
- Seguridad de transmisión / encriptación
- Jerarquización de niveles de acceso
- Niveles de seguridad en el acceso de información
- Firma electrónica
- Transferencia de mensajes para un grupo de usuarios
- Confirmación de la recepción del correo personal
- Transferencia de archivos tipo texto, gráfico, video y voz
- Información con respaldo en el servidor
- Facilidad en la creación de aplicaciones propias
- Integración a Internet
- Actualización de versiones de software
- Integración a Bases de Datos Relaciónales
- Licencia ilimitado número de usuarios

2.1.3.4.2.5. Enlace a un ISP y Servicio de Internet

- Servicio de Internet tipo Dial_Up

2.1.3.5. Cuadro de optimización de recursos para la red de Internet

Tabla 2.2: (Optimización de Recursos)

DESCRIPCIÓN	ESPECIF. TECNICAS	OBSERVACIONES
SERVIDOR INTERNET	**S.O. LINUX 7.0**	**Se clonó un PC normal con mejores características para utilizarlo como proxy**
CABLEADO .ESTRUCTURADO	**Cable UTP y F.O. del edificio**	**Se realizó un tendido de UTP en forma totalmente separado a la F.O.**
WEB SERVER	**S.O. WINDOWS NT 5.0 INSTALADO SERVIS PACK**	**Se utilizará los servicios de WEB del Ministerio de Defensa por disposición de los Altos Mandos Militares ya que se aprovechará dicho recurso hasta que en un futuro y con el presupuesto necesario así como las autorizaciones respectivas se den para adquiera un WEB Server para Fuerzas Armadas centralizado y controlado por el Comando Conjunto de las FF.AA**
HUBS	**IBM INTELIGENTE 3COM INTELIGENTE**	**Se aprovecho los hubs existentes en cada piso**

SWITCH	**IBM**	**Este Switch es el principal de toda la intranet**

2.2. Requerimientos

2.2.1. Banco binacional de datos

La presencia y acción de la subversión así como de otras organizaciones delictivas en el área de la frontera Colombo - Ecuatoriana, ha motivado la necesidad de establecer un Banco Binacional de Datos.

La creación del Banco Binacional de Datos, para intercambiar información entre los dos países con respecto a delitos que afectan la zona fronteriza, permitirá programar acciones a seguir y efectuar una adecuada toma de decisiones a través de una respuesta rápida, oportuna y confiable a los requerimientos de información presentados por autoridades, por ser común el objetivo de mantener el orden público y evitar que esas modalidades delictivas influyan en las relaciones entre los dos países.

2.2.2. Información a intercambiar

Ante las diferentes modalidades delictivas que se presentan en la zona fronteriza, se realizará el intercambio de información en los siguientes aspectos:

- Ordenes de captura y / o requisitoria.
- Hurto y contrabando de vehículos.

- Tráfico de armas, municiones y explosivos.
- Tráfico de material de Intendencia de uso exclusivo de la Fuerza Pública.
- Narcotráfico y lavado de dinero.
- Subversión.
- Extorsión y Secuestro.
- Terrorismo
- Trafico de precursores químicos.
- Falsificación de documentos.
- Control Migratorio.
- Contrabando.
- Daños ecológicos.
- Otros.

2.2.3. Información a Suministrar

En acuerdo entre las dos partes involucradas en el proyecto se llego a definir únicamente que los campos de información son los siguientes.

2.2.3.1. Hurto y contrabando de vehículos terrestres, aéreos, y acuáticos.

- Vehículos hurtados y robados.
- Datos de identificación de los mismos.
- Vehículos matriculados.

- Delincuentes y bandas identificadas.
- Formas de Operación.
- Lugares de Operación.

2.2.3.2. Trafico de armas, municiones y explosivos.

- Identificación del armamento, munición o explosivo (Calibre, tipo, origen, número, lote, etc..)
- Armamento, municiones o explosivos hurtado a los organismos de Seguridad del Estado.
- Delincuentes y Bandas identificadas.
- Formas de operación y rutas.

2.2.3.3 Narcotráfico.

- Personas con orden de captura.
- Personas vinculadas a los procesos judiciales.
- Personas con antecedentes judiciales (Condenas).
- Organizaciones comprometidas.

2.2.3.4 Lavado de dinero

- Casa de Cambio (Ubicación, propietario o administradores, flujo de dinero, operaciones).
- Entidades Financieras.
- Personas vinculadas a procesos judiciales por esta actividad ilícita.

2.2.3.5 Subversión

- Orden de Batalla de grupos subversivos.
- Otra Información requerida.

2.2.3.6 Extorsión y secuestro

- Reporte de personas secuestradas.
- Integrantes de bandas de secuestradores (área de influencia, zonas mas afectadas, etc.).

2.2.3.7 Ubicación del banco de datos.

Como en cada país participan varios organismos de seguridad, la información debe estar concentrada en un solo lugar, de tal forma que puedan acceder a ella sin ningún problema. Los centros encargados de la Administración de la Base de Datos, coordinaran el diseño de la misma y de todos los reportes comunes.

COLOMBIA.

La Administración de la Base de Datos Documental estará bajo la responsabilidad del departamento de Telemática del comando General de las Fuerzas Militares de Colombia, según los usuarios que tengan los respectivos permisos de ingreso, actualización y consultas.

ECUADOR

La Administración de la Base de Datos Documental estará bajo la responsabilidad del departamento de Inteligencia de COMACO de las FF.AA. de Ecuador, según los usuarios que tengan los respectivos permisos de ingreso, actualización y consultas.

2.3 Esquema de Solución de la Propuesta

2.3.1 Propuesta del proyecto

Se propone realizar una aplicación en Lotus Notes, que se instalará en la Dirección General de Inteligencia de Ecuador y en el Departamento D-2 del Estado Mayor en Colombia.

Esta aplicación será estructurada como cliente / servidor, es decir un servidor en cada país con sus respectivos clientes.

Dependiendo de la ubicación de los equipos habrá que certificar y autentificar como servidor y cliente respectivamente a fin de dar la mayor seguridad posible, el medio de comunicación para la replicación de datos será Internet o línea telefónica normal.

La replica entre los servidores tanto de Ecuador para Colombia o viceversa puede ser programada o puede ser configurada para que se active por demanda.

Se tomará en cuenta un medio alternativo de comunicación, en caso que de que se interrumpa temporalmente la comunicación al Internet ya sea por el problema del ISP o por la caída de los enlaces u otras circunstancias.

La seguridad de la información será tomada en cuenta por el encriptamiento tanto físico que será conectado a la salida del servidor, y lógico, además se tomará en cuenta en este proyecto la seguridad a nivel puertos, codificación de campos y de usuarios.

2.3.2 Como acceder a la información

EN COLOMBIA.

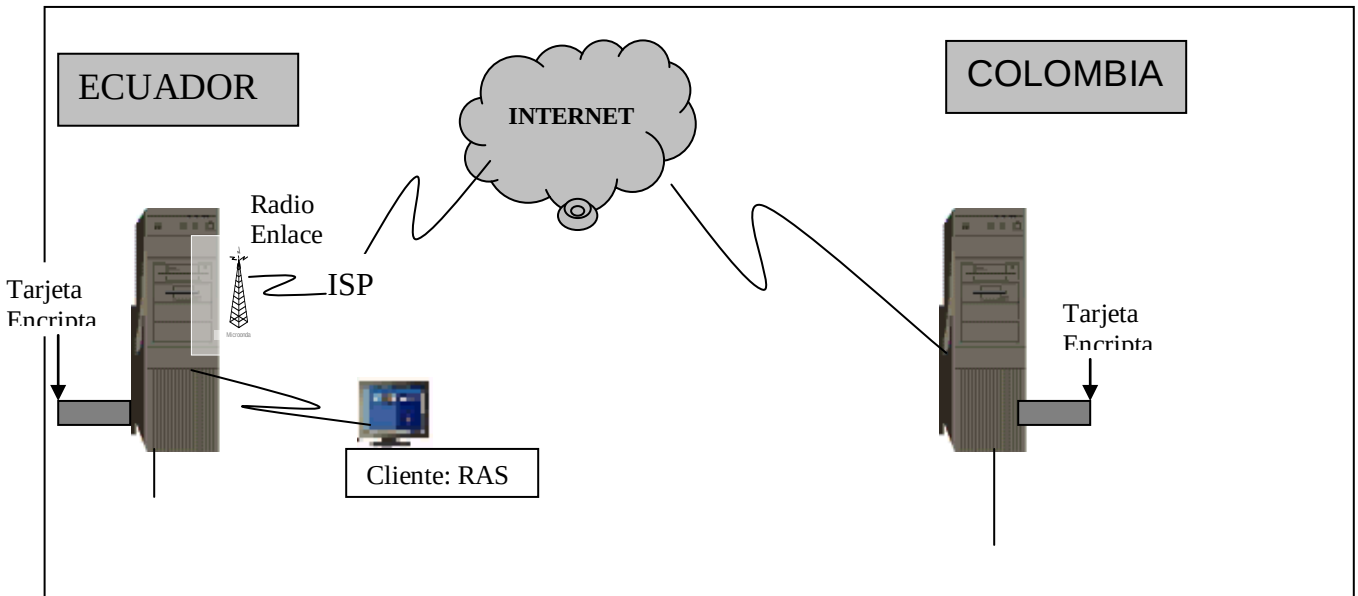
Solicitando al Departamento de Telemática del Comando General de las Fuerzas Militares de Colombia, que sea autentificado en el servidor de Base de Datos Documental por los distintos medios y canales de comunicación, como por intermedio de la misma base de datos.

EN ECUADOR.

Solicitando al Departamento de Inteligencia del COMACO de las FF.AA. del Ecuador, que sea autentificado en el servidor de Base de Datos Documental por los distintos medios y canales de comunicación, como por intermedio de la misma base de datos.

2.3.3 Sistemas de comunicación propuesto actual

El sistema de comunicación propuesta esta diseñado por dos servidores que utilizaran el medio de comunicación el Internet como se muestra en el Gráfico.



Intranet COMACO

Intranet Colombia

Gráfico 2.3: (Sistema de comunicación propuesta)

2.3.4 Actualización de la información

La actualización de la información de Datos debe ser diaria y enviada por los medios autorizados a las centrales de datos de los respectivos países. Para tal fin, los Comandantes regionales y locales fronterizos pueden canalizar a través de sus homólogos, la obtención de información de la base de datos.

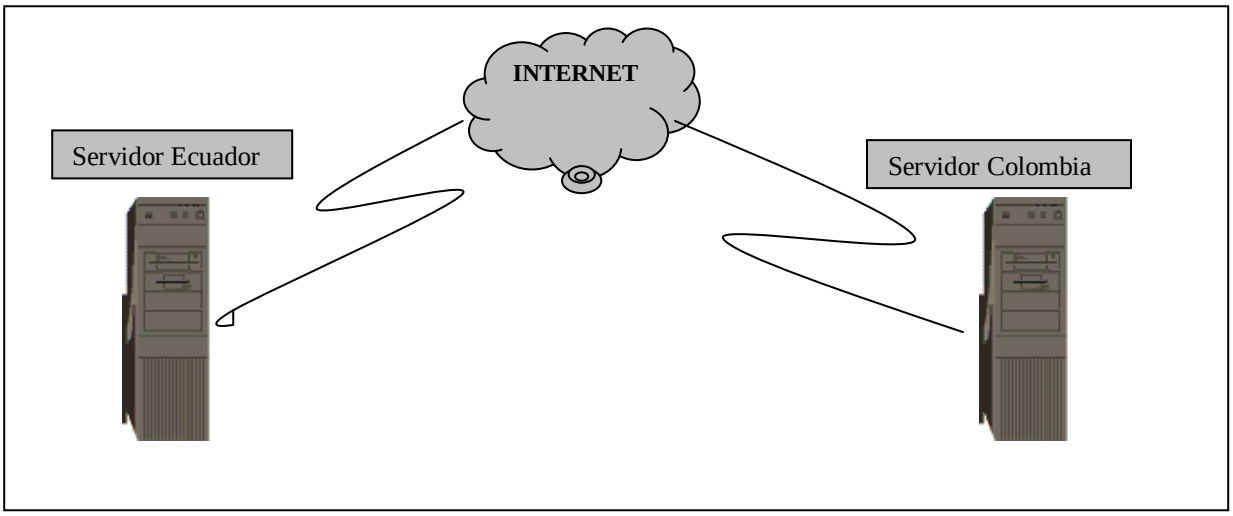


Grafico 2.4: (Replica de Servidores)

2.4.- Seguridad del proyecto

Los medios y dispositivos de seguridad que se proponen utilizar son:

- Firewall
- Tarjeta Encriptadora para aplicaciones

- Protocolo de seguridad SSL (Socket Security Layer), para enviar datos a través de Internet
- Encriptación propia de Lotus Notes a 64 bits.
- Codificación de puerto.
- Codificación por campos.
- Autenticación de Servidor a cliente que habrá que implementar por una sola vez en Colombia, a través de ID de identificación.

CAPITULO 3

MARCO TEÓRICO DE FACTORES DE RIESGO, DETERMINACION DE AMENAZAS Y MEDIOS DE SEGURIDAD

3.1. Introducción

La red Internet es un nuevo y poderoso vehículo de comunicaciones electrónicas que conecta a millones de usuarios y posibilita a las organizaciones conducir negocios de forma totalmente nueva. Pero el conectarse a una red tan grande ofrece beneficios y riesgos. Para proveer seguridad en la red se han desarrollado mecanismos de contención que permite a los usuarios utilizar todo el poder de Internet impidiendo que intrusos no deseados alteren o destruyan su información. De esta manera se asegura la integridad de la información entre la red privada e Internet u otras redes públicas.

3.2. Análisis de factores de riesgos

Se entiende por factor de riesgo una condición del entorno del sistema de información (usuarios, PC's, medios de comunicación, etc.) que, dada una oportunidad, podría dar lugar a que se produjese una invasión de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la

memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.

3.2.1. Las categorías generales de amenazas o ataques:

3.2.1.1. Interrupción.

Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

3.2.1.2. Interceptación

Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

3.2.1.3. Modificación

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

3.2.1.4. Fabricación

Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

3.2.2. Clasificación de los ataques.

3.2.2.1. Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

Obtención del origen y destinatario

De la comunicación, leyendo las cabeceras de los paquetes monitorizados.

Control del volumen de tráfico

Intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

Control de las horas habituales

Del intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataque pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

3.2.2.2 Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad

En este caso el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Reactuación

Es cuando uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes:

Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Enviar un e-mail la cuenta de G-2” podría ser modificado para decir “Enviar un e-mail a la cuenta de la Guerrilla”.

Degradación fraudulenta del servicio:

Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos D2 “Inteligencia Colombia” o se podría interrumpir el servicio de una red inundándola con mensajes espurios “span”. Entre estos ataques se encuentran los de **denegación de servicio**, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

3.3 Medios de seguridades

3.3.1 Redes privadas virtuales (VPNs)

3.3.1.1 Descripción general de las redes virtuales privadas.

Una red privada virtual (*virtual private network*, VPN) es una extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas como Internet. Con una VPN usted puede enviar datos entre dos computadoras a través de redes públicas o compartidas en una manera que emula las propiedades de una enlace punto a punto privado.

Para emular un enlace punto a punto, los datos son encapsulados o envueltos, con una cabecera que proporciona la información de enrutamiento (*routing*) que le permite atravesar la red pública o compartida para llegar a su destino. Para emular un enlace privado, los datos enviados son encriptados para tener confidenciabilidad. Los paquetes (*packets*) que son interceptados en la red pública o compartida son indescifrables sin las claves de encriptación. El enlace en el cual los datos son encapsulados y encriptados se conoce como una conexión de red privada virtual (VPN).

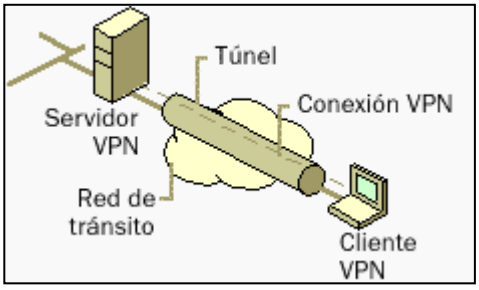


Gráfico 3.1: Red Privada (Virtual Private Network, VPN)

Con las conexiones VPN los usuarios que trabajan en casa o de manera móvil pueden tener una conexión de acceso remoto a un servidor de la organización utilizando la infraestructura proporcionada por una red pública como Internet. Desde el punto de vista del usuario, la VPN es una conexión punto a punto entre la computadora, el cliente VPN, y el servidor de la organización, el servidor VPN. La infraestructura exacta

de la red pública o compartida es irrelevante porque desde el punto de vista lógico parece como si los datos fueran enviados por un enlace privado dedicado.

Con las conexiones VPN las organizaciones también pueden tener conexiones enrutadas (*routed connections*) con oficinas separadas geográficamente o con otras organizaciones por una red pública como Internet, manteniendo a la vez una comunicación segura. Una conexión VPN enrutada a través de Internet opera desde el punto de vista lógico como un enlace WAN dedicado.

Con las conexiones VPN, tanto las conexiones de acceso remoto como las conexiones enrutadas, una organización puede cambiar de líneas rentadas (*leased lines*) o accesos telefónicos (*dial-up*) de larga distancia a accesos telefónicos locales o líneas rentadas con un proveedor de servicio de Internet (*Internet Service Provider*, ISP).

3.3.1.2 Propiedades de la VPN.

Las conexiones VPN que utilizan el PPTP "*Protocolo de Túnel punto a punto" (Point-to-Point Tunneling Protocol*), tienen las siguiente propiedades:

- Encapsulación
- Autentificación
- Encriptación de datos
- Asignación de dirección y servidor de nombres

3.3.1.2.1 Encapsulación.

La tecnología VPN proporciona una manera de encapsular los datos privados con una cabecera que le permite atravesar la red de tránsito.

Encapsulación del paquete PPP

La carga inicial PPP es encriptada y comprimida con una cabecera PPP para crear un paquete (*frame*) PPP. El paquete PPP es luego encapsulado con una cabecera GRE

modificada. El GRE está documentado en el RFC 1701 y el RFC 1702, y fue diseñado para proporcionar mecanismos de propósito general, ligeros y simples, para encapsular datos sobre redes IP. El GRE es un protocolo cliente de IP que usa el protocolo IP 47.

Para PPTP, la cabecera GRE es modificada de la siguiente manera:

- Un bit de confirmación (*acknowledgement bit*) que es utilizado para indicar que un campo de confirmación de 32 bits está presente y es significativo.
- El campo de clave (*key*) es reemplazado con un campo de Longitud de Carga (*Payload Length*) de 16 bits y un campo de identificación de llamada (*Call ID*). El campo de identificación lo establece el cliente PPTP durante la creación de un túnel PPTP.
- Se agrega un campo de confirmación de 32 bits.

Dentro de la cabecera GRE, el Tipo de Protocolo (*Protocol Type*) se establece a 0x880B, el valor *EtherType* para un paquete PPP.

Nota: A veces el GRE es utilizado por los ISPs para mandar información de enrutamiento dentro de la red del ISP. Para evitar que la información de enrutamiento sea redireccionada a los enrutadores de la red troncal (*backbone*) de Internet, los ISP's filtran el tráfico GRE de las interfases conectadas a la red troncal de Internet. Como resultado de este filtrado, los túneles PPTP pueden ser creados utilizando mensajes de control PPTP, pero los datos enviados por el túnel PPTP no son redireccionados. Si usted sospecha que este sea el problema, contacte a su ISP.

Encapsulando el paquete GRE

La carga resultante encapsulada por PPP y GRE es luego encapsulada con una cabecera IP conteniendo las direcciones IP destino y origen apropiadas para el cliente y el servidor PPTP.

Encapsulación en la capa del enlace de datos

Para ser enviado por un enlace LAN o WAN, el datagrama IP es finalmente encapsulado con una cabecera y una cola de acuerdo a la tecnología de la capa del enlace de datos (*data-link*

layer) de la interfase física del emisor. Por ejemplo, cuando los datagramas IP son enviados en una interfase Ethernet, el datagrama IP es encapsulado con una cabecera y una cola Ethernet. Cuando los datagramas IP son enviados sobre un enlace WAN punto a punto, tal como una línea telefónica analógica o ISDN, el datagrama IP es encapsulado con una cabecera y una cola PPP.

Procesamiento de los datos enviados con PPTP

Al recibir los datos enviados por el túnel PPTP, el cliente o el servidor PPTP:

1. Procesa y elimina la cabecera y la cola del enlace de datos.
2. Procesa y elimina la cabecera IP.
3. Procesa y elimina las cabeceras GRE y PPP.
4. Desencripta, descomprime, o ambas, la carga PPP (si se requiere).
5. Procesa la carga para recepción o reenvío.

Los paquetes PPTP

En el Gráfico 3.2. ilustra el camino que toman los datos enviados por el túnel a través de la arquitectura de redes, desde un cliente VPN en una conexión VPN de acceso remoto utilizando un módem analógico. Los siguiente pasos describen el proceso:

1. Un datagrama IP, un datagrama IPX o un paquete NetBEUI son enviados por sus protocolos apropiados a la interfase virtual que representa la conexión VPN usando NDIS.
2. El NDIS envía el paquete a la NDISWAN, la cual encripta o comprime los datos, o ambas cosas, y proporciona una cabecera PPP que consiste solamente del campo de Identificación de Protocolo PPP (*PPP Protocol ID*). No se agregan los campos de banderas (*Flags*) o de Verificación de Secuencia de Paquetes (*Frame Check Sequence*, FCS). Esto supone que la dirección y la compresión de los campos de control fueron negociadas durante la fase del Protocolo de Control de Enlace (*Link Control Protocol*, LCP) del proceso de conexión PPP. Para más información acerca

del PPP y el LCP, vea el "Servidor de Acceso Remoto" (*Remote Access Server*) en este libro.

3. El NDISWAN envía los datos al controlador del protocolo PPTP, el cual encapsula el paquete PPP con una cabecera GRE. En la cabecera GRE, el identificador de llamada (*Call ID*) se establece al valor apropiado para identificar el túnel.
4. El controlador del protocolo PPTP entonces envía el paquete resultante alcontrolador del protocolo TCP/IP.
5. El controlador del protocolo TCP/IP encapsula los datos enviados por el túnel PPTP con una cabecera IP y envía el paquete resultante a la interfase que representa la conexión de acceso telefónico al ISP local usando NDIS.
6. El NDIS envía el paquete resultante al NDISWAN, que proporciona las cabeceras y las colas PPP.
7. El NDISWAN envía el paquete PPP resultante al controlador WAN apropiado que representa el hardware del acceso telefónico (por ejemplo, el puerto asíncrono de una conexión por módem).

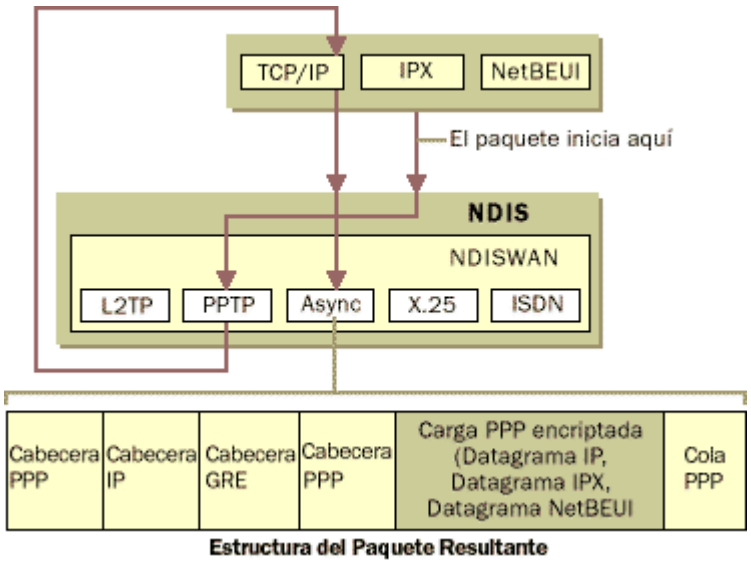


Gráfico 3.2:Desarrollo del paquete PPTP

Nota: Es posible negociar una conexión PPP encriptada para la conexión con el ISP. Esto es innecesario y no se recomienda porque los datos privados enviados, el paquete PPP enviado por el túnel, ya están encriptados. El nivel adicional de encriptación no es necesario y puede impactar el desempeño.

3.3.1.2.2 Autentificación.

Para que la conexión VPN se establezca, el servidor VPN autentifica al cliente VPN que intenta la conexión y verifica que el cliente VPN tiene los permisos apropiados. Si se utiliza la autentificación mutua, el cliente VPN también autentifica al servidor VPN, proporcionando protección contra el suplantamiento de servidores VPN.

3.3.1.2.3 Encriptación de datos.

Para asegurar la confidenciabilidad de los datos que atraviesan la red de tránsito pública o compartida, éstos son encriptados por el emisor y desencriptados por el receptor. El proceso de encriptación y desencriptación depende de que tanto el emisor como el receptor conozcan una misma clave de encriptación.

Los paquetes enviados que sean interceptados a lo largo de la conexión VPN en la red de tránsito son ininteligibles para cualquiera que no tenga la clave de encriptación común. La longitud de la clave de encriptación es un parámetro de seguridad importante. Pueden utilizarse técnicas computacionales para determinar la clave de encriptación. Tales técnicas requieren más poder y tiempo de cálculo entre más grande sea la clave de encriptación. Por lo tanto, es importante utilizar un tamaño de clave lo más grande posible.

Además, entre más información esté encriptada con la misma clave, más fácil es descifrar los datos encriptados. Con algunas tecnologías de encriptación, usted tiene la opción de configurar qué tan frecuentemente se cambian las claves de encriptación durante la conexión.

3.3.1.2.4 Asignación de dirección y servidor de nombres

Cuando se configura un servidor VPN, se crea una interfaz virtual que representa la interfaz sobre la cual se hacen todas las conexiones VPN. Cuando un cliente VPN establece una conexión VPN, se crea una interfaz virtual en el cliente VPN que representa la interfaz conectada a un servidor VPN. La interfaz virtual en el cliente VPN está conectada a la interfaz virtual en el servidor VPN, creando la conexión VPN punto a punto.

A las interfaz virtuales del cliente y del servidor VPN se les deben de asignar direcciones IP. La asignación de estas direcciones es hecha por el servidor. Por defecto, el servidor VPN

obtiene las direcciones IP por sí mismo y los clientes VPN las obtienen utilizando el Protocolo de Configuración Dinámica de Servidor (*Dynamic Host Configuration Protocol*, DHCP). Usted también puede configurar una reserva estática de direcciones IP (*static IP address pool*).

DNS.

La asignación del servidor de nombres, la asignación de servidores del Sistema de Nombres de Dominio (*Domain Name System*) y del Servicio de Nombre de Internet de Windows (*Windows Internet Name Service*, WINS), también ocurre durante el proceso de establecimiento de la conexión VPN. El cliente VPN obtiene las direcciones IP del DNS y WINS desde el servidor VPN para la intranet a la cual está conectada el servidor.

3.3.1.3 Conexiones VPN en Internet y en intranets

Las conexiones VPN pueden ser utilizadas siempre que se requiera una conexión punto a punto segura para conectar usuarios o redes. Las conexiones VPN típicas están construidas sobre Internet o sobre intranets.

3.3.1.4 Conexiones VPN sobre Internet

Al utilizar una conexión VPN sobre Internet, usted evita gastos de larga distancia a la vez que toma ventaja de la disponibilidad global de Internet.

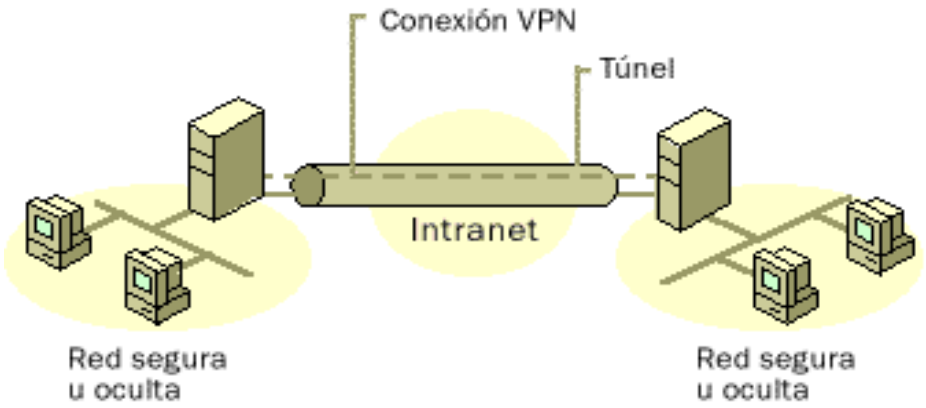


Gráfico 3.3: Conexión VPN's sobre Internet

3.3.1.5 Acceso remoto sobre Internet

En lugar de que un cliente de acceso remoto tenga que hacer una llamada de larga distancia a un servidor de acceso de redes (*Network Access Server*, NAS) corporativo o contratado, el cliente puede llamar a un ISP local. Al utilizar la conexión física establecida con el ISP local, el cliente de acceso remoto inicia una

conexión a través de Internet hacia la el servidor VPN de la organización Una vez que la conexión VPN es creada, el cliente de acceso remoto tiene acceso a los recursos de la intranet privada.

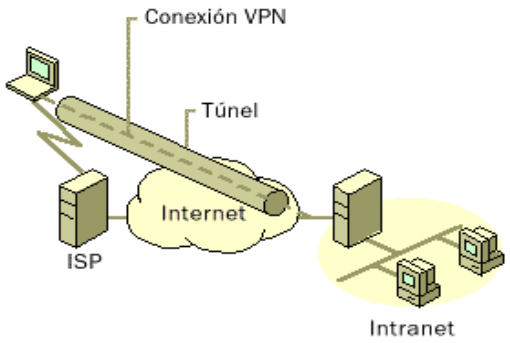


Gráfico 3.4: Acceso remoto sobre Internet.

3.3.1.6 Conectando redes sobre Internet

Cuando las redes se conectan sobre Internet, un enrutador dirige los paquetes hacia otro enrutador a través de una conexión VPN. Para los enrutadores, la VPN opera cono un enlace en la capa de enlace de datos (*data-link layer*).

