ESCUELA POLITÉCNICA DEL EJÉRCITO

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"ANÁLISIS Y DISEÑO DEL SISTEMA DE SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS (COMACO)"

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR:

GINA ALEXANDRA CAPILLA SALAZAR
EMPERATRIZ DE LAS MERCEDES SALDAÑA ALVARADO

SANGOLQUÍ, DICIEMBRE DEL 2005

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por GINA ALEXANDRA CAPILLA SALAZAR y EMPERATRIZ DE LAS MERCEDES SALDAÑA ALVARADO, como requerimiento parcial a la obtención del título de INGENIEROS EN SISTEMAS E INFORMÁTICA.

Sangolquí, Diciembre del 2005

Ing. Walter Fuertes D. MSC.

DEDICATORIA ESPECIAL

A Dios, por haberme sostenido en los momentos más difíciles y haberme permitido culminar mi carrera.

A mi Madre, la persona que siempre me ayudó a salir adelante y que he admirado mucho. A ella, por inculcarme el amor a Dios y haberme entregado cada día de su vida todo su amor, confianza y su comprensión sin importarle su propia vida. Nunca le olvidaré ya que siempre estará presente en mi corazón.
Que Dios la tenga en su gloria.

A mi abuelito, a mi padre y todos mis familiares que siempre me han apoyado.

Y también en forma especial a mi esposo por su comprensión y apoyo incondicional.

Mercedes Saldaña A.

DEDICATORIA ESPECIAL

A mi madre que además de darme la vida, ha estado conmigo todo este tiempo apoyándome incondicional y desinteresadamente, gracias a su amor, comprensión y sacrificio he logrado mi meta, la de llegar a ser una profesional. A esa mujer que es un ejemplo de fortaleza y de lucha por salir adelante sin desvanecer ante ningún obstáculo, a tí por ser la mejor madre.

A mis abuelitos que aunque no los tenga físicamente se que están conmigo de espíritu, mis dos angelitos que supieron inculcarme valores y principios para ser una buena profesional pero sobre todo una buena persona, a ellos que me dejaron su ejemplo de valentía, amor a la vida y a Dios, de lucha por conseguir lo que uno quiere, para ustedes papacitos que siempre estarán en mi corazón.

Gina A. Capilla Salazar

AGRADECIMIENTOS

En primer lugar agradecemos a Dios por habernos permitido culminar con éxito nuestra carrera.

A los Ingenieros Walter Fuertes y Hugo Montesdeoca, director y codirector respectivamente de esta tesis, les agradecemos de todo corazón por habernos guiado acertadamente en el desarrollo de la tesis.

Al Comando Conjunto de las Fuerzas Armadas, por habernos abierto sus puertas para la realización del presente trabajo; en especial al Coronel Fidel Castro, Jefe de GRUTEL.

A nuestros familiares y a todos nuestros amigos que de una u otra manera nos ayudaron en los buenos y malos momentos.

Mercedes Saldaña A. **Gina Capilla S.**

RESUMEN

El presente trabajo tiene como objetivo principal realizar el diseño de un modelo de seguridad para la red de datos del Comando Conjunto de las Fuerzas Armadas (COMACO), Institución Militar que por su función de salvaguardar la integridad del Ecuador, maneja información confidencial, por lo tanto se debe analizar los niveles de seguridad que poseen y con el apoyo de las medidas, técnicas, mecanismos y herramientas de seguridad, lograr un modelo de acuerdo a las necesidades de la Institución.

La metodología a utilizar para el diseño de la red segura de COMACO es el modelo SAFE de CISCO, el mismo que presenta una estructura modular (agrupa componentes y funcionalidades de la red en módulos), por lo que el modelo puede ser tratado de manera independiente, obteniendo ventajas como escalabilidad, gestión de seguridad y calidad de servicio. Para que este modelo funcione correctamente es necesario definir las políticas de seguridad que serán detalladas al final del proyecto.

SUMMARY

The principal objective of this work is to make the design of a security model for the data base of the “Comando Conjunto de las Fuerzas Armadas” (COMACO), Military Institution which for its function of keeping the integrity of Ecuador, manages confidential information and for this it should analyze the security levels that it has and they can manage this with the support of security levels, techniques, mechanisms and tools to get a model which covers its necessities.

The method to be used for the design of a security net of COMACO is the SAFE model of CISCO, which presents a modular structure (groups components and functionalities of the net in modules), for this reason the model can be treated in an independent way, obtaining advantages like to scale, security action and service quality. To make this model to work correctly, it is necessary to define the security policies which will be detailed at the end of the project.

CAPÍTULO 1

INTRODUCCIÓN

1.1. INTRODUCCIÓN

Uno de los avances tecnológicos más importantes de los últimos años es el desarrollo de Internet, formado por un conjunto de redes de ordenadores interconectadas, lo cual es potencialmente beneficioso para los usuarios que desde su computador tienen acceso a toda la información que existe; y para las instituciones porque con un sólo servidor pueden conectarse al Internet mediante el protocolo TCP/IP, familia de protocolos para que todos los ordenadores de una red se puedan comunicar entre sí.

La interconexión entre redes ocasiona riesgos en la Red de Área Local (LAN), los cuales pueden ser ataques que provienen desde el Internet o inclusive computadores personales internos, tales como virus, caballos de troya, gusanos o hackers que aprovechando las deficientes medidas de seguridad tomadas por administradores y usuarios, vuelven vulnerables a las redes de datos.

Para minimizar los riesgos es necesario determinar medidas de seguridad, ubicando una barrera entre el Internet y la LAN por medio de: la administración correcta de los servicios, accesos remotos seguros, políticas de administración de usuarios y la seguridad en la red interna.

1.2. PROBLEMÁTICA

El Comando Conjunto de las Fuerzas Armadas (COMACO), es la entidad que se encarga de organizar, entrenar, equipar y mantener el poder militar, participar en los procesos que garanticen la seguridad de la nación y propendan su desarrollo, con la finalidad de contribuir a la consecución y mantenimiento de los objetivos nacionales permanentes, de acuerdo a la planificación prevista para tiempo de paz, de conflicto y de guerra.

COMACO es quien contacta directamente al Proveedor de Internet y adquiere el servicio. El Departamento de Telemática perteneciente a COMACO es el encargado de asignar el ancho de banda para cada una de las Fuerzas Armadas (Aérea, Naval y Terrestre), la Honorable Junta, el Ministerio de Defensa, el Departamento de Inteligencia y COMACO. Cada una de éstas entidades son responsables de la administración de su ancho de banda.

Cabe destacar que COMACO posee personal administrativo y sus propios servidores para la administración de la información, los cuales son:

- Un Servidor de Correo (MAIL), el cual ofrece el servicio de correo interno y externo.
- Un Servidor de Dominio (DNS), para resolver los nombres, es decir, a cada dirección IP se le puede asignar un nombre, que debe ser único.
- Un Servidor que posee dos servicios: Acceso a Internet, mediante el cual los usuarios pueden ingresar al Internet; y Servicio de Acceso Remoto(RAS), para la conexión de usuarios externos.
- Un Servidor para el ingreso a Internet en el área de Sistemas del Edificio de COMACO, el mismo que funciona como gateway o puerta de enlace para que todos los usuarios del Edificio tengan Internet.

COMACO se divide en siete Direcciones; la Dirección de Telecomunicaciones se encarga del mantenimiento de los servidores, sin existir un Administrador de Red, por lo tanto no poseen políticas de seguridad ni de administración de servidores, encontrando los siguientes problemas:

- No existe políticas de cuentas de usuarios.

- No se ha actualizado la versión del Kernel de los sistemas operativos, de servidores y equipos de comunicación, debido a que no están definidas las funciones para ejecutar esta acción.

- No existen políticas de backups, es decir no se respalda la información de los servidores, así como tampoco existe un plan de contingencias en caso de fallar los servidores principales.

- No se ha adquirido un contrato de servicio de mantenimiento para los servidores, cualquier problema que se presente lo resuelve COMACO, asumiendo toda la responsabilidad.

- No existe un servidor de antivirus centralizado, es por este motivo que no se controlan los virus y los usuarios son los encargados de la actualización de su antivirus, acción que ejecutan esporádicamente. Sólo se ha implementado un antivirus en el servidor de correo para que examine los mails, el mismo que trabaja conjuntamente con el MailScaner.

- Tanto el Router como el Switch cumplen con las principales funciones de seguridad, sin embargo solo fueron configurados una vez y no tienen políticas de creación de claves, no se actualizan versiones de los sistemas operativos, no se realiza un seguimiento de la política de control implementada.

- Se observó que no disponen de un cuarto de comunicaciones con sus respectivas seguridades físicas, por lo que cualquier persona del departamento o ajeno a éste puede tener acceso físico a los equipos.

1.3. JUSTIFICACIÓN

Como se manifestó anteriormente la red de datos tiene problemas de seguridad a nivel administrativo y tecnológico, además a COMACO le interesa proteger la información que manejan sus servidores, la misma que es de índole castrense y confidencial, de las amenazas o ataques provenientes desde el exterior o interior de la LAN, motivo por el cual es conveniente la realización del presente trabajo.

Se cuenta con el auspicio y aprobación de la Dirección del Comando Conjunto de las Fuerzas Armadas (COMACO) al mando del Ing. Fidel Castro (CRNL. EMC.) COMANDANTE DEL GRUPO DE TELECOMUNICACIONES.

1.4. OBJETIVOS

1.4.1. Objetivo General

Analizar y diseñar el sistema de seguridad informático de la red de datos del Comando Conjunto de las Fuerzas Armadas (COMACO) a fin de salvaguardar la integridad de la información manejada por la institución.

1.4.2. Objetivos Específicos

- Analizar la situación actual de la red de datos de COMACO.
- Determinar las vulnerabilidades de la red de datos de COMACO.
- Comprobar los niveles de seguridad que posee la red de datos de COMACO.
- Establecer las políticas de seguridades para un manejo adecuado de la red de datos de COMACO.
- Diseñar el sistema de seguridad basado en las políticas de seguridad establecidas.

1.5. ALCANCE

Se realizará el diseño del Sistema de Seguridad para la Red de COMACO optimizando los recursos que poseen. El diseño deberá regirse al presupuesto que la institución maneja.

La función de COMACO es asignar un ancho de banda a las demás instituciones de las Fuerzas Armadas, siendo responsabilidad de cada una de ellas el buen manejo del canal de acceso hacia Internet.

Al final del proyecto se entregará un documento de Políticas de Seguridad que luego serán implementadas en los respectivos equipos por personal propio de la institución, además implicará cambios administrativos, los mismos que dependerán de la Institución Castrense.

1.6. ESTRUCTURA DEL PROYECTO

El presente documento ha sido estructurado por seis capítulos enumerados a continuación:

- El Capítulo 1 expuesto anteriormente, en donde se describe la introducción y un enfoque general de la tesis.

- Continúa en el Capítulo 2, donde se realiza un análisis del marco teórico para determinar las medidas, técnicas, mecanismos, herramientas y los estándares de seguridad a ser utilizados en el proyecto.

- Posteriormente en el Capítulo 3 se describe la situación actual de la red de datos de COMACO para determinar las vulnerabilidades.

- Consecutivamente en el Capítulo 4 se realiza el diseño de un sistema de seguridad para la red de datos de COMACO.

- Para continuar con el Capítulo 5 en el cual se define las políticas de seguridad que serán el soporte para el esquema de la propuesta de la red segura.

- Finalmente en el Capítulo 6 se determinan las conclusiones y recomendaciones obtenidas en el transcurso del desarrollo del trabajo.

CAPÍTULO 2

MARCO TEÓRICO - SEGURIDAD INFORMÁTICA

2.1. INTRODUCCIÓN

En la actualidad, la utilización de la seguridad informática se ha incrementado, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

"A mas de proteger y conservar los activos de la organización, de riesgos, de desastres naturales o actos mal intencionados, la seguridad informática es imprescindible ya que con esta se reduce la probabilidad de las pérdidas, a un mínimo nivel aceptable, a un costo razonable y asegurar la adecuada recuperación"[2.1.].

Para cumplir con este propósito se debe implementar controles adecuados para las condiciones ambientales que reduzcan el riesgo por fallas o mal funcionamiento del equipo, del software, de los datos y de los medios de almacenamiento.

Consecuentemente es importante conocer las maneras de minimizar dichas amenazas para lo cual es necesario considerar algunos conceptos que ayudarán a entender mejor la Seguridad Informática, dentro de los cuales se consideran los siguientes, que serán descritos en el transcurso de este capítulo:

[2.1.] http://www.monografias.com/trabajos/hackers/hackers.shtml

- ✓ Medidas
- ✓ Técnicas
- ✓ Mecanismos
- ✓ Herramientas
- ✓ Norma ISO 17999

2.2. MEDIDAS DE SEGURIDAD

Las medidas de seguridad son un conjunto de acciones a seguir, para obtener un óptimo funcionamiento en los aspectos eléctrico, físico y ambiental de la institución. Por ejemplo, debe existir controles adecuados para las condiciones físicas que reduzcan el riesgo por fallas o mal funcionamiento del equipo, del software, de los datos y de los medios de almacenamiento. También la seguridad en los sistemas de datos es implementada con el objetivo de proteger la información controlando el acceso y uso no autorizado, modificación o destrucción de datos almacenados o transmitidos por un sistema computacional.

2.2.1. Medidas Eléctricas

Para que el funcionamiento de un centro de datos/cuarto principal de equipos sea el adecuado se debe realizar un análisis de las instalaciones eléctricas y conexiones ya existentes para no tener problemas a futuro.

Se debe tener cuidado con las conexiones al implementar aparatos que protejan a equipos de las variaciones de voltaje, ya que en nuestro país el suministro de energía eléctrica es inestable, y se convierte en un factor negativo cuando se manejan circuitos electrónicos, los cuales son sensibles ante dicha inestabilidad, causando incluso que estos dejen de funcionar. Dentro de los problemas comunes se observa los siguientes:

- **Blackout:** Pérdida de electricidad (apagón).
- **Brownout:** Período prolongado de baja tensión.
- **Noise:** Interferencia aleatoria que afecta a un dispositivo.
- **Sag:** Período reducido de baja tensión
- **Spike:** Pico de alto voltaje momentáneo.

- **Surge:** Período prolongado de alta tensión
- **Transient:** Ruido de línea, interferencia a voltaje normal.

Es por esto que se requiere tomar medidas para prevenir cualquier inconveniente que se presente, tales como:

a) **Circuitos Dedicados:** Son circuitos de energía eléctrica específicos para las necesidades que presenten las instituciones u organizaciones, éste debe poseer un acceso controlado a:

- ***Paneles de Distribución Eléctrica:*** Son las denominadas cajas térmicas y su tamaño será de acuerdo al número de circuitos que se necesite.

- ***Master Circuit Breakers***: El cual controla la activación y desactivación de cada uno de los circuitos creados.

- ***Cableado Eléctrico:*** Son los elementos que permiten la conexión para cada circuito creado de acuerdo a las necesidades de la organización.

b) **Sistema de Energía de Emergencia[(2.2.)]:** Como su nombre lo dice es un sistema de energía utilizado en caso de emergencia, es decir, cuando la energía normal no esté en funcionamiento, para el cual se consideran los siguientes equipos:

b.1) UPS (Uninterruptible Power Supply): Es una fuente de alimentación de energía alterna que funciona a base de baterías, además tiene como objetivo la protección contra picos de tensión. El UPS necesita un mantenimiento preventivo y correctivo para que su funcionamiento sea correcto, y para la elección del UPS adecuado dependerá de la carga que se le vaya a dar. Dentro de los mismos se encuentran los siguientes:

- ***Sistema UPS "de reserva"***: Utilizado para computadoras personales. El switch de transferencia está programado para seleccionar la entrada de CA (corriente alterna)

(2.2.) http://www.itlp.edu.mx/publica/tutoriales/instalacelectricas/43.htm filtrada como fuente de energía primaria, y cambiar al modo de batería/inversor como fuente de respaldo, en caso de que falle la fuente primaria. Cuando esto sucede, el switch de transferencia debe conmutar la carga a la fuente de energía de respaldo de batería/inversor. El inversor sólo se enciende cuando falla la energía; de ahí el nombre “de reserva”.

- ***Sistema UPS “de línea interactiva”***: Utilizado por pequeñas empresas, servidores departamentales y para la Web. En este tipo de diseño, el conversor (inversor) de batería a alimentación CA siempre está conectado a la salida del sistema UPS. Cuando falla la potencia de entrada, el switch de transferencia se abre y el flujo de energía se produce desde la batería hasta la salida del sistema UPS. Con el inversor siempre encendido y conectado a la salida, este diseño ofrece un filtro adicional y produce transientes de conmutación reducida comparado con el sistema UPS de reserva.

- ***Sistema UPS “de doble conversión en-línea”:*** Utilizado por encima de los 10 kVA. Esta tecnología de UPS es igual a la de reserva, excepto por el hecho de que el acceso de energía primaria es el inversor en vez de la red de CA. En este tipo de diseño, durante una falla en la alimentación CA de entrada, el funcionamiento en-línea significa que no existe tiempo de transferencia.

- ***Sistema UPS “con conversión delta en-línea”***: Es una nueva tecnología, creada para evitar los inconvenientes del sistema UPS de doble conversión en-línea. La conversión delta en-línea posee un inversor principal que proporciona una tensión de carga regulada y constante, pero también aporta energía a la salida. Durante una falla o alteraciones en la alimentación CA, se comporta del mismo modo que la doble conversión en-línea.

b.2) Generador Eléctrico: Es un dispositivo que genera energía eléctrica de emergencia cuando la normal no está distribuyéndose; el cual requiere combustible, mantenimiento preventivo y correctivo para su funcionamiento adecuado. Como para toda instalación siempre debe existir un control manual para que pueda ser operado y desconectado si la situación así lo requiera.

- ***Transferencia Manual:*** Una vez que la energía ha dejado de fluir, es necesario que una persona manipule el switch para que éste funcione.

- ***Transferencia Automática:*** Es programado para que después de un determinado tiempo de que haya fallado la energía, éste entre a funcionar.

Es importante considerar los siguientes elementos en el momento de elegir el generador más idóneo, de esto dependerá también su costo.

- ✓ Iluminación.
- ✓ Sistemas de control de acceso físico.
- ✓ Sistemas de protección y detección de incendios.
- ✓ Computadoras, servidores, etc.
- ✓ Dispositivos de comunicaciones
- ✓ Sistemas telefónicos
- ✓ Aire Acondicionado

2.2.2. Medidas Físicas

La selección de la ubicación del cuarto principal de equipos debe realizarse buscando un lugar apropiado, el cual estará lejos del área del tránsito de gran escala, tanto terrestre como aérea; también lejos de equipos eléctricos tales como radares y equipos de microondas, etc. En la medida de lo posible, debe ser construido en un edificio separado, de forma que facilite el control de acceso y disminuya el riesgo. El objetivo es mantenerlo tan lejos como se pueda de cualquier tipo de amenaza.

La seguridad informática no se debe limitar únicamente al hardware y software, también le compete el uso adecuado de las instalaciones donde se manejan, es decir implementar políticas de seguridad para el acceso físico, entonces se recomienda tomar en cuenta lo siguiente:

- Los elementos involucrados en la selección de un sitio seguro, su diseño y configuración.

- Los métodos para asegurar una instalación contra acceso no autorizado,
- Los métodos para asegurar el equipamiento contra robos dirigidos a ellos y a la información que contienen,
- Las medidas de seguridad y ambientales necesarias para proteger el personal, las instalaciones y los recursos asociados.

Para cumplir con lo descrito anteriormente y desarrollar un sistema de seguridad idóneo se debe considerar los siguientes elementos:

a) **Control de Acceso Físico:** Para realizar el control en el acceso físico hacia las instalaciones o hacia el cuarto principal de equipos se debe tomar en cuenta los siguientes elementos:

   - ***Guardias:*** Personas encargadas de custodiar las instalaciones del edificio o específicamente el Cuarto principal de equipos.
   - ***Ventanas de protección:*** Rejas de protección para las ventanas y evitar el ingreso hacia el Cuarto principal de equipos.
   - ***Llaves y cerraduras:*** Instrumentos metálicos que sirven para asegurar las puertas y evitar el acceso de personas no autorizadas hacia las instalaciones.
   - ***Control de acceso al Cuarto principal de equipos:*** Se requiere identificar a las personas que ingresen al centro de datos ya que deben hacerlo solo las autorizadas, por lo que se hace necesario la utilización de:
     - ✓ *Tarjetas de Acceso*, las mismas que pueden contener una foto incorporada, deben permitir ser codificadas digitalmente y su lectura será mediante lectores de proximidad.

- ✓ *Sistemas Biométricos*, incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física (huella digital) y la transforma en una secuencia numérica.

- ➢ ***Sistemas de monitoreo y detección de intrusos:*** Sistema que permite observar las personas que ingresan al Departamento de Sistemas y detectar a las que no están autorizadas. Se debe utilizar dispositivos de circuito cerrado de televisión, tales como monitores, cámaras y sistemas de intercomunicación conectados a un panel de control manejado por guardias de seguridad. Estos dispositivos permiten controlar áreas grandes, concentrando la vigilancia en los puntos de entrada y salida principalmente.

- ➢ ***Alarmas contra robos:*** Todas las áreas deben estar protegidas contra la introducción física. Las alarmas contra robos, las armaduras y el blindaje se deben usar hasta donde sea posible, en forma discreta, de manera que no se atraiga la atención sobre el hecho de que existe un dispositivo de alta seguridad. La construcción de puertas y ventanas deben recibir especial atención para garantizar su seguridad.

b) Control de Inventarios: **Para toda institución u organización es fundamental llevar periódicamente un inventario sobre las cosas que están a su cargo, más aún cuando se habla de equipos de computación, entonces se debe tener un control físico de PC's, laptops, servidores, equipos de comunicación, etc.**

2.2.3. Medidas Ambientales

Las condiciones ambientales son variables y para un Cuarto principal de equipos/Centro de datos es esencial controlar estos inconvenientes tomando en cuenta los aspectos detallados a continuación:

a) Aire acondicionado para centros de datos[2.3.]

El aire acondicionado es indispensable en el Cuarto principal de equipos, por el calor que emanan los dispositivos pueden ocasionar que las computadoras tengan que ser apagadas.

Teniendo en cuenta que las instalaciones de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Para que se realice una buena instalación del aire acondicionado se debe tomar en cuenta los siguientes aspectos:

- ✓ Capacidad del equipo de aire acondicionado
- ✓ Disipación térmica de las máquinas.
- ✓ Disipación térmica de las personas.
- ✓ Cargas latentes, aire de renovación.
- ✓ Pérdidas por puertas y ventanas.
- ✓ Transmisión de paredes, techos y suelo.
- ✓ Disipación de otros aparatos.

Las entradas de aire fresco no deben estar al nivel del suelo y deben colocarse lejos de las áreas donde haya polvo. Deben utilizarse los filtros adecuados para proporcionar aire limpio al cuarto principal de equipos.

El aire acondicionado para la sala de cómputo deberá ser independiente del aire general del edificio. El calor disipado por los diferentes dispositivos de cómputo, obligan a necesitar aire frío todo el año.

[2.3.] http://www.equiposysoluciones.com/AreasE1.asp?aid=3

La alimentación eléctrica deberá provenir directamente desde la planta de generación de energía eléctrica para emergencia, ya que el encendido y apagado automático de motores y compresores ocasionaría una disminución en el voltaje y ruido eléctrico al equipo de cómputo.

- ***Distribución del aire en la sala***

Los componentes de las máquinas se refrigeran, normalmente, mediante la circulación rápida de aire por ventiladores. La entrada de aire se efectúa por debajo de las máquinas a través de las rejillas. El aire caliente es expulsado por la parte superior de las máquinas. Toda esta instalación debe tener un control de apagado manual ya que nunca se puede confiar totalmente en los equipos.

b) Protección contra el agua

Las computadoras, máquinas y equipo en general no se deben colocar en sótanos o en las áreas de planta baja, sino, de preferencia, en las partes altas de una estructura de varios pisos. Claro que la mejor opción es no colocar el cuarto principal de equipos en áreas donde el riesgo de inundación sea evidente.

Los daños por inundación o agua son ocurridos tras la ruptura de cañerías o por el bloqueo del drenaje. Por lo tanto, la ubicación de las tuberías en la construcción de las instalaciones de cómputo y equipo es una decisión importante (no debe ponerse por encima de las áreas donde se colocan los equipos). El daño causado por el drenaje bloqueado es un riesgo cuando el equipo se coloca en algún sótano. Deben instalarse, si es el caso, detectores de agua o de inundación, así como también bombas de emergencia para resolver inundaciones inesperadas.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente, se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso del agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

c) Detección y supresión de incendios

La protección contra el fuego se puede conseguir a través de una correcta construcción del edificio (el cual debe procurarse que sea resistente al fuego). Sin embargo, siempre habrá materiales combustibles, así que es necesario asegurar que el equipo contra incendio esté disponible de forma inmediata y que se pueda controlar el fuego con relativa facilidad.

Si el área del equipo de cómputo tiene una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles y paredes de material no combustible mejorará la seguridad. El techo del centro de datos y el área de almacenamiento de discos y cintas magnéticos deben ser impermeables.

Los detectores de fuego y humo se deben colocar cuidadosamente en relación con los aparatos de aire acondicionado, ya que los conductores de éste pueden difundir el calor o el humo y no permitir que se active el detector. El detector de humo que se elija debe ser capaz de descubrir los distintos tipos de gases que desprendan los cuerpos en combustión. Algunos no detectan el humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad y, en consecuencia, los incendios producidos por un corto circuito tal vez no se detecten.

Los detectores de humo y calor se deben instalar en el centro de datos, junto a las áreas de oficina y dentro del perímetro físico de las instalaciones. Las alarmas contra incendios deben estar conectadas con la alarma central del lugar, o bien directamente al departamento de bomberos. Es importante que estos requerimientos no sólo se apliquen en la construcción de la sala de cómputo, sino también en las áreas adyacentes. Ver Figura 2.1

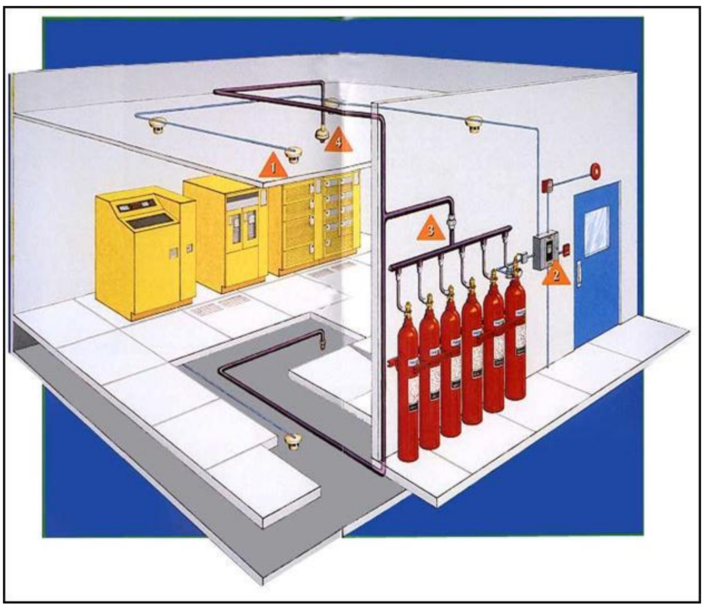


Figura 2.1 Ubicación física de los detectores de humo y alarmas.

La documentación de los sistemas, la programación y las operaciones también necesitan protección contra incendios. La destrucción de esta documentación puede imposibilitar el uso de programas o archivos de respaldo. Se deben establecer procedimientos que garanticen la actualización de toda la documentación como rutina y que las copias de seguridad se almacenen en un lugar lejano, así como las copias de seguridad de los programas y los archivos.

d) Evacuación

Para cualquier imprevisto que pueda ocurrir en la sala donde se encuentran los equipos siempre se debe tener un plan de evacuación o plan de contingencia. Un plan de contingencia es una "presentación para tomar acciones específicas cuando surja un evento o condición que no esté considerado en el proceso de planeación formal"[(2.4.)]. Es decir, se trata de un conjunto de procedimientos de recuperación para casos de desastre; es un plan formal que describe pasos apropiados que se deben seguir en caso de un desastre o emergencia. Materializa un riesgo, ya que se pretende reducir el impacto de éste.

Se recomienda establecer un modelo a partir de aquellas organizaciones que se han preocupado por su desarrollo y crecimiento, han establecido dentro de la estructura orgánica de la institución una función definida para la administración de riesgos y que han obteniendo estupendos resultados como una disminución considerable del impacto físico y económico de los riesgos dentro de la misma organización. El Plan de Contingencia contempla tres tipos de acciones las cuales son:

[(2.4.)] http://www.acnur.org/biblioteca/pdf/1653.pdf

- ***Prevención:*** Conjunto de acciones a realizar para prevenir cualquier problema que podría afectar la continuidad operativa, ya sea en forma parcial o total, del centro de procesamiento de datos, instalaciones auxiliares, recursos, información procesada, en tránsito y almacenada; con la finalidad de estar preparados para hacer frente a cualquier emergencia o eventualidad, de esta forma se reducirá su impacto, permitiendo restablecer a la brevedad posible los diferentes servicios interrumpidos.

- ***Detección:*** Deben contener el daño en el momento, así como limitarlo tanto como sea posible, contemplando todos los desastres naturales y eventos no considerados.

- ***Recuperación:*** Abarcan el mantenimiento de partes críticas entre la pérdida del servicio y los recursos, así como su recuperación o restauración.

2.3. TÉCNICAS

2.3.1. Autenticación y Autorización

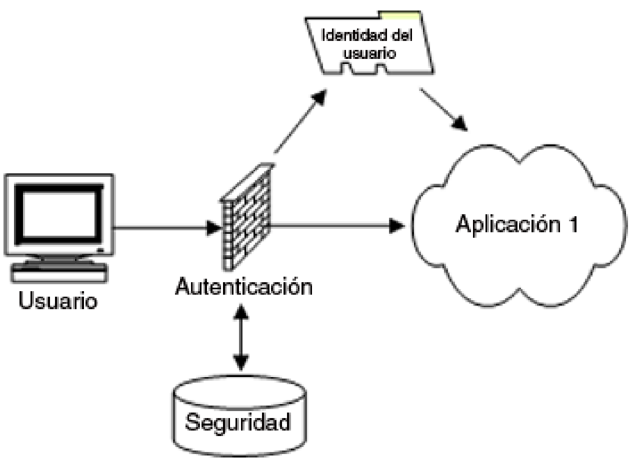


Figura 2.2 Autenticación, autorización y aplicaciones empresariales.

La *autenticación*[(2.5.)] *es* el proceso por el que se comprueba la identidad de alguien o algo, para ver si es lo que dice ser. Ese "alguien" o "algo" se denomina principal. La autenticación requiere pruebas de identidad, denominadas credenciales. Es por ello, que se

[(2.5.)] MERIKE, Kaeo. "Diseño de Seguridad en Redes". 1ra Edición, Pearson Educación S.A., Madrid-España,2003,Pag 19.

obliga al usuario final a especificar ciertas credenciales (normalmente un nombre de usuario y una contraseña) cuya validez se puede comprobar consultando una lista de datos conocidos. Si las credenciales son correctas, se autentica al usuario; de lo contrario, no se le autentica.

La *autorización* se la realiza una vez que se ha autenticado la identidad de un principal, deben tomar decisiones sobre la autorización. El acceso se determina comparando la información del principal con información de control de acceso, como listas de control de acceso (ACL). Es posible que los clientes tengan distintos grados de acceso. Por ejemplo, a algunos clientes se les permitirá un acceso total a todos los datos, mientras que a otros sólo se les permitirá acceso a un subconjunto de los datos y otros tendrán acceso de sólo lectura.

Aunque la autorización se suele considerar como una función de seguridad, en realidad las decisiones que determinan qué usuarios tienen acceso a qué funcionalidades son decisiones empresariales. Por consiguiente, las reglas que implementan la autorización son reglas empresariales, por lo que, en última instancia, el código de autorización seguirá la lógica empresarial y no la lógica de la seguridad. La figura 2.2 muestra la relación existente entre autenticación, autorización y aplicaciones.

2.3.2.Cifrado[(2.6.)]

Consiste en transformar un texto en claro (inteligible por todos), mediante un mecanismo de encriptación, en un texto incomprensible, gracias a una información secreta o clave de cifrado. Se distinguen dos métodos generales:

a) Cifrado Simétrico

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico[(2.7.)] o de clave secreta. Ver Figura 2.3.

[(2.6.)] MERIKE, Kaeo. “Diseño de Seguridad en Redes”. 1ra Edición, Pearson Educación S.A., Madrid-España,2003,Pag 5.
[(2.7.)] MERIKE, Kaeo. “Diseño de Seguridad en Redes”. 1ra Edición, Pearson Educación S.A., Madrid-España,2003,Pag 7.

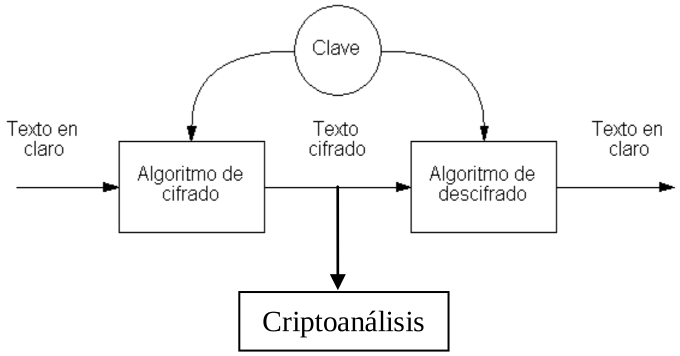


Figura 2.3 Cifrado Simétrico

Estos sistemas son mucho más rápidos que los de clave pública, resultan apropiados para el cifrado de grandes volúmenes de datos, siendo ésta la opción utilizada para encriptar el cuerpo del mensaje, para ello se emplean algoritmos como IDEA, RC5, DES, TRIPLE DES, RAS, etc.

b) Cifrado Asimétrico:

Por otro lado, cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico[2.8.] o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. Ver Figura 2.4.

[2.8.] MERIKE, Kaeo. "Diseño de Seguridad en Redes". 1ra Edición, Pearson Educación S.A., Madrid-España,2003,Pag 10.

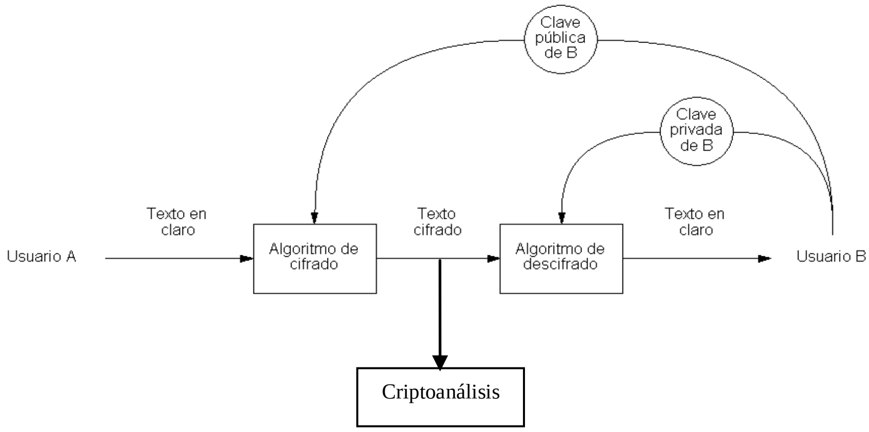


Figura 2.4 Cifrado Asimétrico

El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada ni descifrar el texto. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales, para ello se utilizan los algoritmos de RSA, Diffie-Hellman, etc.

En general, este criptosistema se emplea para cifrar las claves de sesión utilizadas para hacer el documento incomprensible, de modo que puedan ser transmitidas sin peligro a través de la red junto con el documento encriptado, para que en recepción éste pueda ser descifrado. Este sistema se emplea también para firmar documentos y autenticar entidades, como por ejemplo en las firmas digitales.

2.3.3. Firmas Digitales[2.9.]

Es un código informático que permite determinar la autenticidad de un documento electrónico y su integridad, es decir está constituida por un algoritmo de cifrado o encriptación. Una firma digital utiliza el mismo funcionamiento de "clave pública" o algoritmo asimétrico mencionado anteriormente, en donde la clave pública es capaz de identificar si la información proviene de una fuente fidedigna, o sea de la "llave secreta" en cuestión. Su modo de funcionamiento es el siguiente:

[2.9.] MERIKE, Kaeo. "Diseño de Seguridad en Redes". 1ra Edición, Pearson Educación S.A., Madrid-España,2003,Pag 16.

- Cada participante tiene un par de claves, una se usa para encriptar y la otra para desencriptar.

- Cada participante mantiene en secreto una de las claves (clave privada) y pone a disposición del público la otra (clave pública).

- El emisor calcula un resumen del mensaje a firmar con una función hash, la misma que sumariza o identifica un conjunto de información, además de garantizar la integridad de los textos. El resumen es un conjunto de datos de pequeño tamaño que tiene la propiedad de cambiar si se modifica el mensaje.

- El emisor encripta el resumen del mensaje con una clave privada y ésta es la firma digital que se añade al mensaje original.

- El receptor, al recibir el mensaje, calcula de nuevo su resumen mediante la función hash. Además desencripta la firma utilizando la clave pública del emisor obteniendo el resumen que el emisor calculó. Si ambos resúmenes coinciden entonces la firma es válida por lo que cumple los criterios ya vistos de autenticidad e integridad además del de no repudio ya que el emisor no puede negar haber enviado el mensaje que lleva su firma.

Existen dos métodos que las firmas digitales utilizan, los mismos que son detallados a continuación:

a) **Firma digital con árbitro:** Se utilizan criptosistemas de clave única (una sola llave para cifrar y descifrar) en donde dos usuarios con desconfianza mutua se encomiendan a un tercero. El emisor y el receptor tienen sus propias claves por lo que es el árbitro el encargado de recibir el mensaje, desencriptarlo con la llave del emisor, de esta forma el emisor y el receptor no necesitan compartirlas.

b) **Firma digital ordinaria**: En la cual el usuario envía directamente la firma al destinatario, y este debe poder comprobar la validez sin necesidad de un árbitro. A este método pertenecen los sistemas de firmas actuales que se basan en criptosistemas de clave pública.

2.4. MECANISMOS

2.4.1. Firewall

Un firewall es un dispositivo que funciona como barrera defensiva entre redes, permitiendo o denegando las transmisiones de una red a la otra. Normalmente es instalado en el punto donde la LAN se conecta con Internet, como un dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial. Todo tráfico externo pasa a través del firewall, así puede determinar si dicho tráfico es aceptable, de acuerdo a sus políticas de seguridad. Ver Figura 2.5.

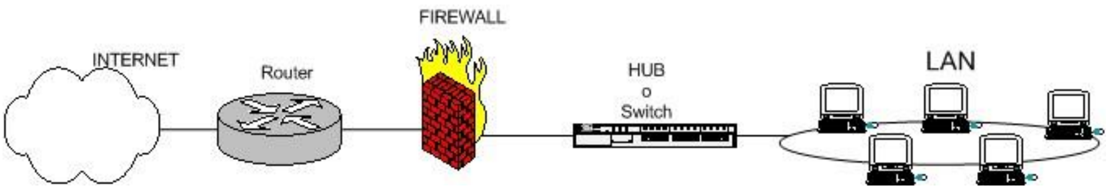


Figura 2.5 Ubicación Física del Firewall

Existen varios tipos de cortafuegos que se describen a continuación, en general, las diferencias entre ellos son la flexibilidad, la facilidad de configuración y la capacidad de manejo de tráfico.

a) Router con filtros[2.10.]

Aunque no puedan llamarse estrictamente cortafuegos, algunos fabricantes de routers ofrecen la posibilidad de filtrado flexible que constituye una solución económica, pero también la menos completa. Además, suelen ser complejos de configurar, lo que limita su utilidad.

Algunos virus informáticos y troyanos que circulan en la actualidad por correo electrónico emplean mecanismos de comunicación que pueden pasar este tipo de restricciones. Con

[2.10.] http://www.sarenet.es/ayuda/consejos/cortafuegos3.shtml una comunicación con el exterior, estos virus pueden propagarse a otras máquinas, enviar información privada del usuario al exterior (por ejemplo, archivos del disco), e incluso recibir instrucciones del exterior para lanzar ataques a otras redes, destruir información del ordenador infectado, etc.

b) Router con software de cortafuegos

El control de tráfico del router funciona como el de un cortafuegos, y puede impedir con garantías el flujo de información no autorizada, incluso los canales encubiertos empleados por los virus. Este tipo de cortafuegos no es flexible en cuanto a posibilidades de configuración que suele ser compleja, pero puede ser válido para configuraciones sencillas.

Dependiendo del modelo de router empleado, permite definir una zona desmilitarizada. Con estos equipos es posible crear redes privadas virtuales, aunque las prestaciones de cifrado no son elevadas, por tanto no son aptos para enlaces de mucha capacidad.

c) Cortafuegos dedicado

Existen equipos diseñados específicamente para trabajar como cortafuegos. La ventaja fundamental de estos aparatos es que todos sus componentes han sido diseñados con los mismos requisitos de seguridad, al contrario de lo que ocurre con otras soluciones.

Algunas marcas de firewalls son: Nokia, Checkpoint, CiscoPix, entre otros. Ver figura 2.6.

Figura 2.6 Cisco Pix Firewall

Algunos cortafuegos dedicados (o "cajas negras") disponen de circuitos que realizan funciones que de otra forma se harían por software, acelerando enormemente las prestaciones. El cifrado en las redes privadas virtuales es lo que más se beneficia de esto;

un router solamente puede hacerlo a velocidades moderadas, mientras algunos cortafuegos dedicados son capes de cifrar un flujo de datos a velocidades de hasta 100 Mbps.

La ventaja fundamental de algunos de ellos es la sencillez de configuración. Muchos problemas de seguridad se deben a errores provocados por equipos complicados o tediosos de configurar.

Otros modelos recientes pueden incorporar un antivirus dentro de la misma unidad, ofreciendo una primera línea de defensa cuyo funcionamiento no se ve afectada por los propios virus; algunos de ellos desactivan el software antivirus de los equipos afectados.

d) Software de cortafuegos que se ejecuta sobre servidor

Esta solución es la que suele ofrecer la mayor flexibilidad; todas las funciones se realizan en software, y por tanto es la que ofrece posibilidades de configuración, soportando varias formas de identificación de usuarios, filtros más configurables, etc.

Sin embargo, este tipo de cortafuegos es de instalación delicada. El sistema operativo sobre el que funcionan, que es un sistema de propósito general como Unix o Windows, no ha sido diseñado con los mismos requisitos de seguridad que el cortafuegos, y dependiendo de la instalación puede ser un punto débil lo suficientemente importante como para anular completamente los beneficios de seguridad del software de cortafuegos.

En cuanto a las redes privadas virtuales, las prestaciones de un cortafuegos de software son inferiores a las de uno dedicado con funciones de cifrado con circuitos dedicados. Es un tipo de seguridad efectiva en redes, porque intenta prevenir los ataques de usuarios externos a la red interna. Tiene múltiples propósitos como:

- ✓ Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- ✓ Prevenir los ataques.
- ✓ Restringir los permisos de los usuarios a puntos cuidadosamente controlados.

2.4.2 Proxy[2.11.]

Es un sistema intermediario entre hosts internos de una red e Internet, de forma tal que reciba las requisiciones de unos y se las pase a los otros, previa una verificación de accesos y privilegios.

Los sistemas Proxy son efectivos solo si se utilizan junto a métodos de restricción de tráfico IP entre clientes y servidores reales. De este modo, un cliente no podrá pasar el servidor Proxy para comunicarse con un servidor real utilizando este protocolo. La comunicación entre el programa cliente y el servidor Proxy puede realizarse de dos formas distintas:

- ***Programa Cliente:*** El cliente debe saber como opera el servidor Proxy, como contactarlo, como pasar la información al servidor real, etc. Se trata de un software cliente estándar que ha sido modificado para que cumpla ciertos requerimientos.

- ***Procedimientos de Usuarios:*** El usuario utiliza un cliente estándar para conectarse con un servidor Proxy y usa diferentes procedimientos (comandos del servidor Proxy) para pasar información acerca del servidor real al cual quiere conectarse. El servidor Proxy realiza la conexión con el servidor real

a) Clasificación de Servidores Proxy

Los servidores Proxy se dividen en: Proxy de Aplicación y de Circuito, información detallada en la Tabla 2.1.

Servidor Proxy de Aplicación	Llamado también servidor dedicado, que conoce sobre una aplicación en particular y provee servicios proxy para ella. Entiende e interpreta comandos de un protocolo en particular. Con este tipo de servidores es necesario contar con uno de ellos para cada servicio.

[2.11.] http://www.microsoft.com/latam/technet/articulos/200104/art02/default.asp

Servidor Proxy de Circuito	Llamado Proxy Genérico, que crea un circuito virtual entre el cliente y el servidor real sin interpretar el protocolo de la aplicación.

Tabla 2.1 Clasificación de Servidores Proxy

b) Ventajas y Desventajas de un Servidor Proxy

Existen varias ventajas al configurar un Servidor Proxy, así como también sus desventajas, las mismas que se las menciona en la Tabla 2.2.

Ventajas	Desventajas
Permite a los usuarios acceder a los servicios de Internet ocultando totalmente la red interna.	Algunos servicios no son viables para trabajar con servidores Proxy (Ej: talk).
Debido a que todo el tráfico pasa a través del servidor Proxy se puede registrar gran cantidad de información con fines de auditoria y seguridad.	Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.
Permite un buen servicio de logs a nivel de cada aplicación.	Los servidores Proxy de circuitos no brindan controles específicos sobre las aplicaciones.
El servidor Proxy de Circuito provee soporte para un conjunto grande de protocolos.	