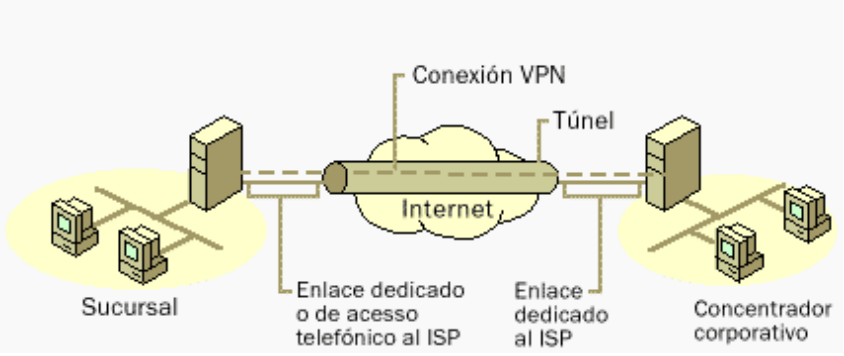


Gráfico 3.5:Conexión VPN conectando dos sitios remotos a través de Internet

3.3.1.7 Conectando redes utilizando enlaces WAN dedicados

En lugar de utilizar un enlace WAN dedicado y caro de larga distancia entre sus oficinas, los enrutadores de las oficinas se pueden conectar a Internet usando enlaces WAN dedicados locales hacia un ISP local. Una conexión VPN de enrutador a enrutador es entonces iniciada por cualquiera de los dos enrutadores a través de Internet. Una vez que se conectan, los enrutadores pueden dirigir tráfico directo o con protocolo de enrutamiento entre ellos usando la conexión VPN.

3.3.1.8 Conectando redes usando enlaces WAN de acceso telefónico.

En lugar de tener un enrutador en una oficina sucursal que haga llamadas de larga distancia a una NAS corporativa o contratada, el enrutador de la sucursal puede llamar a un ISP local. Utilizando la conexión establecida con el ISP local, el enrutador de la sucursal inicia una conexión VPN de enrutador a enrutador con el enrutador concentrador (*hub router*) corporativo a través de Internet. El enrutador concentrador que actúa como un servidor VPN debe de estar conectado al ISP local utilizando un enlace WAN dedicado.

Es posible tener ambas oficinas conectadas a Internet utilizando un enlace WAN de acceso telefónico. Sin embargo, esto solo es factible si el ISP soporta enrutamiento de marcado por demanda (*demand-dial routing*) para sus clientes; el ISP llama al enrutador del cliente cuando un datagrama IP va a ser enviado al cliente. El enrutamiento de marcado por demanda para los clientes no está ampliamente soportado por los ISPs.

Conexiones VPN de acceso remoto

Para las conexiones VPN de acceso remoto, una computadora crea una conexión de acceso remoto a un servidor VPN. Durante el proceso de conexión el servidor VPN asigna una dirección IP para el cliente de acceso remoto y modifica la ruta por defecto en el cliente remoto para que el tráfico de la ruta por defecto sea enviado sobre la interfaz virtual.

Direcciones IP y el cliente VPN de acceso telefónico

Para los clientes VPN de acceso telefónico que se conectan a Internet antes de crear la conexión VPN con un servidor VPN en Internet, dos direcciones IP son asignadas:

- Cuando se crea la conexión PPP, la negociación IPCP con el NAS del ISP asigna una dirección IP pública.
- Cuando se crea la conexión VPN, la negociación IPCP con el servidor VPN asigna una dirección IP de la intranet. La dirección IP asignada por el servidor VPN puede ser una dirección IP pública o una privada, dependiendo si su organización está implementando direccionamiento público o privado en su intranet.

En cualquier caso, la dirección IP asignada al cliente VPN debe estar accesible por los servidores de la intranet y viceversa. El servidor VPN debe tener las definiciones apropiadas en sus tablas de enrutado para accesar a todos los servidores de la intranet y los enrutadores de la intranet deben de tener las definiciones apropiadas en sus tablas de enrutado para accesar a los clientes VPN.

Los datos enviados por el túnel y a través de la VPN son direccionados desde la dirección del cliente VPN asignada por el servidor VPN hasta la dirección de la intranet. La cabecera IP más externa es direccionada entre la dirección IP del cliente VPN asignada por el ISP y la dirección pública del servidor VPN. Debido a que los enrutadores en Internet solamente procesan la cabecera IP más externa, los enrutadores de Internet dirigirán los datos del túnel a la dirección IP pública del servidor VPN.

Un ejemplo del direccionamiento de un cliente de acceso telefónico se muestra en la Gráfico 3.5, donde la organización utiliza direcciones privadas en la intranet y los datos enviados por el túnel están dentro de un datagrama IP.

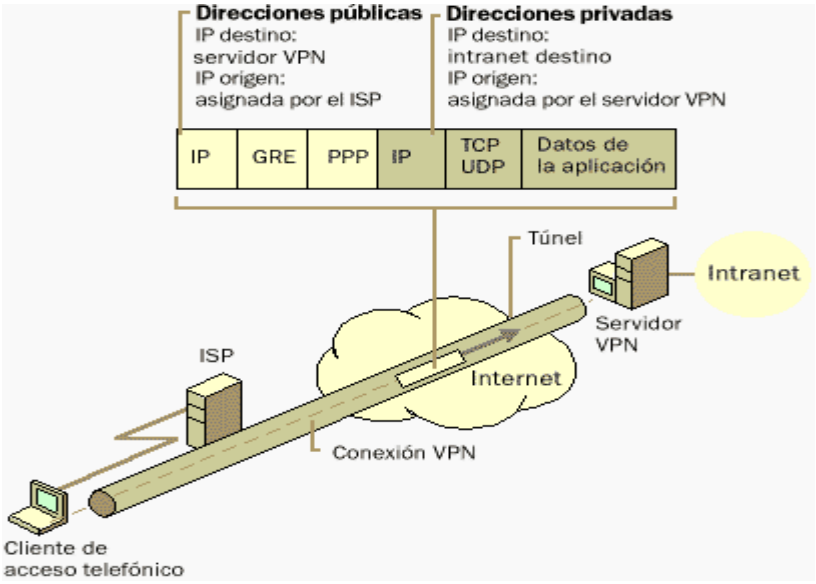


Gráfico 3.6. Direccionamiento público y privado en los datos del túnel PPTP

Cuando un típico cliente de acceso telefónico llama al ISP, recibe una dirección IP pública del NAS del ISP. No se asigna la dirección de un *gateway* por defecto como parte del proceso de negociación IPCP. Por lo tanto, para accesar todas las direcciones de Internet, el cliente de acceso telefónico agrega una ruta por defecto a su tabla de enrutamiento utilizando la interfaz conectada al ISP. Como resultado de esto, el cliente puede redirigir los datagramas IP al NAS del ISP desde donde son enrutados a su localización en Internet.

Para los clientes sin otras interfaz TCP/IP, esto es el comportamiento deseado. Sin embargo, este comportamiento puede causar confusión a los clientes de acceso telefónico que tienen una conexión de LAN existente hacia una intranet. En este escenario, ya existe una ruta por defecto apuntando al enrutador de la intranet local. Cuando el cliente de acceso telefónico crea una conexión con su ISP, la ruta por defecto permanece en la tabla de enrutamiento,

pero es modificada para que tenga una métrica superior. Se agrega una nueva ruta por defecto con una métrica inferior que utilice la conexión del ISP.

Como resultado, las localizaciones de la intranet que no están directamente conectadas a la red no son accesibles durante la duración de la conexión con el ISP. Si la nueva ruta por defecto no se crea, todas las localizaciones de la intranet son accesibles, pero las localizaciones de Internet no lo son.

Un cliente de acceso telefónico con Windows o Linux crea la ruta por defecto. Para evitar que la ruta por defecto sea creada, desactive la casilla de verificación Use default gateway on remote network en la ventana de diálogo PPP TCP/IP Settings de la ficha **Servidor** en una de las definiciones del directorio de acceso telefónico a redes.

Para tener conectividad tanto a las localizaciones de la intranet como a las de Internet mientras la conexión ISP esté activa, deje seleccionada la opción Use default gateway on remote network y agregue las rutas de la intranet a la tabla de enrutamiento del acceso telefónico. Las rutas a la intranet pueden agregarse a través de rutas estáticas persistentes. Cuando se está conectado al ISP, todas las localizaciones de la intranet están accesibles utilizando las rutas de la intranet y todas las localizaciones de Internet están accesibles utilizando la ruta por defecto.

Rutas por defecto y las VPN sobre Internet

Cuando el cliente de acceso telefónico llama al ISP, agrega una ruta por defecto utilizando la conexión al ISP como se muestra en la Gráfico 3.6. En este punto, puede accesar todas las direcciones de Internet a través del enrutador en el NAS el ISP.

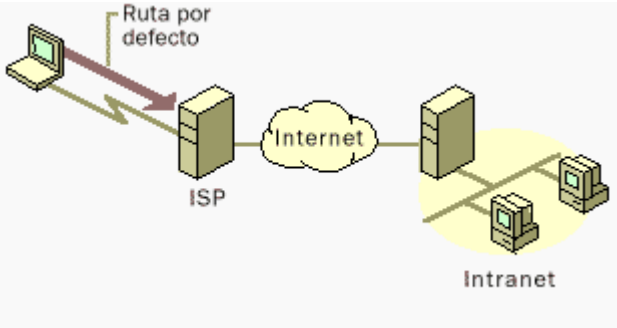


Gráfico 3.7. Ruta por defecto creada cuando se llama al ISP

Una vez que el cliente VPN crea la conexión VPN, se agrega otra ruta por defecto y una ruta al servidor hacia la dirección IP del servidor del túnel, como se ilustra en la Gráfico 3.7. La ruta por defecto previa es grabada pero ahora tiene una métrica superior. El agregar la nueva ruta por defecto significa que todas las direcciones de las localizaciones de Internet, excepto la dirección IP del servidor del túnel, no estarán accesibles mientras dure la conexión VPN.

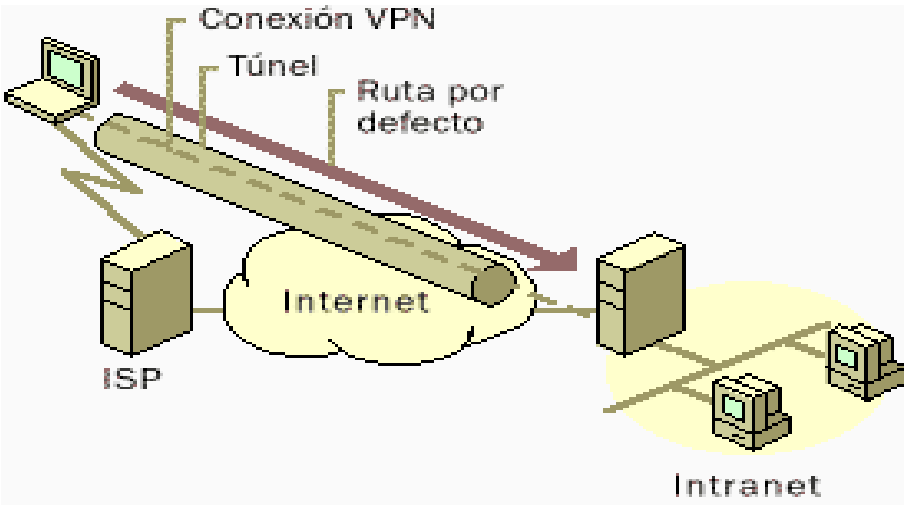


Gráfico 3.8. Ruta por defecto creada cuando se inicia la VPN

Tal como en el caso de un cliente de acceso telefónico a Internet, cuando un cliente VPN de acceso telefónico que usa creación voluntaria de túneles crea una conexión VPN a una intranet privada a través de Internet, una de las siguientes cosas ocurre:

- Las localizaciones de Internet son accesibles y las localizaciones de la intranet no son accesibles cuando la conexión VPN no está activa.
- Las localizaciones de la intranet son accesibles y las localizaciones de Internet no son accesibles cuando la conexión VPN está activa.

Para la mayoría de los clientes VPN conectados por Internet, este comportamiento no representa problema porque generalmente se encuentran utilizando la comunicación a la intranet o a Internet, pero no hacia ambas.

Para los clientes VPN que quieren tener acceso concurrente a los recursos de la intranet y de Internet cuando la VPN está conectada, la solución depende de la naturaleza del direccionamiento IP en la intranet. En todos los casos, configure la conexión VPN de tal modo que no agregue el *gateway* por defecto. Cuando la conexión VPN sea creada, la ruta por defecto persistirá apuntando al NAS del ISP, permitiendo el acceso a todas las direcciones de Internet.

Dependiendo del tipo de direccionamiento que use en la intranet, habilite el acceso concurrente a los recursos de la intranet y de Internet de la manera siguiente:

Direcciones públicas

Agregue rutas estáticas persistentes para los identificadores (IDs) de la red pública de la intranet utilizando la dirección IP de la interfase virtual del servidor VPN como dirección IP del *gateway*.

Direcciones privadas

Agregue rutas estáticas persistentes para los identificadores (IDs) de la red privada de la intranet utilizando la dirección IP de la interfase virtual del servidor VPN como dirección IP del *gateway*.

Direcciones traslapadas o ilegales

Si la intranet está utilizando direcciones traslapadas o ilegales (ID's de la red IP que no son privados y que no han sido registrados por InterNIC o que no se han obtenido de un ISP), esas direcciones IP podrían tener duplicados en direcciones públicas de Internet. Si las rutas estáticas persistentes se agregan al cliente VPN usando los ID's de red traslapados de la intranet, las localizaciones de Internet de esas localizaciones traslapadas no podrán acceder.

En cada uno de estos casos, las rutas estáticas persistentes para los IDs de la red de la intranet necesitan ser agregadas al cliente VPN. Una vez que las rutas persistentes sean agregadas, se grabarán en el registro de configuraciones (*registry*). Con Windows las rutas persistentes no son en realidad agregadas a la tabla de enrutamiento IP (y no son visibles con el comando **route print** en la interfaz de comandos de Windows) hasta que la dirección IP del *gateway* sean accesibles. La dirección IP del *gateway* estará accesible cuando se haga la conexión VPN.

La dirección IP del *gateway* en el comando route de cada ruta a la intranet es la dirección IP asignada a la interfaz virtual del servidor, no la dirección IP de la interfaz del servidor VPN a Internet.

Usted puede determinar la dirección IP de la interfaz virtual del servidor VPN usando el comando ipconfig en la interfaz de comandos de Windows NT. Si usted utiliza DHCP para obtener las direcciones para el acceso telefónico a redes y los clientes VPN, la dirección IP

de la interfaz virtual del servidor VPN es la primera dirección IP obtenida cuando se piden las direcciones de DHCP. Si usted ha configurado una reserva estática de direcciones IP, la dirección IP de la interfaz virtual del servidor VPN es la primera dirección IP de la reserva estática de direcciones IP. También puede determinar la dirección IP de la interfaz virtual del servidor VPN observando los detalles de una conexión VPN activa en el cliente VPN.

Advertencia: En todos los casos, usted debe de agregar las rutas cuidadosamente para asegurarse que el tráfico privado hacia la intranet sea redirigido usando la conexión VPN y no la conexión PPP hacia el ISP. Si se agregan las rutas equivocadas, el tráfico que intentaba redirigir a través de la VPN en forma encriptada será enviada en forma no encriptada a través de Internet. Por ejemplo, si su intranet está utilizando el ID de red pública 207.46.130.0/24 (máscara de subred 255.255.255.0) y usted por error agrega una ruta estática persistente para 207.46.131.0/24, todo el tráfico a la intranet en 207.46.130.0/24 será redirigido a través de Internet en forma no encriptada, en lugar de ser encriptada y enviada a través de la conexión VPN.

Conexiones VPN de Enrutador a Enrutador

Para las VPN's de enrutador a enrutador que utilicen el Servicio de Acceso Remoto y Enrutamiento (*Routing and Remote Access Service*, RRAS). la creación de interfaces por demanda es automatizada con el Asistente de Interfaz de Marcado por Demanda (*Demand Dial Interface Wizard*).

Los nombre de las interfaz de marcado por demanda y las credenciales deben de coincidir para asegurar una conexión VPN de enrutador a enrutador.

VPN's de enrutador a enrutador temporales vs. persistentes

Las conexiones VPN de enrutador a enrutador pueden ser temporales o persistentes.

Las conexiones VPN temporales de enrutador a enrutador se hacen cuando hay paquetes que tienen que ser enrutados a través de una interfase de marcado por demanda y terminan después de un periodo de tiempo específico sin uso.

El tiempo de espera sin uso (*idle time*) es configurado en el cliente VPN (el enrutador que llama). El tiempo de espera sin uso por defecto para interfases de marcado por demanda en el cliente VPN es ilimitado. Use las conexiones VNP temporales de enrutador a enrutador para las sucursales que usen conexiones de acceso telefónico con sus ISP's locales.

Las conexiones VPN persistentes de enrutador a enrutador se hacen cuando el enrutador es encendido y permanece conectado sin importar el tráfico que sea enviado. Si la conexión VPN es terminada, automáticamente se intenta reiniciar de nuevo. Utilice las conexiones VPN persistentes de enrutador a enrutador para conectar oficinas que tengan conexiones permanentes a Internet. El tiempo de espera sin uso (*idle time*) es configurado en la ficha **Dialing** en las propiedades de la conexión de marcado por demanda.

VPNs utilizando conexiones de acceso telefónico con un ISP

Cuando tanto el servidor VPN como el cliente VPN están conectados directamente a Internet usando un enlace WAN permanente, como un T1 o Frame Relay, la conexión VPN puede ser persistente y estar disponible 24 horas al día. Sin embargo, cuando un enlace WAN permanente no es posible o práctico, usted puede configurar una conexión VPN de enrutador a enrutador por demanda usando un acceso telefónico de un ISP.

Una conexión VPN por demanda de enrutador a enrutador, que utilice una conexión de acceso telefónico, consiste de dos interfases de marcado por demanda:

- Una interfase de marcado por demanda para marcara al acceso telefónico del ISP local.

- Una interfase de marcado por demanda para la conexión VPN de enrutador a enrutador.

Una conexión VPN por demanda de enrutador a enrutador se establece automáticamente cuando el enrutador de la sucursal recibe tráfico que será redireccionado a través de la conexión VPN. Por ejemplo, cuando se recibe un paquete que será enrutado a la oficina corporativa, el enrutador de la sucursal primero utiliza un enlace de acceso telefónico para conectarse al ISP local. Una vez que la conexión a Internet está hecha, el enrutador de la sucursal, el cliente VPN, crea una conexión VPN de enrutador a enrutador con el enrutador de la oficina corporativa, el servidor VPN.

Para configurar una conexión VPN por demanda en el enrutador de la sucursal

1. Tiene que crear una interfase para la conexión a Internet configurada para el equipo apropiado (un módem o un dispositivo ISDN), el número de teléfono del ISP local, el nombre de usuario y la clave utilizados para tener acceso a Internet.
2. Tiene que crear una interfase de marcado por demanda para la conexión VPN de enrutador a enrutador con el enrutador de la oficina corporativa configurado para un dispositivo PPTP, la dirección IP o el nombre del servidor de la interfase del servidor VPN con Internet y con un nombre de usuario y clave que puedan ser verificadas en el servidor VPN. El nombre de usuario debe coincidir con el nombre de la interfase de marcado por demanda en el servidor VPN de la oficina corporativa.
3. Tiene que crear una ruta estática al servidor para la dirección IP de la interfase del servidor VPN en Internet que utilice la interfase de marcado por demanda utilizada para llamar al ISP local.
4. Tiene que crear un ruta (o rutas) estática para los IDs de la red IP de la intranet corporativa que utilicen la interfase VPN de marcado por demanda.

Para configurar el enrutador de la oficina corporativa

1. Tiene que crear una interfase de marcado por demanda para la conexión VPN con la sucursal configurada para un dispositivo PPTP. La interfase de marcado por demanda debe tener el mismo nombre de usuario en la credencial de autentificación que el utilizado por el enrutador de la sucursal para crear la conexión VPN.
2. Tiene que crear una ruta o rutas estáticas para los IDs de la red IP de la sucursal que utiliza la interfase VPN de marcado por demanda.

La conexión VPN de enrutador a enrutador es iniciada automáticamente por el enrutador de la sucursal a través del siguiente proceso:

1. Los paquetes enviados al concentrador de la red corporativa por un usuario en la sucursal son redireccionados por el usuario al enrutador de la sucursal.
2. El enrutador de la sucursal revisa su tabla de enrutamiento y encuentra una ruta hacia el ID de la red corporativa, el cual utiliza una interfase VPN por demanda.
3. El enrutador de la sucursal revisa el estado de la interfase VPN de marcado por demanda y encuentra que está en desconectado.
4. El enrutador de la sucursal busca la configuración de la interfase VPN de marcado por demanda.
5. Basado en la configuración de la interfase VPN de marcado por demanda, el enrutador de la sucursal intenta iniciar una conexión VNP de enrutador a enrutador en la dirección IP del servidor VPN en Internet.
6. Para establecer una VPN con PPTP, debe de establecerse una conexión TCP con el servidor VPN. Se crea el paquete de establecimiento de la VPN.
7. Para redirigir el paquete de establecimiento de la VPN al enrutador de la oficina corporativa, el enrutador de la sucursal revisa su tabla de enrutamiento y encuentra la ruta al servidor que utiliza la interfase de marcado por demanda del ISP.

8. El enrutador de la sucursal revisa el estado de la interfase de marcado por demanda del ISP y encuentra que está desconectada.
9. El enrutador de la sucursal busca la configuración de la interfase de marcado por demanda del ISP.
10. Basado en la configuración de la interfase de marcado por demanda del ISP, el enrutador de la sucursal utiliza su módem o adaptador ISDN para llamar y establecer una conexión con su ISP local.
11. Una vez que la conexión ISP está hecha, el paquete de establecimiento VPN es enviado por el enrutador de la sucursal al enrutador de la oficina corporativa.
12. Se negocia una VPN entre el enrutador de la sucursal y el enrutador corporativo. Como parte de la negociación, el enrutador de la sucursal envía las credenciales de autentificación que serán verificadas por el enrutador corporativo.
13. El enrutador corporativo verifica sus interfases de marcado por demanda y encuentra uno que coincida con el nombre de usuario enviado durante la autentificación y cambia el estado de la interfase a conectado.
14. El enrutador de la sucursal redirige los paquetes a través de la VPN y el servidor VPN redirige los paquetes a la localización apropiada en la intranet.

Enrutado dinámico vs. estático

Una vez que las interfaces de marcado por demanda son creadas y se ha decidido entre usar conexiones temporales o persistentes, debe de elegir uno de los siguientes métodos para agregar la información de enrutamiento a la tabla de enrutamiento:

1. Para conexiones temporales, puede agregar las rutas estáticas apropiadas a los IDs de red en las otras sucursales. La configuración manual de las rutas estáticas es apropiada para pequeñas implementaciones con un número pequeño de rutas.

2. Para conexiones temporales, puede utilizar actualizaciones auto-estáticas para actualizar periódicamente las rutas estáticas que están disponibles a través de la conexión VPN de enrutador a enrutador.
3. Para conexiones persistentes, ejecute los protocolos de enrutamiento apropiados en la conexión VPN de enrutador a enrutador tratando a la conexión VPN como un enlace punto a punto.

Nota: A diferencia del enrutamiento de marcado por demanda que usan conexiones físicas directas, no se puede utilizar una ruta IP por defecto para la interfase VPN de marcado por demanda para incluir todas las rutas a la intranet disponibles a través de la VPN. Debido a que el enrutador está conectado a Internet, debe utilizar la ruta por defecto para incluir todas las rutas hacia Internet y configurarlo para utilizar la interfase de Internet.

Las VPN's y los *firewalls*

Un *firewall* utiliza el filtrado de paquetes (*packet filtering*) para permitir o prohibir el flujo de cada tipo específico de tráfico en la red. El filtrado de paquetes IP proporciona una manera de definir de manera precisa qué tráfico IP es permitido a través del *firewall*. El filtrado de paquetes IP es importante cuando usted conecta intranets privadas a redes públicas como Internet.

El Servidor VPN y las configuraciones del *firewall*

Hay dos abordajes para utilizar un *firewall* con un servidor VPN:

- El servidor VPN está conectado a Internet y el *firewall* está entre el servidor VPN y la intranet.
- El *firewall* está conectado a Internet y el servidor VPN está entre el *firewall* e Internet.

Servidor VPN frente al firewall

Con el servidor VPN enfrente del *firewall* conectado a Internet, como se muestra en la Gráfico 3.8, usted necesita agregar los filtros de paquetes a la interfase con Internet que solamente permitan tráfico de la VPN hacia y desde la dirección IP de la interfase del servidor VPN en Internet.

Para el tráfico que entra, una vez que los datos enviados por el túnel son desencriptados por el servidor VPN, son redirigidos al *firewall*, el cual utiliza sus filtros para permitir que el tráfico sea redirigido a los recursos de la intranet. Debido a que solamente el tráfico que está cruzando el servidor VPN es tráfico generado por clientes VPN autentificados, el filtrado del *firewall* en este escenario puede ser utilizado para evitar que los usuarios VPN tengan acceso recursos específicos de la intranet.

Debido a que el único tráfico de Internet que es permitido el paso a la intranet debe pasar a través del servidor VPN, este abordaje también evita que se puedan compartir recursos de la Web y del Protocolo de Transferencia de Archivos (*File Transfer Protocol*, FTP) con usuarios que no estén en la VPN.

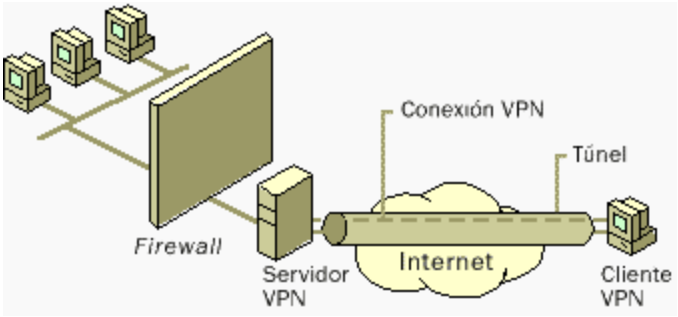


Gráfico 3.9. Servidor VPN conectado a Internet enfrente del *firewall*

Para la interfaz con Internet del servidor VPN, configure los siguientes filtros de entrada y salida utilizando la herramienta administrativa Administrador de RAS y Enrutamiento (*Routing and RAS Admin*).

Filtros de paquetes para PPTP

Configure los siguiente filtros de entrada con la acción del filtro establecido a drop all except listed below:

- Dirección IP destino de la interfaz con Internet del servidor VPN, máscara de subred a 255.255.255.255 y puerto TCP destino a 1723 (0x06BB). Este filtro permite el tráfico PPTP de mantenimiento desde el cliente PPTP al servidor PPTP.
- Dirección IP destino de la interfase con Internet del servidor VPN, máscara de subred a 255.255.255.255 e ID de Protocolo IP a 47 (0x2F). Este filtro permite que pasen los datos del túnel desde el cliente PPTP hacia el servidor PPTP.
- Dirección IP destino de la interfase con Internet del servidor VPN, submáscara de red a 255.255.255.255 y puerto TCP origen a 1723 (0x06BB). Este filtro es necesario solamente si el servidor VPN está actuando como cliente VPN (un enrutador que llama) en una conexión VPN de enrutador a enrutador. Cuando seleccione TCP, el tráfico será aceptado solamente si el servidor VPN inicia la conexión TCP.

Configure los siguientes filtros de salida con la acción del filtro establecida a drop all except listed below:

- Dirección IP origen de la interfase con Internet del servidor VPN, máscara de subred a 255.255.255.255 y Puerto TCP Origen a 1723 (0x06BB). Este filtro permite el paso del tráfico de mantenimiento del túnel PPTP desde el servidor VPN al cliente VPN.
- Dirección IP origen de la interfase a Internet del servidor VPN, máscara de subred a 255.255.255.255 e ID de Protocolo IP a 47 (0x2F). Este filtro permite el paso de datos del túnel PPTP desde el servidor VPN hacia el cliente VPN.
- Dirección IP origen de la interfase a Internet del servidor VPN, máscara de subred a 255.255.255.255 y puerto destino para TCP a 1723 (0x06BB). Este filtro solamente es necesario si el servidor VPN está actuando como cliente VPN (un enrutador que llama) en una conexión VPN de enrutador a enrutador. Cuando seleccione TCP, el tráfico será enviado solamente si el servidor VPN inició la conexión TCP.

Servidor VPN detrás del *firewall*

En una configuración más común, ilustrada en la Gráfico 3.9, el *firewall* está conectado a Internet y el servidor VPN es otro recurso más conectado a una zona desmilitarizada (DMZ). La DMZ es un segmento de una red IP que generalmente contiene recursos disponibles a los usuarios de Internet tales como servidores Web y de FTP. El servidor VPN tiene una interfase hacia la DMZ y una interfase hacia la intranet.

Con este abordaje, el *firewall* debe de configurarse con filtros de entrada y salida en su interfase con Internet para permitir el paso del tráfico de mantenimiento del túnel y los datos del túnel hacia el servidor VPN. Con filtros adicionales se puede permitir el paso de tráfico haci servidores Web, servidores FTP y otros tipos de servidor en la DMZ.

Debido a que el *firewall* no tiene las claves de encriptación para cada conexión VPN, solamente puede filtrar las cabeceras no encriptadas de los datos del túnel, dando como resultado que todos los datos del túnel pasan por el *firewall*. Sin embargo, esto no afecta la

seguridad debido a que la conexión VPN requiere un proceso de autenticación que previene el acceso no autorizado más allá del servidor VPN.

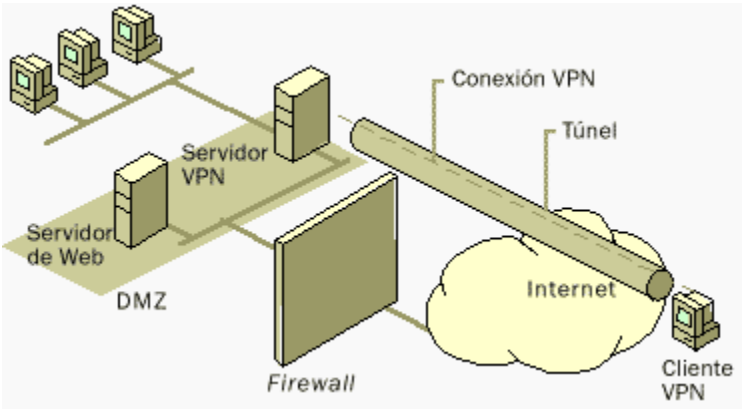


Gráfico 3.10. El servidor VPN detrás del *firewall* en Internet

Para la interfase hacia Internet en el *firewall*, los siguientes filtros de entrada y salida necesitan ser configurados usando el software de configuración del *firewall*.

Filtrado de paquetes PPTP

Configure los siguientes filtros de entrada con la acción del filtro establecida a drop all except listed below:

- Dirección IP destino de la interfase del servidor VPN con la DMZ y el puerto TCP destino a 1723 (0x06BB). Este filtro permite el tráfico de mantenimiento del túnel desde el cliente PPTP hacia el servidor PPTP.
- Dirección IP destino de la interfase del servidor VPN hacia la DMZ y el ID del Protocolo a 47 (0x2F). Este filtro permite el paso de los datos del túnel desde el cliente PPTP hacia el servidor PPTP.
- Dirección IP destino de la interfase del servidor VPN hacia la DMZ y el puerto TCP origen a 1723 (0x06BB). Este filtro es necesario solamente si el servidor VPN está actuando

como un cliente VPN (un enrutador que llama) en una conexión VPN de enrutador a enrutador. Cuando seleccione TCP, el tráfico será aceptado solamente si el servidor VPN inicia la conexión TCP.

Configure los siguientes filtros de salida con la acción del filtro establecida a drop all except listed below.

- Dirección IP origen de la interfase del servidor VPN hacia la DMZ y el Puerto TCP Origen a 1723 (0x06BB). Este filtro permite el tráfico de mantenimiento del túnel PPTP desde el servidor VPN hacia el cliente VPN.
- Dirección IP origen de la interfase del servidor VPN hacia la DMZ y el ID de Protocolo IP a 47 (0x2F). Este filtro permite el paso de los datos del túnel desde el servidor VPN hacia el cliente VPN.
- Dirección IP origen de la interfase del servidor VPN hacia la DMZ y el puerto destino TCP a 1723 (0x06BB). Este filtro es necesario solamente si el servidor VPN actúa como cliente VPN (un enrutador que llama) en una conexión VPN de enrutador a enrutador. Cuando seleccione TCP, el tráfico será enviado solamente si el servidor VPN inicia la conexión TCP.

3.3.2 FIREWALL

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados por usuarios que están fuera de nuestra Intranet, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá

únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este . ver graf 3.10.

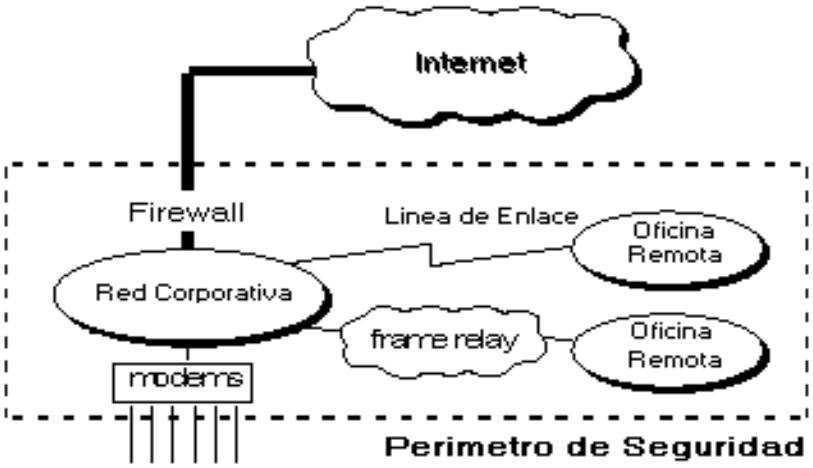


Gráfico 3.11 Perímetro de seguridad

Firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, reglas de enciptacion de datos y discos, normas de protección de virus, y entrenamiento.

3.3.2.1 Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

- El firewall permite al administrador de la red definir un envudo, manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles.

- Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

- El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos.
- Un firewall es un lugar lógico para desplegar un Traductor de direcciones de red (**NAT**), esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs)'.

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet, Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando - únicamente el acceso al Internet esta perdido.

3.3.3 Seguridad con Encriptacion

3.3.3.1 La encriptación en Shadowrun

La encriptación es un problema de seguridad importante en un mundo que depende tanto de la Matriz. Si asumimos que *p=np*, el problema sigue sin tener solución a no ser que se demuestre que *p!=np.* Siempre será más fácil de realizar la encriptación que la desencriptación. Ningún esquema de encriptación es completamente irrompible, pero no es difícil utilizar el potencial de la informática en la encriptación y hacerla arbitrariamente difícil de desencriptar.

3.3.3.2 Criptografía con llave pública

La criptografía con llave pública es una herramienta importante en una sociedad que confía en la criptografía para su seguridad. Básicamente, crea una relación entre dos trozos de código llamados "llaves". Si usas una llave para encriptar ciertos datos, la otra los desencriptará. Si designas una importante como "privada" y la guardas, y la otra como "pública" y la das a conocer al mundo, es posible enviarte un mensaje seguro encriptado con tu llave pública (haciéndolo sólo legible por ti). De la misma forma, si envías un mensaje encriptado a alguien con tu llave privada, pueden verificar que el mensaje es tuyo y pueden desencriptarlo. Así, se puede realizar una transacción segura entre dos personas paranoicas, en la que A manda un mensaje con su llave privada a un segundo, B, que tiene la la llave pública. La persona B desencripta entonces el mensaje doblemente encriptado con su llave privada, y entonces la persona A obtiene su llave pública.

3.3.3.3 Relleno único

El Relleno único es teóricamente el único método de encriptación irrompible. Básicamente, si tienes una inmensa cantidad de basura digital, puedes usarla para codificar una señal digital, y terminar con lo que parece ser más basura. Sólo alguien con ese mismo relleno único puede hacer algo con él. Probablemente se guardaría dentro de una unidad del standar que contenga una cantidad grande de datos sin acceso del exterior, y sólo se usaría para propósitos de encriptación. En su interior habrían, por supuesto, los volúmenes de desechos. Esta unidad podría ser desde un dispositivo diminuto diseñado para usarse con un conector

de datos a un base de datos con terapulsos de datos del tamaño de una caja de la herramienta grande. Puedes deducir cómo de grande necesita ser determinando cuánto espacio ocuparía la comunicación usando las reglas del *Shadowbeat*.

3.3.3.4 Grupo computacional encriptador

Hay maneras, aunque más caras que una recuperación normal, para que partes N proporcionen N entradas confidenciales a un ordenador y que devuelva sólo la respuesta. Cada parte conoce sólo su propia entrada confidencial.
Tras definir algunos algoritmos de crédito típicos como “¿coincide este NIC con este ID?” y llevar a cabo la encriptación, podrías evitar regalar información personal sensible a la Matriz. El administrador local todavía tendría que saberlo, y cualquier institución para la que trabaje tendría que confiar en su administrador, por supuesto.
Naturalmente, los servicios de comprobación tienden a basarse sólo en hardware, esas cajas negras que contienen los códigos de encriptación apropiados.

3.3.3.5 Llenar de paja y limpiar

Es una técnica de codificación que no usa encriptación. Consiste en transmitir datos útiles y "datos ficticios", junto con una llave que le permite al destinatario seleccionar los datos útiles del total, "limpiándolo”. Requiere que las dos partes tengan un esquema organizado de antemano para seleccionar los datos.

3.3.3.6 Criptografía del quántum

La verdadera seguridad está disponible si realizas el tremendo gasto de usar una técnica de hardware basada en el quántum. Requiere tener una conexión directa de fibra, muy cara, entre los dos sitios que quieren mantener comunicaciones seguras. Cualquier intento de escuchar rompería las comunicaciones (debido al problema físico básico del quántum, que

hace que cualquier observador perturbe el fenómeno). Esto se llama criptografía del quántum. El uso principal de semejante sistema sería para la transmisión segura de llaves del encriptación que podrían entonces usarse para transmitir cantidades más grandes de datos en otra parte. Un problema actual en la criptografía del quántum está en la distancia disponible. La mejor que podemos conseguir en 1996 es aproximadamente de 10km antes de que la señal de la fibra desaparezca. Para los propósitos de Shadowrun, podemos asumir que es posible hacer un “repetidor de quántum” que ha resuelto este problema. Naturalmente, esta clase de encriptación todavía sería horrorosamente cara, sobre todo si solo quiere intercambiar ficheros en una red como se hace hoy en día.

3.3.3.7 Shadowruns

La encriptación puede ser la excusa de varios posibles shadowruns. Si sostenemos que si se consigue de alguien los códigos de encriptación privados se podría llegar fácilmente llegar a sus archivos confidenciales, un tecnomante podría dar el gran golpe (por supuesto, todavía podría ser necesario falsificar un examen retinal, huellas digitales, escáner celular, y/o contraseña que podría ser necesario para dicho fin). Podría ser común utilizar a shadowrunners como mensajeros para entregar un relleno único a las personas que necesitan un secreto extremo.

Conseguir llaves privadas importantes (usados por gobiernos, megacorporaciones y bancos) debe ser increíblemente difícil, debido al potencial de uso (y abuso) que tienen. Se animan que los DJ propongan medios detallados de salvaguardar tales cosas: la forma más común es que uno tenga que actuar recíprocamente con un procesador de alguna clase que se negará a dejar una llave privada, pero se podrá fácilmente encriptar con él. Intentar abrir el dispositivo borrará la memoria.

3.3.3.8 ¿Que hay sobre la encriptación en los suplementos?

Básicamente, FASA parece ignorar cuan poderosos pueden ser los algoritmos del encriptación buenos. Sin embargo, intentemos poner un parche razonable en estas cosas:

Podemos asumir que la tecnología de encriptación dada en el Catálogo del Samurai Callejero es hardware de encriptación solo cuando hayas pagado una cierta cantidad de esencia. Algo más que eso requeriría cantidades más grandes de hardware de proceso para traducir anchos de banda rápidamente. No hay ninguna razón para que cualquiera que use un auricular externo realmente bueno no pueda tener comunicaciones sumamente seguras.
Los PAI cifradores (y la utilidad de descifrar para derrotarlos) simplemente es una encriptación molesta, diseñada para detener al invasor, pero no para detener a alguien de poder restaurar los archivos encriptados.

3.3.3.9 Notas de juego

En general, cualquiera que quiera una encriptación irrompible y tenga Teoría de las Computadoras a por lo menos nivel 3 e invierta una semana de investigación puede hacerla (hacer algo verdaderamente irrompible es muy duro, pero pueden hacer la desencriptación arbitrariamente difícil). Pueden fácilmente inventarse esquemas que requeriría todo el poder de la informática y la Matriz para destrozarlos, y son usados igualmente por hombres de negocios y delincuentes.
El truco es, por supuesto, conseguir a la llave de encriptación (y los shadowrunners son justo las personas para intentarlo). Recuerda: cuantas más personas necesitan acceso a algo, más fácil es conseguirlo. No diseñes cualquier medida de seguridad que ni siquiera pueda ser usada por las personas que lo necesiten.

3.3.4 Switch

3.3.4.1 Tecnología de Switch

Un switch es un dispositivo de *propósito especial* diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

3.3.4.2 Donde usar Switch?

Uno de los principales factores que determinan el éxito del diseño de una red, es la habilidad de la red para proporcionar una satisfactoria interacción entre cliente/servidor, pues los usuarios juzgan la red por la rapidez de obtener un prompt y la confiabilidad del servicio.

La confiabilidad del servidor se la determina cuando brindamos acceso solo a direcciones IP autorizadas, las cuales serán solo configuradas desde consola, por lo tanto podemos hablar de un nivel mas de seguridad el que nos brinda el Switch.

Hay diversos factores que involucran el incremento de ancho de banda en una LAN:

- **· El elevado incremento de nodos en la red.**

- · El continuo desarrollo de procesadores mas rápidos y poderosos en estaciones de trabajo y servidores.
- · La necesidad inmediata de un nuevo tipo de ancho de banda para aplicaciones intensivas cliente/servidor.
- · Cultivar la tendencia hacia el desarrollo de granjas centralizadas de servidores para facilitar la administración y reducir el número total de servidores.

La regla tradicional 80/20 del diseño de redes, donde el 80% del tráfico en una LAN permanece local, se invierte con el uso del switch.

Los switches resuelven los problemas de anchos de banda al segmentar un dominio de colisiones de una LAN, en pequeños dominios de colisiones.

En la figura la segmentación casi elimina el concurso por el medio y da a cada estación final más ancho de banda en la LAN.

3.3.5 Router

3.3.5.1 Protocolos de Ruteo

Para disipar esta información de ruteo se utilizan algoritmos especializados (también llamados Protocolos de Ruteo "Routing Protocols") que agilizan y facilitan la transferencia de Información de estas direcciones lógicas (nodos IP), estos algoritmos pueden ser implementados en varios Sistemas Operativos y su selección depende del tipo de conectividad que se emplee, obviamente los equipos Cisco salen a relucir en esta área ya que su objetivo principal es precisamente eficientizar este proceso através de una gran gamma de protocolos de Ruteo. Varios sistemas operativos (Linux,Windows) ofrecen Protocolos de Ruteo primitivos (como RIP) pero carecen de algoritmos especializados de Ruteo como aquellos desarrollados por Cisco (como EIGRP). Algunos protocolos de Ruteo y su funcionamiento son:

- **RIP** *Contenido en Proceso*
- **OSPF** *Contenido en Proceso*
- **EIGRP** *Contenido en Proceso*
- **BGP** *Contenido en Proceso*

3.3.5.2 Donde usar un ruteador?

Las funciones primarias de un ruteador son:

- **Segmentar la red dentro de dominios individuales de brodcast.**
- Suministrar un envío inteligente de paquetes. Y
- Soportar rutas redundantes en la red.

Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los brodcast no pasaran a través del ruteador.
Otros importantes beneficios del ruteador son:

- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- Consolidar el legado de las redes de mainframe IBM, con redes basadas en PCs a través del uso de Data Link Switching (DLSw).
- **Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.**
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

3.3.6 Protocolo SSL

3.3.6.1 Secure Socket Layer (SSL)

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL opera como una capa adicional entre Internet y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, Telnet y otras aplicaciones además de HTTP.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos. Primero se debe hacer una solicitud de seguridad. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como *SSL Handshake*. Una vez se haya establecido una comunicación segura, se deben hacer verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos. Luego que la transacción ha sido completada, se termina SSL.

3.3.6.2 Solicitud de SSL:

Antes de que se establezca SSL, se debe hacer una solicitud. Típicamente esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL. SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio.

Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el *SSL Handshake*.

3.3.6.3 SSL Handshake:

Durante el *hanshake* se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una llave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación SSL.

Los pasos que se siguen son los siguientes:

- Client Hello : El "saludo de cliente" tiene por objetivo informar al servidor que algoritmos de criptografía puede utilizar y solicita una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio.. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define como cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen que métodos pueden utilizar y un algoritmo de hash de una sola vía. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.

- Server Hello : El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de que algorítmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.

- Aprobación del Cliente: El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo desencriptando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la encripta utilizando la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave

se le envía al servidor y en caso de que el handshake tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

- Verificación: En este punto ambas partes conocen la llave secreta, el cliente por que la generó y el servidor por que le fué enviada utilizando su llave pública, siendo la única forma posible de desencriptarla utilizando la llave privada del servidor. Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones encriptada con la llave secreta. Si ambas partes confirman la validez de las transacciones, el handshake se completa, de otra forma se reinicia el proceso.

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión. El handshake se realiza solo una vez y se utiliza una llave secreta por sesión.

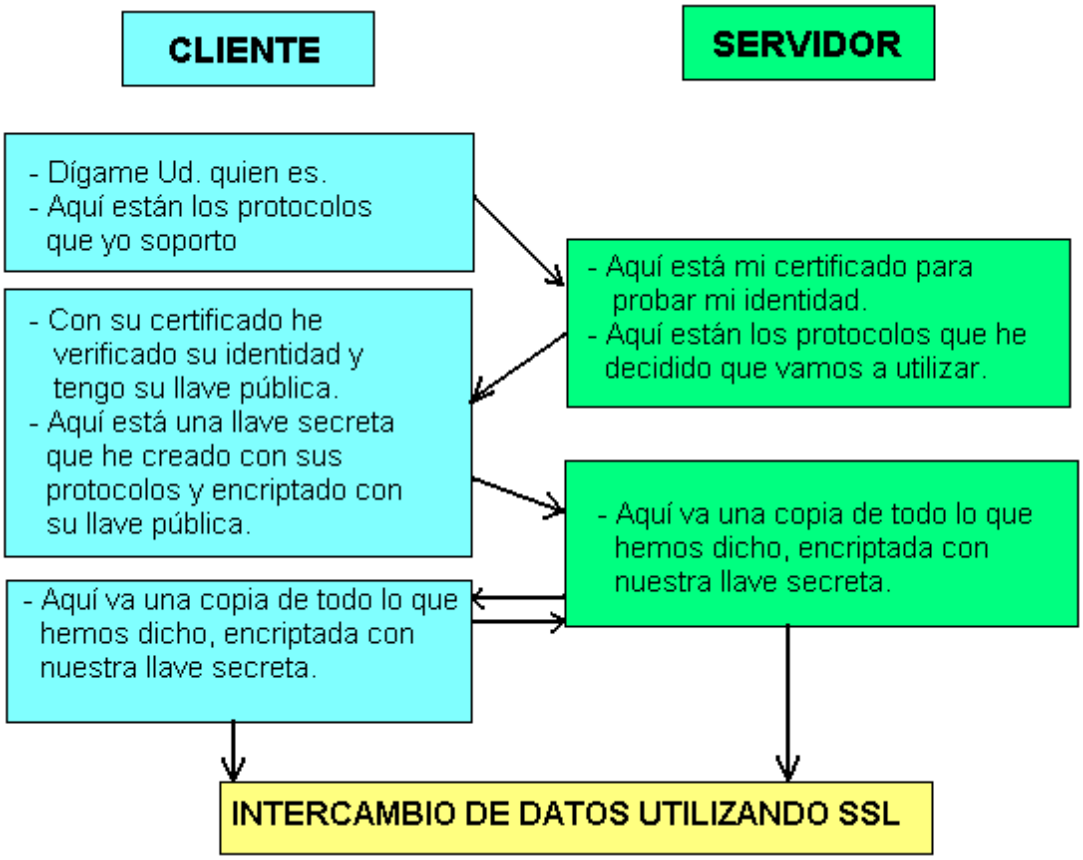


Gráfico 3.12: En la figura se ilustra el proceso de handshake

3.3.6.4 Intercambio de datos:

Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash de una vía acordado durante el handshake), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

3.3.6.5 Terminación de una sesión SSL:

Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

3.3.7 Administración del Dominio.

3.3.7.1 Seguridad en Base de Datos Notes

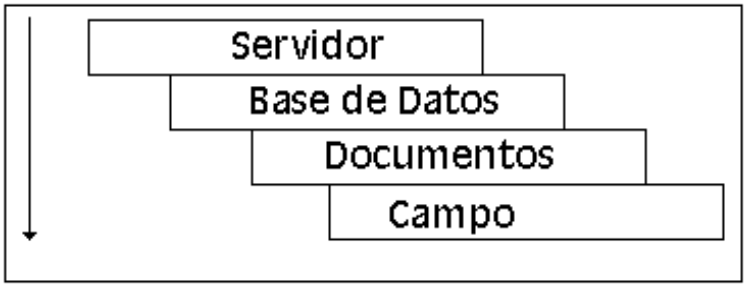


Gráfico 3.13: Nivel de Seguridad en bases de datos Notes

Cada nivel de seguridad de Notes restringe el acceso a la información y no puede prevalecer sobre un nivel de seguridad superior.

3.3.7.1.1 ID de Usuario.
La base fundamental y esencial de la seguridad en Lotus Notes radica en el identificador del usuario (ID), que es un archivo de extensión id el cual se crea al momento en que el administrador del sistema crea un nuevo usuario y almacena todos los permisos y atributos que tendrá en el Dominio.

3.3.7.1.2 Seguridad en servidores.

Para que un usuario pueda trabajar en la base de datos del servidor de Notes, debe estar registrado en dicho servidor, este acceso viene determinado por los certificados anexos al archivo id del usuario y del administrador.

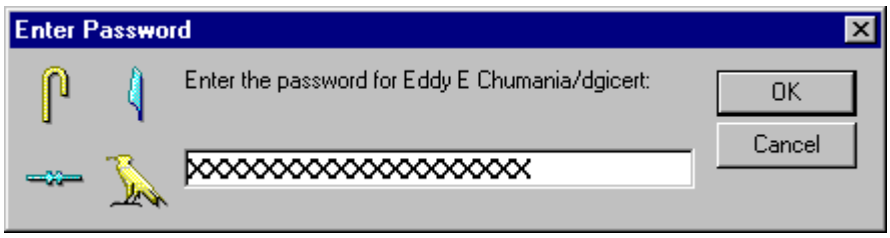


Gráfico 3.14: Seguridad del servidor Notes

3.3.7.1.3 Seguridad en Base de datos.

Las bases de datos poseen una lista de control de acceso, permite el controlar quien puede abrir la base de datos, para las respectivas operaciones que realiza el usuario.

Esta información puede protegerse del acceso directo desde fuera del entorno Notes, mediante la opción de codificación.

3.3.7.1.4 Seguridad en Documentos.

Un documento puede restringir el acceso a la información que contiene, Incluso si los usuarios intentar acceder a el disponen de un nivel de acceso de elctor a la base de datos. Hay que tomar en cuanta que un documento hereda de su formulario original la lista de control de acceso y los lectores que aparecen en el campo de lectores.

Se puede agregar funciones de seguridad a los formularios de una forma más rápida siempre y cuando los nombres de los usuarios a la base de datos se encuentre ya organizados en grupos.

3.3.7.1.5 Seguridad en Campos.

Un usuario con nivel de acceso de diseñador o de autor puede restringir la lectura de una parte determinada de un documento activado la codificación de campos. Si de asocian claves de codificación a un documento, se codificaran todos los campos codificables a dichos documentos. Los usuarios que tengan claves de codificación correcta podrán decodificar el campo para visualizar el contenido.

Un diseñador puede evitar que los autores modifiquen partes de sus propios documentos, seleccionando la opción de seguridad de los campos, se necesita nivel de acceso de Editor o superior.

CAPITULO 4

DISEÑO, CONSTRUCCION E IMPLEMETACION DE LA BASE DE DATOS DOCUMENTAL PARA INTERCAMBIO DE INFORMACION CALIFICADA ENTRE ECUADOR Y COLOMBIA.

4. Diseño Físico de Intranet / Extranet para ECORED

4.1 Medios de Comunicación a utilizar

Los medios de comunicación a utilizar serán como prioridad la comunicación por Internet ver graf. 4.1

La segunda opción es la de utilizar el medio de sistema de comunicación microondas publico internacional utilizando un módem externo, y realizando una llamada internacional graf. 4.2.

Para la segunda etapa de esta proyectado que entrara en funcionamiento el sistema privado de microondas internacional (Gráfico 4.3) para su comunicación, ya que una vez que entre en funcionamiento este sistema quedara como primera opción para la comunicación, y como plan de contingencias quedara el medio de comunicación el Internet, y como tercera opción quedara luego la comunicación vía módem utilizando el sistema microondas publico internacional.

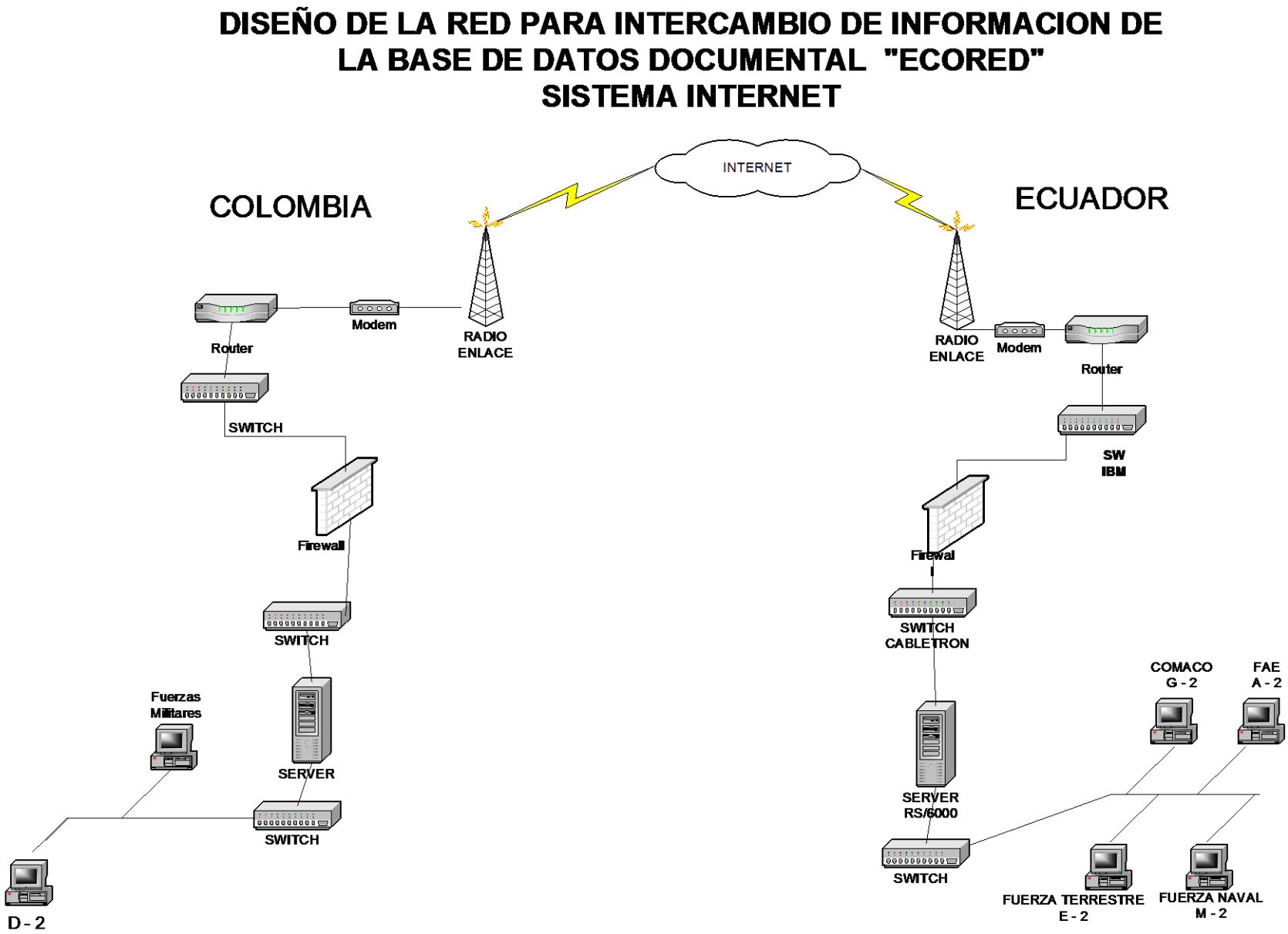


Gráfico 4.1: Comunicación por Sistema Internet

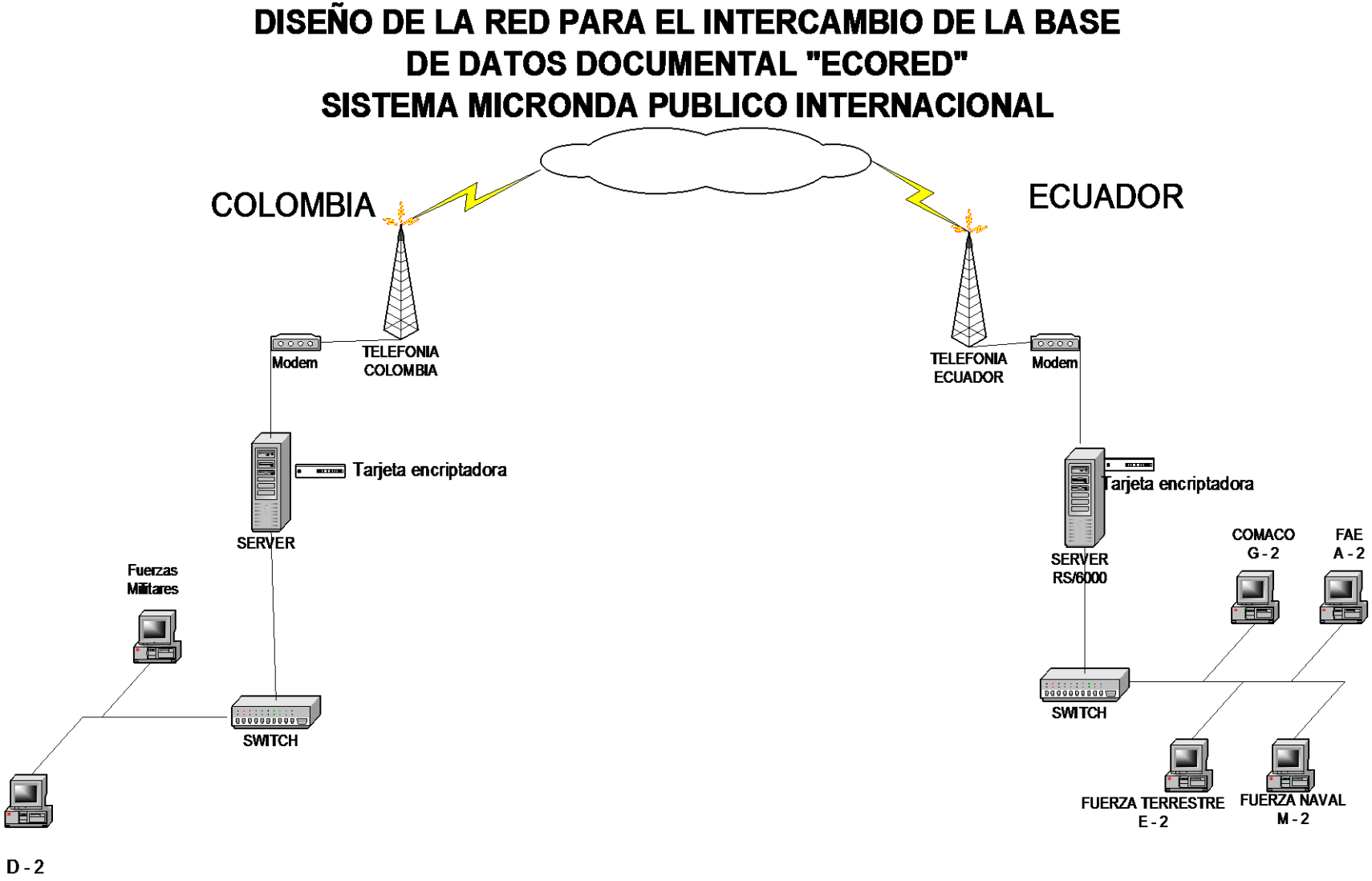


Gráfico 4:2. Comunicación por Sistema Microondas

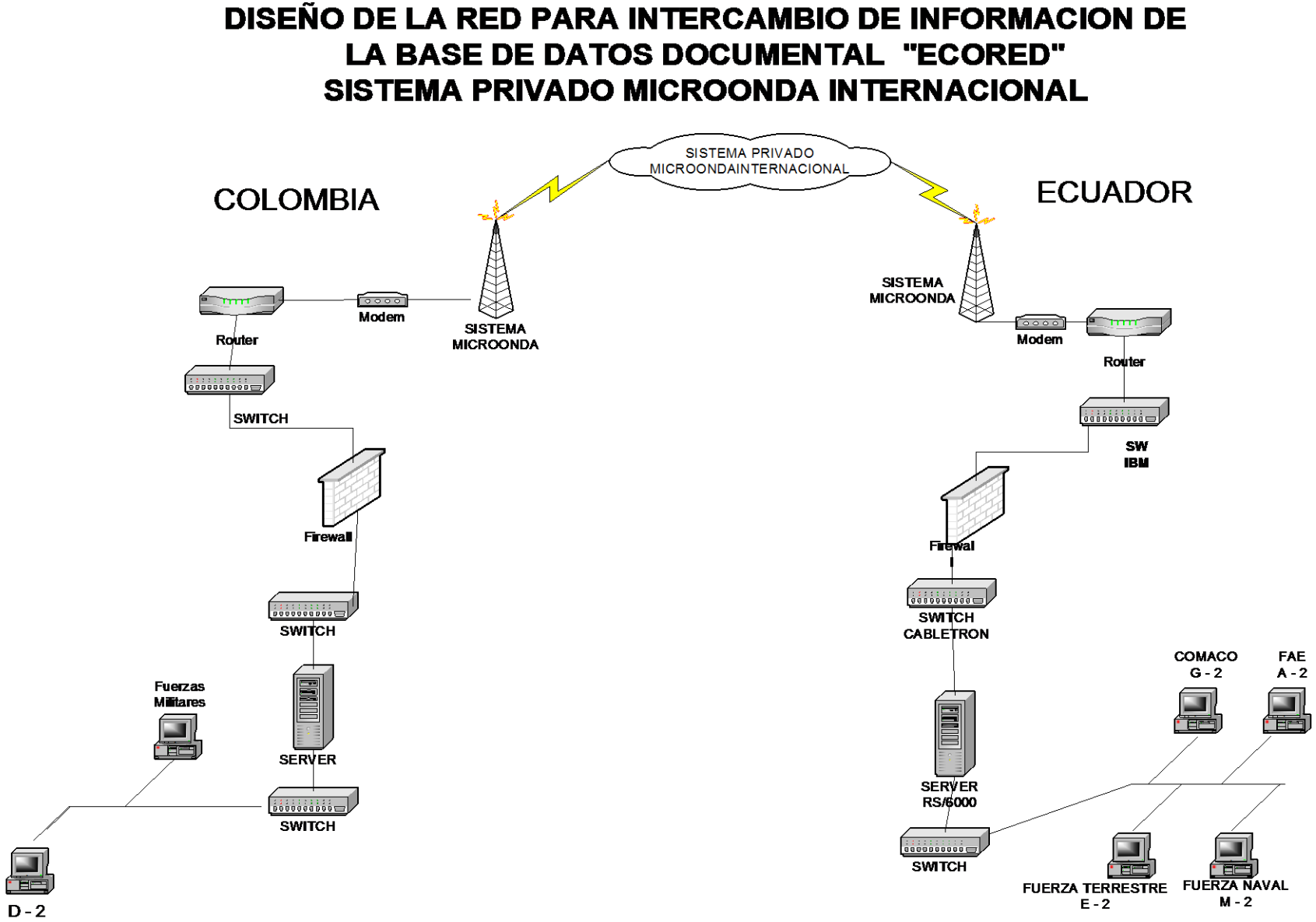


Gráfico 4:3. Comunicación por Sistema Microondas Privado Internacional

4.2 Propuesta Tecnológica

Para llevar a cabo el proyecto se instalara y se configurara el Lotus Domino Server sobre el servidor AIX, el flujo de información se realizara mediante dos métodos de comunicación utilizando el Internet, vía módem, o vía Microondas privado entre Ecuador y Colombia.