Tabla 2.2 Ventajas y Desventajas de un Servidor Proxy

2.4.3. VPN (Red Virtual Privada)

Es una red privada que se extiende, mediante un proceso de encriptación de los paquetes de datos, a distintos puntos remotos, usando una infraestructura pública de transporte, como se puede observar en la Figura 2.7.

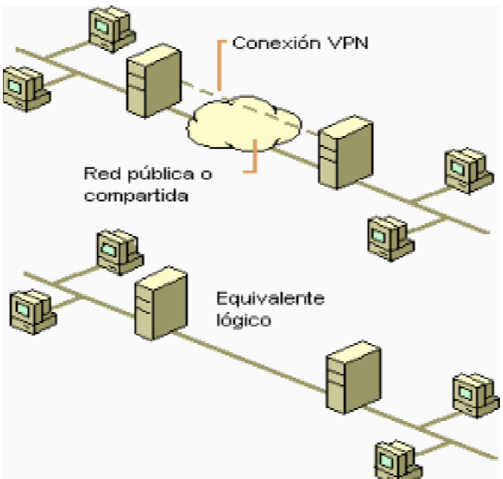


Figura 2.7. VPN (Red Virtual Privada)

En la Figura 2.8 se muestra como viajan los datos a través de una VPN. Los datos parten de un servidor dedicado hacia al firewall, llegando después a la nube de Internet, donde se genera un túnel dedicado únicamente para la información que con una velocidad y un ancho de banda garantizados, se envían al firewall y servidor remotos.

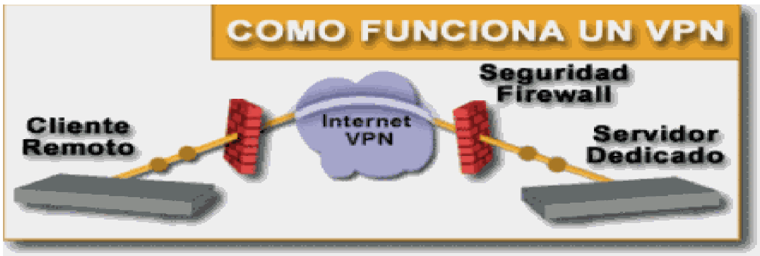


Figura 2.8. Funcionamiento de una VPN

Las VPN pueden enlazar las oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos IP, IPSec, Frame Relay, ATM.

2.4.4. RAS (Servicio de Acceso Remoto)[2.12.]

El acceso remoto permite a usuarios que tienen sus computadoras ubicadas en un sitio remoto a la red, crear una conexión lógica hacia la red de la empresa o hacia el Internet. Generalmente es usado por organizaciones para conectar la laptop de un empleado que esté trabajando fuera de la empresa o para conectar las computadoras de la casa a la red de la organización y así el empleado pueda leer su correo o acceder a los archivos compartidos y mediante el proveedor del servicio de Internet (ISP) pueda conectarse al Internet.

[2.12.] http://www.telefonicapr.com/prtc/portal/channel2/0,1045,2108_39244,00.html

Las conexiones de acceso remoto pueden ser mediante llamadas telefónicas entrantes o por medio de una red virtual privada (VPN).

a) **Llamadas Telefónicas Entrantes:** Un cliente de acceso remoto utiliza la infraestructura existente de telecomunicaciones, esto significa que usa una línea analógica de teléfono para crear temporalmente un circuito físico o un circuito virtual a un puerto del servidor de acceso remoto. Una vez que el circuito físico o virtual está creado, los demás parámetros de la conexión pueden ser negociables.

b) **VPN (Red Virtual Privada):** Un cliente VPN utiliza una dirección IP de la red para crear una conexión virtual punto a punto con el servidor de acceso remoto actuando como un servidor VPN. Una vez que la conexión virtual punto a punto está creada, los demás parámetros de la conexión pueden ser negociables.

2.4.5. Routing

El principal equipo que realiza routing es el router, dispositivo diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN. Suelen estar interconectados, formando una especie de "telaraña" que hace posible el tráfico de datos entre redes separadas físicamente, por ejemplo la Red de redes, Internet, cuando un ordenador envía una serie de paquetes de datos a otro situado en otra ciudad o país, estos son encaminados de router a router a lo largo del camino entre ambas máquinas.

Cada paso de un paquete de un router a otro se denomina "salto", y el principal objetivo de todos y cada uno de los routers que intervienen en la transferencia del paquete es que éste llegue a su destino en el menor número posible de saltos, por la mejor ruta posible. Para poder realizar esta tarea, los routers se comunican constantemente entre sí, informándose de las rutas bloqueadas, de las máquinas intermedias que se encuentran caídas o saturadas de tráfico, aprendiendo con ello cuál es el router idóneo para enviarle los paquetes recibidos.

La protección de un Router es una defensa que se encuentra a menudo en una red donde se restringe el flujo del tráfico entre la red de la empresa e Internet. Opera en una política de seguridad y usa ACL's (Access Control Lists o Lista de Control de Acceso) que acepta o deniega paquetes. Este módulo está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser denegado.

La protección también debe estar diseñada para restringir el flujo de salida de cierto tipo de tráfico. Los routers están siendo cada vez más complejos y algunos tienen propiedades desconocidas para el auditor y a veces para la organización auditada. El papel del auditor es en parte determinar la función del router dentro de la Zona Desmilitarizada (DMZ), red donde una empresa sitúa los servidores que desea hacer accesibles desde Internet.

Entre las principales características de un Router podemos encontrar que ayuda a:

- ✓ Verificar el tipo de router con información reunida de la obtencion de Inteligencia.
- ✓ Verificar si el router está dando servicio de traducción de direcciones de red (NAT).
- ✓ Verificar las intrusiones con opciones TTL estratégicas en los paquetes, (Firewalking) hecho en el módulo de escaneo de puertos.
- ✓ Verificar la configuración de las ACL's del router
- ✓ Examinar la ACL del router en contra de las políticas de seguridad y en contra de la regla "Denegar Todo".

- ✓ Verificar si el router está filtrando el tráfico de la red local hacia afuera.

- ✓ Verificar que el router esté haciendo detección de direcciones falsas.

- ✓ Verificar las intrusiones desde un escaneo inverso en el módulo de escaneo de puertos.

- ✓ Probar las capacidades externas del router desde el interior.

- ✓ Cuantificar la habilidad que tiene el router para manejar fragmentos de paquetes muy pequeños.

- ✓ Cuantificar la habilidad del router para manejar paquetes grandes.

- ✓ Cuantificar la habilidad del router para manejar fragmentos coincidentes como los usados en ataques del tipo TEARDROP, basado en el envío de fragmentos de paquetes en lugar de paquetes completos.

2.5. HERRAMIENTAS

2.5.1. IDS (Sistema de Detección de Intrusos)[2.13.]

La seguridad de un sistema se puede clasificar en: activa y preventiva. La seguridad activa de un sistema consiste en protegerlo todo lo posible ante potenciales intentos de abuso del mismo. Un firewall es un buen ejemplo de seguridad activa, trata de filtrar el acceso a ciertos servicios en determinadas conexiones para evitar el intento de forzamiento desde alguno de ellos.

[2.13.] http://www.monografias.com/trabajos11/intru/intru.shtml

Por otro lado, la seguridad preventiva es aquella que se implanta en un sistema para que informe si éste tiene una incidencia de seguridad. No pretende proteger el sistema, pretende alertar de que algo extraño esta sucediendo en él. Un buen ejemplo de seguridad preventiva es un sistema de detección de intrusos, para lo cual se debe considerar dos conceptos importantes para entender el funcionamiento de un IDS:

- ***Intrusión:*** Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso. (No sólo penetraciones contra un sistema).
- *Sistema de detección de intrusos:* **Mecanismo cuyo objetivo es detectar, identificar y responder ante una intrusión. (No tiene por que ser un programa o producto concreto).**

Un sistema de detección de intrusos es aquel que permite recabar información de distintas fuentes del sistema en el que se implanta, para alertar de una posible intrusión en las redes o máquinas. La alerta puede ser del hecho de que existe un intento de intrusión, como del modo en el que éste se está realizando y en algunos casos por parte de quién esta siendo efectuado. Se puede considerar un sistema de detección de intrusos como un *control de auditoría* que permitirá tomar

decisiones a la hora de realizar una auditoría de seguridad del sistema.

Un sistema de detección de intrusos surge como una medida preventiva, nunca como una medida para asegurar los sistemas, ayudan al administrador de dicho sistema a permanecer al tanto de cualquier intención maligna contra el sistema que administra.

a) Características principales de un IDS

- ✓ **Debe ejecutarse continuamente sin intervención o supervisión de un operador humano.**

- ✓ **Debe ser confiable, lo suficiente como para ejecutarse en background, pero no debe ser una caja negra, es decir, que su funcionamiento interno pueda ser examinado.**

- ✓ **Debe ser capaz de tolerar fallas, en el sentido de que pueda sobrevivir a una caída del sistema, sin tener que reconstruir su base de datos de conocimientos al reiniciarse.**

- ✓ **El sistema debe estar en capacidad de automonitorearse para asegurar su correcto funcionamiento.**

- ✓ **Debe ser ligero, es decir su ejecución no debe cargar al sistema de una manera tal que le impida ejecutar otras tareas con relativa normalidad**

- ✓ **Debe observar desviaciones del comportamiento estándar.**

- ✓ **Debe poder adaptarse al comportamiento cambiante del sistema, es decir, si la configuración del sistema cambia, el IDS se adaptará.**

- ✓ **Debe ser difícil de engañar.**

b) Clasificación de los IDS[2.14.]

Los IDS pueden clasificarse según el método de detección y según el tipo de monitoreo. Según el método de detección, se tienen los siguientes:

- *Detección de mal uso:* **Consiste en observar cualquier proceso que intente explotar los puntos débiles de un sistema en específico. Las acciones que integran el mencionado proceso, se denominan patrones o firmas del ataque. Estas firmas**

[2.14.] http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node282.html

pueden ser simples, como cadenas de caracteres, estructuras de memoria o bits, pero también pueden ser más complejas como vectores o expresiones matemáticas. Una ventaja de este método es que permite centralizar las labores de detección en el conjunto de firmas que posee el IDS, minimizando así, la carga de procesamiento del sistema.

- *Detección de anomalías:* **Se basa en monitorear constantemente el sistema para así detectar cualquier cambio en los patrones de utilización o el comportamiento del mismo. Si algunos de los parámetros monitoreados sale de su regularidad, el sistema generará una alarma que avisará al administrador de la red sobre la detección de una anomalía. Este tipo de detección es bastante compleja, debido a que la cuantificación de los parámetros a observar no es sencilla y a raíz de esto, se pueden presentar los siguientes inconvenientes:**

  - ✓ **Pueden generarse falsas alarmas si el ambiente cambia repentinamente, por ejemplo, cambio en el horario de trabajo.**
  - ✓ **Un atacante puede ir cambiando lentamente su comportamiento para así engañar al sistema.**

Según el tipo de monitoreo, se describen los siguientes:

- *Detección orientada al host (HIDS):* **Se basa en el monitoreo y análisis de información, que refleja el estado del host donde éste reside. La mayoría de la información que este tipo de sistema recopila es obtenida a través del sistema operativo del host. Esto último causa complicaciones debido a que la información que se procesa no contiene registros del comportamiento de bajo nivel de la red.**

- *Detección orientada a la red (NIDS):* **Fundamentan su monitoreo en información recolectada de la red. Generalmente, ésta información es capturada mediante mecanismos de fisgoneo, el cual consiste en habilitar la interfaz de red en modo promiscuo para que así capture todos los paquetes que reciba, incluso aquellos que no le han sido destinados. En base a este mecanismo, se pueden definir patrones o firmas de ataques, según la estructura, información y ocurrencia de los paquetes.**

2.5.2. Analizador de Red

Las herramientas de análisis y monitoreo de la red permiten resolver problemas de tráfico en la red, monitorear el rendimiento, detectar posibles fallas a tiempo, detectar y controlar las vulnerabilidades de la red etc.

Algunas herramientas se utilizan para escanear puertos, entre las más importantes sobresalen las siguientes:

a) **Nmap**[(2.15.)]: Esta herramienta controla los puertos abiertos en una máquina de la red, con comandos tales como lsof o netstat pero solamente en su propia máquina. Nmap puede dar mucha información, por ejemplo, puede decir cual es el SO funcionando, cuales son los puertos abiertos y peligrosos.

b) **Nessus:** Es un auditor de seguridad remoto. El cliente "The Nessus Security Scanner" es una herramienta de auditoría de seguridad que hace posible evaluar módulos de seguridad intentando encontrar puntos vulnerables que deberían ser reparados. Está compuesto por dos partes: un servidor, y un cliente. El servidor/daemon, "nessusd" se encarga de los ataques, mientras que el cliente, "nessus", se ocupa del usuario por medio de una interfaz gráfica. Una de las más importantes características de nessus es la forma en que se obtiene los reportes, los mismos que son fiables, detallados y sugieren una solución para vulnerabilidades encontradas. Si una vulnerabilidad es encontrada, nessus le informa que puede ser una falsa alarma, esto puede ocurrir, por ejemplo, con versiones actualizadas de algunos programas; una vulnerabilidad recientemente corregida puede ser detectada como un riesgo potencial, sin embargo, para esta clase de cosas, las plantillas son rápidamente actualizadas.

c) **SAINT: (**Security Administrator's Integrated Network Tool). Es la Herramienta de Red Integrada para el Administrador de Seguridad. Saint es otra herramienta no-libre de evaluación de seguridad. Incluye escaneos a través de un firewall, chequeos de seguridad actualizados de los boletines de CERT Y CIAC, 4 niveles de severidad (rojo, amarillo, marrón y verde) y una interfaz HTML rica en características. A diferencia de esas herramientas basadas exclusivamente en Windows, SAINT corre exclusivamente sobre UNIX. Saint solía ser gratuito y "open source" pero ahora es un producto no-libre.

d) **SARA:** (Security Auditor's Research Assistant). Es el Asistente de Investigación para el Auditor de Seguridad. SARA es una herramienta de evaluación de vulnerabilidades que está basada en el modelo SATAN, promueve un ambiente colaborativo y es actualizada periódicamente para tener en cuenta las últimas amenazas.

[(2.15.)] http://www.nautopia.net/archives/es/varios_redes/nmap/escaneando_con_nmap.php

Otras herramientas pueden detectar "portscans" o intrusiones, dentro de las cuales se destacan las siguientes:

a) Logcheck: Envía al administrador mensajes por correo electrónico informando de las anomalías en los archivos de registro del sistema. Logcheck es parte del Proyecto Abacus de herramientas de seguridad. Es un programa creado para ayudar en el procesamiento de los archivos de registro de UNIX generados por varias herramientas del Proyecto Abacus. "Logcheck ayuda a localizar problemas y violaciones de seguridad en los archivos de registro automáticamente y te envía los resultados por correo electrónico"[(2.16.)]. Este programa es de uso gratuito en cualquier sitio.

b) Portsentry: Programa de detección de barrido de puertos (incluyendo "escaneo indetectable") en las interfaces de red del computador. Como medida de alarma, puede bloquear al atacante por medio de "denegación de hosts", bloqueando el ruteo hacia la máquina hostil o por medio de reglas de firewall. Es parte del set de programas "Abacus".

c) Snort[(2.17.)]: Es un sistema de detección de intrusiones de red, capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda, identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ej. buffer overflows, escaneos indetectables de puertos (stealth port scans), ataques a CGI, pruebas de SMB (SMB Probes), intentos de reconocimientos de sistema operativos (OS fingerprinting). Snort utilizar un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular. Mucha gente también sugirió que la Consola de Análisis para Bases de Datos de Intrusiones (Analysis Console for Intrusion Databases, ACID) sea utilizada con Snort. Otra característica importante de Snort es la capacidad de alertar en tiempo real, siendo estas alertas enviadas a syslog, un archivo de alerta separado o incluso a una computadora con Windows a través de Samba.

(2.16.) http://david.f.v.free.fr/ponencias/deteccion_de_intrusos/node6.html
(2.17.) http://www.nautopia.net/archives/es/varios_redes/snort/snort.php

Muchas herramientas forman parte del proceso de encriptación, funcionando en varias áreas, tales como:

a) **OpenSSH:** Secure Shell. Esta herramienta permite iniciar sesión y ejecutar comandos en una máquina remota de una forma segura, utiliza la encriptación de los datos circulando por la red, es decir, provee de comunicaciones cifradas y seguras entre dos hosts sobre una red insegura. Esta herramienta reemplaza al comando telnet y a los comandos remotos tales como rsh, rlogin. Incluye scp que remplaza a los comandos ftp y rcp.
b) **OpenSSL:** Secure Sockets Layer. El proyecto OpenSSL es un esfuerzo de cooperación para desarrollar un set de herramientas robusto a nivel comercial, completo en características, y "Open Source" implementando los protocolos SSL v2/v3 y TLS v1 (Transport Layer Security) así como también una biblioteca de cifrado de propósito general potente. El proyecto es administrado por una comunidad de voluntarios a lo ancho del mundo que utilizan Internet para comunicarse, planear, y desarrollar el set de herramientas OpenSSL y su documentación relacionada.

c) **GnuPG / PGP:** Para proteger los archivos y comunicaciones con cifrado avanzado. PGP es un programa de encriptación diseñado por Phil Zimmerman que ayuda a proteger nuestra información de curiosos y otros riesgos. GnuPG es una muy respetada implementación del estándar PGP (el nombre del ejecutable es, en realidad, gpg). Mientras GnuPG es software libre, PGP puede costar algo de dinero para algunas aplicaciones.

2.5.3. Sniffer

La estructura de Internet, y de las redes en general, posee grandes ventajas al permitir el intercambio de información entre millones de ordenadores. Es sin embargo esa misma topología la que facilita la labor de los "sniffers", programas especialmente diseñados para espiar los datos que circulan por la red.

En una red, la información se divide en paquetes para su transporte. Para poder llevar a cabo esta labor, los ordenadores necesitan de una combinación de hardware y software. En la parte física, podemos encontrarnos por ejemplo con un módem, una tarjeta RDSI, un dispositivo de infrarrojos o una tarjeta para red local. En el apartado del software, es necesario los controladores de dispositivo para que el sistema operativo pueda comunicarse con el hardware anteriormente descrito y los protocolos de red que permitirán a los ordenadores establecer un lenguaje común para el intercambio de paquetes.

Como ejemplo, se puede fijar en la composición de una red de área local, típica en oficinas y grupos de trabajo, basadas en el estándar Ethernet, y que en la actualidad suelen trabajar con velocidades de entre 10 y 100 Mbits/seg. En los ordenadores que formen parte de la red local podemos encontrar el componente físico formado por una tarjeta de red Ethernet, mientras que el sistema operativo contará con los controladores de dispositivo correspondientes a dichas tarjetas y el protocolo que utilicen como lenguaje común todos los ordenadores de la red para comunicarse, como por ejemplo TCP/IP. Por último, para que los ordenadores puedan intercambiar datos entre si se necesita un canal, que en este caso suele estar formado por el cableado de la red, coaxial o par trenzado, que permitirá que los paquetes de datos viajen de un ordenador a otro.

Cuando un equipo de la red quiere enviar información a otro se envían paquetes de datos con la dirección del destinatario, estos paquetes pasan por todas las tarjetas o interfaces de red, y únicamente el ordenador que tiene la dirección de destino coge los paquetes de información y contesta, comenzando la comunicación, mientras que el resto de los equipos los desecha ya que no están dirigidos a ellos.

Esta situación debería ser la normal en cualquier red, sin embargo es posible configurar una tarjeta Ethernet en modo "promiscuo", de manera que capture todos los paquetes de datos que viajan por la red aún sin llevar su dirección como destino, escuchando así todo el tráfico que circula. A partir de esta técnica, llevada a cabo con herramientas software y/o hardware conocidas como "sniffers", es posible hacerse con cualquier dato que circule por la red: contraseñas, números de tarjetas de crédito, información confidencial, etc.

En el cuadro 2.1. se puede observar los datos capturados a través de un snnifer tales como: tiempo de respuesta (1), MAC destino (2), MAC fuente (3), IP activas en la red (4), al desplegar esta opción visualizaremos el conjunto de datos transmitidos.

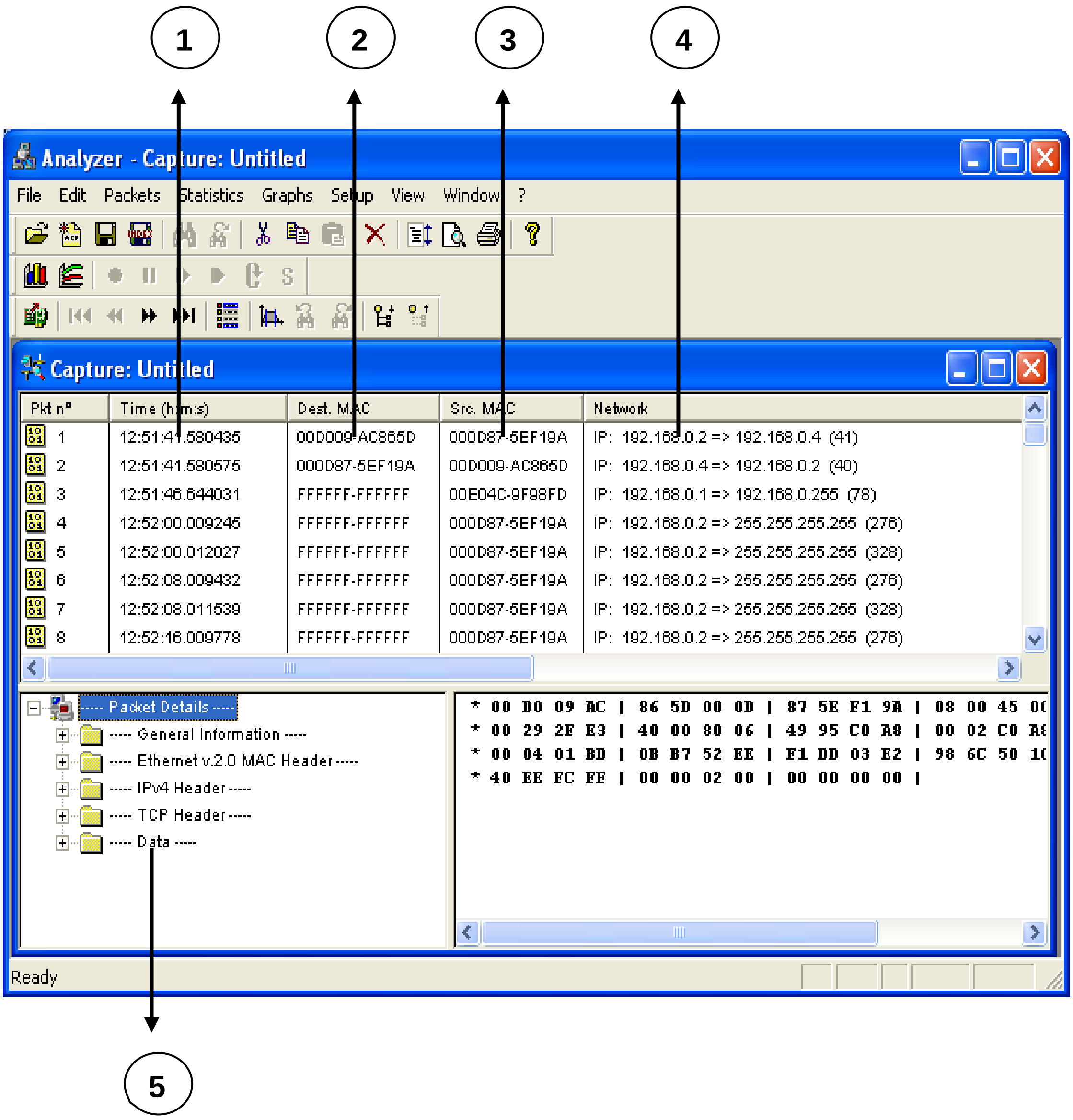


Tabla 2.3. Resultados obtenidos a través de un Sniffer

2.6. ISO 17999

La ISO (International Standarization Organization) es la entidad internacional encargada de favorecer la normalización en el mundo. Con sede en Ginebra, es una federación de organismos nacionales, éstos, a su vez, son oficinas de normalización que actúan de delegadas en cada país, como por ejemplo: AENOR en España, AFNOR en Francia, DIN en Alemania, etc. con comités técnicos que llevan a término las normas. Se creó para dar más eficacia a las normas nacionales.