En el primer método de comunicación por el enlace dedicado del COMACO, hacia Internet, con un ancho de banda de 387Kbps, el cual nos garantiza que la conexión será mucho mas rápida, y mejorara con el segmento satelital que se obtendrá a continuación.

Para el segundo método utilizando el módem, tanto en Ecuador como en Colombia, para lo cual tenemos que configurar los servidores de Ecuador y Colombia con direcciones IP especificas para la comunicación por el módem, esto lo realizamos por seguridad, ya que cualquiera podría hacer una llamada al servidor y establecer comunicación y con esto garantizamos que la comunicación se establece solo entre direcciones IP autentificadas en el servidor AIX de Ecuador, esto se realizara en caso de que se perdiera el enlace dedicado.

Además tenemos un tercer método de comunicación que es el sistema microondas privado internacional entre Ecuador y Colombia (a realizar), que se utilizara en caso de fallar en el enlace dedicado del Ministerio de Defensa Nacional, cabe indicar que una vez que entre en funcionamiento el sistema microondas privado internacional entre Ecuador y Colombia este sistema será el que entre en funcionamiento y quedaría como segunda opción de comunicación el Internet y como tercera opción la comunicación por módem realizando llamada Internacional.

La aplicación ECORED para el plan Colombia se desarrollara en Lotus Notes. Haciendo uso de formas, vistas, guías para la interface de usuario y el lenguaje de formulas para el

desarrollo de la aplicación, y además aprovechando las seguridades propias de Lotus tanto a nivel campos, usuarios, base de datos, encriptamiento a 64 bits y al nivel de protocolos que será descrito en el *capitulo 5*.

EQUIPO	ESPECIFICACIONES
Servidor de Aplicaciones Ecuador	❑ Arquitectura abierta ❑ Tecnología RISC ❑ Procesador de 32 bits ❑ 332 Mhz. ❑ RAM 128 MB exp. 1GB ❑ Memoria cache 512 MB ❑ HD 9 GB ❑ Tape Backup 4 GB 4 mm. Expandible a 8 GB ❑ Soporte Arreglo de discos ❑ Unidad de diskette 1.44 MB compatible DOS ❑ Puertos paralelos 1 Centronics compatible (DB-25) ❑ No. De slots disponibles luego de la configuración requerida mínima 2 ❑ No. Puertos seriales mínimo 2 ❑ Controlador de disco Fast Wide SCSI-2 ❑ Tarjeta de red Ethernet/Fast Ethernet, TP (10/100) ❑ Monitor Color de alta resolución de 17" ❑ **Teclado tipo UNIX** ❑ CD-ROM de última tecnología SCSI-2, 20 X mínimo
Servidor a Aplicaciones Colombia	❑ Tecnología NT ❑ Procesador de 32 bits ❑ 333 Mhz. ❑ RAM 128 MB exp. 1GB ❑ Memoria cache 512 MB

	❑ HD 8 GB ❑ Unidad de diskette 1.44 MB compatible DOS ❑ Puertos paralelos 1 Centronics compatible (DB-25) ❑ No. De slots disponibles luego de la configuración requerida mínima 2 ❑ No. Puertos seriales mínimo 2 ❑ Tarjeta de red Ethernet/Fast Ethernet, TP (10/100) ❑ Monitor Color de alta resolución de 17" ❑ **Teclado Windows** ❑ CD-ROM de última tecnología SCSI-2, 20 X mínimo
Multimodem **USRobotics 56000**	❑ **5600 bps de velocidad** ❑ 2 entradas en línea

Tabla 4.1: Descripción de Hardware/Software

4.3 Diseño de la aplicación ECORED.

4.3.1 Metodología adoptada para el desarrollo de la aplicación

Para la aplicación ECORED se creara una base de datos, tomando como plantilla los formularios estructurados en el Anexo "C" al manual de procedimiento operativo vigente"secreto" celebrado en Ipiales.

4.3.2 Comprensión del proceso

Un proceso consiste en una secuencia de pasos necesarios para llevar a cabo un objetivo especifico tales como solicitud de compra, aprobación de solicitud. Estos procesos. Estos procesos eliminan del trabajo a elementos aleatorios, haciendo que este sea mas eficaz y resulte mas previsible, a la vez que reduce el tiempo necesario para dicho proceso que nos permitirá formar a los nuevos empleados. El flujo de trabajo describe la forma en que las personas llevan a cabo dicho proceso.

La aplicación que se desarrollara facilitara el proceso, haciendo que el trabajo resulte más sencillo y mucho mas eficiente, y sobre todo que la información tenga mas control sobre quien la genera y donde, para luego poder ser auditada.

4.3.3 Representación del proceso

Un proceso puede ser representado mediante un diagrama de flujo. En las aplicaciones en las que la información fluye entre usuarios o entre base de datos, por medio de diagrama se clarifica los elementos fundamentales del proceso.

Representar las tareas de cada fase, en vista de que la comprensión de este tipo de diagrama resulta bastante sencilla a los usuarios que manejan la información.

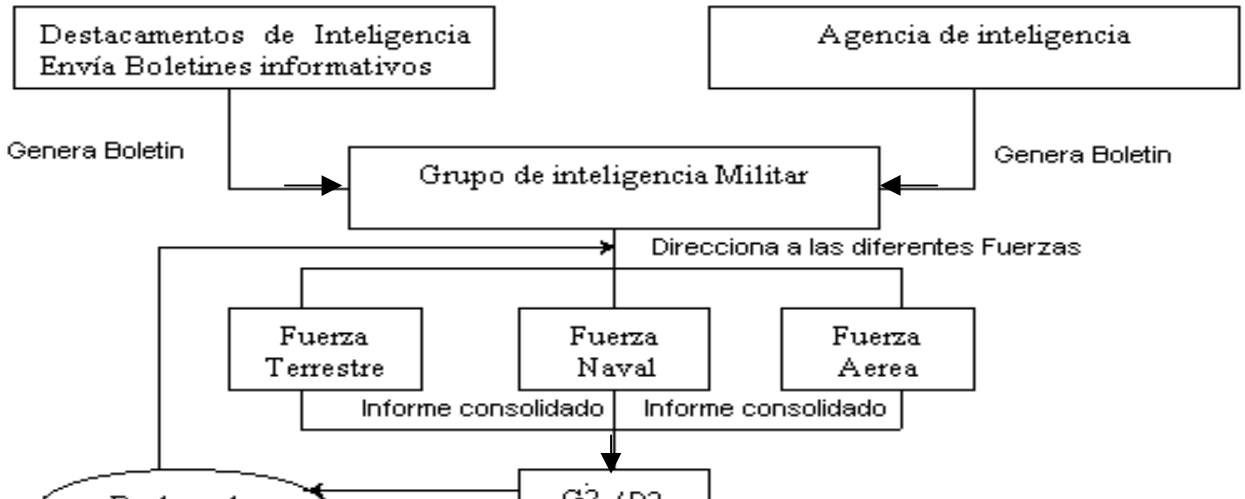


Gráfico: 4.4: Generación de Información

4.3.4 Identificación del tipo de aplicación

La comprensión de la naturaleza de la aplicación ha desarrollar normalmente pueden caracterizarse como un tipo o una combinación de varios tipos, que a continuación se muestran:

- Aplicaciones de discusiones.
- Aplicaciones de consultas.
- Aplicaciones de difusión de la información.
- Aplicaciones de seguridad.
- Aplicaciones de aprobaciones.

4.3.5 Planificación del flujo de la información

En Notes, la información puede fluir interiormente, hacia una base de datos, a través de formularios. Debe planificar la manera en que se desea que fluya la información, ya que esta decisión afectara a la forma en que habrá de diseñar los elementos individuales de la aplicación.

4.4 Presentación de formularios

4.5 Prototipo de aplicación

4.5.1 Aspectos generales

El prototipo es una valiosa herramienta para confirmar si los formularios son amigables y fáciles de llenar, para que los usuarios comprendan el flujo de la información y que todo funciona de acuerdo al procedimientos operativos vigentes.

Una vez finalizado el prototipo de la aplicación, conviene que lo revisen una selección de usuarios que probablemente serán los encargados de la operación del sistema, junto a estos usuarios procederemos a llenar datos y asegurarse de que todos comprendan el objetivo de la aplicación.

Durante la sección de revisión, los usuarios deberán ponerse de acuerdo sobre los cambios que habrán de introducirse antes de desarrollar la aplicación y de que la misma entre en fase de comprobación. Es recomendable experimentar con diseños alternativos sin tener que emplear mucho tiempo en el desarrollo.

Durante la fase del desarrollo de un prototipo, se debe tener en cuenta que si el prototipo va ha pasar ha convertirse en la aplicación final, se debe procurar diseñar de forma sistemática y amigable para el usuario.

A diferencia de otros entornos de diseño, Lotus Notes permite crear la aplicación definitiva partiendo de un prototipo, claro esta que dicho prototipo deberá contener los formularios y las vistas principales con un numero suficiente de campos o si es posible en su totalidad de los campos que interactuan en la aplicación.

4.5.2 Creación del prototipo de aplicación

Un prototipo es un modelo que nos permite acercarnos a la realidad, además es un modelo a pequeña escala que contiene los elementos del formulario que servirá para la aplicación, el

objetivo del prototipo es demostrar el flujo y el aspecto global que presentara, la presentación del prototipo no pretende ser una aplicación comprobada, depurada y totalmente operativa, por lo que no deberá emplear demasiado tiempo en la construcción del prototipo.

4.5.3 Características de la aplicación

Proyecto :	ECORED "RED PROTEGIDA DE DATOS ECUADOR – COLOMBIA"
Informático Responsable:	Egrado. Ing. Geovanni Simbaña León Egrado. Ing. Ivan Peñafiel Bastidas
Usuarios Responsables.	M2,G2,E2,G2,D2 Direcciones de Inteligencia
Procesos Relevados	Generación de Información

Tabla 4.2: Característica de la aplicación

4.5.4 Areas Involucradas

Las áreas involucradas son:

- Destacamentos de Inteligencia
- Agencia de Inteligencia
- Grupo de Inteligencia Militar
- Fuerzas Militares (FT,FN, FA, COMACO)
- D-2 del Comando General de las Fuerzas Militares Colombianas y sus Fuerzas.

4.5.5 Situación informática actual del proyecto

Actualmente el proyecto recibe la documentación clasificada vía e-mail, encriptada por medio de un software llamado PGP, el cual es desincriptado en Ecuador e impreso para ser

archivado, esta información no tiene respaldo magnético en Ecuador, es decir cuando el correo es eliminado.

4.5.6 Ingreso de Documentación

4.5.6.1 Documentación clasificada para ECORED

Los documentos de ECORED son generados por los grupos de inteligencia militar tanto de Ecuador como de Colombia y cada cual recibe información de los diferentes destacamentos de Inteligencia militar o desde las diferentes agencias de inteligencia, que son canalizadas en Ecuador, a las direcciones de inteligencia de las FF.AA. del Ecuador, esto quiere decir que la dirección de inteligencia de la FAE “A2”, Inteligencia de la Fuerza Terrestre “E2” y Inteligencia de la Marina “M2”, y luego pasan a G2 para su revisión si el resultado de la revisión es positivo se procederá al proceso de publicación, si es negado se devuelve para las diferentes correcciones; En el caso de Colombia sigue el mismo procedimiento pero con la diferencia que el departamento que revisa la información es la D2 del Comando General de las Fuerzas Militares Colombianas, para el proceso de publicación con los documentos generados en el plan Colombia.

4.5.6.2 Confidencialidad de la documentación.

Se mantiene la debida reserva sobre los documentos generados en ECORED en archivos que se guarda en seguridad externa en archivo, la persona que desee información debe obtener una autorización previa para revisarla.

4.5.6.2 Consulta de documentos.

Las diferentes unidades de inteligencia de acuerdo a su rol de creación tienen acceso a dicha información que puede ser parcial o total según el rol que desempeñe la aplicación.

4.5.7 Principales problemas que se pretenden resolver con el Sistema.

4.5.7.1 Funcionales

- La organización casi completamente manual que actualmente se lleva.
- Perdida de documentos valiosos.
- La inconveniencia que representa el manejo de documentos físicos.
- Controlamos creadores de documentos.

4.5.7.2 Técnicos

- El aprovechamiento de los recursos con que cuenta la institución.
- Falta de difusión por medios idóneos de la información que el proyecto ECORED la genera.

4.5.8 Descripción del sistema

La aplicación ECORED de la base de datos documental bajo Lotus Notes, haciendo uso de formas, vistas, guías para las interfaces de usuarios, y el lenguaje de formula para el código de la aplicación.

La aplicación en primera instancia presenta según el usuario un menú de navegación, la cual brinda una orientación clara de las opciones respectivas, con un formato de Web.

Cada una de las opciones genera un mismo formulario pero de acuerdo al tema y al código de generación que se obtiene por medio del user.id, el código de país y el código de la fuerza que la genera.

4.5.9 Volumen de datos

El volumen de datos será de acuerdo a los problemas que se susciten en la frontera, pero por lo regular se recibe y se envía un boletín semanal sobre casos de interés binacional.

4.5.10 Criterios de evaluación

Cualitativos:

- La mejora de respuesta en la realización de tareas de los encargados de procesar la información.
- Satisfacción de los usuarios.
- La forma de organización que adopten los operadores del sistema.

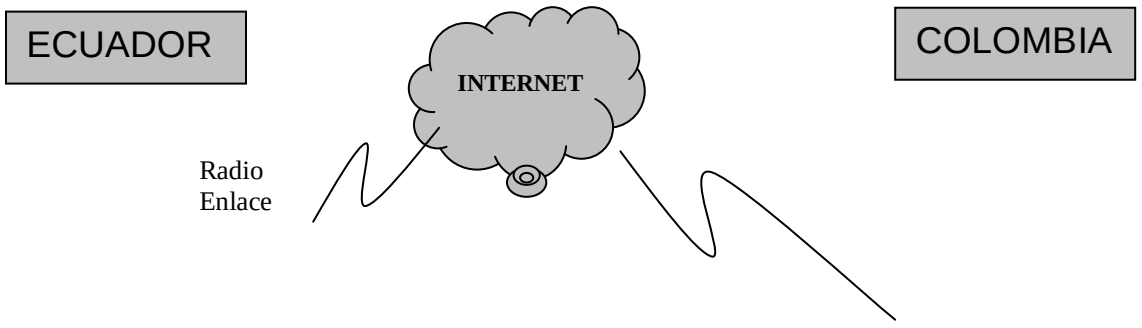
Cuantitativos

- El numero de usuario que acceden a la información.
- La mejora en tiempos de búsqueda de documentos.

4.5.11 Alcance de la aplicación

Después de cumplidas las etapas previstas de implantación, la aplicación tendrá un alcance general en cuanto a la parte cliente, es decir que cualquier persona que cuente al menos instalado el cliente de Lotus, y su user.id podrá ingresar a la aplicación, ya sea localmente o remotamente vía Internet.

4.5.12 Esquema de solución de la aplicación.



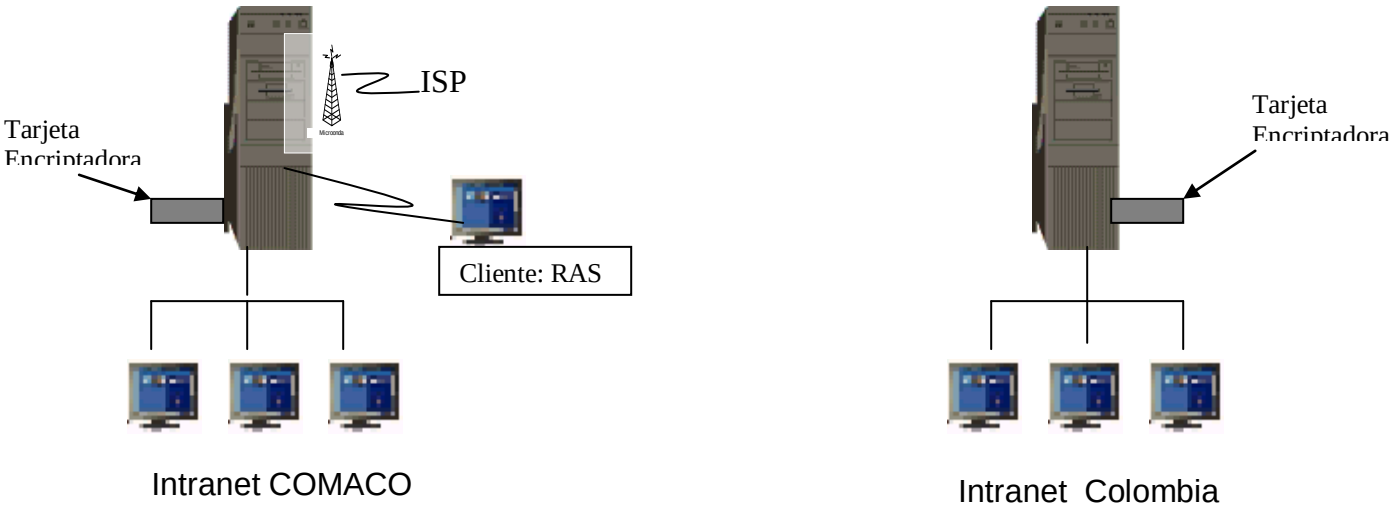


Gráfico 4.5 Esquema de solución de la aplicación

4.5.13 Control y seguridad de la aplicación.

4.5.13.1 En ambiente Lotus Notes

Para la aplicación en Lotus Notes nos presenta varios niveles de seguridad: autenticación, control de acceso, campos con niveles de seguridad y roles, restricción de Anónimos, Defaul y Encriptacion al nivel de Protocolo, que se describirán en Capitulo 5.

4.5.13.2 Control y seguridad
El control y la seguridad del proyecto esta descrita en el capitulo 5.

4.6 Desarrollo e Implementación
4.6.1 Construcción de la aplicación
La construcción de la aplicación se consigue, tomando como base el prototipo generado, con sus respectivas observaciones realizadas por los usuarios y de esto tenemos los siguientes resultados.

El sistema de ingreso de información ECORED consta de dos tipos de ingreso y visualización

de información, tanto para administrador y para usuario.

1. **Administrador**

2. **Usuarios**

4.6.1.1 Administrador

El menú para el administrador podrá encontrar un menú de opciones amplio en el cual consta de una opción de ingreso de nuevos formularios, consultas.

Dentro de la administración tenemos que revisar el correo que nos indicara si se suscitó un nuevo incidente para lo cual procedemos ha abrir nuestro correo de administrador lo revisamos y tenemos un documento anexado, que con un clic procedemos ha abrirlo y corregirlo donde como administrador tenemos iconos que permiten mandar a corregir los documentos, cuando no este de acuerdo con la información o si llegasen a faltar datos, y si esta todo correcto procedemos ha aprobar y por cuanto se publica y se autoriza la replica entre los servidores.

4.6.1.2 Usuarios

Para los Usuarios se implemento una estructura idéntica de ingreso de información lo que sí tiene modificaciones en la parte de consultas ya que esta tiene solo consultas por tipo de casos que esta unidad o usuario que la genero, cabe destacar que no puede consultar información de otros usuarios o dependencias ni consultas generales de la base de datos pues estos permisos solo los tiene el administrador.

Además ya una ves generado un documento cuando procedemos a guardar implícitamente se envía un correo a el administrador para que corrija el documento y lo publique.

4.6.2. Diccionario de Datos

BASE DE DATOS

BASE DE DATOS:	**Ecuador_colombia_ecored.nsf**
UBICACIÓN:	**/notes/data:**
DESCRIPCION:	**Almacenamiento de información sobre los casos generados en el plan Colombia**

FORMULARIOS

Formulario	**Formulario_ecored**

Tipo:	**Documento**
Descripcion:	**Formulario principal**

BASE DE DATOS

BASE DE DATOS:	**Ecuador_colombia_ecored.nsf**
UBICACIÓN:	**/notes/data:**
DESCRIPCION:	**Almacenamiento de información sobre los casos generados en el plan Colombia**

FORMULARIO

Formulario	**Formulario_ecored**
Tipo:	**Documento**
Descripcion:	**Formulario principal**

CAMPO	TIPO	DESCRIPCION	FORMULA
paisorigen_elaboracion	Texto, Calculado	Nombre del país que origino el reporte	"ECUADOR"
cod_doc	Texto, Calculado al crear	Código de documento generado.	aa = aa + 1;@If(paisorigen_elaboracion = "COLOMBIA");"EC" + "/" + @Name([CN]; @UserName) + "/" + aa;"CO" + "/" + @Name([CN]; @UserName) + "/" + (aa);
dependencia_elaboracion	Palabras clave, Editable	Dependencia que elaboro el informe COMACO FAE MARINA FUERZA TERRESTRE D – 2	@Name([OU2]; dependencia_elaboracion);
elaborado_elaboracion	Nombres, Calculado	Persona responsable de realizar el informe	@UserName
fecha_elaboracion	Fecha/Hora Calculado	Fecha de elaboración de informe	@Today
hora_elaboracion	Fecha/Hora Calculado	Hora de la elaboración del informe	@Now
asunto_elaboracion_1	Palabras clave Editable	Asunto del caso generado Aspecto Subersivo Narcotrafico Trafico de Armas Municiones Explosivos	

caso_elaboracion	Palabras clave Editable	El tipo de caso que suscitó la creación del documento	@If(caso_elaboracion = "");@Failure("Este Campo no puede estar Vacio por favor ingrese datos ");@Success;@ProperCase(caso_elaboracion);
latitud	Texto, Editable	Posición según latitud	@IsNumber(latitud);
resumen_elaboracion	Texto enriquecido Editable	Resumen del caso	
hora_hechos	Fecha/Hora Editable	Hora que se suscito los echos	@Now
fecha_hechos	Fecha/Hora Editable	Fecha que se suscito los echos	@Today
pais_hechos	Palabras clave Editable	País donde se suscito los echos: Colombia Ecuador	
lugar_hechos	Texto, Editable	Lugar aproximado donde se suscito los echos	
COLOMBIA_1	Sección, Editable	Datos de Colombia	
c_ciudad_hechos_ecuador	Texto, Editable	Datos de Ecuador	
c_prov_hechos_ecuador	Texto, Editable	Provincia donde se generaron los echos en Ecuador	
c_parroq_hechos_ecuador	Texto, Editable	Parroquia donde se generaron los echos en Ecuador	
c_conton_hechos_ecuador	Texto, Editable	Cantón donde se generaron los echos en Ecuador	
COLOMBIA	Sección, Editable	Datos de Colombia	
c_ciudad_hechos	Texto, Editable	Ciudad donde se generaron los echos en Colombia	
c_municipio_hechos	Texto, Editable	Municipio donde se generaron los echos en Colombia	
c_corregimiento_hechos	Texto, Editable	corregimiento donde se generaron los echos en Colombia	
c_sitio_hechos	Texto, Editable	Sitio aproximado donde se ha generado los echos	
id_traf_arm	Texto, Editable		
Nacionalidad_traf_arm	Palabras clave Editable	Origen de donde se origino el trafico. Ecuador Colombia	

foto_traf_arm	Texto enriquecido Editable	Foto del armamento encontrado en la operación	
descripcion_traf_arm	Texto, Editable	Breve descripción del trafico de las armas incautadas	
tipo_armas	Palabras clave, Editable	Tipo de armas incautadas un pequeño detalle.	
calibre_armas	Palabras clave, Editable	Calibre de las armas incautadas.	
numero_serie_armas	Texto, Editable	Numero de serie de las armas incautadas en la opracion	
capacidad_proveedor_armas	Texto, Editable	Descripcion de la capacidad del proveedor de las armas.	
cantidad_armas	Texto, Editable	Numero de armas incautadas en la operación	
marcas_armas	Palabras clave Editable	Detalle de la marca de las armas incautadas	
modelos_armas	Palabras clave Editable	Detalle del modelo de las armaras incautadas.	
pais_fabricante_armas	Palabras clave Editable	Nombre del país fabricante del armamento	
estado_armas	Texto, Editable	El estado en el que se encuentran las armas.	
tipo_municion	Palabras clave Editable	Detalle del tipo de munición que se encontro.	
cantidad_municion	Texto, Editable	Numero de cantidad del armamento que se incauto.	
estado_municion	Texto, Editable	Estado en el que se encuentra la munición.	
marca_municion	Palabras clave Editable	Marca de la munición o municiones.	
pais_fabricante_municion	Palabras clave Editable	Nombre del país fabricante de la munición.	
Calibre	Palabras clave Editable	Detalle del calibre de la munición.	
cantidad_explosivos	Texto, Editable	Cantidad de explosivos encontrados en el operativo.	
tipoclase_explosivos	Palabras clave Editable	Que clase de explosivos fueron hallados.	
detonadores_explosivos	Texto, Editable	Detalle de que tipo de detonadores se incuatron.	
calibre_municion	Palabras clave Editable	Detalle del calibre de la munición incautada.	

varios_municion	Texto, Editable	Detalle extra de municione encontradas items que no contemple el formulario.	
marcas_municion	Palabras clave Editable	Nombres de las marcas de munición que se incauto.	
pais_fabricante_explosivos	Palabras clave Editable	Nombre del país que fabrico los explosivos.	
mechas_explosivos	Texto, Editable	Detalle de las mecha decomisadas en el operativo.	
estopines_explosivos	Texto, Editable	Detalle de los estopines incautados	
lotes_explosivos	Texto, Editable	Número de lotes encontrados en la operación.	
lugar_adquisiscion	Texto, Editable	Lugar en el que se realizo el apresamiento.	
cantidad_adquisiscion	Texto, Editable	Cantidad que se decomiso.	
vendedores_adquisiscion	Texto, Editable	Nombre de los vendedores y quienes adquirieron el material.	
fecha_adquisiscion	Fecha/Hora Editable	Fecha en la que se realizo la incautación.	@Now
comprador_adquisiscion	Texto, Editable	Nombre del comprador del botín.	
sumas_pagadas_adquisiscion	Números, Editable	Cantidad de dinero que se incauto en la operación.	
fecha_embarque	Fecha/Hora Editable	Fecha en la que se realizo el embarque de las municiones.	@Now
hora_embarque	Fecha/Hora Editable	La hora en la que serealizo el embarque de las municiones.	@Now
medios_embarque	Texto, Editable	Medios empleados para realizar el embarque.	
lugar_embarque	Texto, Editable	Lugar en que se realizo el embarque de las municiones.	
metodos_embarque	Texto, Editable	Metodos empleados para realizar el embarque.	
personas_invol__embarque	Texto, Editable	Personas que se encuentran involucradas en el embarque.	
fecha_desembarque	Fecha/Hora Editable	Fecha en la que se realizo el desembarque.	@Now
hora_desembarque	Fecha/Hora Editable	Hora en la que se realizo el desembarque.	@Now

medios__desembarque	Texto, Editable	Medios empleados en el desembarque.	
lugar_desembarque	Texto, Editable	Lugar en la que se realizo el desmbarque.	
metodos_desembarque	Texto, Editable	Metodos empleados en el desembarque.	
perosnas_invol_desembarque	Texto, Editable	Personal involucrado en el desembarque del material incautado.	
otros_medios	Texto enriquecido Editable	Otros medios adicionales que se emplearon para el desembarque.	
idgrupo_subver	Texto, Editable	Identificación del grupo subversivo.	
composicion_subver	Texto, Editable	Composición del grupo suvbersivo.	
dispos_subver	Texto, Editable	Dispositivo empleado en el arresto al grupo subversivo.	
fuerza_subver	Texto, Editable	Nombre de la fuerza subversiva.	
terreno_subver	Texto, Editable	Descripción del terreno en el que se encontraban acentado el grupo guerrillero.	
contacto_subv	Texto, Editable	Nombre de la persona con la que se hizo el contacto.	
toma_poblac_subv	Texto, Editable	Detalle si hubo toma de población.	
emboscada_tropas_subv	Texto, Editable	Detalles de la emboscada a las tropas subversivas.	
per_secuest_subv	Texto, Editable	Nombre de las personas secuestradas por el grupo guerrillero.	
emboscada_propias_subv	Texto, Editable	Detalle si hubo infiltraciones en propias tropas.	
bajas_enemi_subv	Texto, Editable	Detalle del numero de bajas enemigas.	
hostigamiento_subv	Texto, Editable		
armas_rec_subv	Texto, Editable		
atentados_terroritas_subv	Texto, Editable	Detalle del atentado terrorista.	
idper_narco	Texto, Editable	Identificación de los narcotraficantes.	
nacionper_narco	Texto, Editable	Nacionalidad de las personas detenidas	
fotoper_narco	Texto enriquecido Editable	Fotografia de las personas detenidas en el operativo.	

descrper_narco	Texto, Editable	Descripción de las personas apresadas.	
fotografia_insumo_narco	Texto enriquecido Editable	Fotografia de los insumos incautados en la operación.	
nombre_narco_insumo	Texto, Editable	Nombre de los insumos incautados.	
marca_insumo_narco	Texto, Editable	Marca de los insumos incautados.	
cantidad_insumo_narco	Texto, Editable	Cantidad de insumos incautados.	
recipiente_insumo_narco	Texto, Editable	Detalle del material que utilizaban los narcotraficantes para el almacenamiento.	
lugar_embar_narco	Texto, Editable	Lugar en donde se realizo el embarque narcotráfico.	
fecha_embar_narco	Texto, Editable	Fecha del embarque de los narcóticos.	
metodosutiliz_embar_narco	Texto, Editable	Métodos utilizados en el embarque.	
medios_empleados_embar_narco	Texto, Editable	Medios empleados en el embarque.	
lugar_desem_narco	Texto, Editable	Lugar de desembarque.	
fecha_desem_narco	Texto, Editable	Fecha de desembarque de narcotráfico.	
medios_desem_narco	Texto, Editable	Medios empleados para el desembarque.	
sumas_pagadas_procedencia_narco	Texto, Editable	Cantidad incautada en la operación.	
tipo_vehiculo_narco	Texto, Editable	Detalle del tipo de vehículo decomisados en el operativo.	
terreno_area_narco	Texto, Editable	Detalle del terreno para el despegue de aeronaves.	
actividad_area_narco	Texto, Editable	Frecuencia con la que se realizan vuelos narcos.	
contacto_narco	Texto, Editable	Nombre de la persona con la que se hizo el contacto.	
bajas_enemigas_narco	Texto, Editable	Detalle del número de bajas enemigas.	
toma_poblacion_narco	Texto, Editable	Detalle de poblaciones tomadas por los narcotraficantes.	
atentado_terrorista_narco	Texto, Editable		
foto_aeronave	Texto, Editable	Fotografía de o las aeronaves	

		incautadas.	
matricula_aeronave	Texto, Editable	Numero de matricula de la aeronave.	
clasificacion_aeronave	Texto, Editable	Clasificación de la aeronave incautada.	
fuselaje_aeronave	Texto, Editable	Detalle del fuselaje de la aeronave.	
color_aeronave	Texto, Editable	Color de la aeronave incautada.	
posicion_planos_aeronave	Texto, Editable	Detalle del posicionamiento de los planos de la aeronave.	
propulsion_aeronave	Texto, Editable	Tipo de propulsión de la aeronave.	
tren_aterrisaje_aeronave	Texto, Editable	Detalle del tren de aterrisaje de la aeronave.	
numero_serie_aeronave	Texto, Editable	Detalle de la matricula de la aeronave.	
otras_caracteristicas_aeronave	Texto, Editable	Detalles extras de la aeronave que nos ayudan para la identificación de la aeronave incautada.	
bandera_aeronave	Palabras clave Editable	Nombre de la bandera o país de fabricación de la aeronave.	
actividad_aeronave	Texto, Editable	Activiadad a la que se dedicaba la eronave.	
logitud_aeronave	Texto, Editable	Longitud en metros de la aeronave.	
velocidad_maxima_aeronave	Texto, Editable	Detalle de la velocidad maxima a la que la aeronave puede volar.	
pontecia_aeronave	Texto, Editable	Potencia maxima a la que puede llegar la aeronave.	
capacidad_pasajeros_aeronave	Texto, Editable	Capacidad de pasajeros que puede llevar.	
comunicacion_aeronave	Texto, Editable	Tipo de dispositivos de comunicación con la que cuenta la aeronave.	
tipo_vh_t	Texto, Editable	Descripción del tipo de vehículo terrestre incautado.	
modelo_vh_t	Texto, Editable	Modelo del vehículo incautado.	
marca_vh_t	Texto, Editable	Marca del vehículo.	
año_vh_t	Texto, Editable	Año de fabricación del vehículo.	
localidad_matricula_vh_t	Texto, Editable	Localidad en la que el vehículo fue matriculado.	
color_carroceria_vh_t	Texto, Editable	Color de la carrocería del	

		vehículo.	
matricula_vh_t	Texto, Editable	Detalle de la matricula del vehículo.	
nacionalidad_vh_t	Palabras clave Editable	Identificación del país de origen del vehículo.	
numero_chacis_vh_t	Texto, Editable	Numero del Chasis del vehículo.	
numero_motor_chasis	Texto, Editable	Numero del Motor del vehículo.	
actividad_realiza_vh_t	Texto, Editable	Actividad que estaba realizando el vehículo en momento de la detención.	
otras_carroceria	Texto, Editable	Detalle de otras caracatersiticas de la carrocería del vehículo.	
foto_dueño_trans_terres	Texto enriquesido Editable	Foto del dueño del transporte o del chofer.	
nombre_dueño_trans_terres	Texto, Editable	Nombre del dueño del transporte	
iddueño_trans_terres	Texto, Editable	Identificación del dueño del trasmporte cedula de identidad i pasaporte etc.	
nacionalidad_dueño_trans_terres	Palabras clave Editable	Nacionalidad del dueño del transporte.	
motivo_detencion_vh_t	Texto, Editable	Motivo por el cual fue detenido el vehículo.	
lugar_detencion_vh_t	Texto, Editable	Detalle del lugar en el que fue detenido el transporte.	
fecha_detencion_vh_t	Texto, Editable	Fecha en la que fue detenido el documento.	
fund_legal_detencion_vh_t	Texto, Editable	Fundamento legal para la detención.	
activ_desemp__trans_terres	Texto, Editable	Actividad que se dedica el transporte en el momento de la detención.	
domicilio_trans_terres	Texto, Editable	Identificación del domicilio del detenido.	
responsable_operacion_vh_t	Texto, Editable	Nombre de la persona responsable de la operación.	
numero_detenidos_vh_t	Texto, Editable	Numero de personas detenidas en el transporte.	
material_incautado_vh_t	Texto, Editable	Detalle de material incautado en el vehículo.	
antecedentes__vh_t	Texto, Editable	Antecedentes anteriores del vehículo detenido.	
rutas_utilizadas_vh_t	Texto, Editable	Detalle de las rutas utilizadas por el vehículo incautado.	

sitios_frecuentes_vh_t	Texto, Editable	Sitios a los que frecuentaba el vehículo.	
frecuencia_visita_vh_t	Texto, Editable	Frecuencia con la que el vehículo visitaba determinado lugar.	
contactos_sitio_vh_t	Texto, Editable	Detalle de los contactos con los cuales el chofer tenia en el lugar.	
nombre_vehiculo	Texto, Editable	Nombre con el cual se le identifica el vehículo en el lugar.	
matricula_vehiculo_fluvial	Texto, Editable	Numero de matricula del vehículo fluvial.	
puerto_registro_vehiculo_fluvial	Texto, Editable	Nombre del puerto en el que ancla el vehículo.	
bandera_vehiculo_fluvial	Palabras clave Editable	Nombre de nacionalidad del vehículo.	
tip_embarcacion_vehiculo_fluvial	Texto, Editable	Tipo de embarcación que fue incautada.	
act_desarrolla_vehiculo_fluvial	Texto, Editable	Actividad que realiza el vehículo fluvial.	
tonelage_vehiculo_fluvial	Texto, Editable	Detalle de la capacidad de carga del vehículo fluvial.	
casco_vehiculo_fluvial	Texto, Editable	Detalle del casco del vehículo fluvial.	
materiales_vehiculo_fluvial	Texto, Editable	Tipo de material que se incauto en el vehículo.	
estructura_vehiculo_fluvial	Texto, Editable	Tipo de estructuta con la cual esta confecionado el transporte.	
propulsion_vehiculo_fluvial	Texto, Editable	Tipo de propulsión que utiliza el transporte para movilizarse.	
rutas_vehiculo_fluvial	Texto, Editable	Ruta por al cual se desplaza frecuente mente el transporte.	
frec_visita_vehiculo_fluvial	Texto, Editable	Frecuencia con la que el vehículo llega al mismo puerto.	
estado	Texto, Editable	Estado en el cual se encuentra el transporte.	

ACCIONES:

ACCION	DESCRIPCION	FORMULA

Guardar	Acción que nos permite guardar un documento en la base de datos.	revisor := @DbLookup("" : "NoCache"; @DbName; "parametros"; "revisor"; "revisor");FIELD estado := "En Trámite";REM "Defino quien tiene que revisar el documento";FIELD revisor_actual := revisor;@MailSend(revisor; ""; ""; "Nuevo Incidente"; "Se a iniciado un nuevo incidente"; ""; [IncludeDoclink]);@PostedCommand([FileSave]);REM "@PostedCommand([FileCloseWindow])";
Nuevo	Acción que nos permite hacer un nuevo documento según sea el caso.	@IsNewDoc
Enviar_Documento_Corregir	Acción que permite al supervisor enviar un email a la persona que creo el documento para que corrija el documento en mensión.	REM "Estado Correguir";FIELD estado := "Correguir";REM "Defino quien tiene que revisar el documento";FIELD revisor_actual := elaborado_elaboracion;REM "Envío correo de notificación de corrección";@MailSend(elaborado_elaboracion; ""; ""; "Correguir Incidente"; "Se necesita correguir el inciente"; ""; [IncludeDoclink]);REM "Grabo y cierro ";REM "@PostedCommand([FileCloseWindow]);";@PostedCommand([FileSave]);"";
Editar Documento	Acción que nos permite realizar modificaciones a un documento que se desea realizar cambios.	@Command([EditDocument]; "1");
Salir de la Aplicación	Acción que nos permite salir de la aplicación si esta editando un nuevo documento le pregunta si desea guardarlo.	@Command([FileCloseWindow]);

VISTAS

Vista:	Enero
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos

	creados en el mes de Enero
Criterio de Selección:	SELECT @Created >= [01/01/2001] & @Created <= [31/01/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Febrero
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Febrero
Criterio de Selección:	SELECT @Created >= [01/02/2001] & @Created <= [28/02/2001]!&[29/02/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Marzo
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Marzo
Criterio de Selección:	SELECT @Created >= [01/03/2001] & @Created <=

	[31/03/2001];

Columna	Formula	Descripción
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Abril
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Abril
Criterio de Selección:	SELECT @Created >= [01/04/2001] & @Created <= [30/04/2001];

Columna	Formula	Descripción
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Mayo
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Mayo
Criterio de Selección:	SELECT @Created >= [01/05/2001] & @Created <= [31/05/2001];

Columna	Formula	Descripción
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Junio
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Junio
Criterio de Selección:	SELECT @Created >= [01/06/2001] & @Created <= [30/06/2001];

Columna	Formula	Descripción
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Julio
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Julio

Criterio de Selección:	SELECT @Created >= [01/07/2001] & @Created <= [31/07/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Agosto
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Agosto
Criterio de Selección:	SELECT @Created >= [01/08/2001] & @Created <= [31/08/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Septiembre
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Septiembre
Criterio de Selección:	SELECT @Created >= [01/09/2001] & @Created <= [30/09/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Octubre
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Octubre
Criterio de Selección:	SELECT @Created >= [01/10/2001] & @Created <= [31/10/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Noviembre
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Noviembre
Criterio de Selección:	SELECT @Created >= [01/11/2001] & @Created <= [30/11/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Diciembre
Tipo:	Estándar
Descripción:	Vista que presenta un reporte de todos los documentos creados en el mes de Diciembre
Criterio de Selección:	SELECT @Created >= [01/12/2001] & @Created <= [31/12/2001];

Columna	**Formula**	**Descripción**
País:	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Suceso:	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.

Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Armamento.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en el trafico de armas municiones y explosivos.
Criterio de Selección:	SELECT asunto_elaboracion_1="Trafico de Armas Municiones Explosivos"

Columna	**Formula**	**Descripción**
Trafico de Armas Municiones y Explosivos	Asunto_elaboracion1	El nombre del país en donde se realizaron los hechos.
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos

Vista:	Colombia.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Colombia sobre cualquier caso.
Criterio de Selección:	SELECT paisorigen_elaboracion="COLOMBIA"

Columna	**Formula**	**Descripción**
País	Paisorigen_elaboracion	El nombre del país en donde se realizaron los

		hechos.
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Ecuador.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Colombia sobre cualquier caso.
Criterio de Selección:	SELECT paisorigen_elaboracion="ECUADOR"

Columna	**Formula**	**Descripción**
País	Paisorigen_elaboracion	El nombre del país en donde se realizaron los hechos.
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Dependencia:	Dependencia_elaboración	Dependencia que elaboro el informe.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	COMACO.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Ecuador en la dependencia del Comaco.
Criterio de Selección:	SELECT dependencia_elaboracion="COMACO"

Columna	Formula	Descripción
Dependencia	dependencia_elaboracion	Dependencia que elaboro el informe.
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	FAE.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Ecuador en la dependencia de la Fae.
Criterio de Selección:	SELECT dependencia_elaboracion="FAE"

Columna	Formula	Descripción
Dependencia	dependencia_elaboracion	Dependencia que elaboro el informe.
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Fuerza Terrestre.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Ecuador en la dependencia de la Fuerza Terrestre.
Criterio de Selección:	SELECT dependencia_elaboracion="FUERZA TERRESTRE"

Columna	Formula	Descripción
Dependencia	dependencia_elaboracion	Dependencia que elaboro

		el informe.
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	MARINA.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Ecuador en la dependencia de LA Marina.
Criterio de Selección:	SELECT dependencia_elaboracion="MARINA"

Columna	**Formula**	**Descripción**
Dependencia	dependencia_elaboracion	Dependencia que elaboro el informe.
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.

Vista:	Narcotrafico.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Ecuador en el ámbito de Narcotráfico.
Criterio de Selección:	SELECT asunto_elaboracion_1="Narcotrafico"

Columna	**Formula**	**Descripción**
Narcotrafico.	Asunto_elaboracion1	Tipo de caso al que se hacer referencia
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Fecha:	Fecha_hechos	Fecha en la que

		sucedieron los acontecimientos.
Dependencia	Dependencia_elaboracion	Dependencia que elaboro el Informe.

Vista:	Secuestro.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Ecuador en el ámbito de Secuestro
Criterio de Selección:	SELECT asunto_elaboracion_1="Secuestro"

Columna	**Formula**	**Descripción**
Secuestro	Asunto_elaboracion1	Tipo de caso al que se hacer referencia
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.
Dependencia	Dependencia_elaboracion	Dependencia que elaboro el Informe.

Vista:	Terrorismo.
Tipo:	Estándar
Descripción:	Vista en la que se presenta los documentos creados en Ecuador en el ámbito de Terrorismo.
Criterio de Selección:	SELECT asunto_elaboracion_1="Terrorismo"

Columna	**Formula**	**Descripción**
Terrorismo.	Asunto_elaboracion1	Tipo de caso al que se hacer referencia
Nombre del Caso	caso_elaboración	Nombre del caso que al que hace referencia.
Fecha:	Fecha_hechos	Fecha en la que sucedieron los acontecimientos.
Dependencia	Dependencia_elaboracion	Dependencia que elaboro el Informe.

4.6.3 Presentación de la Aplicación
Se presenta una descripción gráfica de los formularios, vistas, agentes y las opciones de

cómo utilizar cada una de ellas, en el *Anexo B*

4.6.4 Implementación y configuración del Hardware

4.6.4.1 Servidor RS6000

Para la configuración de los servidores se ha seguido los estándares recomendados por el fabricante en vista que el Lotus Notes tiene como plataforma primaria el AIX.

4.6.4.2 Windows NT

Se configuro este servidor para que se alojé el otro dominio de la aplicación.

4.6.4.3 Lotus Notes Server

Para su implementación y configuración del Lotus Domino Server se ha seguido los estándares recomendados por el fabricante, Además se configuro otro servidor con diferente dominio, para que se ejecute cuando se inicializa el servidor de Notes Domino.

4.6.4.4 Validación y análisis de resultados

La información ingresada por los usuarios responsables de las fuerzas COMACO, FUERZA TERRESTRE, FAE, MARINA y otras unidades que se incrementen de acuerdo a las necesidades que a futuro se presenten, esta información se mantendrá durante 6 meses luego de lo cual se sacara un backup de la base de datos con dispositivos propios de la institución cuyo volumen alcanza 8 gigas para luego de esto ser encerrada la base de datos y comenzar nuevamente con el proceso de ingreso de información e intercambio de la misma.
Los accesos de usuarios a esta información esta estimada en un promedio de 100 documentos consultados mensualmente.

4.6.4.4 Usuarios responsable de la información
Los usuarios responsables del manejo de la información serán como anteriormente se especifico las diferentes unidades de Inteligencia.

4.6.4.4 Usuarios finales
Los usuarios finales serán los Directores de Inteligencia de las diferentes fuerzas, además del Director de Inteligencia del Comando Conjunto de las Fuerzas Armadas, que dispondrán de toda la información que se maneje a lo largo del desarrollo del denominado Plan Colombia.

CAPITULO 5

NORMAS Y PROCEDIMIENTOS DE SEGURIDAD PARA “ECORED”

5.1 SEGURIDAD EN ECORED.

5.1.1 Seguridad Administrativa

los Departamentos que están a cargo del manejo y utilización de la información son: A2, E2, M2, G2, D-2 con sus respectivas fuerzas, con sus respectivos responsables del manejo de la información calificada que se generara en Plan Colombia.

- **A2**: Departamento de Inteligencia de la Fuerza Aérea Ecuatoriana FAE
- **E2**: Departamento de Inteligencia de la Fuerza Terrestre Ecuatoriana F.T.
- **M2**: Departamento de Inteligencia de la Fuerza Naval del Ecuador F.N.
- **G2**: Departamento de Inteligencia del Comando Conjunto de las Fuerzas Armadas COMACO
- **D-2**: Del Comando General de las Fuerzas Militares de Colombia

Los usuarios de ECORED, son personas idóneas, especialistas y con experiencia en manejo de información calificada, los mismos que son los responsables del manejo y custodia de la información, dentro y fuera de las Direcciones de Inteligencia de las Fuerzas Armadas, y están prohibidos de sacar datos para divulgarlos.

El flujo y manipulación de la información en una red, obligatoriamente es controlada y supervisada por el Administrador de la Base de Datos, quién es el encargado del control técnico y lógico de la red.

El proceso de la documentación calificada en un Sistema de Información Computacional, corre el peligro de que llegue a conocimiento del enemigo, pese a las medidas adoptadas, lo cual obliga a tomar otras medidas como: concientizar al personal de la importancia que significa su aporte responsable y desinteresado a la función que desempeña. Impartición de charlas, seminarios y conferencias de seguridad computacional. Adquisición de tecnología de punta y capacitación del personal en este campo.

Representa un riesgo para la seguridad institucional nacional e internacional, la divulgación no autorizada, pérdida, o robo de la documentación, especialmente la calificada; por lo que, su procesamiento es de permanente control y supervisión de los diferentes estamentos de seguridad del las FF.AA.EE y a la del Comando General de las Fuerzas Militares de Colombia.

La tecnología avanzada, ha dado lugar para que toda información se procese a través de un computador, cuyos resultados son almacenados en archivos magnéticos (discos duros, disquetes, CDS, Cintas magnéticas) de fácil transporte sin autorización, lo que representa mayor riesgo su preservación; sin embargo que el principio de seguridad, esta normada en el Reglamento de Seguridad RT-3-IV en vigencia.

5.1.2 Seguridad Física

Conjunto de medidas que se adoptan orientadas a impedir el acceso a personas no autorizadas a las instalaciones de un Centro Informático, a fin de preservar la integridad física de los medios disponibles.

Los recursos de la G2 en el departamento de la Sección Técnica son protegidos, especialmente restringiendo el acceso a sus instalaciones

físicas, mediante medidas de control flexibles que son planificadas, ejecutadas y supervisadas permanentemente por el Oficial de Seguridad; por lo tanto, de éste depende el lograr un nivel de control y protección de los recursos con rigidez, aprovechando la tecnología de punta contemporánea utilizando varias formas de seguridad, como son: sistema de vigilancia por medio de circuito cerrado de televisión, censores, set de monitoreo, etc.

La Sección Técnica es una instalación cerrada con conexiones eléctricas especiales de alto poder y a tierra, se dispone de un interruptor principal para que en casos de emergencias, se desconecte inmediatamente el circuito de la red; además existen controladores físicos como el acumulador de energía (UPS), capaz de conservar la energía en todos las computadoras de la red por un determinado tiempo, cuando se suprima la corriente eléctrica, a fin de que los operadores graben la información procesada, evitando pérdidas de tiempo y recursos.

Con el fin de garantizar el normal funcionamiento de los equipos en red, cada computador dispone de un estabilizador de voltaje y sus conexiones eléctricas a tierra.

Las instalaciones y Sistemas de Información, están expuestos a robos, asaltos, toma de instalaciones, terremotos, incendios, etc. Para contrarrestar estos riegos en el ámbito militar, existe los diferentes Planes de Seguridad que están a cargo del Oficial de Seguridad, quién requiere periódicamente la actualización de los mismos y realiza simulacros con el personal.

5.1.3 Seguridad Computacional o Lógica

Conjunto de medidas que se adoptan, orientadas a impedir a personas no autorizadas el acceso a las redes informáticas y traten de manipular la información con propósitos ilícitos, así como la utilización discriminada del Software disponible.

Las computadoras son instrumentos que permiten procesar y almacenar gran cantidad de información, tanto en el disco duro como en dispositivos magnéticos de memoria virtual como disquetes, cintas, CDS, etc., presentando facilidades de copiar, adulterar, borrar en pocos segundos; por lo que, los Operadores están autorizados en sus computadoras (terminales), solamente del procesamiento de la información recibida del Servidor y luego de sacar los resultados, borrar de la memoria o del disco duro, especialmente la información calificada, a fin de evitar la fuga de información.

Los diferentes procedimientos de preservación de la información dentro de los dispositivos magnéticos, son controlados por el Administrador de la Base de Datos, tomando en consideración “LA NECESIDAD DEL SABER” y con medidas como:

- Utilización de la información, mediante los niveles de acceso desde el Escalón Superior hasta el último usuario, existiendo restricciones para el uso de determinada información, dependiendo del campo o factor dentro de un Departamento o Sección. El Comandante esta facultado a disponer de toda la información sin modificarla.

- Para cada Operador está asignado claves de acceso, del usuario o PASSWORD y de operación o LOGIN, la primera se utiliza para el encendido inicial de la computadora y la

segunda para tener acceso a la red. Las claves son individuales y cambiadas constantemente por el Oficial de Seguridad.

- La clave además puede ser cambiada automáticamente tomando en cuenta fechas de caducidad, para dicho usuario.

- Programas de mantenimiento de las computadoras: Instalación o configuración de Software actualizado, escánear (scandisk), desinfección (antivirus), etc. Cuando se trata de fallas técnicas, las respectivas coordinaciones con las casas comerciales proveedoras, mientras dure la garantía.

Para cada usuario está asignado claves de acceso, del usuario o PASSWORD y de operación o LOGIN, la primera se utiliza para el encendido inicial de la computadora y la segunda para tener acceso a la red.

Los Programas de Gestión y la Base de Datos, están almacenados en el Servidor, desde donde los Operadores capturarán la información que le compete, respetando los niveles de acceso y autorizaciones del Administrador de Datos. Estos Programas de Gestión, serán actualizados conforme a la tecnología avanzada y dure el proyecto ECORED.

Todo usuario debe tener configurado el monitor con un protector de pantalla que tenga PASWORD, con un tiempo máximo de cinco minutos.

5.2 ESCENARIOS DEL REPORTE DE ANALISIS

5.2.1 Escenario 1

5.2.1.1 Redes Exclusivamente Privadas

5.2.1.1.1 Arquitectura

- **Redes privadas**
- **Protocolos propietarios**
- **Usuarios Internos**

5.2.1.1.2 Vulnerabilidades

- **Uso no autorizado de recursos**
- **Implantación software malicioso (virus, sniffers, etc.)**
- **Conexiones externas incontroladas**
- **Acceso no autorizado a la red interna**

5.2.1.1.3 Amenazas

- **Usuarios internos (descuido error)**
- **Empleados deshonestos (daños intencionados)**
- **Intrusos**

5.2.1.1.4 Contramedidas

- **Establecimiento de una política de usos y usuarios (password)**
- **Formación de usuarios**
- **Software de detección de virus**
- **Control de configuraciones**

5.2.2 Escenario 2

5.2.2.1 Redes Privadas + Servidor Web Aislado

5.2.2.1.1 Arquitectura

- **Red privada**
- **Servidor WEB Externo**
- **Proveedor servicio Internet**
- **Usuarios externos**

5.2.2.1.2 Vulnerabilidades

- **Cambio de la información residente en el servidor**
- **Degradación del servicio**
- **Suplantación de identidad**

5.2.2.1.3 Amenazas

Internas:

- **Usuarios internos (descuido error)**
- **Empleados deshonestos (daños intencionados)**
- **Intrusos**

Externas:

- **Hackers:**

5.2.2.1.4 Contramedidas

- **Software del servidor acreditado**
- **Limitar y controlar el acceso al servidor (webmaster)**
- **Backup de la información**

- **Monitor de accesos**
- **Configuración del servidor (sólo servicios web)**
- **Aplicación de parches**

5.2.3 Escenario 3

5.2.3.1 Red Privada + Servidor Interactivo

5.2.3.1.1 Arquitectura

- **Servidor Interactivo (Formularios, CGIs)**
- **Información sensible**

5.2.3.1.2 Vulnerabilidades

Scripts inseguros (propias y del resto de servidores)

Información sensible

- **Robo de información (confidencialidad)**
- **Modificación (Integridad)**
- **Falsificación (Autenticidad)**

5.2.3.1.3 Amenazas

- **Información Basura**
- **Secreto de la información**
- **Instrucción en el servidor**

5.2.3.1.4 Contramedidas

- **Servidor WEB seguro (SSL)**
- **Cifrado de mensajes**
- **Confirmación por otros medios (Autenticidad)**

5.2.4 Escenario 4

5.2.4.1 Red Interna + Servidor Interactivo + Acceso Corporativo

5.2.4.1.1 Arquitectura

- **Acceso corporativo (usuarios con acceso a Internet)**
- **Red Interna con protocolos TCP/IP**
- **Cortafuegos, Control del punto de acceso a la red**

5.2.4.1.2 Vulnerabilidades

- **Ataque de la red Interna**
- **Implantación de software malicioso**
- **Puertas traseras incontroladas (módems internos)**
- **Configuración del punto de acceso (cortafuegos)**

5.2.4.1.3 Amenazas

Acceso a Internet (medio inseguro y promiscuo) por usuarios internos

Acceso no autorizado a la red interna (que utiliza protocolo TCP/IP)

- **Por el cortafuegos**
- **Por puertas internas**

5.2.4.1.4 Contramedidas

Configuración del punto de acceso (cortafuegos)

- **Base de reglas (Origen, Destino, Servicio)**
- **Normas (aceptar, rechazar, cifrar, cortar)**

Administración del cortafuegos

Monitorización de la red interna

5.3 SEGURIDAD EN EL SISTEMA DE CUENTAS

La 0forma más fácil para llevar a cabo un acceso no autorizado en un sistema es a través de la cuenta de otra persona, para evitar esto la medida de seguridad que presenta el sistema es el nombre de usuario y la contraseña.

Es importante, para que la seguridad no se vea comprometida, controlar viejas cuentas, evitar contraseñas fácilmente adivinables y supervisar todo lo que pueda facilitar un acceso a una cuenta por parte de una persona que no sea su propietario.

5.3.1 Control de los passwords

La contraseña es la medida más importante de seguridad. Si se consigue romper esta barrera el posible intruso adquiere la identidad del propietario. Esto es crucial en el caso de que se vea involucrada la de root. Es fundamental un buen control de las contraseñas y de las posibles cuentas que no estén siendo usadas, para lo cual se debe considerar:

- No utilizar el nombre de la cuenta (login), tal cual, al revés, en mayúsculas...
- No utilizar nuestros nombres, ni apellidos.
- No utilizar nombres de familiares.
- No emplear información personal que pueda ser obtenida fácilmente.
- No emplear una contraseña sólo con números o con la misma letra.
- No emplear palabras que se encuentren en los diccionarios.
- No utilizar palabras de menos de seis letras.
- Mezclar letras mayúsculas y minúsculas.
- Utilizar palabras que sean fáciles de recordar para que no haya que escribirlas.
- Emplear una contraseña que pueda ser tecleada rápidamente sin necesidad de mirar al teclado.