La norma UNE/ISO/IEC 17999 es un código de buenas prácticas para gestionar la seguridad de la información de una organización, de tal forma que le permita en todo momento garantizar la confidencialidad, integridad y disponibilidad de la información que maneja.

- ***Confidencialidad:*** Sólo el personal o equipos autorizados pueden acceder a la información.

- ***Integridad:*** La información y sus métodos de proceso son exactos y completos.

- ***Disponibilidad:*** Los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando se requieran.

La creación de esta norma responde a la necesidad de proporcionar una base común a las organizaciones desde el punto de vista técnico, organizativo y jurídico, y cuyo cumplimiento implique que dicha organización mantenga una infraestructura y un esquema de funcionamiento que garantizan la seguridad de la información que maneja.

2.6.1. Normas y Procedimientos

La norma básicamente comprende las siguientes 10 secciones, a su vez divididas en 127 controles (jurídicas, técnicas y organizativas).

- Política de Seguridad.
- Organización de la Seguridad.
- Clasificación y control de activos de información.
- Gestión de la Seguridad de la información y el personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Mantenimiento y desarrollo de sistemas.
- Gestión de la Continuidad del negocio.
- Conformidad.

Una empresa para adaptarse a esta norma, deberá llevar a cabo una labor de consultoría, es decir, deberá seguir los siguientes procedimientos.

- Definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), es decir sobre qué proceso o procesos va a actuar ya que no es necesaria la aplicación de la norma a toda la entidad.
- Identificar los activos de información.
- Realizar un análisis de riesgos, el cual determinará las amenazas y vulnerabilidades de los activos de información previamente inventariados.
- Seleccionar los controles.
- Determinar, bajo el principio de proporcionalidad, las medidas correctivas a adoptar para disminuir las deficiencias o anomalías detectadas.
- Generar la documentación, esto significa crear una política de seguridad, procedimientos básicos de gestión de la seguridad de la información, protocolos de actuación, registros, etc.

2.7. DETERMINACIÓN DE VULNERABILIDADES DE LA RED

2.7.1. Análisis de Vulnerabilidades

La red de Internet permite situaciones tales como: participar en foros, enviar correos electrónicos, encontrar información hasta mantener una entrevista con otra persona en otro punto del planeta. Por otra parte, esta apertura hace vulnerables a las redes corporativas por tanto exige tomar medidas preventivas para evitar intrusiones no deseadas.

Para determinar las vulnerabilidades de un sistema es necesario profundizar en las características de los ataques a los que puede ser sometidos, por ejemplo: acceder a sistemas protegidos de forma fraudulenta, en una escala que va desde la mera constancia de su éxito, hasta la destrucción de datos, obtención de información confidencial, colapso del sistema, etc.

Dichos ataques podrán ser detectados mediante herramientas de diagnostico las mismas que alertan de conexiones no deseadas y que permiten hacer un seguimiento de éstas, así como poder decidir sobre qué conexiones se permite y cuales no (herramientas de control y seguimiento de accesos), y aquellas que se centran en la seguridad del sistema (herramientas que chequean la integridad del sistema), para detectar una vez que el sistema ha sido asaltado el alcance de los posibles daños.

2.7.2. Evaluación de Riesgos

Las redes computacionales han creado un entorno en el que se puede acceder, trasladar o destruir electrónicamente los datos si no hay mecanismos de bloqueo que protejan la información de la empresa. Aparecen nuevos riesgos que deben ser gestionados, proporcionando una solución sistemática que sirve para determinar medidas de seguridad corporativas apropiadas.

La evaluación de riesgos se realiza mediante la combinación de la identificación de activos vitales, la asignación de un valor al activo y la determinación de la probabilidad de quebrantamientos de la seguridad. Una vez identificados los activos críticos, valorados los costes y probabilidad asociados a la puesta en peligro, destrucción o no disponibilidad de estos recursos, es posible tomar una decisión sobre el nivel de riesgo aceptable para la Institución, por tanto el resultado de la valoración de riesgos debe ser única ya que depende de las necesidades comerciales, el grado de confianza de sus usuarios y la ubicación de los activos vitales.

a) Identificación de los activos de red

La Institución debe comprender lo que desea proteger, qué acceso es necesario para tales activos y cómo operan conjuntamente estas consideraciones. Los posibles activos de la red a tener en cuenta son:

- ***Hardware:*** Estaciones de trabajo, computadores personales, impresoras, routers, switches, módems, servidores de Terminal y firewall.

- ***Software:*** Programas fuente, programas de objeto, utilidades, programas de diagnóstico, sistemas operativos y programas de comunicación.

- ***Datos:*** Datos almacenado en-línea y archivos fuera de línea, copias de seguridad, registros de auditoría, bases de datos y datos en tránsito sobre los medios de comunicación.

- ***Personas:*** Usuarios, administradores y personal de mantenimiento de hardware.

- ***Documentación:*** Programas de software, evaluaciones internas de hardware y software, sistemas y procedimientos administrativos locales.

b) Valoración de los Activos

La clasificación de los datos en función de los distintos niveles de importancia pueden ser un paso preliminar a la hora de establecer su valor. Un sistema sencillo de alto, medio y bajo puede ser el punto de partida que sirva para evaluar la importancia relativa de los datos. Los datos pueden adaptar múltiples formas, entre los cuales se incluyen las siguientes:

- ***Datos Administrativos:*** La correspondencia y otra información similar, como los registros y la información del personal que esté a disposición del público .

- ***Datos Financieros:*** Información presupuestaria y relativa a los gastos de las operaciones corporativas.

- ***Datos de Cliente:*** Información relacionada con el cliente que es de naturaleza personal, o información desarrollada como fruto de test, observaciones o recomendaciones.

- ***Datos de Investigación:*** Información de apoyo de la actividad de investigación de una Institución.

- ***Datos Exclusivos:*** Información que no puede ser relevada al público sin el permiso del propietario.

c) Amenazas y Puntos Débiles

Una amenaza puede ser cualquier persona, objeto o evento que, si se consuma, puede potencialmente causar daños en la red o en el dispositivo en la red. Las amenazas pueden ser maliciosas, como la modificación intencional de información sensible; o accidentes como un error en el cálculo o la eliminación accidental de un archivo.

d) Valoración de los Riesgos

En todas las posibles amenazas, hay que evaluar el riesgo, existiendo metodologías que lo calcule en términos cuantitativos, cualitativos o una combinación de ambos. La evaluación cuantitativa utiliza datos empíricos, probabilidades y estadísticas conocidas. El análisis cualitativo utiliza una valoración intuitiva. Independientemente del mecanismo que se use, el aspecto relevante es cómo se cuantifica la pérdida, y la probabilidad de la pérdida deberá ser coherente y significativa para los que toman las decisiones sobre protección frente a los riesgos.

CAPÍTULO 3

ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1. FUNCIONAMIENTO DE LA RED

Las instalaciones del Comando Conjunto de las Fuerzas Armadas “COMACO” se encuentran dentro del Complejo Ministerial, lugar que comparte con los edificios en donde funcionan las Comandancias de las diferentes ramas de las Fuerzas Armadas.

La red de datos del Comando Conjunto de las Fuerzas Armadas se divide en dos segmentos de red: el denominado GRUTEL (Grupo de Telecomunicaciones), ubicado en el Palomar, lugar donde se encuentran los diferentes servidores y equipos de comunicación.

Y el otro es el Edificio de COMACO, en donde se encuentra la parte administrativa del mismo., como se puede ver en la figura 3.1.

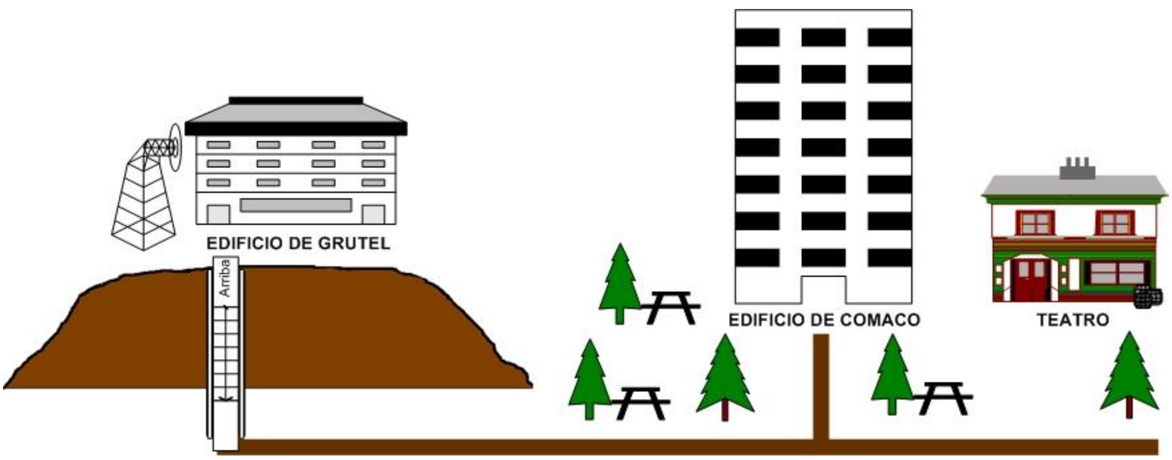


Figura 3.1. Ubicación Física de COMACO

3.1.1. Conexión de servidores y equipos de comunicación.

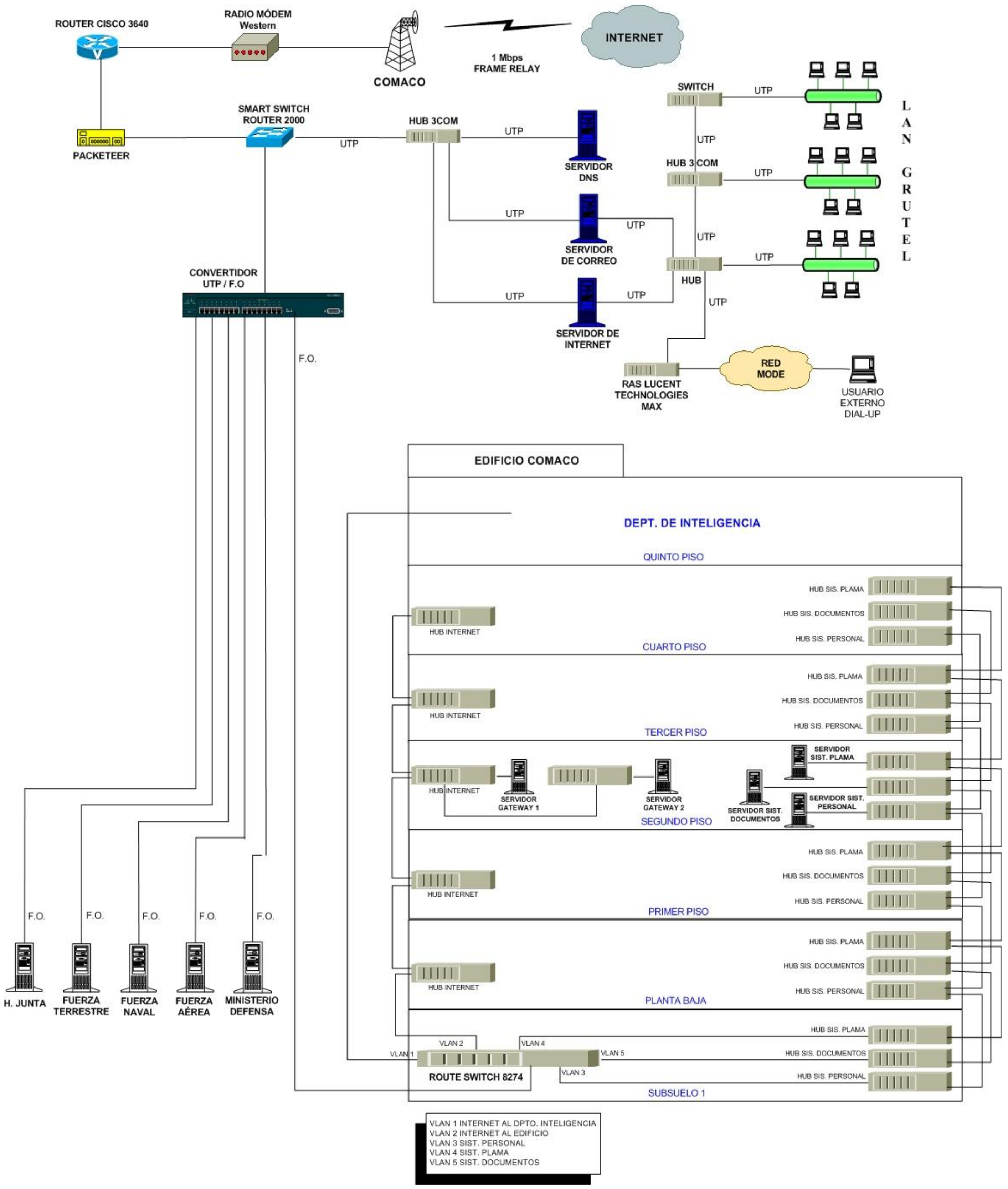


Figura 3.2. Red de Datos del Comando Conjunto de las Fuerzas Armadas

a) GRUTEL

GRUTEL se encuentra en un edificio de dos plantas; en la planta baja se encuentran los servidores y equipos de comunicación de diferentes características, las mismas que se pueden ver en el Anexo A; en la planta alta se encuentran distribuidas las computadoras personales para los usuarios. La distribución de dichos equipos se puede observar en el Anexo B.

La figura 3.3. muestra la conexión entre los servidores y equipos de comunicación ubicados en las instalaciones del Grupo de Telecomunicaciones (GRUTEL).

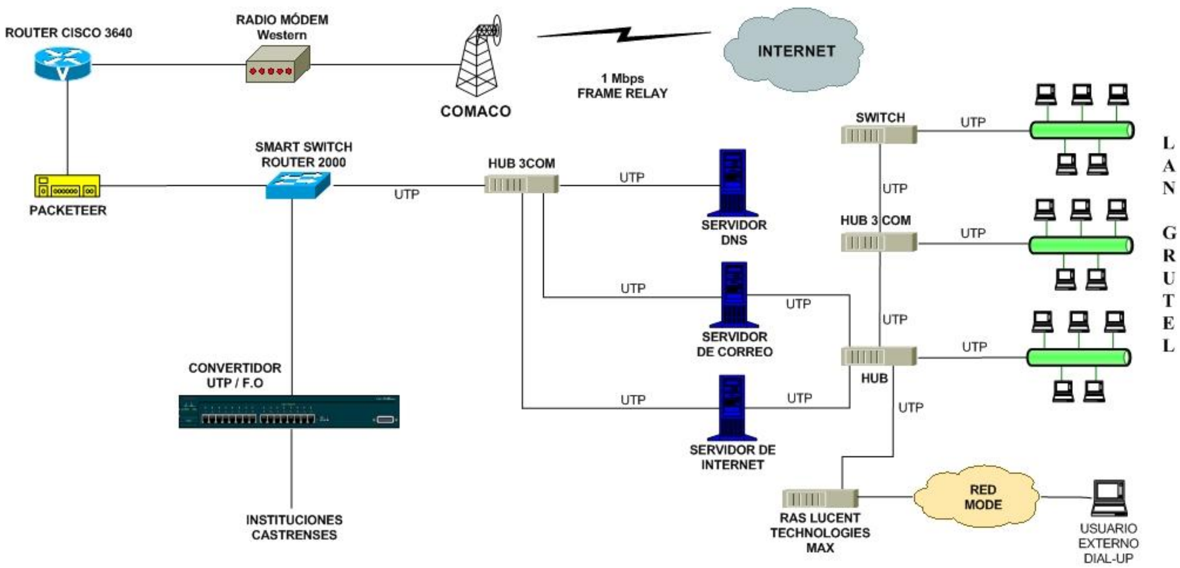


Figura 3.3. Red de Datos de GRUTEL

La señal de Internet que proviene del Proveedor de Internet llega hacia COMACO a través del Router "Cisco 3600", dispositivo que se encarga de la interconexión entre la red de Internet a través de un puerto serial, y la red LAN de COMACO mediante un puerto ethernet.

El Router se conecta al Packeteer, equipo que permite la administración del ancho de banda, es decir asigna un canal con un determinado ancho de banda a cada una de las Instituciones Relacionadas: Honorable Junta, Fuerza Terrestre, Fuerza Naval, Fuerza Aérea, Ministerio de Defensa, Departamento de Inteligencia y Edificio de COMACO.

Además este equipo tiene la capacidad de restringir el acceso a programas del Internet que puedan congestionar la red, por ejemplo: KAZAA, IMESH, etc.

El Packeteer se conecta al Switch “Smart Switch Router 2000”, dispositivo en el cual están configuradas siete VLAN’s (Redes de Área Local Virtuales) para distribuir la señal del Internet mediante fibra óptica hacia cada una de las Instituciones Castrenses, la administración del uso del Internet es responsabilidad de cada Institución.

El Switch se conecta al Hub 3COM, concentrador que transmite la señal a los servidores de GRUTEL: servidor DNS, servidor de Correo, servidor de acceso al Internet, a continuación se detallan las funciones de cada uno de los servidores:

- Un servidor Proliant en el cual está configurado el DNS, servidor que tiene la función de traducir nombres de dominio a direcciones IP’s. La resolución de nombres lo hace a nivel de red LAN y de Internet.

- Un servidor Proliant para el Mail, servidor que permite enviar y recibir correos electrónicos, el cual posee dos tarjetas de red, una que se conecta a la red externa, es decir al Internet; y la otra tarjeta que se conecta a la red interna a través del Hub Cabletrón.

- Un computador Clon Pentium 4 para el acceso a Internet mediante proxy transparente, el mismo que permite que los usuarios naveguen en el Internet, servidor que posee dos tarjetas de red, una tarjeta que se conecta a la red de Internet y la otra a la red interna a través del Hub Cabletrón.

El Servidor de Acceso Remoto, cuya función es dar acceso a la red LAN, a usuarios remotos; se conecta mediante la red LAN a un equipo denominado RAS “Lucent Technologies MAX”, (equipo que crea la base de datos de los usuarios remotos y realiza la autentificación de los mismos), el cual permite la conexión de un usuario remoto mediante un módem analógico hacia Internet, lo que funciona por medio la Red MODE (Red de comunicaciones privada de las Fuerzas Armadas), ya que el RAS se conecta a la Central Telefónica PABX (Central Telefónica para uso particular) y a dicha central se conectan los usuarios que tengan acceso a la Red MODE.

b) Edificio de COMACO

El Edificio de COMACO está separado físicamente de GRUTEL, así lo muestra la figura 3.1., teniendo una edificación de siete pisos con sus respectivas dependencias mencionadas a continuación, en la cual se encuentra toda la parte administrativa del Comando Conjunto:

- **Subsuelo 1: C3-I2 Comando Control Comunicaciones – Inteligencia Informática**
- **Planta Baja: Dirección de Personal**
- **Primer Piso: Dirección de Logística**
- **Segundo Piso: Dirección de Comunicaciones**
- **Tercer Piso: Estado Mayor del Comando Conjunto de las Fuerzas Armadas**
- **Cuarto Piso: Dirección de Operaciones**
- **Quinto Piso: Departamento de Inteligencia**

Es importante mencionar que el Edificio de COMACO posee dos redes física y lógicamente independientes, las cuales son descritas de la siguiente manera:

- Una red interna que no tiene salida al Internet, en donde se encuentran tres sistemas específicos, los mismos que son:
  - ✓ PLAMA, es el sistema denominado Plan Maestro en donde se manejan los presupuestos.
  - ✓ Sistema de Documentos, donde se manejan los archivos.
  - ✓ Sistema de Personal, en el cual se manejan los datos de los empleados.

Que por motivos de seguridad y políticas de la Institución no se tuvo acceso a la información que se manejan en estos sistemas, debido a la confidencialidad que ellos representan.

- Y la otra red que está diseñado sólo para el acceso a Internet y correo electrónico, red a la cual se refiere nuestro tema de estudio.