- No escribirlos en ningún sitio, ni siquiera ficheros.

5.3.1.1 Consejos para crear password

- Dónde vienes, mortal un poema o canción y quedarnos una Tomar línea de con la primera letra de cada palabra, por ejemplo, eligiendo a Aleixandre:
- “¿De que del barro has llegado para un momento brillar y regresar después a tu apagada patria?" el posible password (con 10 palabras bastan), “Ddvmqdbhl".
- Poner alternativamente entre una consonante y una vocal, dos vocales, esto proporciona palabras que no tienen sentido y que normalmente son pronunciables, como “routboo", “quadpop" .
- Elegir dos palabras cortas y unirlas por un símbolo de puntuación.

5.3.2 Control de las cuentas

5.3.2.1 Cuentas con vida limitada

Estas cuentas suelen suponer un agujero de seguridad importante, no sólo porque alguien pueda entrar en ellas, sino porque si se produce un acceso no autorizado es muy difícil de detectar. Para evitar esto hay que poner fecha de expiración en todas las cuentas.

5.3.2.2 Cuentas multiusuario

Hay que tener también un especial cuidado con las cuentas públicas. A ellas acceden usuarios que permanecen poco tiempo en el sistema. Lo mejor es crearlas para un fin concreto y borrarlas después.

No deben tener palabras de acceso tan simples como “guest" o “visitor" y nunca deben permanecer en el fichero de passwords del sistema.

También suelen plantear problemas de seguridad algunas cuentas que se instalan para ejecutar ciertos comandos sin acceder a la máquina. No tienen contraseña, por tanto pueden ser usadas por cualquiera. Algunas de ellas tienen como identificador de usuario el cero. Estas cuentas prácticamente “invitan" a los crackers a entrar en ellas. La forma de acceder es sencilla, si un usuario puede acceder al sistema, reemplazando los comandos por unos suyos, podrá ejecutarlos con permisos de *root*.

5.4 Seguridad en el sistema de ficheros

Las barreras de entrada que nos encontramos en el sistema de ficheros son los derechos sobre los mismos.

Cada fichero o directorio de nuestro sistema tiene asociado 3 conjuntos de bits asociados a los permisos: uno del usuario, dueño del fichero, otro para el grupo al que pertenece y otro para el resto de los usuarios. Cada grupo contiene los tres bits conocidos de permisos, uno de lectura, otro de escritura y otro de ejecución.

En ocasiones se abusa de esta facilidad. Si un hacker, llegar a ser un determinado usuario, puede ser posible que sea capaz de ejecutar programas como ese usuario. Si gana el EUID o podrá editar el fichero de passwords y crearse una cuenta de root.

Hay que tener cuidado con los ficheros que tienen el bit de setuid activado puesto que pueden suponer brechas de entrada al sistema.

5.5 Control de los dispositivos

La seguridad de los dispositivos es una característica importante en nuestros sistemas. Los programas los emplean para acceder a los datos en los discos o en memoria. Si no están adecuadamente protegidos el sistema está abierto a un posible ataque. Es importante que se sigan las siguientes líneas:

5. Los ficheros /dev/kmem, /dev/mem *y* /dev/drum no deben poder leerse por todos los usuarios.
6. Los dispositivos de disco como /dev/sd0a *y* /rxylib deben pertenecer al root y al grupo operator y debe tener modo 640.
7. Con muy pocas salvedades, todos los otros dispositivos deben pertenecer al root. Una excepción son los terminales cuya pertenencia cambia al usuario que ha accedido al sistema desde él. Cuando abandona el sistema vuelve automáticamente al root.

5.6 Seguridad en red

5.6.1 Clonación de máquinas

Un sistema puede pasar por otro asumiendo su dirección y el nombre de host. La dirección de red no es única para cada máquina. Es cierto que está almacenada en un chip de la tarjeta de red pero se puede cambiarla usando el comando:

```
% ifconfig le0 ether x:x:x:x:x:x
```

es posible, por tanto, adquirir la identidad de otro través de otra máquina del mismo tipo.

5.6.2 Escuchando la red

En el caso de Ethernet cualquier sistema conectado a la red puede escuchar las conversaciones entre los otros sistemas. Si es un acceso remoto, entonces la contraseña puede ser visible. A esto se le conoce como snooping (ver). Los controladores ethernet, normalmente, leen todos los paquetes que le llegan pero los que tienen otro destino son descartados. Se puede hacer, sin embargo, que la tarjeta actué en forma simulada. En este caso interpretará todos los paquetes que le lleguen.

5.6.3 Autentificación de red

Debido a la posibilidad de escuchar los paquetes que circulan por la red, es importante que no se transmitan passwords sin encriptar por ella. Pero el hecho de enviar las contraseñas encriptadas plantea el problema de la comunicación de las claves. Uno de los servicios que usan autentificación de red es el de RPC.

5.6.3.1 Características de seguridad de las modalidades de autentificación

La autentificación DES usa el estándar de encriptación DES y criptografía de llave pública para llevar a cabo la autentificación de usuarios y sistemas. En el sistema de criptografía de llave pública el cliente y el servidor obtienen una clave común denominada de conversación. El servidor deduce la clave conversación combinando la clave pública del cliente con su clave privada y viceversa

5.7 SEGURIDAD DEL DNS

El servicio DNS (Domain Name System), es una amplio conjunto de bases de datos distribuida usado a lo largo de la Internet, proporcionando correspondencia entre los nombres de host y las direcciones de IP de los mismos. Existe la posibilidad de abusar de este servicio

para poder entrar en un sistema. Suposiciones durante la fase de autentificación, pueden conllevar serias grietas de seguridad importantes. El problema de seguridad es similar al que existe en el NIS. La autentificación se lleva a cabo en muchos casos a partir del nombre o la dirección. Las aplicaciones de alto nivel, usan en la mayoría de los casos los nombres para la autentificación, puesto que las tablas de direcciones son mucho más difíciles de crear, entender y mantener. Si por ejemplo alguien quiere suplantar una máquina por otra no tiene más que cambiar una de las entradas de la tabla que relaciona su nombre con su dirección. Este es el problema fundamental de DNS. Para conseguir esto una máquina debe obtener primero el número ID de la petición DNS, para ello debe construir el paquete de respuesta y usar la opción de enrutamiento de fuente, para hacerlo llegar al que llevó a cabo la petición.

5.8 FTP Y TELNET

El protocolo de transferencia de ficheros (FTP), se implementa mediante los programas ftp *y* ftpd. Las viejas versiones de los mismos presentaban ciertos fallos de seguridad por lo que se debe desactivar FTP, y TELNET en el servidor de Internet y AIX que es nuestro servidor de Lotus Domino, para la aplicación ECORED.

5.9 EL SERVICIO DE CORREO ELECTRÓNICO

El correo electrónico es uno de los servicio más usados. El programa sendmail se usa para recibir y mandar los mensajes de correo electrónico. Sobre este programa, se dice, que está repleto de bugs y que no hay ningún programador que logre comprenderlo del todo. Antiguas versiones tienen agujeros bien conocidos.

Son necesarias, también, ciertas medidas de seguridad a la hora de su instalación:

1. Eliminar el alias de “decode". para los ficheros /etc/aliases y /usr/lib/aliases.
2. Si creamos alias para que los mensajes sean enviados a programas, hay que estar completamente seguro de que es imposible obtener un shell o enviar un mensaje a un shell de esos programas.
3. Asegurarse que el password “withard" se elimina del fichero de configuración, sendmail.cf.
4. Hay que asegurarse que el sendmail no tenga el comando “Debug".

5.10 SUPERVISIÓN Y AUDITORÍA

Un requisito importante de seguridad es la posibilidad de visualizar qué es lo que está pasando y qué ha pasado en nuestro sistema. Para ello hay que controlar los ficheros a los que se acceda de forma no autorizada, así como la supervisión de nuestro propio sistema para detectar cualquier agujero de seguridad.

5.10 ESTRATEGIAS DE SEGURIDAD EN LOS SERVIDOR DE LOTUS NOTES

5.10.1 Seguridad de Hardware

5.10.1.1. AIX

El protocolo de transferencia de ficheros (FTP), se implementa mediante los programas ftp *y* ftpd. Las viejas versiones de los mismos presentaban ciertos fallos de seguridad por lo que se debe desactivar FTP, y TELNET en el servidor de Lotus Domino, para la aplicación ECORED.

Estas restricciones la realizamos de la siguiente manera

1.-Procedemos editar el archivo *inetd.conf* que se encuentra dentro de *etc/inetd.conf* para desavilitar el ftp y telnet.

2.-Una vez editado el archivo inetd.conf procedemos a poner comentarios en ftp y en Telnet.

Ejemplo:

***ftp**

***Telnet**

Luego que hemos puesto comentario a Telnet y Ftp procedemos a salir y grabar con *Esc: wq*

3.- Para que funcione y se aplique los cambios en el servidor procedemos a refrescar de la siguiente manera *refresh –s inetd.conf*

Además los servidores deben tener instalados una tarjeta encriptadora tanto en el servidor de Ecuador como en el Servidor de Colombia, que nos garantiza un nivel de seguridad, que nadie pueda descifrar la información que viaja por ese canal de comunicación, además garantiza que solo este servidor tenga la llave para poder establecer comunicación y poder actualizar la información.

Cada equipo (Servidor) tanto en Ecuador como en Colombia tienen su tarjeta de red con una dirección MAC única y propia de cada fabricante de tal forma que para el envío ó recepción de la información el sistema reconoce al destinatario para hacer entrega respectiva.

5.10.1.2. FIREWALL

Un Firewall es un sistema o grupo de sistemas que impone uno o un grupo de políticas seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red que están disponibles dentro de esta y por los que están fuera de ella, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad para el proyecto se describirán a continuación, donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento.

5.10.1.2.1. Estrategias del Firewall para seguridad en “ECORED”

Protección de los servidores de Ecuador como de Colombia por medio de un filtro llamado ecored.in, que contiene las siguientes reglas.

- Solo pueden comunicarse entre servidores para realizarse la replica, para lo cual hemos optado por configurar a los servidores con direcciones IP reales, para que solo se comuniquen por medio del Firewall se filtrara el paso basándose en direcciones IP. Esto se realiza de la siguiente manera:

Procedemos a configurar IP, NETMASK, Puerta de Enlace al Router con:

Set ether0 address 200.32.69.193

Set ether0 net mask 200.32.69.193

Set default 200.32.69.193.

Verificamos la configuración con Sh ether0 y la creación del filtro comaco.in, como se muestra a continuación:

Grafico 5.1: Configuración de la Interface Ether0

Luego de esto verificamos todas los filtros creados y además habilitamos puertos tales como TCP, IP como se muestra a continuación:

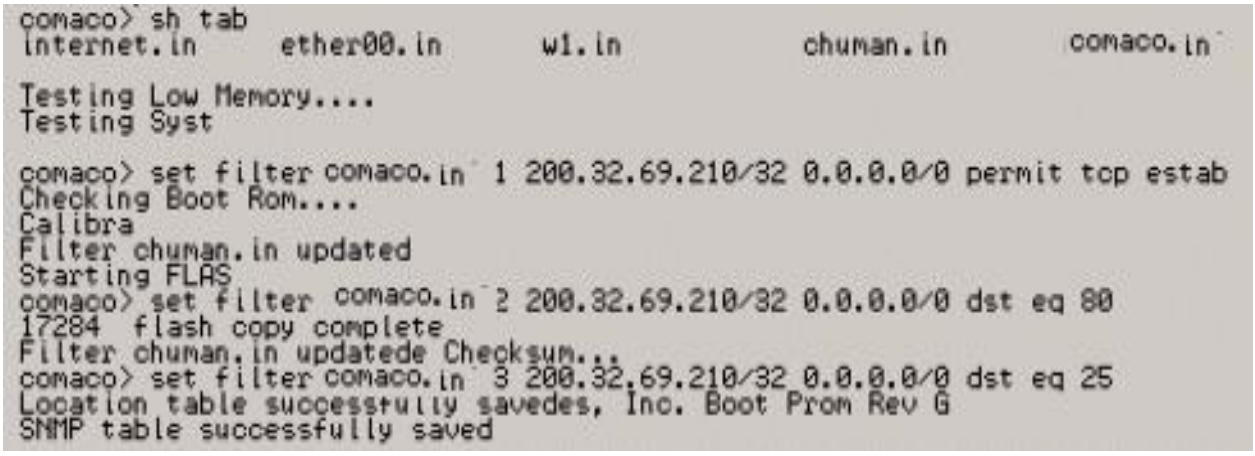


Grafico 5.2: Configuración del filtro comaco.in

Verificamos creación de políticas en el filtro con:

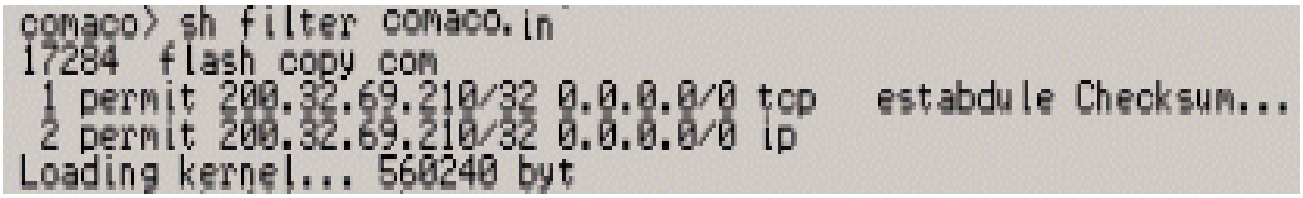


Grafico 5.3: Configuración de puertos para filtro comaco.in

Ya una ves habilitado puertos de TCP y de IP podemos comunicarnos con el otro servidor asignado una política al filtro que consta de que solo puedan verse las direcciones 200.32.69.210 con la 209.69.152.234 como se muestra a continuación:

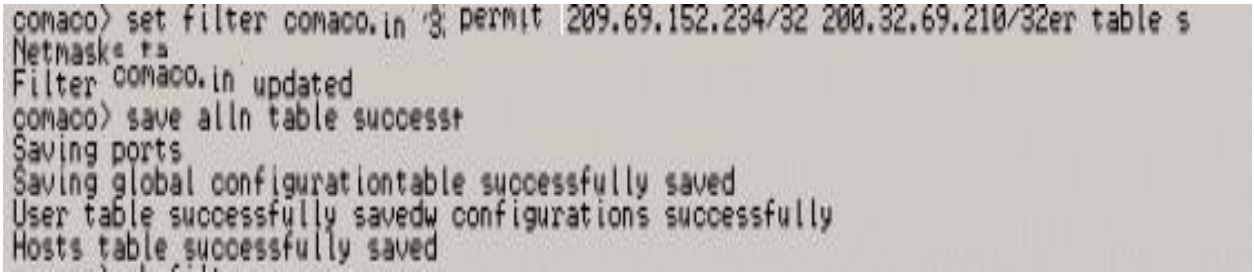


Grafico 5.4: Configuración de Direcciones para filtro comaco.in

Además procedemos a deshabilitar puertos de Telnet y FTP para el servidor de la Base de Datos Documental ECORED, para garantizar una mayor seguridad.

Otro regla de seguridad es al de deshabilitar la posibilidad de realizar PING al SERVIDOR tanto de Ecuador como de Colombia.

5.10.1.3. DISEÑO DE LA RED CON SEGURIDAD

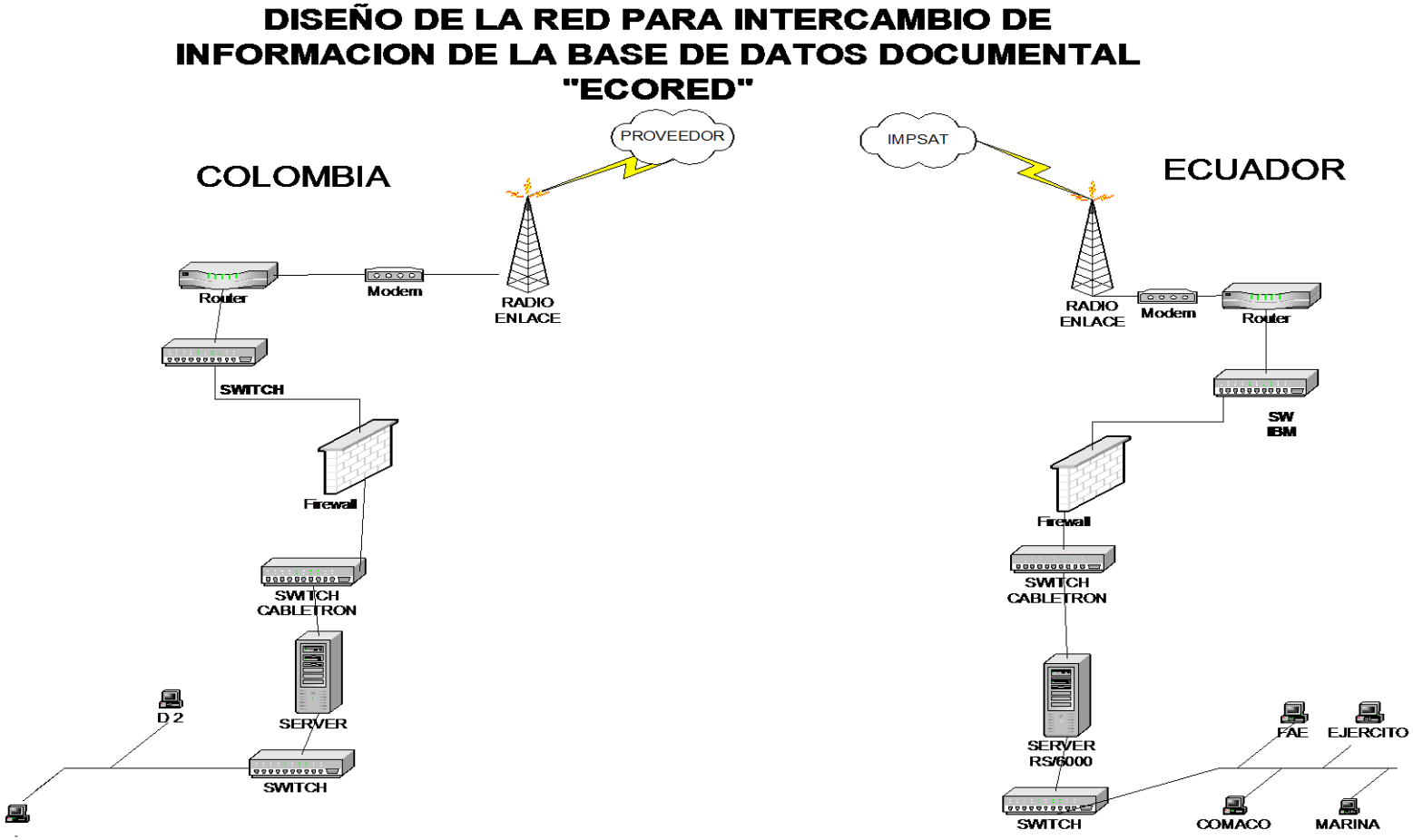


Grafico 5.5: Seguridad de "ECORED"

5.10.2 Seguridad de Software

Para la aplicación en Lotus Notes nos presenta varios niveles de seguridad: autenticación, control de acceso, campos con niveles de seguridad y roles, restricción de Anónimos, Defaul y Encriptación a nivel de Protocolo.

Autenticación.- A través de esto el usuario tiene confiabilidad en la identificación, es bidireccional entre el servidor y el usuario, es siempre usada entre un usuario y el servidor o entre dos usuarios.

Control de Acceso ACL.- Regula que tipo de acceso se tiene y a que fuente de información (componer, leer, escribir, borrar) existen varios niveles: Depositor, lector, autor, editor, diseñador, administrador.

Campos y niveles de seguridad.- En cierto tiempo un usuario puede necesitar distribuir campos y niveles de información de un documento con un determinado usuario, mientras asegura que otros usuarios no puedan ver esto. La encriptación involucra cifrado o escrambling de tal manera que aún si se tiene acceso a por error individual, esto no puede ser entendido. La encriptación es habilitada en cuatro niveles en Notes.

- Niveles de mensajes. Los mensajes individuales que pueden ser encriptados para uno a más entidades de recepción.
- Niveles de red. Previene que alguien extraño husmee o intente ingresar en el tráfico de una red LAN o monitoreo la línea, el contenido es ilegible para el intruso.
- Nivel de campo. Las bases de datos pueden ser diseñadas para encriptar campos del documento es así que solo usuarios específicos pueden lee luego.

- Nivel de base de datos. Encriptación protege la base de datos almacenada en el disco duro de ser accesada por otra persona que no sea la que posee el ID o password utilizado para encriptar la base de datos.

Roles.- Se deben establecer roles para usuarios o grupos, para garantizar la presentación de documentación solo para las personas o grupos autorizadas para generar o visualizar documentos.

Anónimos y Default.- Se debe tomar en cuenta y sobre todo mucho cuidado cuando se crea un usuario o grupo de trabajo, por cuanto al momento de creación se asigna los valores Anónimo o Deafault, por lo tanto el usuario o grupo obtiene permisos que no debería de acuerdo a los permisos del administrador.

Encriptación a nivel de Protocolo.- La encriptación a nivel de protocolo es uno de los niveles de seguridad propios de Lotus Notes, que garantiza que solo los servidores certificados o los que estecen dentro del dominio tengan acceso al servidor, por cuanto pueden establecer comunicación solo entre servidores ya que solo ellos pueden entenderse y comunicarse.

5.10.2.1 La seguridad en una aplicación

Notes proporciona una infraestructura de seguridad de múltiples niveles que permite asegurar el sistema comenzando por el propio dominio y descendiendo hasta el nivel de los campos. La seguridad de los servidores y el control del acceso al dominio es responsabilidad del administrador de servidores. Como diseñador de bases de datos, puede controlar el acceso de los usuarios a su aplicación hasta el contenido de un campo. También puede controlar el acceso a determinados elementos, como son el diseño y los agentes de la base de datos.

Las funciones utilizadas determinarán el grado de seguridad de la aplicación. La codificación y la Lista de control de acceso de la base de datos proporcionan una verdadera seguridad. La creación de listas de acceso a los formularios y la ocultación de elementos de diseño permiten dificultar el acceso pero no son funciones de seguridad.

Para restringir o limitar el acceso a los componentes de una base de datos, utilice estas funciones:

- La Lista de control de acceso de la base de datos (LCA) determina quién puede o no puede acceder a la base de datos. Para los usuarios que pueden acceder a una base de datos, los niveles de acceso y los roles determinan las acciones específicas que pueden realizar (por ejemplo, crear o eliminar documentos).
- Las listas de acceso al formulario, junto con la LCA de la base de datos, controlan quién puede leer o editar todos los documentos creados con un formulario.
- Los campos de acceso al documento (campos de lectores y de autores), junto con la LCA de la base de datos, controla quién puede leer o modificar determinados documentos.
- La codificación le permite asegurar la información a nivel de los campos. Puede codificar el contenido de cualquier campo para que sólo los lectores que dispongan de la clave de codificación puedan acceder al mensaje o campo. Los gerentes de bases de datos pueden codificar toda la base de datos.
- Los roles nos permite restringir accesos a diferentes tipos información según el rol que desempeñe
- Limite los usuarios que pueden crear agentes y los lugares en que éstos pueden ejecutarse. La mayoría de los usuarios pueden crear agentes privados que se ejecutan en

bases de datos locales; algunos usuarios también pueden crear agentes compartidos que se ejecutan en servidores y que pueden ser utilizados por otros usuarios.

- **Asegure el diseño de una base de datos para impedir que los usuarios modifiquen los elementos de diseño.**

5.10.2.2 Codificación de documentos

Se denomina documento codificado a aquél que contiene uno o varios campos codificables que están asociados a una o a varias claves de codificación. El proceso de codificación puede tener lugar automáticamente (a través del diseño del formulario) o manualmente (por parte de los autores y de los editores). Cuando se asocian varias claves de codificación a un documento, Notes, automáticamente, codifica todos los campos codificables con todas las claves especificadas. No es posible asociar una clave distinta a cada uno de los campos.

Las claves de codificación pueden ser secretas (claves que deberá enviar de forma explícita a los usuarios para que éstos puedan descodificar un determinado campo) o públicas (claves que ya están asociadas al documento de persona de un usuario en el Registro de nombres público). Este último tipo de claves se utiliza para codificar los documentos de correo.

5.10.2.3 Lectura de la información codificada

Los usuarios sólo pueden leer la información codificada si sus archivos ID de usuario o sus documentos de persona del Registro de nombres público disponen de la clave de codificación adecuada. Si un usuario no dispone de dicha clave, podrá leer las partes no codificadas de un documento, pero los campos codificados aparecerán vacíos.

Para poder leer la información de un documento que tiene asociadas varias claves de codificación, es suficiente con que los usuarios dispongan de una de ellas.

5.10.2.4 Edición y almacenamiento de la información codificada

Los usuarios cuyos archivos ID no disponen de la clave de codificación adecuada no pueden editar los documentos codificados. Sí pueden crear nuevos documentos, pero deben guardarlos sin codificar; para ello, deben eliminar la clave de codificación en el cuadro de información sobre el documento.

Si un formulario o documento tiene asociadas varias claves de codificación secretas, los usuarios necesitan disponer de todas ellas para poder editar y guardar información codificada haciendo uso de las claves originales. Si no disponen de ellas, aún tienen la oportunidad de codificar los documentos usando sus propias claves; para ello, deberán cambiar la lista de claves original por la suya propia en el cuadro de información sobre el documento.

5.10.2.4 Eliminación y cambio de las claves de codificación para un documento

Los autores pueden eliminar la función de codificación o cambiar las claves asociadas a sus propios documentos (siempre y cuando tengan permiso para editarlos y dispongan de todas las claves de codificación asociadas). Los editores pueden eliminar la función de codificación o cambiar las claves asociadas a cualquier documento.

5.10.3 Seguridad de los datos codificados

Si un usuario realiza una copia de la base de datos, los datos permanecen codificados, incluso si la copia se lleva a cabo desde el sistema operativo. Los datos codificados también están seguros si se intenta acceder a ellos desde programas creados con el API de Notes.

Las búsquedas de texto en índice que incluyen la opción Indexar los campos codificados mostrarán los datos codificados a cualquier usuario que tenga acceso a la base de datos. Asimismo, si un usuario que tiene la capacidad para descodificar documentos crea el índice, dicho usuario podrá leer el índice de texto como un archivo de texto ASCII en el servidor.

5.10.3.1 Control del acceso a una base de datos durante su diseño

Toda base de datos dispone de una Lista de control de acceso (LCA) que determina qué usuarios pueden acceder a ella y qué tipo de actividades pueden realizar. Mientras esté diseñando la base de datos, limite el acceso de manera que únicamente usted, otros diseñadores y el gerente de la base de datos tengan acceso a la misma. Una vez finalizado el diseño, el gerente podrá volver a modificar la LCA para poner la aplicación a disposición de todos los usuarios.

5.10.3.2 Creación de formularios, vistas y agentes públicos aspectos generales

La lista de acceso público, al igual que los campos de lectores y de autores, funciona junto con la Lista de control de acceso de la base de datos para ampliar el acceso de los usuarios a determinadas vistas, formularios y documentos. Mediante la creación de formularios y vistas disponibles para usuarios con acceso a documentos públicos podrá permitir que los usuarios con un nivel de acceso Sin acceso o Depositante puedan visualizar determinados documentos, formularios y carpetas sin tener que asignarles el nivel de acceso de Lector a toda la base de datos. Los usuarios que tienen este nivel de acceso en la Lista de control de acceso de la base de datos verán sólo los documentos, las carpetas y las vistas que han sido definidas como disponibles para los usuarios con acceso a documentos públicos en sus respectivos cuadros de información. La creación de agentes disponibles para usuarios con

acceso a documentos públicos permite que los usuarios con un nivel de acceso Sin acceso o Depositante puedan visualizar y utilizar cualquier agente de ejecución manual.

5.10.4 Limitaciones

5.10.4.1 Limitación de los usuarios que pueden actualizar los documentos de una carpeta

Si desea que sólo determinados usuarios puedan actualizar los documentos de una carpeta, cree una lista de acceso de edición para la carpeta. Podrá añadir usuarios a la lista en la medida en la que ya tengan como mínimo un nivel de acceso de Autor en la Lista de control de acceso de la base de datos.

1. Seleccione la base de datos y seleccione Ver - Diseño.
2. En el panel de navegación, haga clic en Diseño - Carpetas.
3. Haga doble clic en la carpeta.
4. Seleccione Diseñar - Propiedades de la carpeta.
5. Haga clic en el icono en forma de llave (pestaña Seguridad).
6. En el apartado Pueden actualizar el contenido:, desactive la opción Todos los autores y los de nivel superior.
7. Haga clic en cada usuario, grupo, servidor o rol de acceso que desee incluir en la lista. Notes muestra una marca de verificación junto a cada nombre seleccionado.
8. Haga clic en el icono Persona si desea agregar los nombres de personas o de grupos utilizando un Registro de nombres personal o público.
9. Para eliminar un nombre de la lista, vuelva a hacer clic en él.

10. Guarde la carpeta.

5.10.4.2 Limitación del acceso a los documentos

Notes proporciona un sistema de seguridad de varios niveles que le permite una gran flexibilidad a la hora de controlar el acceso a toda o a parte de una aplicación. El nivel de seguridad superior se gestiona a través de la Lista de control de acceso (LCA) de la base de datos. Con el uso de los parámetros de la LCA, podrá controlar cuidadosamente quién tiene acceso la aplicación y especificar el tipo de acceso permitido. Por ejemplo, puede permitir que un usuario pueda leer, crear y editar los documentos de una base de datos y permitir que otro sólo pueda leer documentos.

El acceso a los documentos puede restringirse de las formas siguientes:

- Creando una lista de acceso de lectura a una vista o carpeta que limite los usuarios que pueden ver la vista o carpeta.
- Creando una lista de acceso de edición a una vista o carpeta que limite los usuarios que pueden actualizar los documentos de la vista o carpeta.
- Creando una lista de acceso a un formulario para limitar el acceso a todos los documentos creados con el formulario.
- **Creando campos de lectores y de autores para limitar el acceso a determinados documentos creados con un formulario.**

5.10.4.3 Uso de un campo de lectores para limitar el acceso a determinados documentos

Para limitar el acceso a los documentos creados con un determinado formulario, incluya un campo de tipo Lectores en el formulario. Un campo de lectores es una lista de usuarios en la que se indica quién puede leer los documentos creados con el formulario. Por ejemplo, si desea que sólo puedan acceder al archivo personal de un empleado los miembros del departamento de Recursos humanos, el propio empleado y su jefe, incluya sus nombres en un campo de lectores. Los usuarios que no tengan un nivel de acceso de Lector al documento no podrán verlo en las vistas.

Si un formulario dispone de una lista de acceso, los nombres incluidos en el campo de lectores se agregarán a ella. En caso contrario, será el campo de lectores el que controle el acceso el formulario.

El campo de lectores permite precisar la Lista de control de acceso, pero no la sustituye. Si un usuario tiene asignado el nivel Sin acceso a la base de datos no podrá leer el documento, aunque su nombre figure en el campo de lectores. Los usuarios con un nivel de acceso de Editor o superior no pueden leer los documentos si no han sido incluidos en el campo de lectores.

Sin embargo, los usuarios con un nivel de acceso de Editor o superior podrán editar el documento si:

- Se encuentran en la lista de acceso de lectura del formulario, en el campo de lectores o en el campo de autores.

- **El documento carece de lista de acceso de lectura, de campo de lectores y de campo de autores.**

5.11 POLITICA DE SEGURIDAD EN EL SERVIDOR DE INTERNET

- **Autenticación y controles de seguridad.**
- **Escenarios para conectar una Intranet a Internet**
- **Sugerencias sobre como utilizar las herramientas de monitorización para detectar, supervisar e impedir fallas de seguridad**

5.11.1 Derecho de usuario Inicio de sesión local

Para asignar el derecho de usuario Inicio de sesión Local a todas las cuentas utilizadas con IIS, es necesario utilizar el Administrador de usuarios o el Administrador de usuarios para dominios. Las cuentas que utiliza IIS son:

5.11.2.1 Acceso Anónimo

El acceso anónimo al servidor Lotus Notes Domino esta restringido en el servidor, por cuanto la replicación será de servidor de Ecuador al Servidor de Colombia

Los servicios WWW, FTP y Gopher. No hay diferencia entre un nodo anónimo de una intranet y un nodo anónimo de Internet.

Internet Explorer y la mayoría de los visualizadores WEB no suministran un nombre de usuario ni contraseña cuando se conectan a un servidor web, por lo IIS debe utilizar la cuenta IUSR_nombre-computadora.

El acceso anónimo se encuentra activado en forma predeterminada y se establece en la lengüeta Servicio de cada uno de los servicios. La información de la cuenta IUSR_nombre-computadora, o cualquier otra especificada en la lengüeta Servicio debe coincidir con los valores que tiene dicha cuenta en el Administrador de usuarios; no se permite el acceso a los usuarios si el nombre y la contraseña no coinciden.

5.11.2.2 Autenticación de usuarios

Se puede utilizar las cuentas de usuario de Windows NT para controlar el acceso a algunos archivos y directorios. Cuando se encuentra deseleccionado la casilla de verificación "Permitir anónimos" en la ficha "Servicio", **la primera petición de cada cliente hace que aparezca un cuadro de diálogo de autenticación. Si se selecciona "Permitir anónimos" junto con "Básico" (texto simple) o "Autentificación Desafío / respuesta de Windows NT", se solicita al usuario el nombre del usuario y la contraseña siempre que intente acceder a un recurso de una unidad con sistema de archivos de Windows NT (NTFS), en caso de que las propiedades de dicho recurso no permitan el acceso a la cuenta IUSR_nombre-computadora**

5.11.2.3 Autentificación de usuarios en una Intranet

Puesto que IIS utiliza las cuentas de usuario de Windows NT, se puede utilizar las cuentas existentes de la red y la estructura del Dominio, y administrar las cuentas de usuario con el administrador de usuarios. Y además se puede implementar la siguientes seguridades: Permitir anónimos, Autentificación Desafío / respuesta de Windows NT y Básica

5.11.2.4 Autentificación de usuarios en Internet

Los principios anteriormente presentados en las Intranets también son válidos para la autentificación de usuarios de Internet

5.11.2.5 Cifrado de Datos privados SSL

Da la seguridad de la red mediante la combinación de criptografía de clave pública y cifrado de datos, en donde hay que generar una clave pública y privada, las claves son generadas por el administrador de claves, y, a demás cabe indicar que las claves no se activan hasta que se envíe el archivo de petición de certificado, que genera el Administrador de claves.

5.11.3 Seguridad en FTP

5.11.3.1 Acceso anónimo FTP

FTP siempre utiliza la seguridad de nivel de usuario, es decir, el usuario debe iniciar una sesión para acceder al servidor de FTP, todas las transmisiones FTP se realizan en texto plano.

El servidor de FTP se debe configurar para permitir inicio de sesión anónimos, para lo cual requiere que el usuario escriba anónimos como nombre de usuario y su dirección de correo de Internet como contraseña, los usuarios anónimos pueden acceder a los archivos situados en la cuenta IUSR_nombre-computadora

5.11.4 Buzón de recepción

Se puede crear un buzón de recepción para los clientes de Internet, de manera que éstos puedan dejar archivos en él. El buzón de recepción debe encontrarse en un disco con formato NTFS.

5.11.5 Conexión de Intranets a Internet

Se puede crear un buzón de recepción para los clientes de Internet, de manera que éstos puedan dejar archivos en él. El Buzón de recepción debe encontrarse en un disco con formato NTFS. Para crear un buzón de recepción, haga clic en Propiedades, seguridad y, a continuación en Permisos. Fije los permisos de todos los usuarios como sólo escritura. Después de haber fijado los permisos a sólo escritura, los usuarios de Internet pueden dejar archivos en el directorio buzón de recepción, pero no pueden consultar ni copiar ninguno de los archivos que contiene. Sólo los usuarios internos con los permisos adecuados podrán leer estos archivos.

CAPITULO 6
CONCLUCIONES Y RECOMENDACIONES

6.1 CONCLUCIONES

Habiendo finalizado la elaboración del presente trabajo y alcanzado en su totalidad los objetivos trazados podemos concluir.

- **El reemplazo de los procesos manuales de ingreso de documentación al archivo de la sección técnica, se lo ha completado con éxito.**

- **Al implementar esta modalidad de almacenamiento documental automatizada, se ha logrado optimizar en un 70% las posibilidades de acceso directo a la información por parte de los funcionarios del Comando Conjunto de las Fuerzas Armadas.**

- **El registro y almacenamiento de documentos se estaban convirtiendo en un acuciante problema tanto por el tiempo de inclusión en el sistema, como en el espacio físico que ocupa por lo que ubicar un documento se convierte en una difícil tarea. Con la implementación de la aplicación se pasa ha almacenar los documentos en medios magnéticos de gran capacidad.**

- **La infraestructura tanto de hardware como de software con la que venia trabajando en COMACO estaba subutilizada, con la implementacion se trato de aprovechar al máximo la tecnología.**

- **Uno de los principales logros del desarrollo del proyecto ha sido la elaboración de sistema en un campo tan nuevo y distinto a los tradicionales, como es el las Base de Datos Documentales.**

- **La aplicación fue diseñada para que ingresen datos atreves de un cliente Notes, que además presta una familiaridad con el ambiente Web.**

6.2 RECOMENDACIONES

- **Poner en funcionamiento lo mas rápido posible la tarjeta encriptadora de datos para tener un nivel de seguridad.**

- **Cuando se enlacen a la red microondas de Colombia poner énfasis en cifrar la información ya que pueden ser interceptados por los enemigos, y la información sea mal utilizada o maleada.**

- **Tener los servidores en lugares seguros donde tengan acceso personas identificadas.**

- **Procurar tener respaldos de la información en medios magnéticos en periodos máximos de un mes.**

- **Por motivos de seguridad se recomienda tener aislado tanto lógica y física la red de datos y no como esta este momento en una red virtual del C3I2.**

6.3 BIBLIOGRAFIA

- Lotus Development Corp. Copyright 1998
  Lotus Domino Server Administratios Guide

- Jame Calabria y Sue Plumley
  Lotus Notes e Internet

- Copyright IBM Corp1997, 1999
  Network Intallation Management Guide and Reference

- Copyright IBM Corp1997, 1999

Guía de instalación y configuración rápida

- Lotus Education Coyrigth 1999 Lotus Development Corporation
  Desarrollo de Aplicaciones 1

- Lotus Education Coyrigth 1999 Lotus Development Corporation

WEB SITES

REDES PRIVADAS VIRTUALES (**VPN**/VPDN)
www.canalpyme.com/redes.htm
Servicios/**Redes** IP (**VPN** s).
www.alarcos.com/servicios/servicio1.asp

Virtual Private Network - **VPN**
www.microsoft.com/spain/msdn/estudiantes/redes/servicios/ VPN.asp

VPN Red de Área Local
www.cyt.net/redesconexion/lanwanvpn.htm

Descripción general de las **redes virtuales** privadas
www.microsoft.com/latam/technet/hoy/intranet/art09/art091.asp

Redes privadas virtuales Cómo balancear la necesidad de acceso remoto con la de extrema seguridad
www.lacompu.com/desarrollo/notas/redes.php3

SSL
http://www.jjf.org/sd/jjfsd3.htm

Internet e Intranet **TCP**/**IP**
www.microsoft.com/latam/mspress/subjects/subjectil_p1.htm

Protocolos **TCP**/**IP**. **...** FTP, SMTP,. TELNET. SNMP, X-WINDOWS,. RPC, NFS. **TCP**. UDP. **IP**, ICMP, 802.2, X.25. ETHERNET, IEEE 802.2, X.25.
members.es.tripod.de/janjo/janjo1.html

Protocolos de Red
www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

Lotus Notes
www.mty.itesm.mx/rectoria/dda/usols/lotus.htm
Lotus Notes
webdi.cem.itesm.mx/di/ca/lotus.html

AIX

www.terra.com.ve/informatica/que-es/aix.cfm

Grupo en AIX
wzar.unizar.es/estudiantes/aegee/foto5.html

ANEXOS

A. Manual de Usuario de la Base de Datos Documental Ecuador Colombia "ECORED"

1. Modo de Autentificación

El sistema de ingreso de información binacional consta de dos menús de ingreso y visualización de información para el Usuario.

3. **Administrador**
4. **Usuario**

1.1 Administrador

En este menú el administrador podrá encontrar un menú de opciones amplio en el cual consta de una opción de ingreso de nuevos formularios y consultas de diferentes opciones, para el ingreso de un nuevo formulario debe posicionarse con el mouse sobre la palabra "FORMULARIO NUEVO".

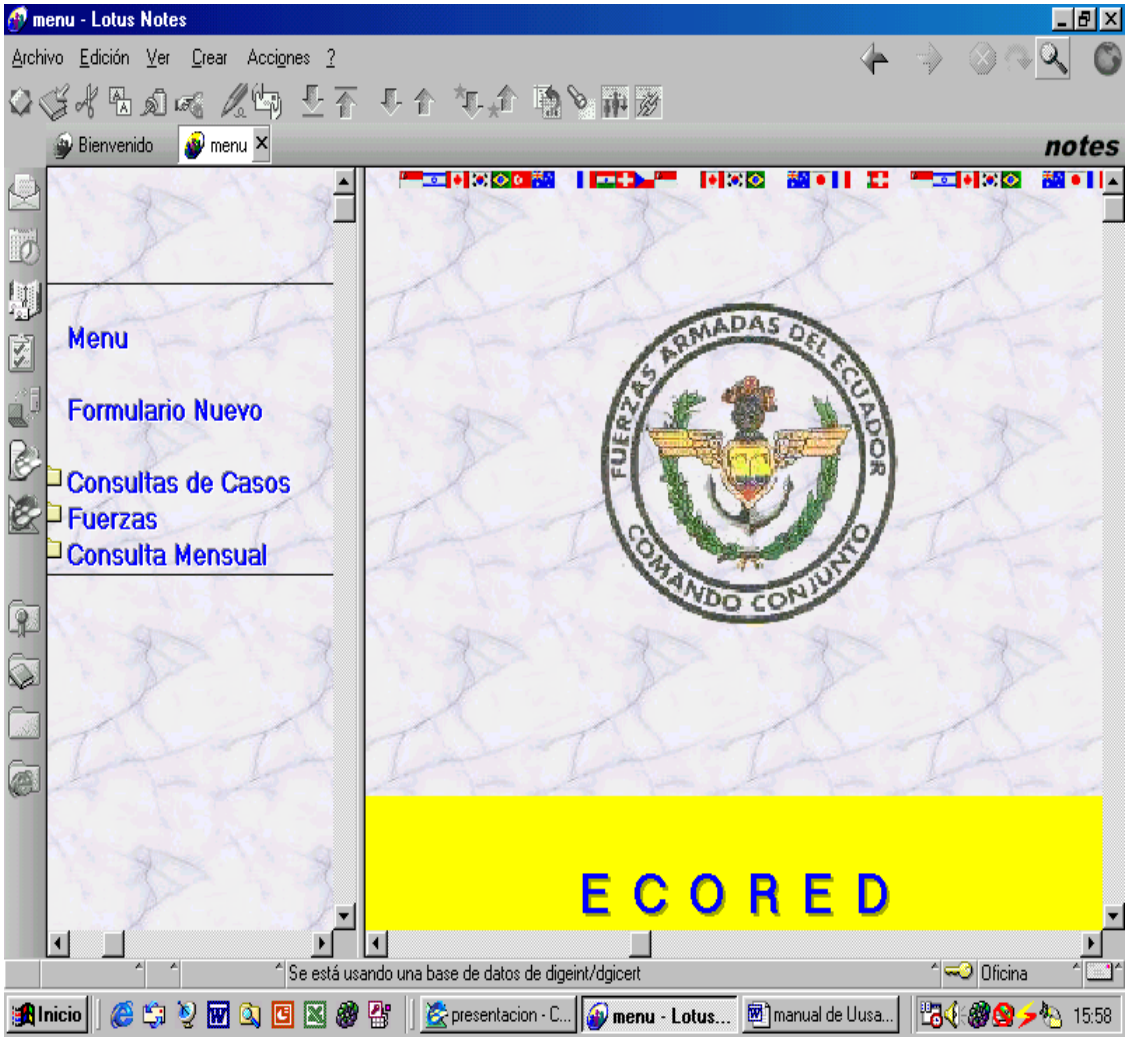


Grafico A-1 (Pantalla principal de Administrador)

Según la necesidad proceder a dar un clic sobre la palabra, seguido de esto le presentara en la parte central de la pantalla el formulario de ingreso de datos de la Ecored, como se muestra en el grafico A-2

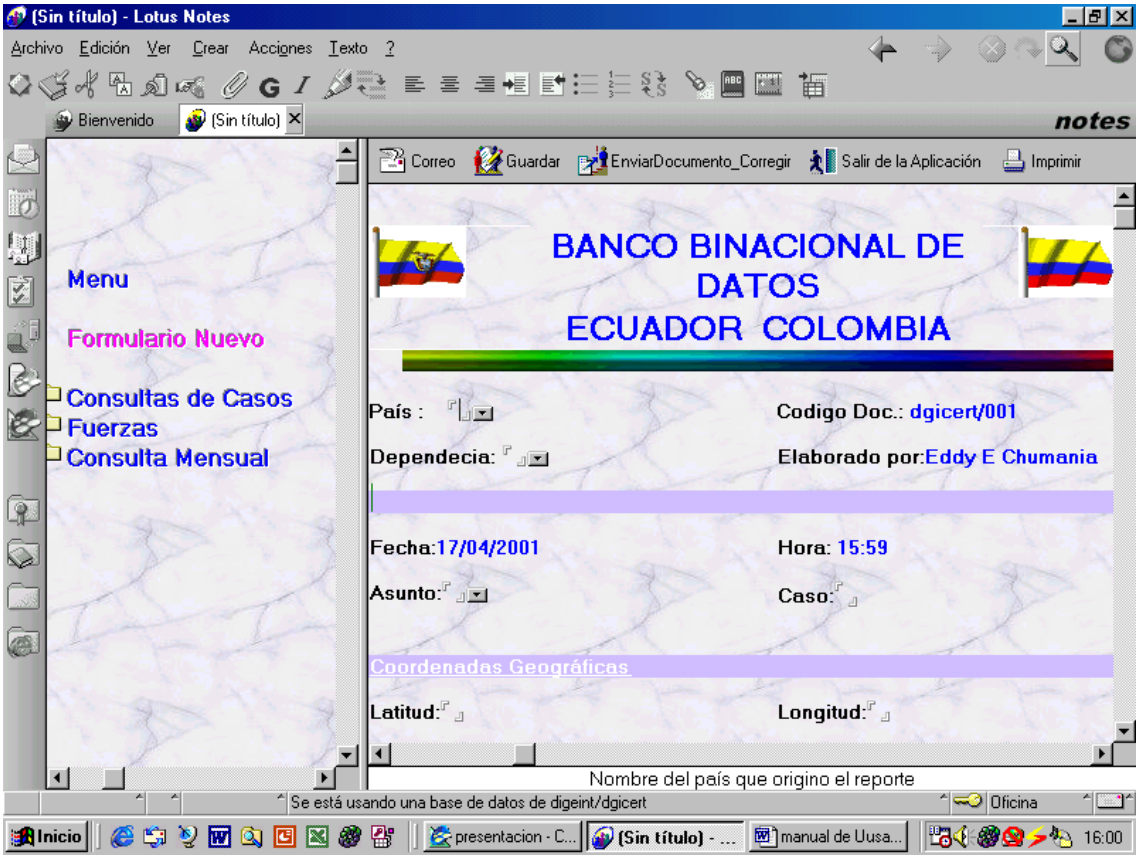


Grafico A-2(Presentación de formulario de Ingreso de Información)

Una ves que hemos realizado esta operación tenemos que llenar el formulario con la información pertinente para lo cual tenemos secciones de selección múltiple, secciones de múltiple selección y valores, información predeterminada por el sistema.

1.1.2 Secciones de Múltiple Selección Simple

En estas secciones lo que nos presenta es un campo en el cual en la parte derecha del mismo nos presenta un pequeño triangulo invertido ver (grafico A-3) en el cual nosotros damos un clic y nos despliega la información que en este campo podemos ingresar ver (grafico A-4) que por motivos de aplicación nos presenta dichas opciones y con dar un clic sobre la palabra seleccionada esta se carga automáticamente en el campo ver (grafico A-5)

Grafico A-3 (Presentación de pestaña de selección)

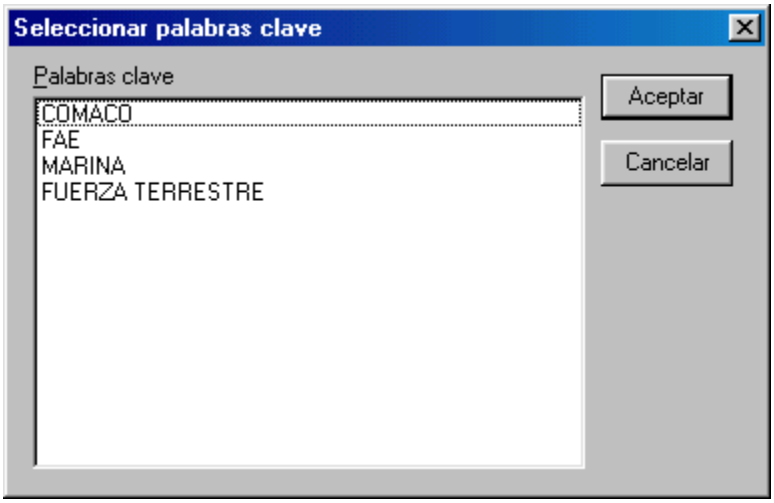


Grafico A-4(Menú de selección de la pestaña)

Grafico A-5 (Presentación de la opción escogida)

1.1.3 Secciones de Múltiple Selección y Valores

Esta opción es parecida a la anterior con la diferencia de que en esta usted podrá ingresar información que no se encuentre contemplada en los INTEMS presentados para dicho campo ver (grafico A 6 , A7).

Grafico A-6 (Modelo de pestaña de múltiples valores)

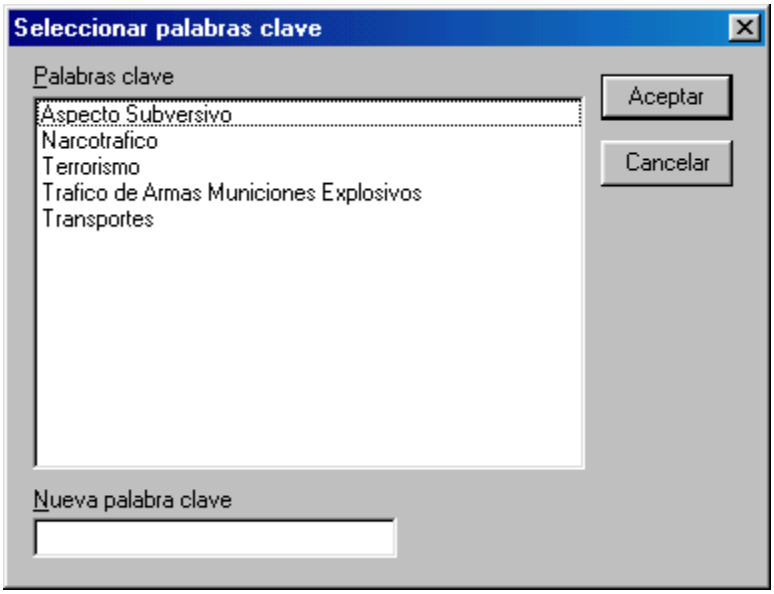


Grafico A-7 (Modelo de menú de múltiple selección)

1.1.4 Información predeterminada por el Sistema

Esta información viene dada por el sistema operativo como por ejemplo la hora y fecha de igual manera los datos del usuario que esta ingresando la información a la aplicación ver (grafico A-8).

Nota: Para no tener problemas con el ingreso de información en estos campos es aconsejable verificar que la hora y fecha del sistema estén correctos antes de ingresar a la aplicación ya que la fecha y hora serán cargadas directamente desde el sistema.

Grafico A-8 (Formato de Fecha y Hora)

Grafico A-9 (Formato de la persona que elabora el documento)

Visualización de Calendario.

Esta es una ayuda de ingreso de información para el usuario en la cual el campo nos presenta un calendario el cual nos permite escoger las fechas de una manera mas rápida y recordar alguna fecha que no recordemos. Ver (grafico A-10)

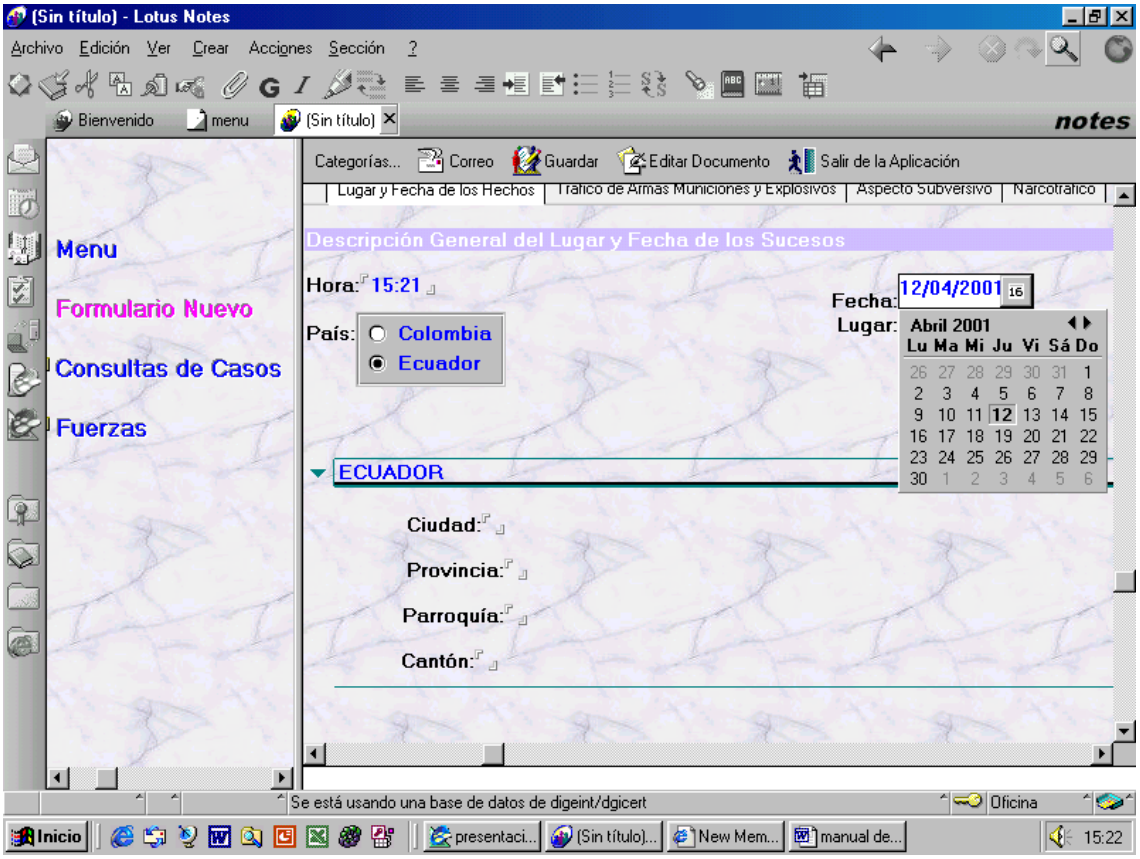


Grafico A-10(Presentación del calendario de selección de fecha)

1.1.5 Secciones Plegables

Esta opción se presenta plegada y con un botón de selección es activada y nos presenta la sección plegada en la cual hay campos de ingreso de información estos campos pueden plegarse y desplegarse ver (grafico A-11 y A-12)

1.1.5.1 Sección Plegable

Grafico A-11 (Muestra de la sección desplegable)

1.1.5.2 Sección Desplegada

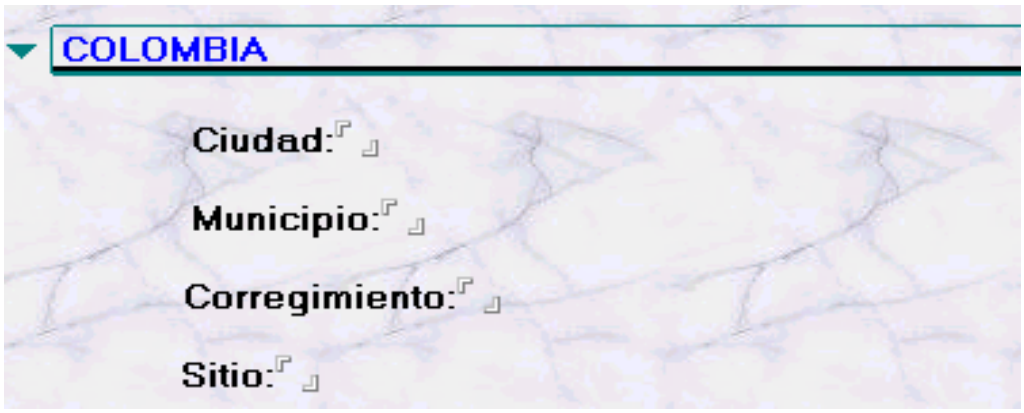


Grafico A-12(Muestra de una sección desplegada)

1.1.6 Menú de Opciones

En este menú podemos encontrar una serie de opciones para con el documento ver grafico A-13

Grafico A-13 (Menú de opciones de la aplicación)

1.1.7 Correo

Esta opción nos permite enviar correo entre los dos países y usuarios internos realiza la función normal del correo común funciona con un clic sobre la opción.

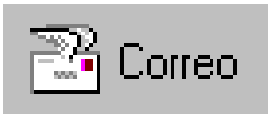


Grafico A-14 (Botón de envío de correo)

Guardar

Esta opción nos permite almacenar el nuevo documento en la base de datos local o directamente al servidor de acuerdo al modo de trabajo.

Nota: **Se trabajara de una manera Local para luego de que el documento este terminado sea enviado al supervisor.**

Grafico A-15 (Botón de guardar documentos)

Enviar Documento a Corregir

En esta opción se hace referencia a enviar el documento a corregir por que le falta algo en su contenido esta opción es exclusiva del supervisor.

Grafico A-16 (Botón de envío de documento a corregir)

Editar Documento

Esta opción nos permite hacer modificaciones a documentos creados pero esta opción es exclusiva solo para documentos creados por el mismo usuario.

Grafico A-17(Botón de edición de un documento ya almacenado)

Salir de la Aplicación

Esta opción nos permite salir de la aplicación de una manera directa y rápida.

Grafico A-18(Botón de salir de la aplicación)

CONSULTAS DE INFORMACIÓN

En este menú tenemos diferentes tipos de consulta que se presenta para el administrador con la cual puede tener un mejor campo de consulta para lo cual se a determinado los siguientes parámetros de consultas ver el grafico A-19.