A continuación se muestra en la figura 3.4. la red de datos actual del edificio de COMACO:

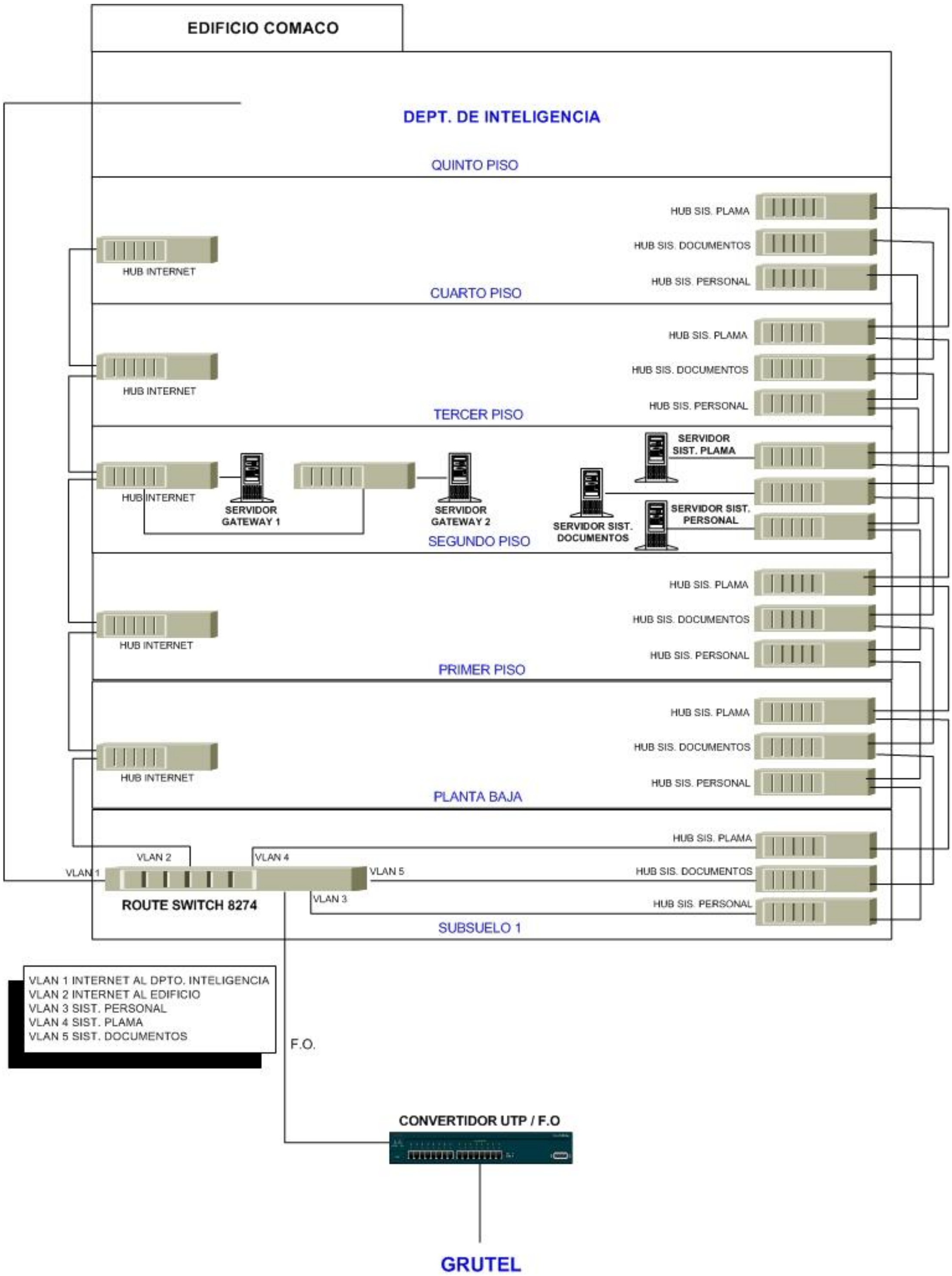


Figura 3.4. Red de Datos Actual del Edificio de COMACO

Como se puede observar en la figura 3.2, GRUTEL es quien provee del servicio de Internet al Edificio de COMACO; mediante fibra óptica llega al Switch "ROUTE SWITCH 8274", que se encuentra en el Cuarto de Control (lugar donde se encuentra el RACK principal de distribución del cableado estructurado), en el que se configuran dos VLAN's para la distribución del Internet; una red asignada al Departamento de Inteligencia, dependencia que funciona en el mismo edificio de COMACO, la misma que posee su propio sistema de seguridad ya que maneja información sumamente confidencial.

La otra red llega al RACK principal de cableado estructurado por el cual se distribuye hacia todos los pisos, en cada piso existe un RACK de distribución y un Hub al cual se conectan los usuarios respectivos. La conexión de piso a piso se realiza mediante verticales, y la distribución hacia los usuarios que se encuentras en cada piso se la realiza horizontalmente.

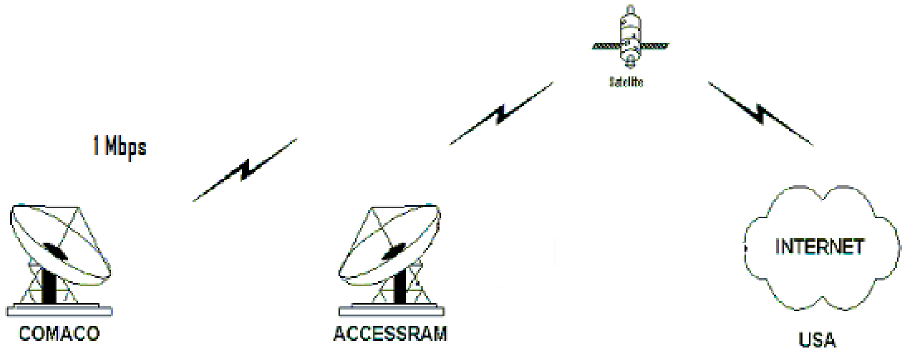
Del RACK principal llega la señal de datos al RACK que se localiza en el segundo piso, luego se conecta al Hub "HubStack" que se conecta al Servidor de Internet que está en el Departamento de Informática, también en este departamento se encuentra un Hub 3COM el cual se conecta al RACK, al hub se conecta el otro servidor de Internet que funciona únicamente para el Departamento de Informática, y desde éste se distribuye hacia los usuarios del área informática.

Cabe anotar que en el segundo piso se encuentra el área de Informática en el que se localizan dos servidores de Internet, uno sólo para dicha área, el cual está conectado a un Hub 3COM y éste a los usuarios del área de Informática. El otro servidor está conectado hacia los demás usuarios mediante el RACK y Hub de cada piso como se mencionó anteriormente.

3.1.2. Enlaces hacia Internet y a Instituciones Relacionadas.

a) Enlace hacia Internet

Según se muestra en la figura 3.5, el enlace de última milla es vía microondas con tecnología spread spectrum, que trabaja en la Banda de 5.8 Ghz, para lo cual COMACO posee una



antena que se conecta al ISP (Proveedor de Internet), con una velocidad de enlace de 1 Mbps.

Figura 3.5. Enlace de última milla

La señal de la antena ingresa por el Radio "Western", radio que es utilizado para la transmisión de datos, el cual se conecta al Módem "RAD", dichos equipos son administrados por el ISP, motivo por el cual no se permitió el acceso a su configuración. El módem se conecta al Router "CISCO 3600" a través de la interface v-35. El método de acceso al medio es mediante el protocolo Frame Relay.

b) Enlace hacia Instituciones Relacionadas con COMACO

Como se muestra en la figura 3.6, en el Switch SMART ubicado en GRUTEL se han definido VLAN’s para la distribución del enlace de Internet, hacia cada una de las Instituciones Castrenses (Fuerza Naval, Fuerza Terrestre, Fuerza Área, Ministerio de Defensa Nacional, Departamento de Inteligencia y Edificio de COMACO.), físicamente están unidas a través de enlaces de fibra óptica, siendo responsabilidad de la administración de la señal de Internet, cada una de las instituciones mencionadas anteriormente.

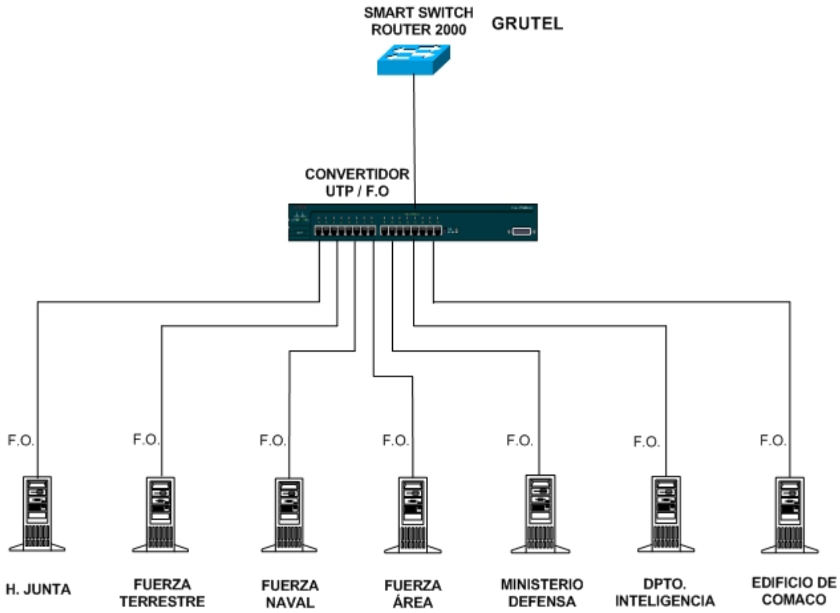


Figura 3.6. Enlace hacia Instituciones Relacionadas

3.1.3. Características de equipos de comunicación y servidores.

La red de datos del Comando Conjunto posee en su estructura los siguientes equipos de comunicación y servidores, para lo cual se mencionará las principales características relacionadas con la seguridad, las características adicionales se las puede revisar en el Anexo A.

a) GRUTEL

RADIO

MARCA: Western

MODELO: Tsunami 10 base T+E1 Spread Spectrum 31850-42B20

UBICACIÓN: GRUTEL, área de Telemática, propiedad del ISP

INTERFACES				
INTERFACE	**VELOCIDAD**	**CONEXIÓN**	**PROTOCOLO**	**DESTINO**
T1/E1	10 Base T	Módem	802.11A	Antena

Tabla 3.1. Características del Radio

MÓDEM

MARCA: RAD
MODELO: FCD-E1L
UBICACIÓN: GRUTEL, área de Telemática, propiedad del ISP

INTERFACES			
INTERFACE	**VELOCIDAD**	**CONEXIÓN**	**DESTINO**
BNC	64 Mbps	Router	Radio

Tabla 3.2. Características del Módem

ROUTER

MARCA: CISCO 3600 Series
MODELO: 3640
UBICACIÓN: GRUTEL, área de Telemática
IOS: 11.01

CARACTERÍSTICAS PRINCIPALES	INTERFACES			
		S 0	**Eth 0**	**Eth 1**
Software CISCO 3620 Series IOS IP Plus IPSec56	**IP**	Eth 0	69.65.131.177	
32MB DRAM Máximo Dram 128MB	**Velocidad**	sincrónico de alta velocidad	10/100 BASE-TX	10/100 BASE-TX

8MB FLASH Máximo Flash 32MB	**Conexión**	Radio	Packeteer	
Tiene configurado políticas como SHAPPER que realiza la administración del ancho de banda.	**Protocolo**	HDLC	HDLC	
Posee configuración de ruteo y políticas ACL (Access Control List).	**Destino**	Internet	Red LAN	
Se restringe la navegación y la ejecución del comando telnet externamente.				

Tabla 3.3. Características del Router

PACKETEER

MARCA: Packeteer

MODELO: 2500

UBICACIÓN: GRUTEL, área de Telemática

SOFTWARE: PacketShaper

CARACTERÍSTICAS PRINCIPALES	**INTERFACES**			
Throughput Máximo 10Mbps	**INTERFACE**	**VELOCIDAD**	**CONEXIÓN**	**DESTINO**
Máximo número de servidores "host" IP* 10.000	Eth 0	10/100Mbps	Router	Internet
Puede clasificar el trafico por aplicaciones, protocolos, puertos.	Eth 1	10/100Mbps	Switch	Red LAN
Gestión del dispositivo mediante: Puerto serie de consola tipo DB-9, Interfaz para navegadores Web, Interfaz para Líneas de Comando Telnet, Soporte de Packeteer a SNMP MIB y MIB-II.	Serial, puerto de consola RS-232 DB-9			

Tabla 3.4. Características del Packeteer

SWITCH

MARCA: Cabletron

MODELO: Smart Switch Router 2000

UBICACIÓN: GRUTEL, Área de Telemática

IOS: SSR 2000 Versión E9.0.0.0

CARACTERÍSTICAS PRINCIPALES	INTERFACES				
Throughput de ruteo: 6 millones de paquetes por segundo (Mpps)	**INTERFACE**	**IP**	**VELOCIDAD**	**CONEXIÓN**	**PROTOCO**
Ruteo IP/IPX	16 puertos eth	216.219.15.73	10/100 BASE-TX	Packeteer	TCP-IP
QoS al nivel de aplicación					
Filtros de seguridad en capas 2/3/4					
Administrable vía SNMP					
Soporte de 4096 VLANs					

Tabla 3.5. Características del Switch

SERVIDORES

MARCA	MODELO	UBICACIÓN	IOS	INTERFACES				
				INTERFACE	VELOCIDAD	CONEXIÓN	PROTOCOLO	DESTI
COMPAQ	Proliant ML370	GRUTEL Area de Telemática	LINUX Red Hat 7.3	NIC	10/100Mbps	Hub 3COM	TCP-IP	Intern
				NIC	10/100Mbps	Hub	TCP-IP	LAN
COMPAQ	Proliant ML370	COMACO Area de Telemática	LINUX Red Hat 7.3	NIC	10/100Mbps	Hub 3COM	TCP-IP	Intern
				NIC	10/100Mbps	Hub	TCP-IP	LAN
CLON	Intel Inside Pentium 4	COMACO Area de Telemática	LINUX Red Hat 7.3	NIC	10/100Mbps	Hub 3COM	TCP-IP	Intern
				NIC	10/100Mbps	Hub	TCP-IP	LAN
CLON	Intel Inside Pentium 4	Edificio de COMACO	LINUX Red Hat 7.3	NIC	10/100Mbps	Hub	TCP-IP	Intern
				NIC	10/100Mbps	Hub	TCP-IP	LAN
CLON	Intel Inside Pentium III	Edificio de COMACO	LINUX Red Hat 7.3	NIC	10/100Mbps	Hub	TCP-IP	Intern
				NIC	10/100Mbps	Hub	TCP-IP	LAN
OBSERVACIONES En GRUTEL no existe cableado estructurado, ni canaletas que cubran el cable. En el Edificio de COMACO si existe cableado estructurado con sus respectivos RACKs El DNS tiene dos discos duros de 16 GB, el MAIL dos de 16 GB, Internet discos de 80, 40 y 30 GB.								

Tabla 3.6. Características de los Servidores

HUBS

EQUIPO	MARCA	MODELO	UBICACIÓN	INTERFACES

				INTERFACE	CONEXIÓN	DESTINO
HUB	3COM	3C16593B SUPER STACK 3 BASELINE DUAL SPEED HUB	GRUTEL Área de Telemática	RJ-45 24 puertos Fibra Óptica 1 puerto	SWITCH	SERVIDOR (DNS, MAIL e INTERNET)
SWITCH	CABLETRON	HubStack 10 base T Hub with LANVIEW SEHI-24	GRUTEL Área de Telemática	RJ-45 24 puertos	SERVIDOR PROXY	USUARIOS
HUB	3COM	3C16593B SUPER STACK 3 BASELINE DUAL SPEED HUB	GRUTEL Área de Telemática	RJ-45 24 puertos	HUB SATCK	USUARIOS
SWITCH	CABLETRON	SMART SWITCH 2200 2E42-27	GRUTEL Área de Telemática	RJ-45 24 puertos	SUPER STACK	USUARIOS

Tabla 3.7. Características de los Hubs y Switches

RAS

Equipo RAS “Lucent Technologies MAX” Modelo MX60-E1-AC-60IX que posee cuatro interfaces E1, una interface LAN y un puerto de consola para administración en sitio, este equipo actualmente utiliza una interface.

b) EDIFICIO DE COMACO

- Un switch ROUTE SWITCH 8274, que se encuentra en el cuarto de comunicaciones del Edificio de COMACO, al que llega la señal de Internet para la distribución hacia todo el edificio, mediante una VLAN distribuye también al Departamento de Inteligencia. Además en este switch se encuentran creadas las VLAN's para el acceso a los sistemas PLAMA, Personal y Documentos.

- Subsuelo1: Hub HubStack SEHI-22 10 base T marca Cabletron con dos interfaces Ethernet, Fast Ethernet para 22 puertos.

- Planta Baja: HubStack SEHI-22 10 base T con dos interfaces Ethernet, Fast Ethernet para 22 puertos.
- Primer Piso: Intel Express 330T Stackable Hub con dos interfaces Ethernet, Fast Ethernet con una velocidad de transferencia de datos de 100 Mbps, modo de comunicación es Full-duplex y Half-duplex, cantidad de puertos 24 dBi Ethernet 10Base- T, Ethernet 100Base-TX .

- Segundo Piso: Tres hubs, un 3COM, un HubStack SEHI-22 y el ultimo es Intel Express 330T Stackable Hub. El Hub 3COM con dos interfaces Ethernet, Fast Ethernet con una velocidad de transferencia de datos de 100 Mbps, modo de comunicación es Full-duplex, cantidad de puertos 24 dBi Ethernet 10Base- T, Ethernet 100Base-TX; en el área de Informática, en el Edificio de COMACO para la distribución horizontal hacia los usuarios.

- Tercer Piso: Dos hubs 3COM SuperStack 3 con dos interfaces Ethernet, Fast Ethernet con una velocidad de transferencia de datos de 100 Mbps, modo de comunicación es Full-duplex y Half-duplex, cantidad de puertos 24 dBi Ethernet 10Base- T, Ethernet 100Base-TX.

- Cuarto Piso: Un hub 3COM con dos interfaces Ethernet, Fast Ethernet con una velocidad de transferencia de datos de 100 Mbps, modo de comunicación es Full-duplex, cantidad de puertos 24 dBi Ethernet 10Base- T, Ethernet 100Base-TX.

3.2. RECOPILACIÓN DE INFORMACIÓN

Para conocer la situación actual de la red de datos, se visitó las instalaciones del Comando Conjunto, en donde se recopiló la información que servirá de base para el diseño del sistema de seguridad, cumpliendo con los procedimientos, reglas, permisos y restricciones que están definidas por la institución.

3.2.1. De Servidores y Equipos de Comunicación

Es indispensable conocer los servidores y equipos de comunicación que posee la institución, en el cual reposa la información de la red informática, la cual fue obtenida del Administrador de Red. Dicha red cuenta con 5 servidores, que trabajan con el sistema operativo Linux versión 9.0 y el Kernell 2.4, además equipos de comunicación como el Router CISCO, Smart Switch, Packeteer y RAS Lucent.

a) Manejo de claves de superusuarios

Existe un administrador de las claves de superusuarios tanto para servidores como equipos de comunicación (Router, Switch, Packeteer y RAS) , el cual se encarga de cambiarlas mensualmente, a falta de él cualquier técnico del área de sistemas lo puede realizar. Cada vez que es cambiada una clave, es registrada en un libro con la fecha de modificación y expiración; libro al cual tienen acceso todas las personas que ingresan al Cuarto Principal de Equipos / Centro de Datos , puesto que se encuentra en lugar visible.

No se maneja ningún estándar para la creación de las claves de superusuarios de servidores y equipos de comunicación, siendo incluso fáciles de descifrarlas, porque utilizan un pequeño grupo de palabras, las mismas que son rotadas mensualmente, es decir palabras obvias y fáciles como: modelo del servidor, nombre del área, etc.

El acceso para la administración de los servidores es mediante su propio periférico (monitor, teclado y mouse), y el acceso a la administración de los equipos de comunicación se lo realiza a través del utilitario telnet, que se lo realiza desde cualquier computador que esté dentro de la red LAN de GRUTEL.

b) Actualización de sistema operativo y parches

Los sistemas operativos de los servidores no son actualizados periódicamente porque pueden causar problemas de compatibilidad y se podría perder información si no se toma las precauciones necesarias en el momento de realizar actualizaciones.

Para los servidores se utiliza el sistema operativo Linux Redhat 9.0 con el kernell 2.4, el mismo que no es actualizado periódicamente, el cual se actualiza sólo cuando se cambia de versión al sistema operativo.

En lo que se refiere a los sistemas operativos de los equipos de comunicación se puede decir lo siguiente:

- **El Router CISCO 3600 posee el IOS 12.2 (3B), sistema operativo que no ha sido actualizado desde que se lo adquirió.**

- **El RAS Lucent Technologies MAX 6000 posee el sistema operativo propio del fabricante y no ha sido actualizado desde que se lo compró.**

- **El PACKETEER posee el sistema operativo propio del fabricante el que no ha sido actualizado desde que se lo compró. Este equipo utiliza un software llamado packetshaper.**

El sistema operativo utilizado en las computadoras personales, en su mayoría, es Windows XP, teniendo un número pequeño con Windows 98 y Windows Me. Las computadoras personales tienen instalado servipack, el mismo que es obtenido del Internet, por lo tanto no poseen las licencias necesarias. Este servipack no es actualizado periódicamente, se lo instala sólo cuando el computador es formateado y configurado el sistema operativo nuevamente.

c) Mantenimiento preventivo y correctivo

COMACO no posee un convenio con la empresa de los equipos de comunicación y servidores, para que se realice un mantenimiento periódico; no se planifica un mantenimiento preventivo, cuando existe el problema el administrador de red o los técnicos realizan el mantenimiento correctivo, es decir, dan una solución al problema que suscita en ese momento.

El servidor de mail no posee antivirus que examine los correos entrantes y salientes de cada uno de los usuarios. Mientras que en las computadoras personales se instala antivirus bajados del Internet, los mismos que no tienen sus respectivas licencias, tales como: Mackafee, Avast, Norton, etc.

COMACO no cuenta con un stock de repuestos para realizar el mantenimiento adecuado de los servidores, equipos de comunicación y computadoras personales, esto significa, que cuando algún dispositivo deja de funcionar, es reemplazado por uno nuevo que es adquirido en ese momento al distribuidor que lo tenga disponible.

d) Ubicación física de servidores

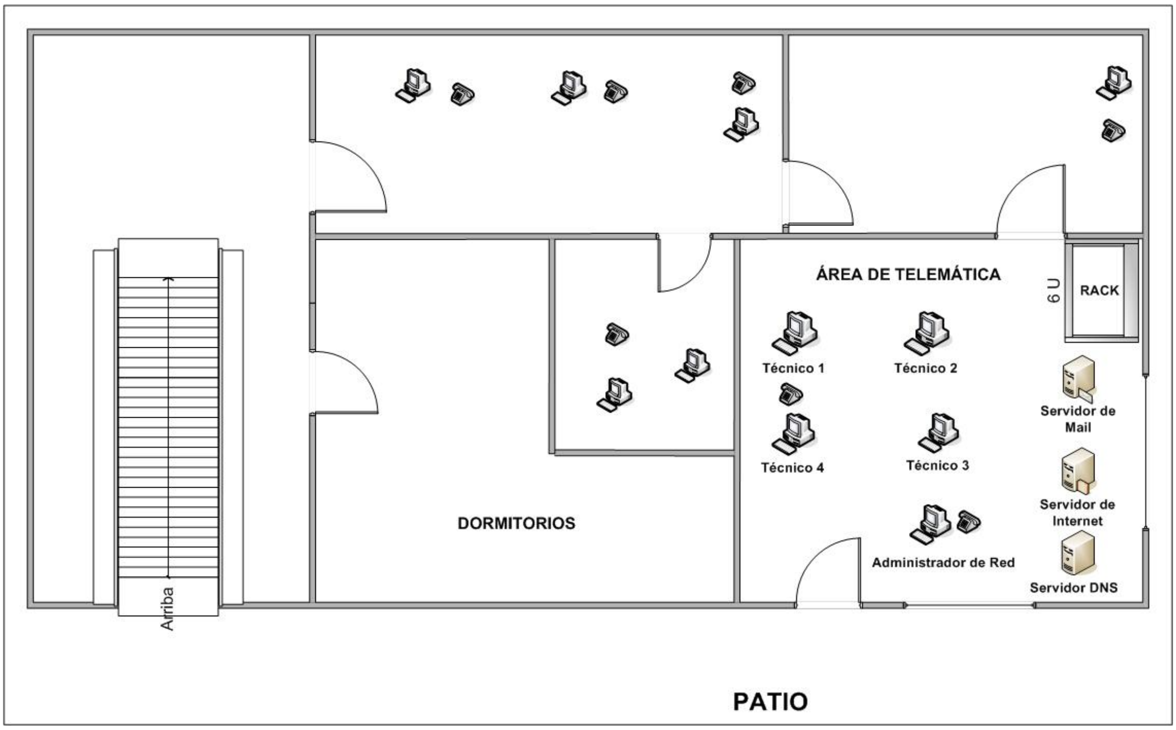


Figura 3.7 Ubicación Física de los Servidores

Como muestra la Figura 3.7, los servidores y el RACK de los equipos de comunicación se encuentran en el área de Telemática, el cual tiene dos puertas de acceso, el acceso uno permite salir hacia el patio, puerta que permanece cerrada cuando el administrador o los técnicos no se encuentran en el área; mientras que el acceso dos da hacia las oficinas de comunicaciones, las mismas que tienen salida al patio a través de escaleras, dicha puerta permanece abierta permitiendo el ingreso de personas que no pertenecen al área.