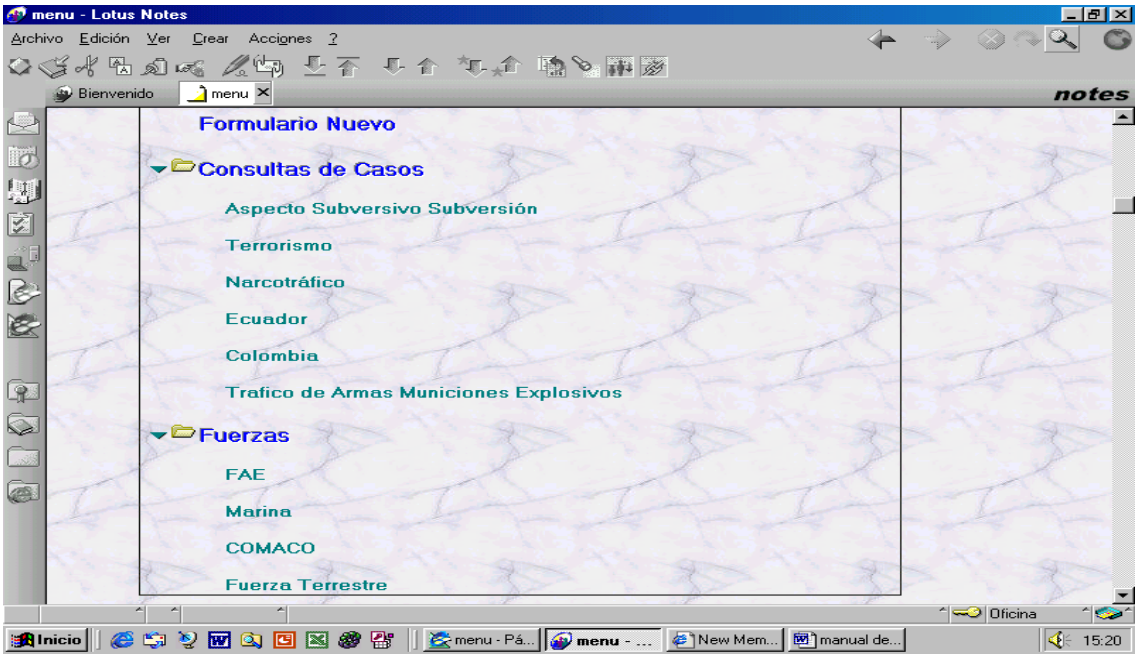


Grafico A-19(Pantalla principal de consulta)

Este tipo de consulta nos permite tener información del caso al que se haga referencia de una manera fácil, sencilla y rápida y la información que se presenta es en línea, basta con hacer desplegar cualquiera de los dos menús de consulta que tenemos tanto por casos como por Fuerzas que desarrollaron la información luego que se despliega se selecciona cual es la consulta que nos interesa se da un clic sobre esta y en la pantalla central nos despliega información acerca del tema escogido ver gráfico A-20

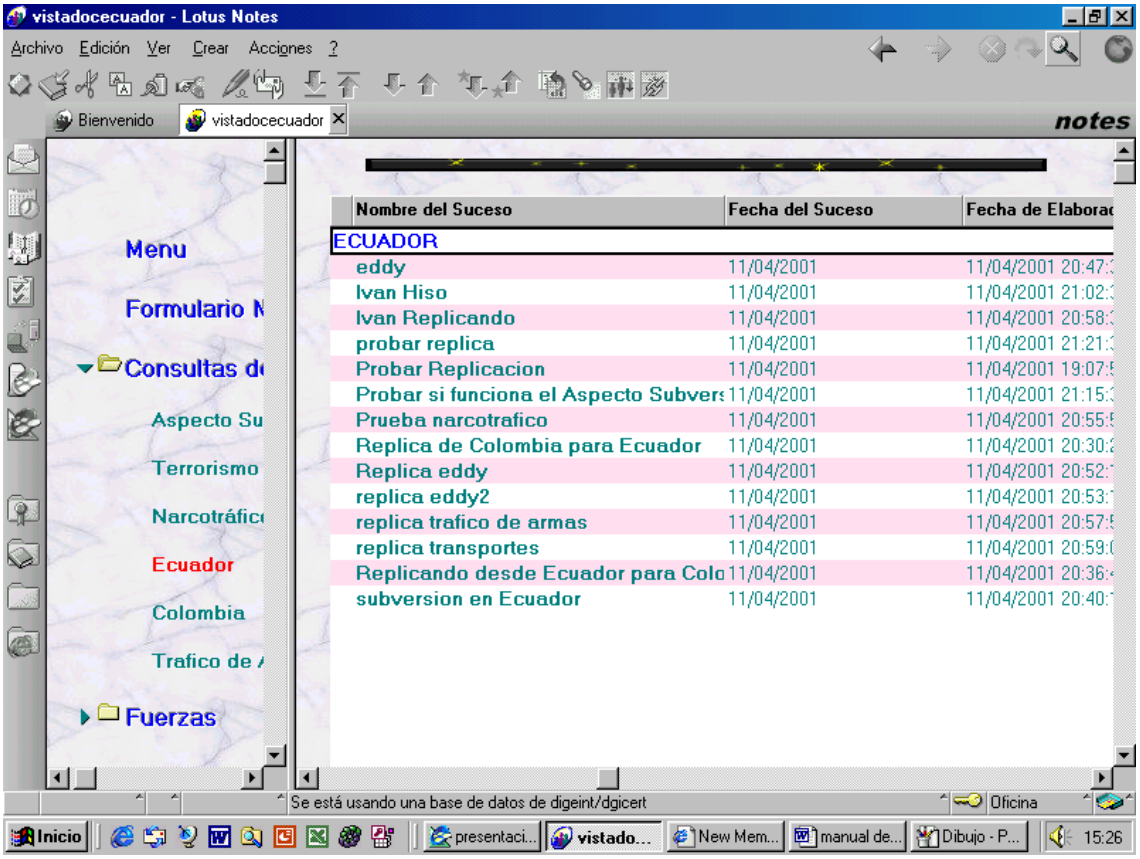


Grafico A-20(Presentación de una consulta por País)

Luego que se ha desplegado todos los documentos que por ese caso se ha generado si deseamos mas al detalle se tiene que dar doble clic sobre el documento y este se despliega presentando toda la información que este contenga. ver grafico A-21

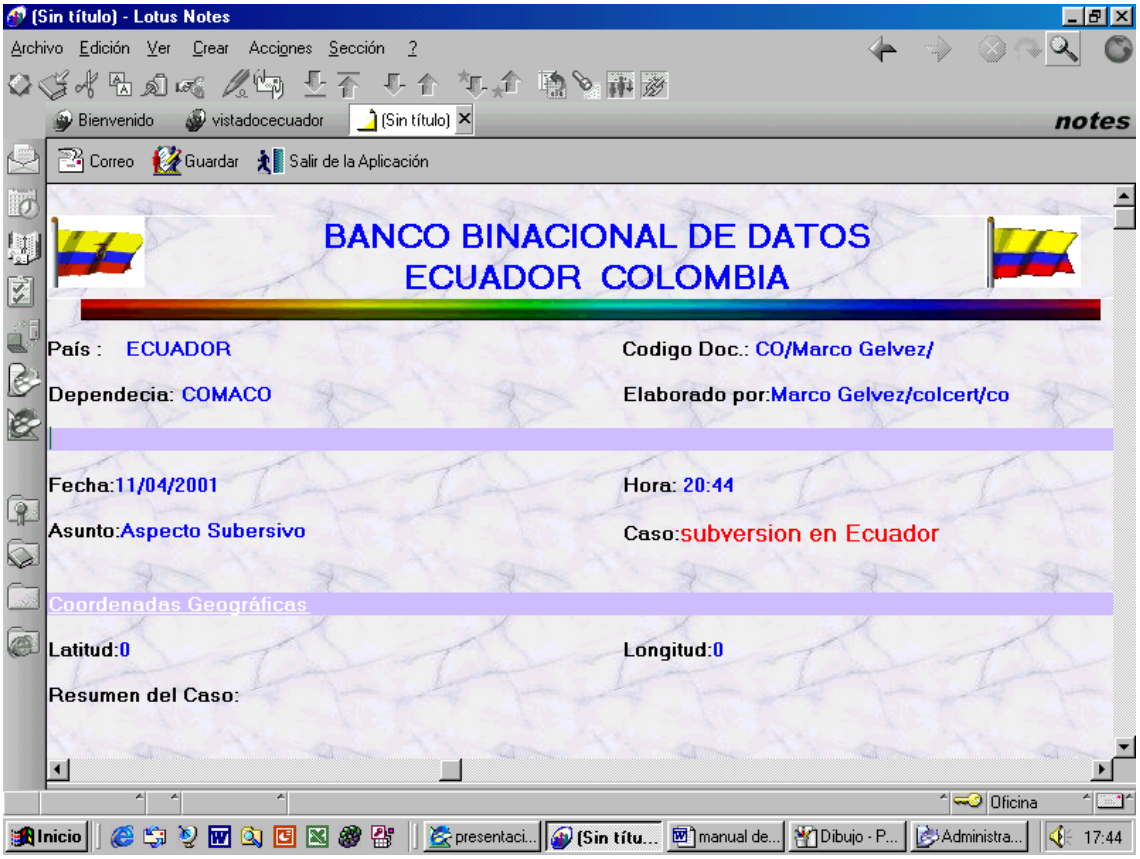


Grafico A-21(Presentación del documento consultado)

Los mismos pasos se repiten en las demás opciones de consulta.

Nota: Para los usuarios tiene la misma metodología de consulta, sin importar que perfil haya sido asignado por el administrador en su creación.

Consulta por mes de acontecimientos

En esta alternativa nos presenta un tipo de consulta por mes en el que podemos visualizar todos los documentos generados en el año.

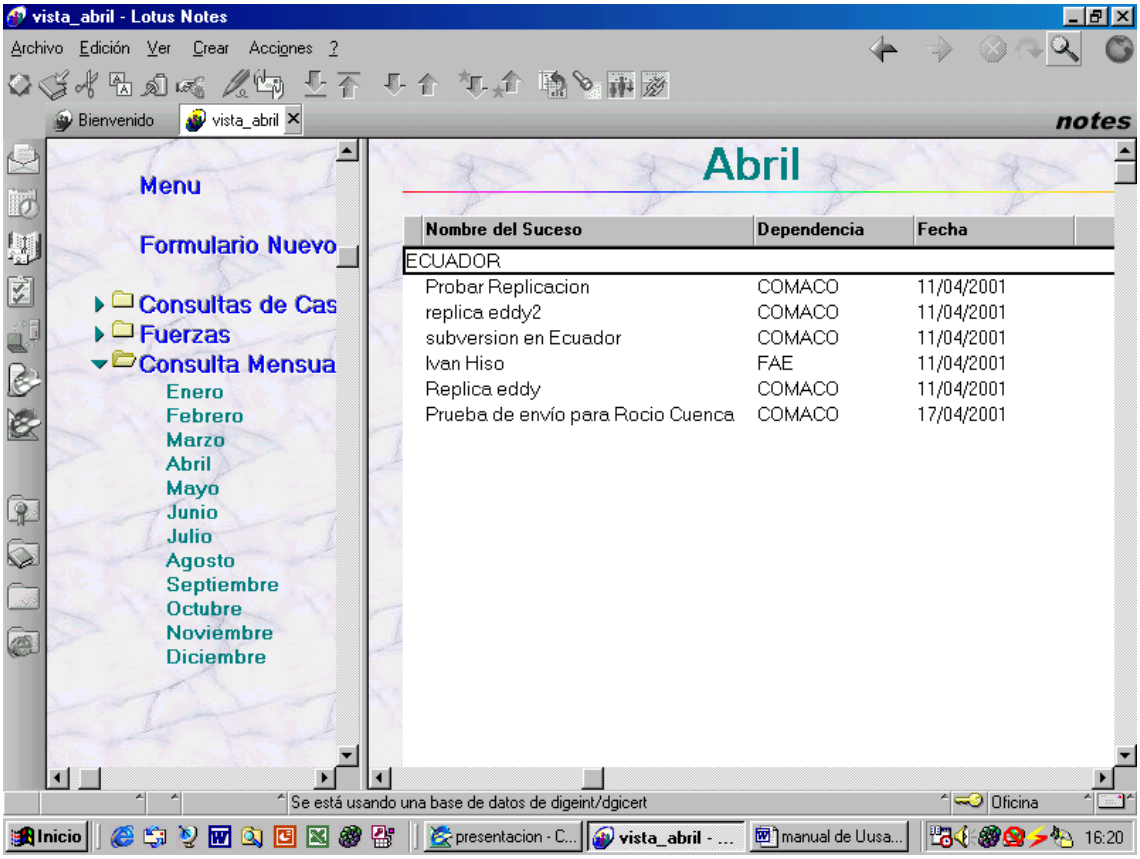


Grafico A-22(Pantalla principal de consulta por mes)

1.2 USUARIOS

Para los Usuarios se implemento una estructura idéntica de ingreso de información lo que si tiene modificaciones es en la parte de consultas que esta tiene solo consultas por tipo de casos que esta unidad o usuario genero no puede consultar información de otros usuarios o dependencias ni consultas generales de la base de datos pues estos permisos solo los tiene el administrador ver grafico A-23.

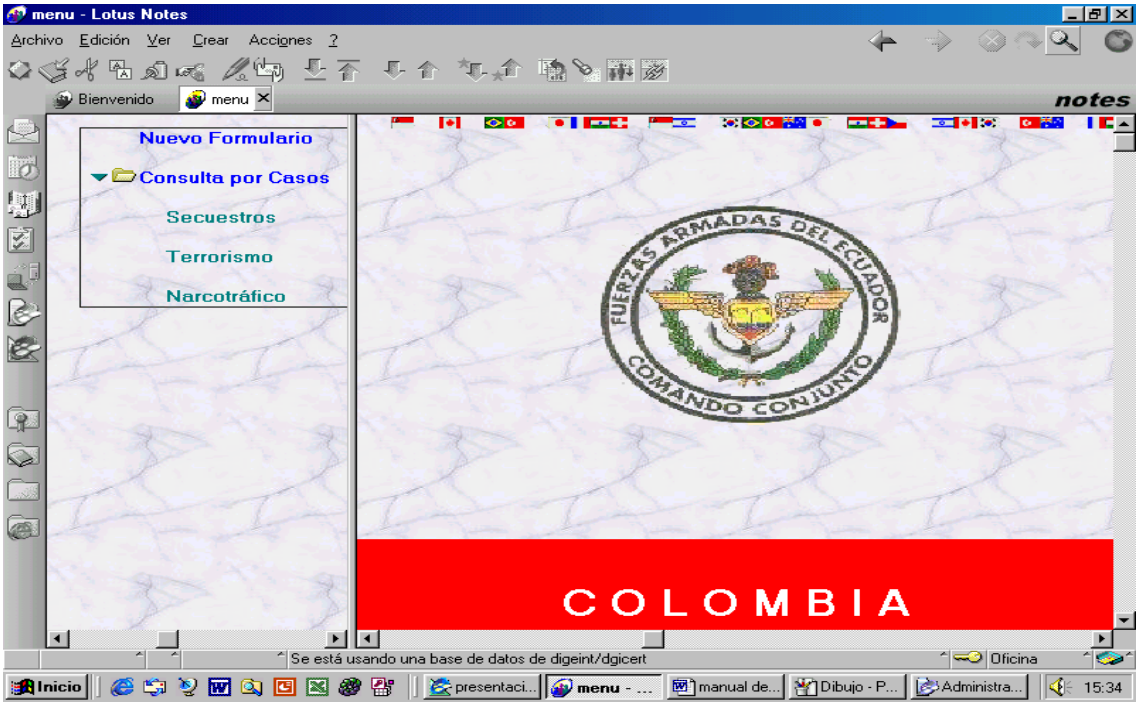


Grafico A-23(Pantalla principal de Usuario)

De igual manera para las consultas como el caso del administrador pero con las limitaciones del usuario . Grafico A-24

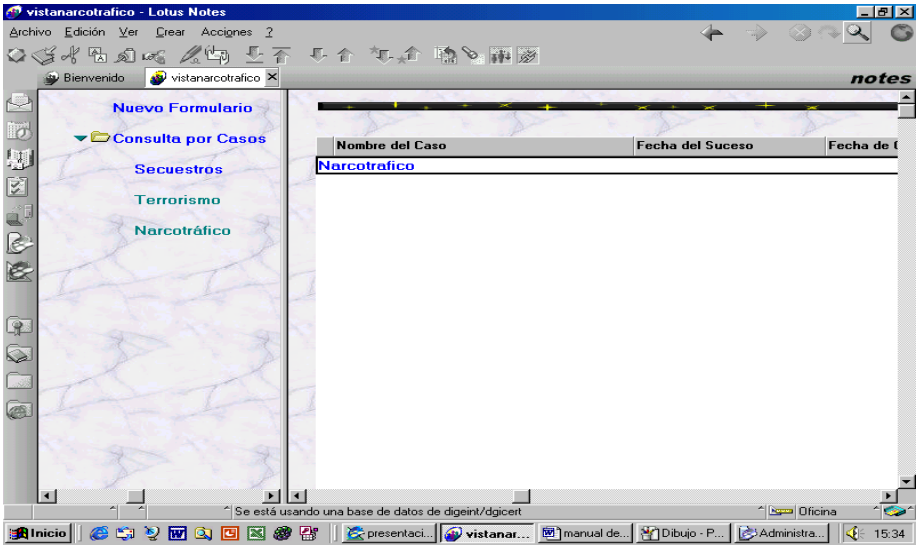


Grafico A-24(Pantalla principal de consulta por casos)

B. PASOS PARA INGRESAR BASE DE DATOS DOCUMENTAL

1. Requerimientos

HARDWARE:

64 MB de RAM, mínimo

Pentiun III de 500 Mhz., mínimo

Disco Duro 10 GB, mínimo

CD ROM 52 X mínimo

Floppy 3 1/2

Fax/Modem 56 Kbps

Monitor color 14 pulg.

Teclado

Mouse

SOFTWARE S.O.:

Windows 95/98/2000/NT/XP

Lotus Notes Versión 5.0 o superior

COMUNICACIONES

Línea telefónica

Cuenta de Internet

2.- Ingreso al aplicativo

Una vez ingresado en Windows, elegir Inicio/Programas/Lotus Aplication/Lotus Notes como se muestra en el grafico B-1

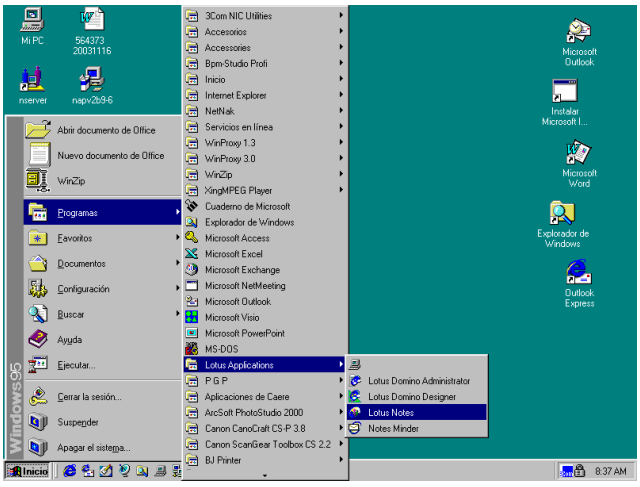


Grafico B-1 (Como iniciar Lotus)

3.- Si le pide insertar el diskette u otro dispositivo de almacenamiento de autenticación favor insertarlo, caso contrario le pedira un pasword, favor ingresar **admcolombia.**

4.- Dar un click en File/tools/switch ID

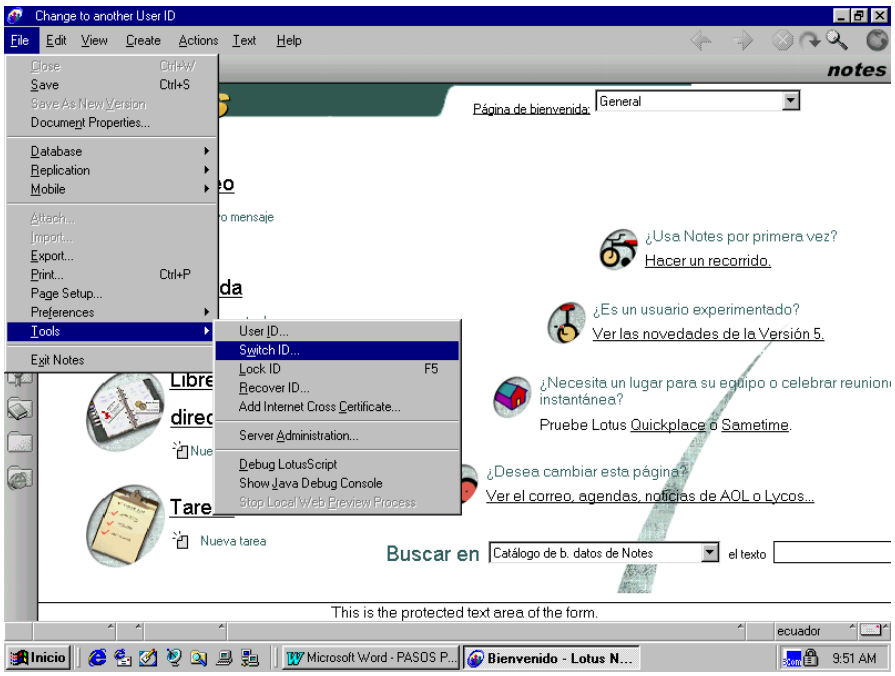


Grafico B-2 (Pantalla de cómo cargar el aplicativo)

5.- Elegir el archivo ID que se encuentra en el diskette Fmcolomb.id, o en otro directorio (archivo adjunto)

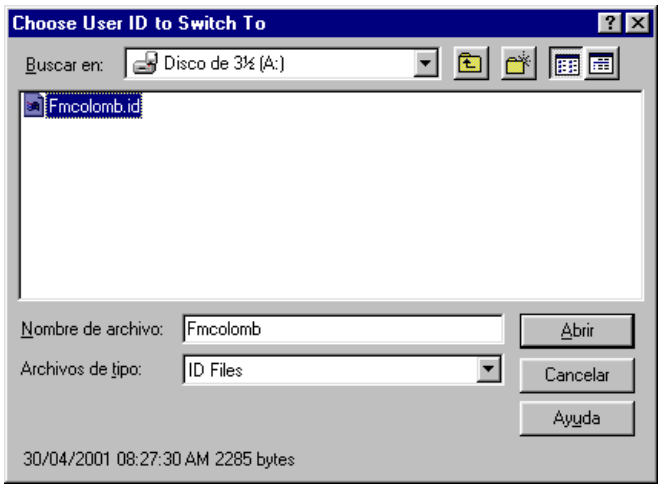


Grafico B-3 (Pantalla ingreso de usuario)

6.- Poner abrir y digitar la clave ffmmcolombia

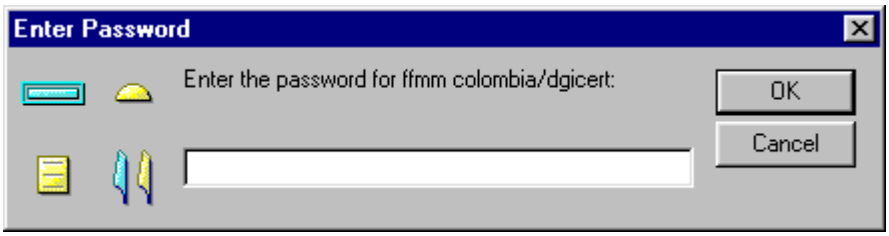


Grafico B-4 (Pantalla ingreso password del usuario)

7.- Inmediatamente aparecerá la siguiente pantalla

Grafico B-5 (Pantalla principal de Administrador)

8.- Configuración para ingresar a la base de datos documental.: File/Mobile/Locations

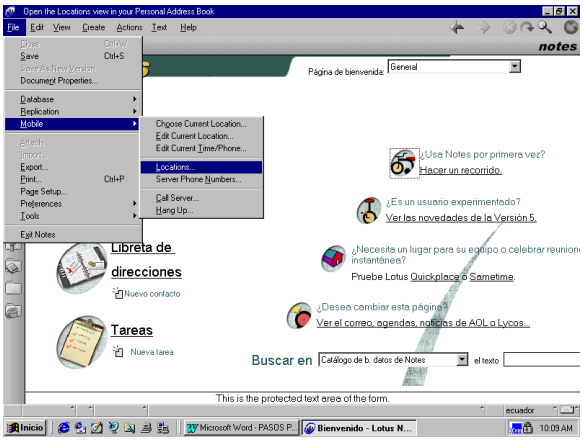


Grafico B-6 (Pantalla Ingreso al aplicativo)

9.- Elegimos Conexiones/Agregar conexión .de la siguiente pantalla

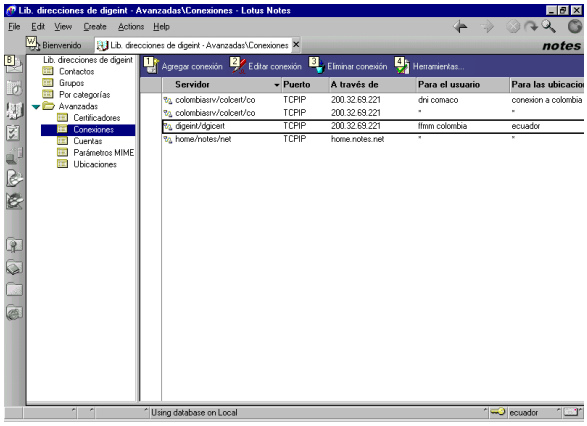


Grafico B-7 (Agregar conexión al servidor)

10.- Aparecerá la siguiente pantalla en donde ingresamos:

Tipo de conexión Red Local

Usar puerto LAN TCP/IP (activar)

Nombre del servidor digeint/dgicert

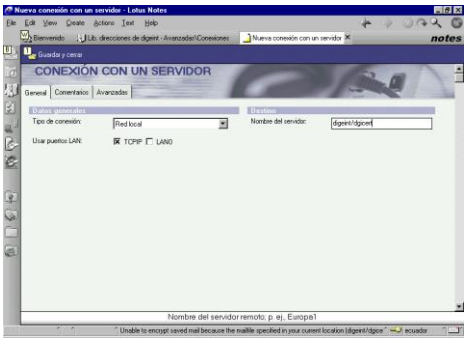


Grafico B-8 (Configuración de conexión con el servidor)

11.- En la pestaña de avanzadas ingresamos:

Solo desde estas ubicaciones ecuador

Sólo para el usuario ffmm colombia/dgicert (debe estar por defecto)

Prioridad de uso normal

Dirección del servidor destino 200.32.69.221

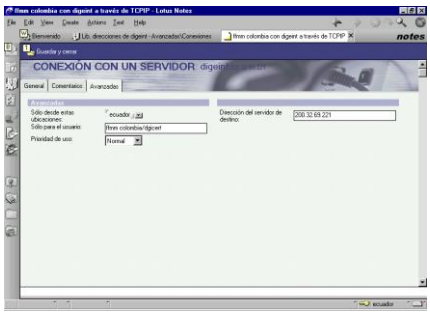


Grafico B-9 (Configuración adicional para conexión con el servidor avanzado)

12.- Posteriormente y en la pantalla del punto 9, nos dirigimos a ubicaciones y damos click en agregar ubicación e ingresamos los siguientes datos:

En pestaña General

Tipo de ubicación Red local

Nombre de la ubicación ecuador

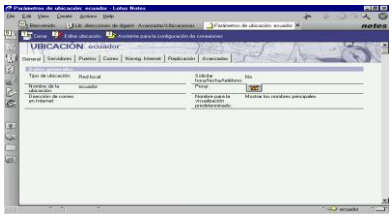


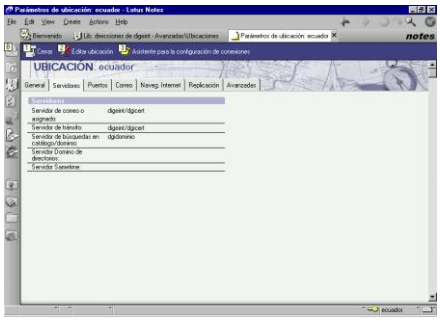
Grafico B-9 (Configuración adicional para conexión con el servidor general)

En la pestaña de servidores

Servidor de correo o asignado digeint/dgicert

Servidor de tránsito digeint/dgicert

Servidor de búsqueda en catalogo dgidominio



Dominio

Pestaña de puertos: Activar TCPIP

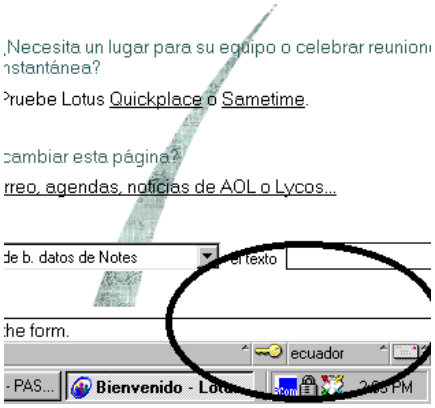
Pestaña Correo:

Ubicación del archivo de correo:	En el servidor
Archivo de correo:	mail\fcolombi.nsf
Dominio de correo de Notes:	dgidominio
Dominio de Internet para las direcciones de Notes al conectarse directamente a Internet:	
Escritura anticipada del nombre del destinatario:	Primero local y luego en el servidor
Activar la escritura anticipada del nombre del destinatario:	En cada carácter
Búsqueda del nombre del destinatario:	Detenerse tras hallar el primero
Enviar correo saliente:	A través del servidor Domino
Formato para los mensajes dirigidos a direcciones de Internet:	Texto enriquecido de Notes

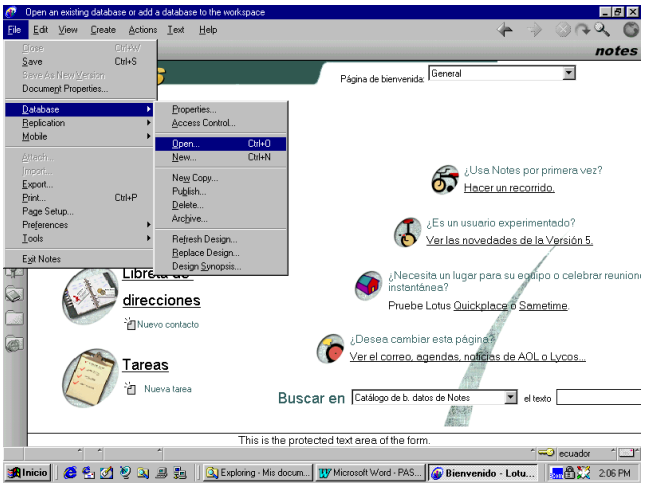
13.- Guardar y salir de Lotus Notes

14.- Realizar la Conexión a Internet con su empresa proveedora.

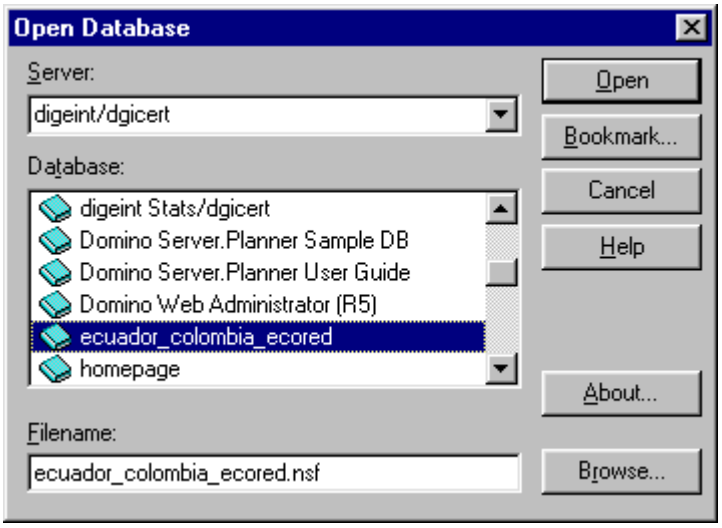
15. Iniciar nuevamente Lotus, ingrese su password, y asegurese que en la parte inferior derecha se encuentr en ecuador



16.- Dirigirse a File/Database/Open



17.- Digitar digeint/dgicert o 200.32.69.221, y elijo ecuador_colombia_ecored



18.- Dar click en Open, e inmediatamente aparecerá el aplicativo, y se podrá trabajar tal como se lo indica en el manual de operación entregado.