No existe ningún sistema de acceso al área de los servidores y equipos de comunicación debido a que las puertas son de apertura con llave, lo cual no permite llevar un registro de las personas que ingresan a dicha dependencia.

El Cuarto Principal de Equipos / Centro de Datos posee un circuito eléctrico propio, el que consta de dos breakers, siendo utilizados, uno para los servidores y otro para las computadoras personales que utilizan el administrador de red y los técnicos.

En el departamento de conmutación existen UPS's, que son utilizados para el sistema de comunicaciones, que también

ofrecen energía a los servidores y equipos de comunicación, mientras se activa el generador eléctrico de transferencia automática, pero éstos UPS's no soportan a las computadoras personales restantes de la red de GRUTEL.

El Cuarto Principal de Equipos / Centro de Datos no cuenta con un sistema de aire acondicionado, por lo que el calor que emanan los equipos se concentra dentro del departamento, motivo por el cual las ventanas son abiertas.

Existe un sistema general de detección de incendios con un detector de humo en cada uno de los departamentos de COMACO, el cual funciona a través de una alarma, pero dicho sistema no es específico para el área de los servidores. Cabe mencionar que los sistemas de movimiento y detección de incendios no se encuentran en funcionamiento.

COMACO tiene extintores que actualmente se encuentran en mantenimiento, para después ser colocados en lugares estratégicos y de fácil acceso.

3.2.2. De los Usuarios

Los usuarios como parte de la red de datos del Comando Conjunto, utilizan aplicaciones que permiten el manejo y procesamiento de información, para la cual se siguen normas.

Es importante mencionar que los usuarios no requieren de un nombre de usuario y una contraseña para el acceso a Windows, únicamente se crean usuarios a nivel de correo.

a) Creación, modificación y eliminación de usuarios

Para la creación de un usuario de correo en la Red de Información del Comando Conjunto de las Fuerzas Armadas "COMACO", se sigue los siguientes pasos:

- Si el usuario es militar, éste solicita verbalmente al Jefe de GRUTEL, la creación de una cuenta de correo. El Jefe de GRUTEL se comunica verbalmente con el administrador de la red o los técnicos para autorizar la creación del usuario.
- Si el usuario es civil, éste envía una solicitud de creación de una cuenta de correo dirigida al Jefe de GRUTEL, pidiendo su respectiva autorización;

- El Jefe de GRUTEL autoriza la creación de la cuenta dejando constancia en la solicitud, la misma que es archivada como respaldo .

- Una vez aprobado, el Jefe de GRUTEL se comunica verbalmente con el Administrador de la red o los técnicos y pide que se cree la cuenta de correo del usuario civil.

- Inmediatamente el Administrador de red o los técnicos proceden a la creación de la cuenta.

La administración de las cuentas de mail está a cargo del Administrador o a falta de éste cualquier técnico del área.

No existe ningún estándar para la creación de las cuentas de correo, en la mayoría de los casos el usuario escoge el nombre de usuario.

Para la eliminación de cuentas, el Administrador de red o los técnicos, rara vez revisan el servidor de correo, eliminando las cuentas inactivas.

b) Mantenimiento de claves de usuarios

Al ser creados los usuarios y haber sido asignados los nombres de usuarios y contraseñas, éstas solo son modificadas si se presenta algún tipo de inconveniente con respecto a intrusos en la Red, detectados por el Administrador.

Con lo que tiene que ver con las claves del Servidor Principal o Administrador, esta si se la cambia a diario y esto está a cargo del Administrador que en este caso es una sola persona, para el resto de personas de no tener ninguna novedad por parte de los usuarios de la red no se realiza cambio, lo único que puede hacerse si así lo requiere el usuario, es el usar una contraseña temporizada, pero la mayor parte de usuarios no lo hacen.

3.3. SEGURIDADES EN LA RED EXISTENTES

Por ser el Comando Conjunto de las Fuerzas Armadas una Institución en la que reposa la seguridad de un País, las seguridades que existen deben ser escogidas luego de un exhaustivo análisis, y tomando en cuenta todos los avances tecnológicos existentes en el mercado.

Los avances de la tecnología también traen problemas para las personas e instituciones que hacen uso de Redes de Información para lo cual todos los que usan dicha herramienta deben contar con algún tipo de seguridad para su información junto a los avances de la informática y las comunicaciones en los últimos años, ha surgido una hueste de apasionados de estas tecnologías, que armados con sus ordenadores y conexiones a redes como Internet, ha logrado humillar a instituciones tan potencialmente seguras.

Existe una serie de grupos que tienen un carácter supranacional, y que se extiende a través de su hábitat natural: Internet, a través de este medio intercambian información y experiencias, al mismo tiempo que logran un cierto grado de organización. Esto ha disparado la alarma en algunos ámbitos gubernamentales, dado que una acción coordinada que afectara a varios sistemas estratégicos de un país puede ser igual de desestabilizadora que las actividades terroristas.

De todas formas, el exceso de prudencia es contrario a la innovación y, por tanto, se están adoptando medidas que garanticen una cobertura suficiente: la adquisición de herramientas de software para la gestión de red, firewalls (cortafuegos, programas especializados en la protección de redes y sistemas), y software de auditoría; la elaboración de planes de seguridad tanto física como lógica y de las políticas correspondientes; y, por último, la mentalización de los usuarios para el correcto uso de los servicios que se prestan.

3.3.1. Listas de control de acceso en equipos de comunicación

En el router se encuentra configurado las listas de control de accesos que permite o niega el ingreso a la administración del equipo, a las direcciones IP's que intenten hacerlo.

Las listas de control de acceso (ACL Access Control List) son secuencias de sentencias de permiso (permit) o denegación (deny) que se aplican a los paquetes que atraviesan dicha interfaz, en el sentido indicado (entrada/salida), con riguroso orden según hayan sido declaradas. Cualquier tráfico que pasa por la interfaz debe cumplir ciertas condiciones que forman parte de la ACL.

Las ACL filtran el tráfico de red controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete para determinar si se debe enviar o descartar, según las condiciones especificadas en la ACL. Entre las condiciones de las ACL se pueden incluir la dirección origen o destino del tráfico, el protocolo de capa superior, u otra información.

Las ACL son utilizadas para priorizar tráfico, para mejorar el rendimiento de una red, restringir acceso de tráfico no deseado, aumentar la seguridad, introducir control administrativo o de protocolos como e-mails, etc.

Al conjunto de sentencias que forman la ACL se le llama grupo. Los pasos a seguir para crear una ACL son:

- Definir la lista que formará un grupo

    access-list ***número*** .....sentencia..

    access-list ***número*** .....sentencia..

La última sentencia implícitamente es negar (deny any)

- Se aplica dicha ACL sobre las interfaces en el sentido deseado

    ip access-group ***número*** ***(entrada/salida)***

3.3.2. Software de seguridad implementado

COMACO por ser una Institución Militar, la más importante del país, maneja información sumamente confidencial, la misma que si llega a manos maliciosas puede causar problemas muy graves, es por esto que es necesario mantener dicha información a buen recaudo, motivo por el cual existe una red de datos interna, la cual maneja tres sistemas específicos que son: PLAMA (Plan Maestro en donde se manejan los presupuestos), Sistema de Documentos (sistema que manejan los archivos) y Sistema de Personal (base de datos de los empleados). Dicha red no tiene conexión hacia el mundo exterior, esto significa que las computadoras personales en donde están configuradas estos sistemas, no pueden tener la configuración del Internet, los usuarios no pueden acceder al Internet desde éstas computadoras.

En cada uno de los servidores existe un pequeño programa de IP-tables que se ejecuta cuando el servidor está en funcionamiento, dicho programa enlista a ciertas IP's sospechosas que han intentado ingresar al servidor, y la siguiente vez que el intruso quiera acceder no podrá hacerlo.

Todos los servidores tienen bloqueado el acceso a su dirección IP, esto quiere decir que ninguna persona externa podrá realizar un ping a ninguna de las direcciones IP's de los servidores así como tampoco podrán realizar Telnet ya que éste comando está deshabilitado.

Mediante el PacketShaper se puede bloquear la navegación a páginas web específicas, las mismas que distraen a los empleados en la realización de su trabajo. Se crea la lista con las direcciones de las páginas web a las cuales se niega el acceso, la misma que puede ser modificada cuando el administrador lo crea conveniente.

3.3.3. Funcionamiento de Packeteer

Este equipo tiene implementado PacketShaper que es un software de gestión del tráfico de aplicaciones, basado en la inteligencia a nivel de aplicación de Packeteer, PacketShaper supervisa, controla y acelera el tráfico en la red, proporcionando así una elevada calidad de servicio a las aplicaciones críticas y permitiendo el alineamiento de los recursos de red de una organización con sus necesidades de negocio.

El enfoque en cuatro pasos de PacketShaper para salvaguardar el rendimiento de las aplicaciones permite controlar los nodos congestionados de la Red de Área Extendida (WAN) y de acceso a Internet.

a) Clasificación: *PacketShaper clasifica automáticamente el tráfico de red en categorías, basándose en criterios de aplicación, protocolo, subred, URL y otros. PacketShaper va más allá de los esquemas estáticos de correspondencia de número de puerto y de dirección IP. Identifica cientos de aplicaciones, desde Oracle y SAP hasta Gnutella y KaZaA.*

b) Análisis: PacketShaper recopila más de 60 métricas por cada tipo de tráfico, a fin de proporcionar un análisis detallado de la utilización de la red, del rendimiento de aplicaciones y de la eficiencia de la red. Un diagnóstico en profundidad revela la fuente de problemas complejos de rendimiento.

c) Control: PacketShaper protege y acelera las aplicaciones críticas gracias a la asignación del ancho de banda, el control del tráfico y la aceleración de éste mediante políticas predeterminadas. Así, pueden especificarse mínimos y máximos de ancho de banda para proteger las aplicaciones críticas, prohibir el tráfico no autorizado y contener a aplicaciones que desbordan los recursos sin ser urgentes. Distribuya dinámicamente el ancho de banda por aplicación, usuario o cliente. La tecnología de aceleración Xpress de PacketShaper combina la compresión con inteligencia a nivel de aplicación con técnicas de gestión activa para simplificar el despliegue y maximizar el beneficio.

d) Informes: PacketShaper ofrece una gran variedad de información: informes, gráficas y estadísticas vía Protocolo Simple de Gestión de Red (SNMP) y XML. Gracias a los compromisos sobre el nivel de servicio (SLAs), pueden definirse los estándares de rendimiento, comparar el rendimiento actual con los objetivos de nivel de servicio y generar informes sobre el cumplimiento de dichos objetivos.

3.4. DETERMINAR VULNERABILIDADES DE LA RED

3.4.1. Análisis de Vulnerabilidades

Originalmente se obtuvo las facilidades para instalar y configurar la herramienta que permitiría detectar los puntos débiles de la red de datos de COMACO denominada NESSUS, que es un auditor de seguridad remoto que hace posible evaluar módulos de seguridad intentando encontrar puntos vulnerables que deberían ser reparados; compuesto por dos partes: un servidor, y un cliente. El servidor/daemon, "nessusd" se encarga de los ataques, mientras que el cliente, "nessus", se ocupa del usuario por medio de una interfaz gráfica. La características principal es la forma en que se obtiene los reportes, los mismos que son fiables, detallados y sugieren una solución para vulnerabilidades encontradas; debido a cambios internos en el área de Telecomunicaciones fue negada la implementación de la herramienta mencionada anteriormente, motivo por el cual no fue posible la obtención de los datos de vulnerabilidades. En sustitución de esto la Evaluación de Riesgos, tratado a continuación:

3.4.2. Evaluación de Riesgos

La Evaluación de riesgos se realiza basada en valores como se puede ver en la Tabla 3.8. para obtener la matriz de riesgos que se observa en la Tabla 3.9.

Ponderación	Descripción
1	Mínimo
2	Grave
3	Crítico

Tabla 3.8. Valoración del Riesgo

CAPÍTULO 4

DISEÑO DEL SISTEMA DE SEGURIDAD

4.1. INTRODUCCIÓN

En este capítulo se presenta el diseño funcional de la red de datos segura, adaptando el modelo SAFE[4.1.] (Modelo de Seguridad para las redes de la Institución) desarrollado por la empresa Cisco Systems, Inc. Este modelo mira la red de datos como una estructura modular, es decir que agrupa componentes y funcionalidades de la red en módulos, tal como se puede observar en la Figura 4.1; por lo que el diseño de seguridad puede ser tratado de manera independiente, módulo por módulo, obteniendo ventajas adicionales como escalabilidad, gestión de seguridad, calidad de servicio y soporte para tecnologías multimedia.

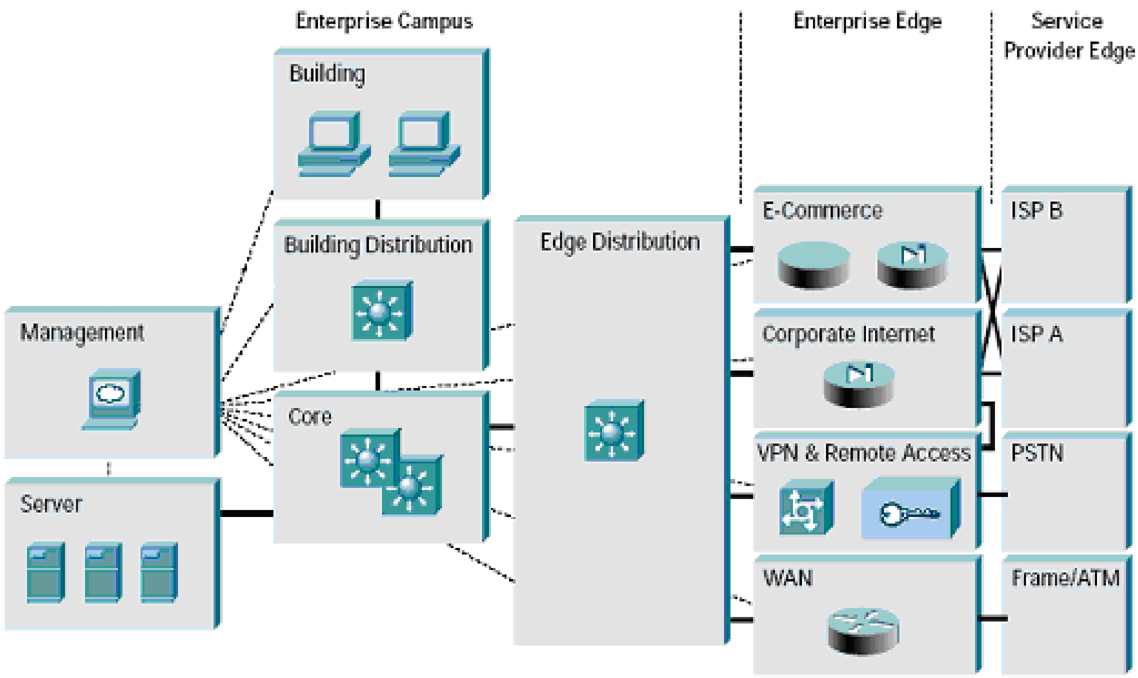


Figura 4.1 Modelo de Seguridad SAFE

(4.1.) http://www.cisco.com/safe_wp.pdf

Se utiliza SAFE debido a que no se pudo obtener datos reales de los requerimientos de seguridad porque no fue posible la implementación de una herramienta para detectar las vulnerabilidades de la red de datos, ya que COMACO maneja información importante y confidencial.

El modelo SAFE se divide en tres bloques funcionales, Campus de la Empresa, Borde de la Empresa y el correspondiente a los proveedores de servicios de telecomunicaciones, este último no será implementado por la Institución, porque SAFE define características que debe cumplir un proveedor para disminuir ataques hacia la red. Estos módulos realizarán papeles específicos dentro de la red y tienen requerimientos de seguridad puntuales, pero dependiendo de sus funciones pueden ser agrupados para esquematizar la red real.

Dentro del Campus de la Empresa se puede observar los siguientes módulos con sus respectivas funcionalidades:

- Módulo Administración: Su meta principal es facilitar la gestión y control de datos de todos los dispositivos y hosts dentro de la Institución.

- Módulo Edificio: Este módulo agrupa a todas las estaciones de trabajo y sus concentradores que se encuentran en el campus de la Empresa.

- Módulo Distribución del Edificio: Está constituido por los dispositivos que permiten la interconectividad entre el módulo Edificio y los demás módulos de la red.

- Módulo Núcleo: Constituye el módulo central de la red, su función es la de administrar rutas y conmutar tráfico tan pronto como sea posible.

- Módulo Servidor: En este módulo se encuentran todos los servidores, datos y aplicaciones que utilizan los usuarios de la red.

- Módulo Borde: El objetivo de este módulo es ofrecer conectividad entre los elementos de la periferia y la red interna de la Institución, a través de su núcleo.

Dentro del módulo Borde se encuentran los siguientes módulos:

- Módulo WAN: Su finalidad es permitir el tráfico entre oficinas remotas de la Institución y la matriz, utilizando para ello protocolos como Frame Relay, ATM, etc.

- Módulo VPN y Acceso Remoto: Se encarga de determinar el tráfico VPN proveniente de usuarios y sitios remotos, así como de usuarios tradicionales que se conecten vía llamadas telefónicas entrantes.

- Módulo E-Commerce: Este módulo abarca las aplicaciones de comercio electrónico dentro de la Institución, y es uno de los más delicados, ya que debe lograr el equilibrio entre: facilidad de acceso y seguridad.

- Módulo Internet Corporativo: Se encarga de la conectividad entre los usuarios internos a los servicios de Internet y de los usuarios externos hacia la información de la Institución que esté disponible al público.

El modelo SAFE es un sistema de defensa y protección de datos para organizaciones y empresas de todos los tamaños, que brinda una solución de inversión a bajo costo para así prestar buenos servicios. Al usar esta arquitectura no es necesario la utilización de equipos Cisco Systems, Inc. debido a que dicho modelo ofrece las pautas de seguridad hacia el acceso a Internet con tecnologías diferentes.

SAFE se basa en la seguridad por módulos, emulando los requerimientos funcionales de las redes de la Institución, las decisiones de la implementación varían de acuerdo a los requisitos de la funcionalidad de cada red, sin embargo los objetivos de diseño son enumerados según el orden de prioridad:

- Políticas de Seguridad contra ataques.
- Informe y gestión de la seguridad.
- Autenticación y Autorización de usuarios y administradores hacia los recursos críticos de la red.
- Detección de intrusos hacia los recursos de la red.

Los módulos de la arquitectura SAFE proveen flexibilidad a los usuarios, los mismos que pueden ser desarrollados por fases, según las necesidades de la Institución, lo que permite optimizar la infraestructura de seguridad existente, identificando dónde y por qué los productos de seguridad críticos y las tecnologías (Firewall, NIDS, VLAN's) son necesarios.

A continuación se presenta un diagrama de la red de datos actual de COMACO distribuida en los módulos y funciones propuestos por el modelo SAFE. Ver Figura 4.2

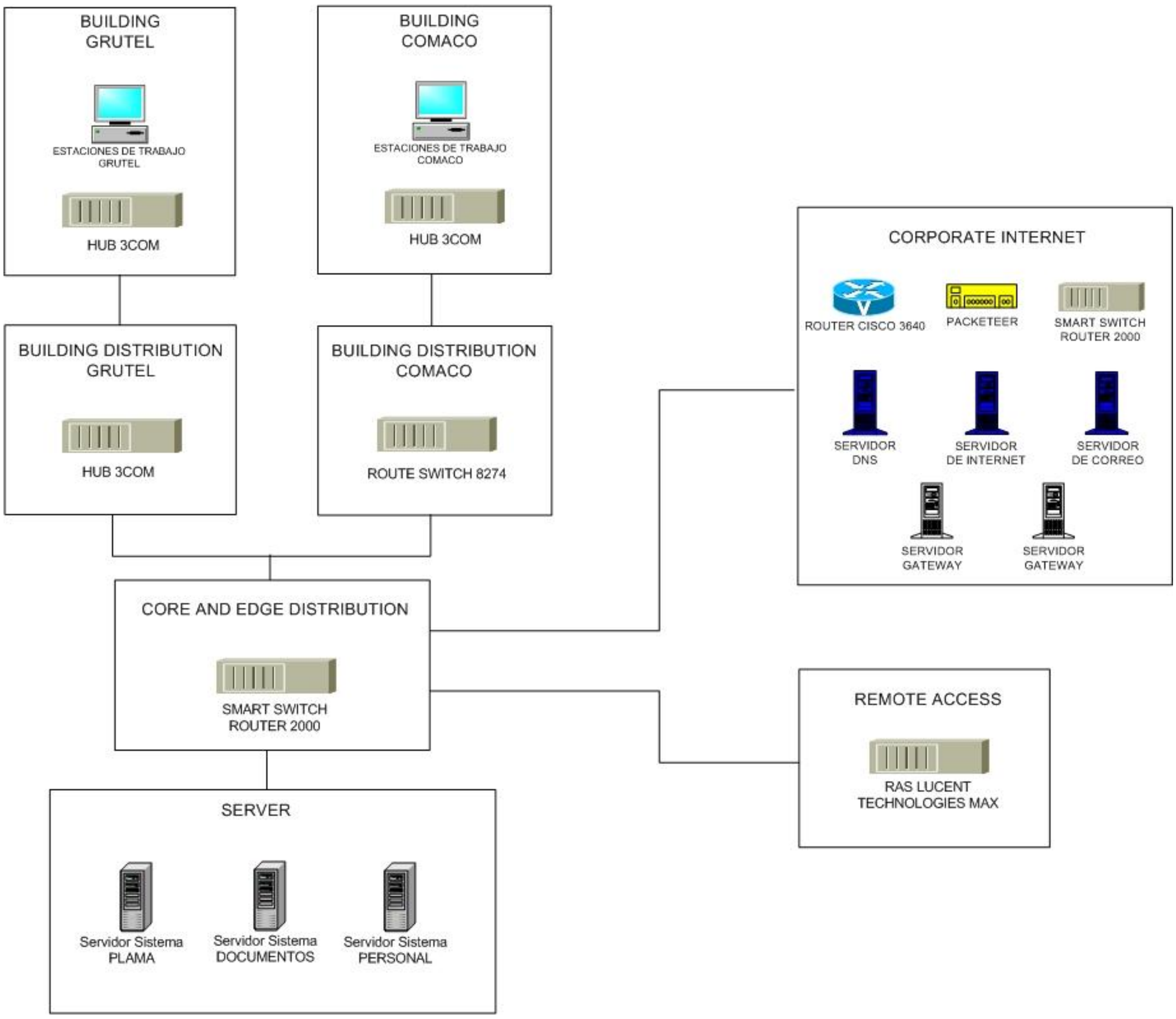
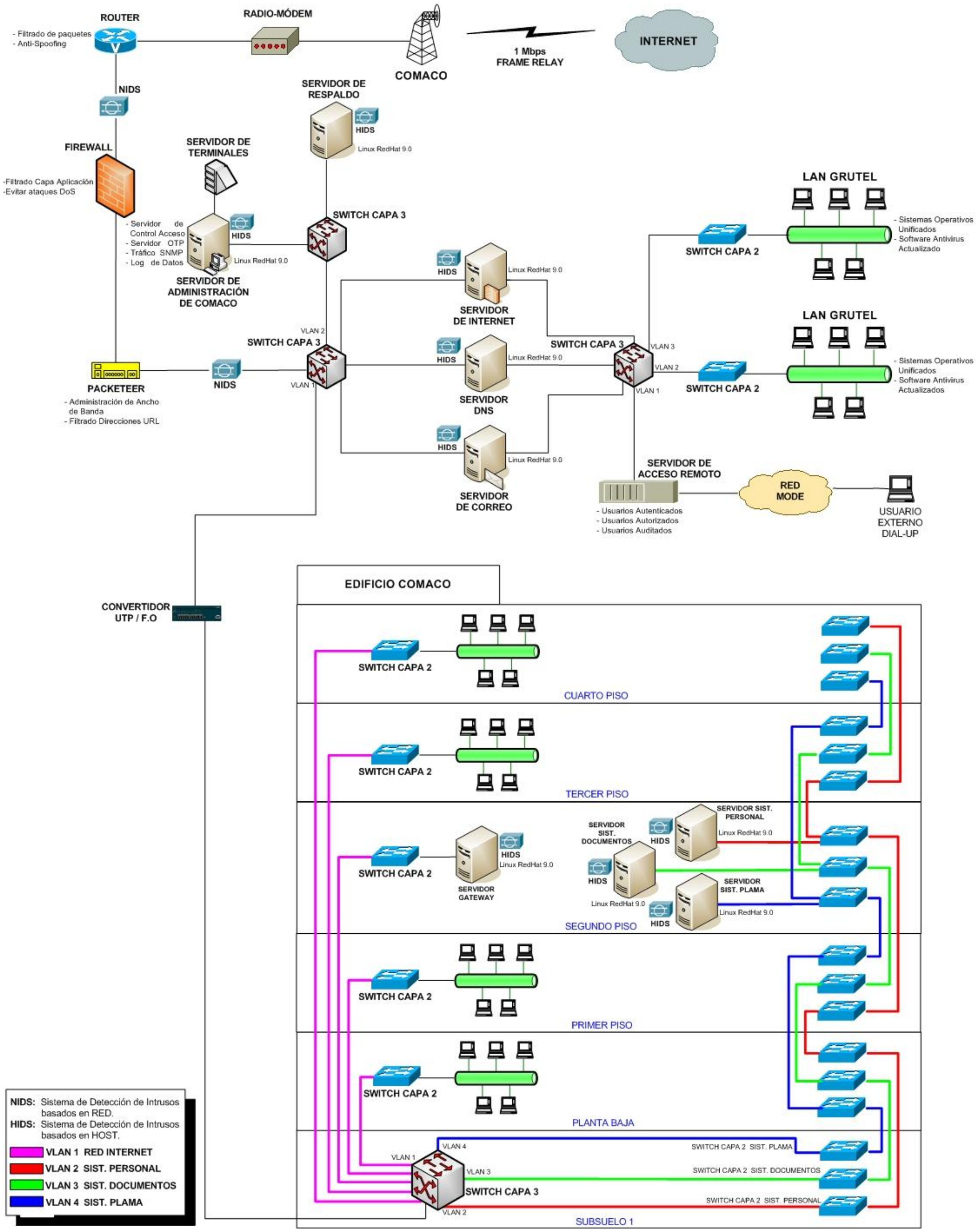


Figura 4.2 Diagrama Lógico de la red de datos de COMACO actual adaptada a SAFE

4.2. PROPUESTA DE DISEÑO DE LA RED SEGURA DE COMACO

En esta sección se describe las seguridades específicas para cada uno de los módulos que integran la red de datos de



COMACO. Ver Figura 4.3

Figura 4.3 Modelo de Seguridad Propuesto de la red de datos de COMACO

En la Figura 4.4 se observa el diagrama de la red de Administración de COMACO propuesta, la misma que se estructura en una red fuera de banda separada de la de producción, evitando de esta manera que el flujo de tráfico se congestione.

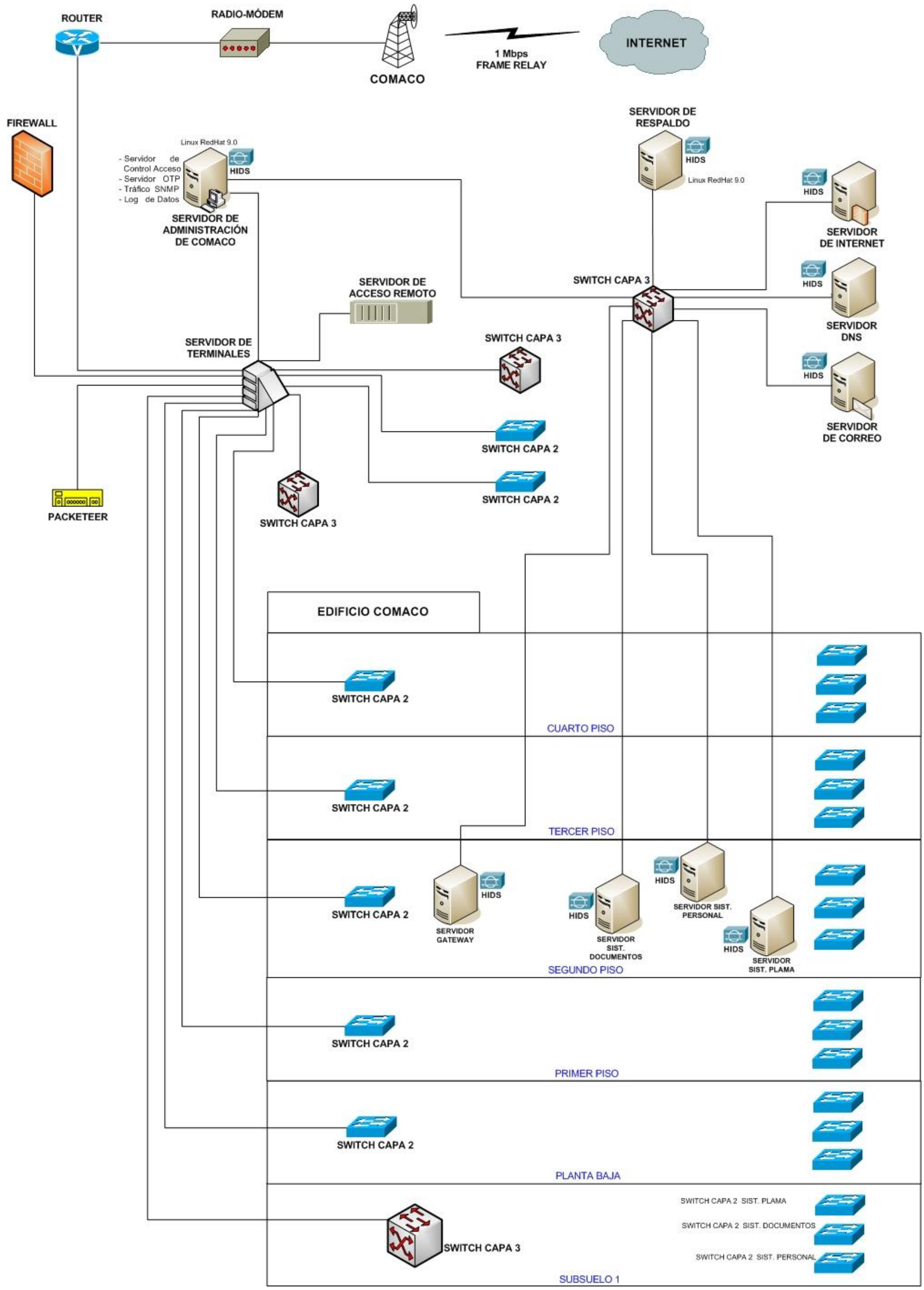


Figura 4.4 Red de Administración de COMACO Propuesta

4.2.1. MÓDULO ADMINISTRACIÓN PROPUESTO

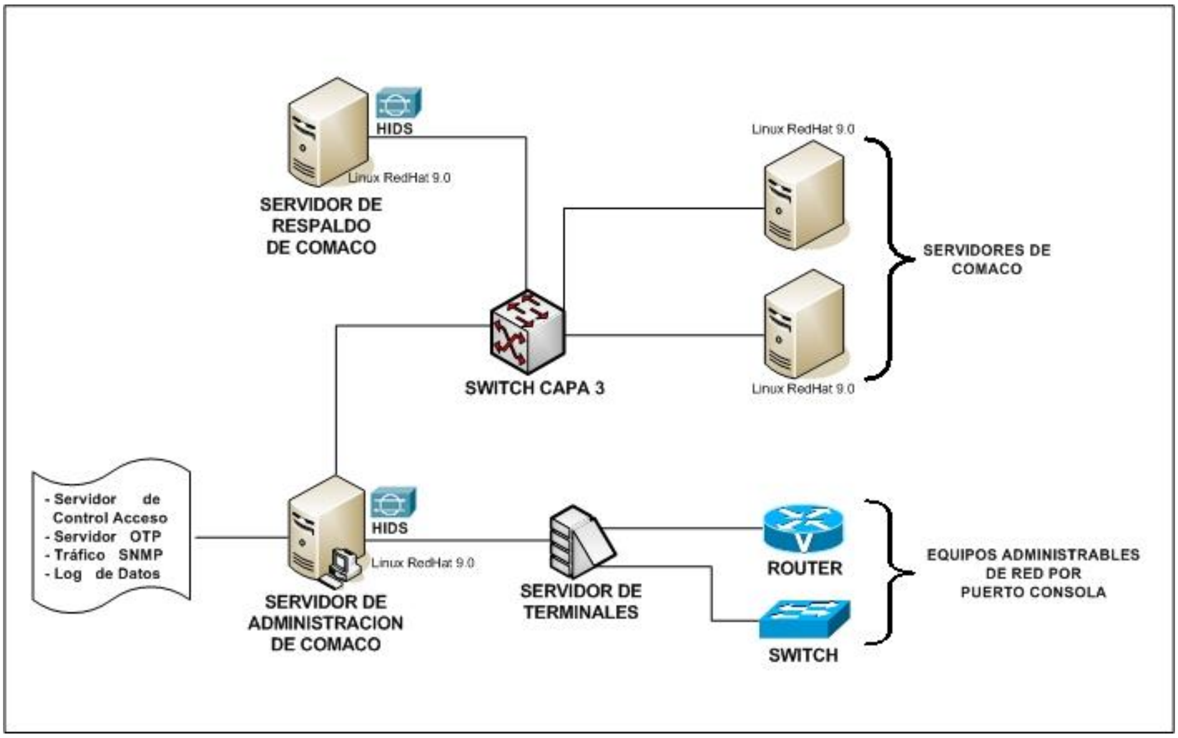


Figura 4.5. Módulo Administración Propuesto

La red de datos de COMACO dentro de su infraestructura no cuenta con hardware y software que permitan la administración de los dispositivos existentes, por lo que es necesario la implementación del Módulo Administración, cuyo objetivo principal es facilitar la administración segura de todos los dispositivos y hosts dentro de la Institución. Este módulo propone equipos que garanticen, por un lado el acceso a los servicios que ofrece la red y por otro, recopilar la información almacenada en los diferentes archivos logs (registro de accesos fallidos o exitosos, tráfico de ingreso y salida, etc.) propios de cada dispositivo de la red de datos.

Por la información confidencial que se intercambia entre éste módulo y los dispositivos administrados, es necesario evitar que el tráfico con fines administrativos sea interceptado desde cualquier punto de la red. Además, se debe evitar ataques por

suplantación de identidad, acceso no autorizado y ataques de claves. Para esto se implementará en un solo servidor todas las funciones tales como: servicio de control de acceso, servicio OTP (On-Time Password), tráfico SNMP (Simple Network Management Protocol) y log de datos de la red; el cual estará conectado hacia un Terminal Server que será el punto de unión de todos los puertos de consola de los dispositivos a ser administrados, y para la administración de los servidores se realizará mediante una tarjeta de red independiente; de esta manera la subred administrativa será creada completamente separada de la red de producción, es decir, que la administración se realizará en una red OOB (Fuera de Banda). Los servidores serán administrados mediante una tarjeta de red independiente que estarán conectados un switch capa 3, el mismo que será utilizado únicamente para la gestión en la red OOB (Fuera de Banda).

Porque la red administrativa tiene acceso total a todos los componentes de los módulos de la red, puede ser un blanco muy atractivo para los hackers. La primera amenaza es que un hacker intente acceder a la red administrativa, la misma que se puede atenuar configurando correctamente las seguridades de todos los demás módulos.

El control de acceso a este servidor será a través de un firewall, que será configurado en el módulo Internet Corporativo, a fin de evitar la apropiación de la información que fluye por la red administrativa, de todos los componentes de los módulos de la red. Y las VLAN's implementadas en el módulo Núcleo que obligan a que todo el tráfico sea redireccionado hacia el firewall para su debido filtrado, evitan que un dispositivo que va a ser atacado, no pueda comunicarse con otros hosts en la misma subred, mitigando de esta manera la amenaza conocida como explotación de la confianza, ataque donde un individuo se aprovecha de una relación de confianza dentro de una red.

Para contrarrestar los ataques de contraseñas, se implementará un servidor OTP (On-Time Password), cuya función es asignar

claves diferentes en cada acceso, para garantizar que al querer descifrar la contraseña , solamente obtenga información irrelevante. En este servidor también se instalará un HIDS (Sistema de Detección de Intrusos en el Host) configurado para que en cualquier situación anormal se de una respuesta inmediata.

El tráfico SNMP (Protocolo Simple de Gestión de Redes), que permite la gestión remota de los dispositivos de red, tales como switch, router y servidores; constituye un hueco de seguridad peligroso, por lo que solamente los dispositivos que requieren modificaciones serán administrados desde el servidor, los demás tendrán sólo permisos de lectura. El SNMP puede ser configurado como lectura/escritura únicamente en una red OOB (Fuera de Banda).

Como se mencionó anteriormente, en el servidor estará configurado para recopilar el contenido de la información presente en los archivos syslog, de los cuales se puede obtener datos importantes como: cambios en las configuraciones y violaciones de seguridad registradas en cada uno de los dispositivos administrativos, esta información no minimiza los ataques, sino que sirve como alerta sobre situaciones anormales que sucedan en la red.

Es necesario la implementación de un servidor de Backup, el cual permitirá realizar los respaldos de la información de los servidores y las configuraciones de los dispositivos, sin originar tráfico en la red de producción, aprovechando la red OOB (Fuera de Banda).

4.2.2. MÓDULO EDIFICIO PROPUESTO

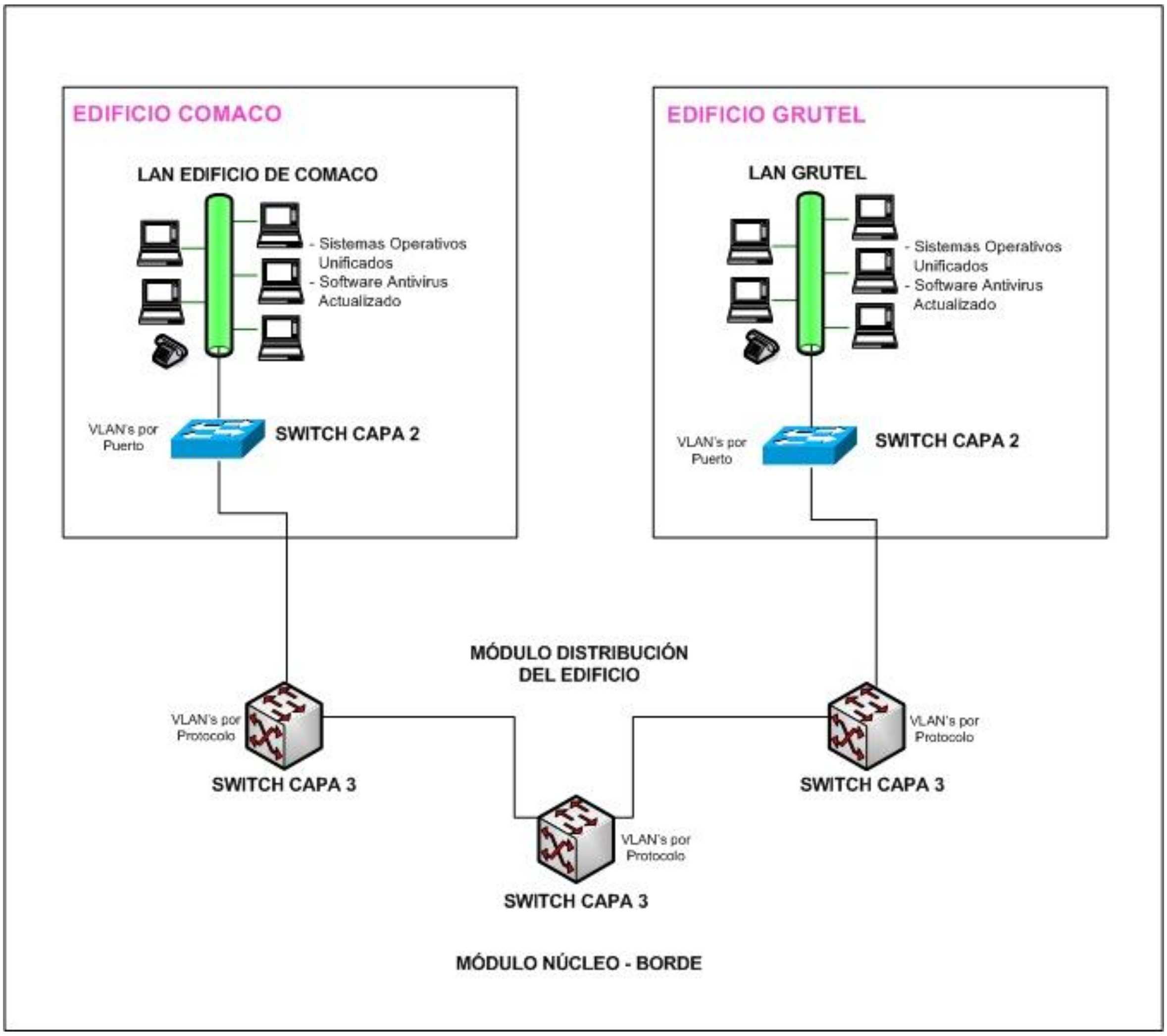


Figura 4.6 Módulo Edificio Propuesto

El módulo Edificio se define como una porción de la red que contienen estaciones de trabajo, teléfonos, concentradores. El objetivo principal de este módulo es proporcionar servicios a los usuarios finales.

Las vulnerabilidades primarias para los sitios de trabajo del usuario final son los virus y los troyanos, que se refieren a un software malicioso que se une a otro programa para ejecutar una función particular indeseada en el sitio de trabajo de un usuario; así como también la recolección de información, mapeo de recursos, y pueden ser provocados por personas con libre acceso a los recursos de la red como: empleados descontentos, aficionados al download, usuarios curiosos o descuidados al mantener claves simples o máquinas desatendidas.

En este módulo los computadores y los concentradores están bajo la administración de la Institución, por lo tanto es necesario evitar que los datos que circulan por el medio de comunicaciones sean extraídos por programas tipo sniffer, ataque que permite la obtención de gran cantidad de información sensible enviada sin encriptar como: usuarios, claves, direcciones de correo, números de tarjetas de crédito.

Para conseguir un nivel de seguridad adecuado en este módulo, se requiere implementar normas y procedimientos que regulen y auditen la actividad del usuario interno en la ejecución de tareas.

Un esquema de seguridad adecuado para este módulo dentro de la Institución debe incluir concentradores tipo switch capa 2 con capacidad para configurar VLAN, en el que se debe considerar lo siguiente:

- Inhabilitar todos los puertos sin uso, esta disposición evita que los hackers se conecten por medio de esos puertos sin uso y se comuniquen con el resto de la red.
- Los puertos no deben ser configurados como AUTO, impidiendo que cualquier usuario de la red pueda recibir todo el tráfico que circula por ella.
- A cada puerto se asocia un número limitado de direcciones MAC, evitando la inundación de estas direcciones y otros ataques.
- Como las VLAN's no proporcionan funciones de seguridad tales como confidencialidad y autenticación, se debe tener cuidado en la seguridades cuando se implemente LAN virtuales en cualquier ambiente. La filtración además de la segmentación de VLAN proporciona una defensa en el acceso entre dos subredes.

Las estaciones de trabajo que conforman este módulo son consideradas como el medio de mayor disponibilidad para atacar la red, ya que existen numerosas plataformas de hardware, sistemas operativos y aplicaciones, que necesitan ser actualizados con sus respectivos parches, los mismos que serán evaluados en un sistema de prueba antes de ser implementado en la red. Los usuarios finales deben cumplir estrictamente las normas de seguridad detalladas en el capítulo anterior referente a políticas de seguridad.

Es indispensable implementar un software antivirus en las estaciones de trabajo, el cual será actualizado periódicamente, y se recomienda versiones corporativas existentes en el mercado.

4.2.3 MÓDULO DISTRIBUCIÓN DEL EDIFICIO PROPUESTO

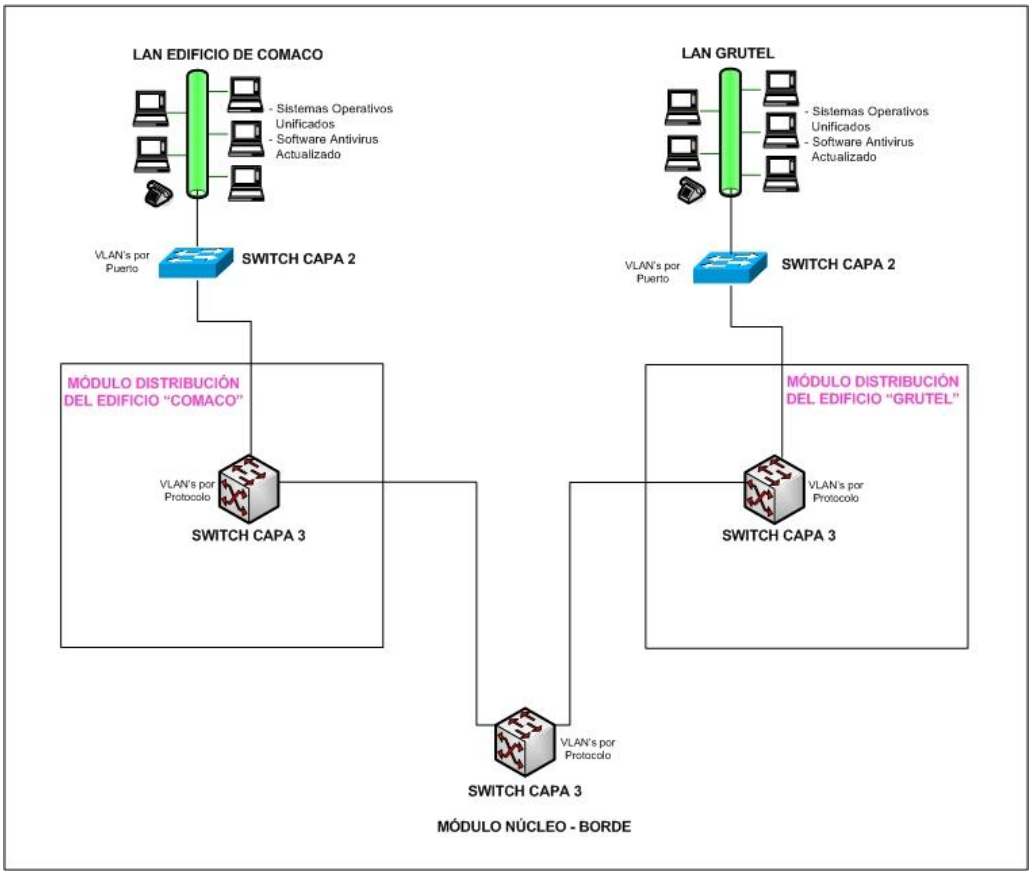


Figura 4.7 Módulo Distribución del Edificio Propuesto

El objetivo del módulo Distribución del Edificio es agrupar todos los equipos que permiten la distribución de servicios hacia el módulo Edificio, éstos incluyen el encaminamiento, calidad de servicio (QoS) y control de acceso, siendo así, estos equipos deben controlar el acceso a la información para mantener su confidencialidad y evitar el ataque de spoofing interno (suplantación de la dirección IP origen), que son técnicas empleadas para realizar ataques como la denegación de servicios.

La detección de intrusos será implementada en los módulos que contienen los recursos que son probables de ser atacados por su

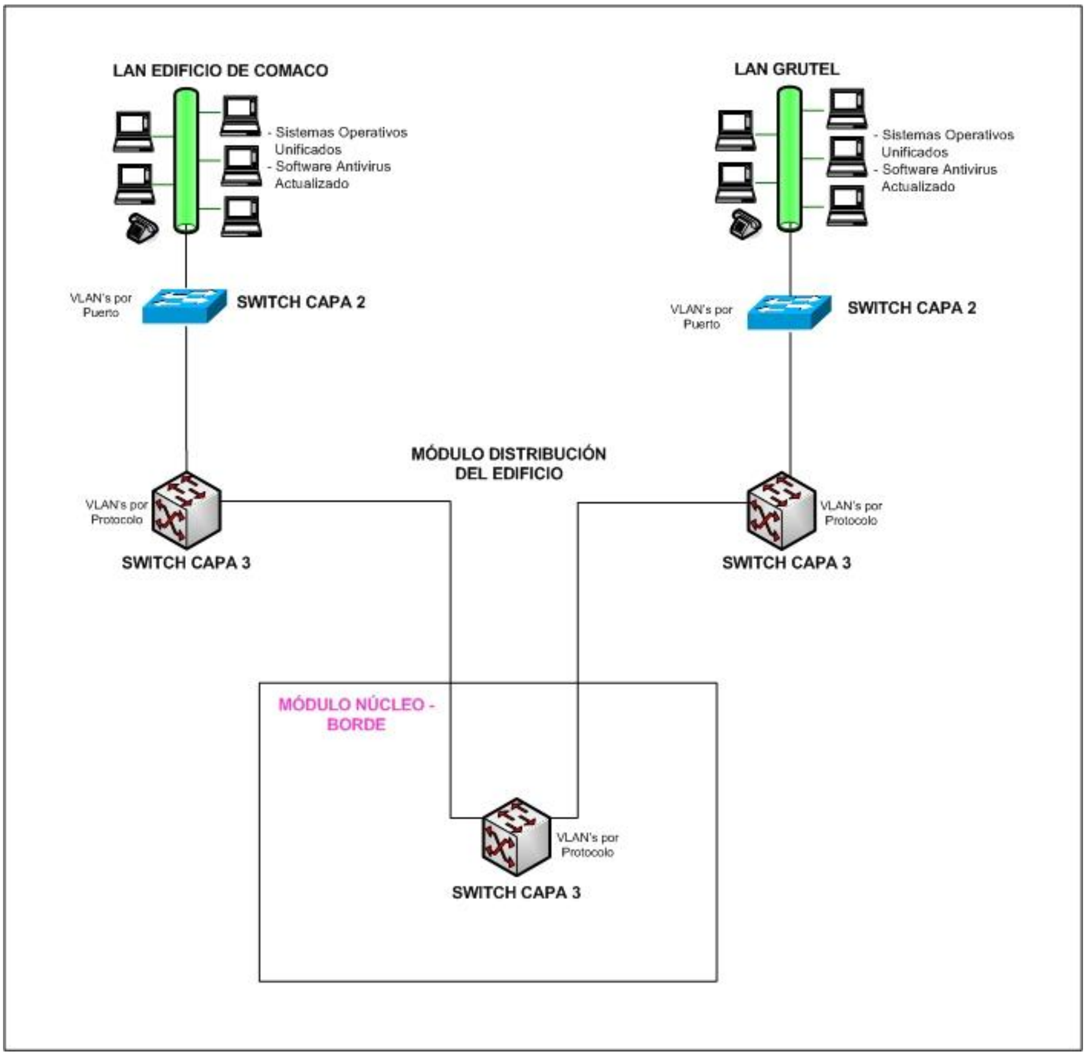
contenido (servidores, acceso remoto, internet, etc.). Este segmento proporciona la primera línea de defensa y prevención contra ataques originados internamente.

Para la configuración se necesita un switch de capa 3 que debe cumplir con las características principales de seguridad, debido a la infraestructura de COMACO se necesitan dos equipos que cumplan con la función de Distribución del Edificio. GRUTEL posee un HUB que en este momento realiza la función del módulo de Distribución del Edificio, el mismo que no cumple con los requerimientos de seguridad, tales como: es un medio compartido, todos los puertos son un solo dominio de colisión, no permite privacidad, prioridad, QoS (calidad de servicio) y configuración de VLAN's; motivo por el cual debe ser cambiado por un switch de capa 3. El Edificio de COMACO posee un RouteSwitch 8274 que cumple con las funciones de seguridad por lo tanto es el apropiado para este módulo.

4.2.4. MÓDULO NÚCLEO-BORDE PROPUESTO

El objetivo del módulo Núcleo-Borde es filtrar y conmutar el tráfico tan rápido como sea posible de una red a otra, y facilitar la conectividad de los elementos del borde hacia la red interna. Ver Figura 4.8.

La plataforma de hardware que permite realizar este control de acceso es un switch de capa 3, el cual garantiza el tráfico de datos entre nodos de la red por medio de VLAN's (redes



virtuales) y port trunking (duplicación de la capacidad de transmisión), definidas en el Sistema Operativo del equipo. Adicionalmente la configuración de este dispositivo debe cumplir con lo expuesto en el RFC 2827 que tiene como objetivo prevenir spoofing de direcciones locales.

Figura 4.8 Módulo Núcleo-Borde Propuesto

La configuración de este switch debe impedir el acceso al dispositivo utilizando telnet o SNMP, y a su vez establecer niveles de acceso a fin de otorgar diferentes derechos de uso de la información almacenada en él.

Debe ser aplicada en este dispositivo la opción de STP (Spannig Tree Protocol) que permite deshabilitar puertos que no son utilizados, además todos los puertos que tengan esta característica deben ser agrupados dentro de una misma VLAN en el switch.

El uso de las VLAN's dentro de este dispositivos prevee un nivel de seguridad adicional al de las redes de área local tradicionales que permite dirigir el tráfico de las aplicaciones solamente entre puertos que corresponden a la misma VLAN evitando así que los puertos aislados escuchen esta información.

El equipo que actualmente posee COMACO posee las características que se requieren para el módulo Núcleo-Borde, entonces se mantendrá el mismo Smart Switch Router 2000, tomando en cuenta que se debe actualizar periódicamente su sistema operativo con sus respectivos parches, así como también se debe configurar de manera que se cumpla con lo descrito en el párrafo anterior.

4.2.5. MÓDULO SERVIDOR PROPUESTO

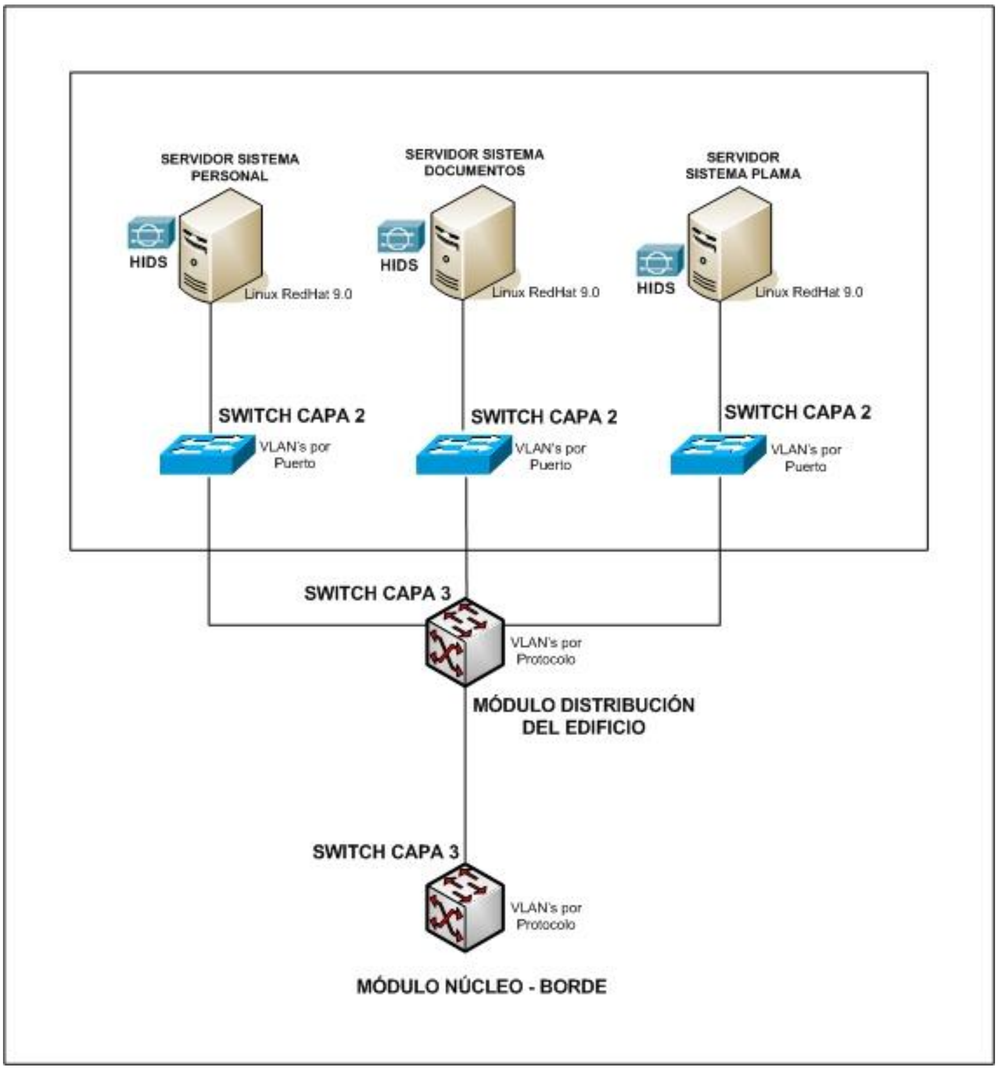


Figura 4.9 Módulo Servidor Propuesto

El objetivo principal de este módulo es proporcionar servicios, aplicaciones a los usuarios finales y dispositivos, el tráfico en este módulo es examinado por la detección de intrusos dentro del switch de capa 3, configurado en el módulo Núcleo-Borde.

COMACO posee una red interna que no tiene conexión al Internet, en donde se encuentran tres servidores, cada uno de los cuales tiene implementado un sistema específico, los mismos que son: PLAMA (Plan Maestro para presupuestos), Documentos y Personal; que por motivos de seguridad y políticas de la Institución no se tuvo acceso a la información y configuración que se manejan en estos tres servidores. Por lo que no fue posible la obtención de los requerimientos, razón por la cual se propone el diseño del modulo de servidor basado en el Modelo SAFE.

Los servidores pueden convertirse en el punto de los ataques originados internamente, por lo cual un primer nivel de seguridad en este módulo será cumplir con las políticas de seguridad de servidores y manejo de contraseñas detalladas en el capítulo de Políticas de Seguridad.

Para garantizar el acceso hacia los servidores se debe implementar un servidor RADIUS como mecanismo de autenticación de usuarios, servidor que permite las funciones de seguridad “AAA” (Autenticación, Autorización, Auditoría) y el uso de las herramientas como detectores de intrusos de hosts.

Cada uno de los servidores que conforman este módulo en la red de datos, debe incorporar un HIDS (Sistema de Detección de Intrusos en el Host) para incrementar la seguridad, ya que en estos servidores se almacena información importante para la Institución, como sus sistemas transaccionales, bases de datos, históricos, presupuestos etc; y son considerados críticos en el funcionamiento de la red. Esta configuración de seguridad, los HIDS (Sistema de Detección de Intrusos en el Host) en los servidores y los NIDS (Sistema de Detección de Intrusos en la Red) en el switch del módulo Núcleo-Borde, permitirá complementar el sistema de detección de intrusos.

4.2.6. MÓDULO INTERNET CORPORATIVO PROPUESTO

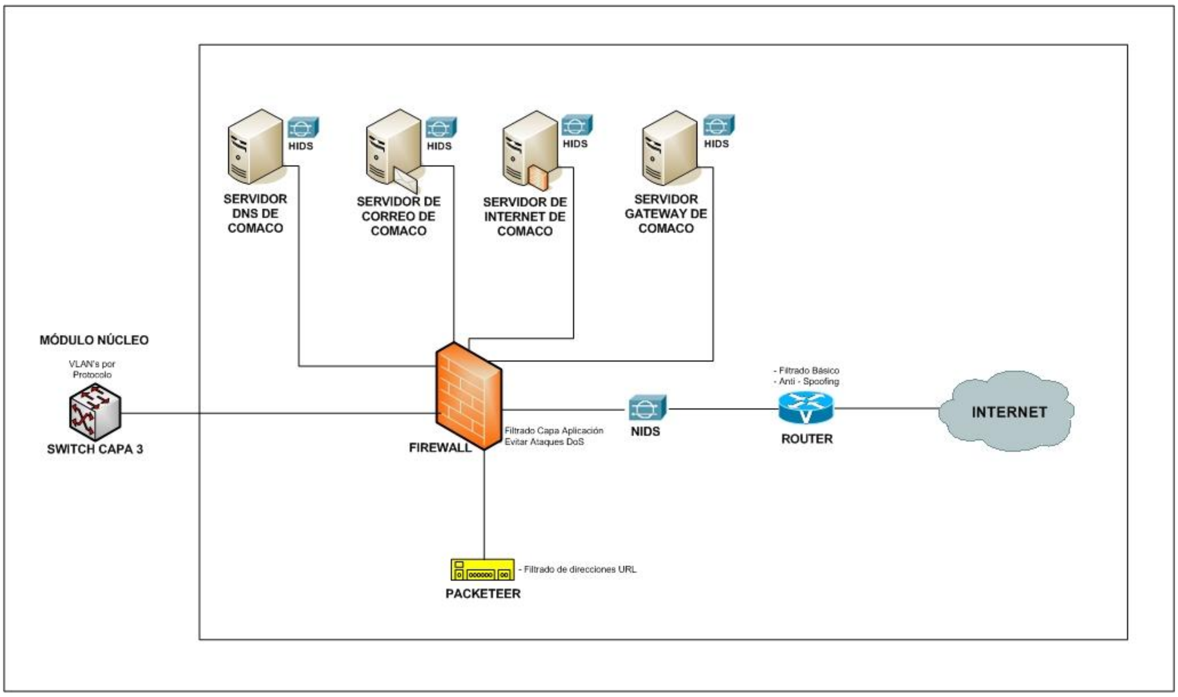


Figura 4.10 Módulo Internet Corporativo Propuesto

El módulo Internet Corporativo proporciona a los usuarios internos, conectividad para el acceso de los servicios de Internet, y a los usuarios de Internet acceso a los servidores públicos, mediante una conexión dial-up detallada en el siguiente ítem de Acceso Remoto.

En necesario monitorear y controlar el uso de Internet, a fin de que esta herramienta se emplee para beneficio de la Institución y no sirva como medio de difusión de archivos basura que pueden llevar inmersos, virus o troyanos que terminen afectando el rendimiento de la red. Más detalladamente se puede observar en el capítulo de Políticas de Seguridad.

En este módulo es necesario contar con un Firewall, que es un sistema o grupo de sistemas que imponen una política de seguridad entre la organización de la red privada e Internet, puesto que determina los servicios de red que pueden ser accesados por los usuarios externos para utilizar los recursos de red. Para que un firewall sea efectivo, todo tráfico de información a través de Internet deberá pasar por este, para poder ser inspeccionado, y así proteger los servicios públicos del Internet y los usuarios internos, uno de los beneficios claves de un firewall en Internet es simplificar los trabajos de administración una vez que se consolida la seguridad en el equipo. COMACO posee en su servidor de Internet, la configuración de un firewall-software basado en políticas de iptables, el mismo que cumple con los aspectos descritos .

Las principales características de seguridad que debe poseer el Firewall son:

- Debe limitar conexiones de half-open (en espera de asentimiento) para proteger ataques SYNC hacia los servidores.

- Debe adicionar filtrado de direcciones opuestas, los ataques de retorno se autorizan solamente para una conexión específica y únicamente mientras esta se encuentra activa. Una vez cerrada la sesión no se autoriza ningún paquete de retorno. Esto no es solo conveniente con fines administrativos, sino que ofrece también un mayor nivel de seguridad.

- Cuando un servidor público es atacado, el firewall debe ser capaz de filtrar cualquier requerimiento no autorizado generado por dicho servidor hacia cualquier localización de la red. En adición VLAN's evita que el servidor comprometido ataque a otros servidores en el mismo segmento.

Se debe implementar un servidor de filtrado de direcciones URL, que para la red de COMACO será el Packeteer; mediante el cual se apruebe o se niegue el acceso a sitios no permitidos señalados en el capítulo de políticas de seguridad, este dispositivo de filtrado URL debe mantener su base de datos actualizada. También necesita la implementación de un HIDS (Sistema de Detección de Intrusos en el Host) que protejan ataques que evitan con artificios engañosos el Firewall.

El router es el primer equipo de la red interna encargado de recibir información proveniente de Internet, que debe cumplir con la configuración de técnicas de seguridad como ACL extendidas, NAT, u otras con estándares de seguridad vigentes en la Institución a fin de evitar filtraciones de usuarios y tráfico desconocido que pueda alterar el funcionamiento de la red de datos interna, para lo cual se debe seguir los RFC's 1918, que especifica las redes que son reservadas para uso privado y que nunca se deben considerar a través del Internet público; y 2827, que filtra cualquier tráfico de salida en su red que no tenga una dirección fuente en el rango de IP's de la Institución. Su administración debe realizarse utilizando canales de comunicación seguros, como se describe en la sección del módulo Administración.

También se debe considerar los siguientes aspectos para el Router:

- Deshabilitar el acceso al router mediante el comando TELNET.
- Deshabilitar el acceso mediante SNMP (Protocolo Simple de Gestión de Red), que controla el router.
- Controlar el acceso al router mediante el uso de un TACACS (Terminal Access Controller Access Control System Plus), el mismo que permite el ingreso al equipo mediante la autenticación de usuarios.
- Deshabilitar los servicios innecesarios.
- Acceso al router en varios niveles (lectura, lectura/escritura).
- Autenticación del administrador, para permitir actualizar tablas de ruteo.

Cualquier tráfico IPSec destinado al módulo de Acceso Remoto debe ser ruteado apropiadamente, esto significa que la filtración en la interface conectada a este segmento debe estar configurada para permitir que solamente el tráfico IPSec cruce por ella y cuando el paquete es originado y enviado desde y hacia los pares (head-end) autorizados.

Para asegurar que las redes mantengan el nivel de seguridad se debe supervisar continuamente los ataques y realizar pruebas regularmente del estado de su infraestructura de seguridad. NIDS (Sistema de Detección de Intrusos en la Red) permite que un equipo destinado para la detección de intrusos pueda trabajar sobre una aplicación. Los sistemas de detección de intrusos pueden superar y responder a los acontecimientos de la seguridad mientras ocurre algún tipo de ataque, además proporciona una capa adicional de seguridad, protegiendo el entorno de red y las redes internas cada vez más vulnerables.

Los NIDS (Sistema de Detección de Intrusos en la Red) como medida de seguridad monitorean, auditan o registran la información del uso de Internet y si aparece alguna actividad sospechosa como algún problema en el tránsito de los datos o simplemente la pérdida de la perspectiva de la red, NIDS (Sistema de Detección de Intrusos en la Red) genera una alarma localizando con precisión los cuellos de botella potenciales del ancho de banda. Siendo el administrador el único que puede tomar o no la acción correcta para gestionar sobre el sistema, y hacer uso de la información proporcionada por los archivos logs del sistema.

Al colocar el NIDS (Sistema de Detección de Intrusos en la Red) en el lado público del Firewall alertará sobre intentos de intrusión provenientes de Internet y permitirá detectar el rastreo de puertos que típicamente, señala el comienzo de una actividad de hacking.

El segmento de los servicios públicos (DNS, MAIL, INTERNET) deben tener una aplicación NIDS (Sistema de Detección de Intrusos en la Red) para detectar ataques que los puertos configurados en el Firewall dejaron pasar, estos pueden ser ataques de la capa de aplicación contra un servicio especifico o un ataque de contraseña contra un servicio protegido. Cada uno de los servidores tiene software de detección de intrusos al Host (HIDS), para monitorear la actividad del sistema operativo, así como la actividad en las aplicaciones comunes del servidor (HTTP, FTP, SMTP, etc.). El DNS debe responder solamente a comandos autorizados para eliminar cualquier respuesta innecesaria que pueda asistir a los hackers en el reconocimiento de la red. El servidor SMTP incluye los servicios que inspeccionan el contenido del correo para atenuar los ataques de virus, troyanos, generados contra la red interna que se producen generalmente a través del sistema de correo. El Firewall, filtra estos mensajes del SMTP en la capa de aplicación para permitir solamente comandos necesarios al servidor de correo.

4.2.7. MÓDULO ACCESO REMOTO PROPUESTO

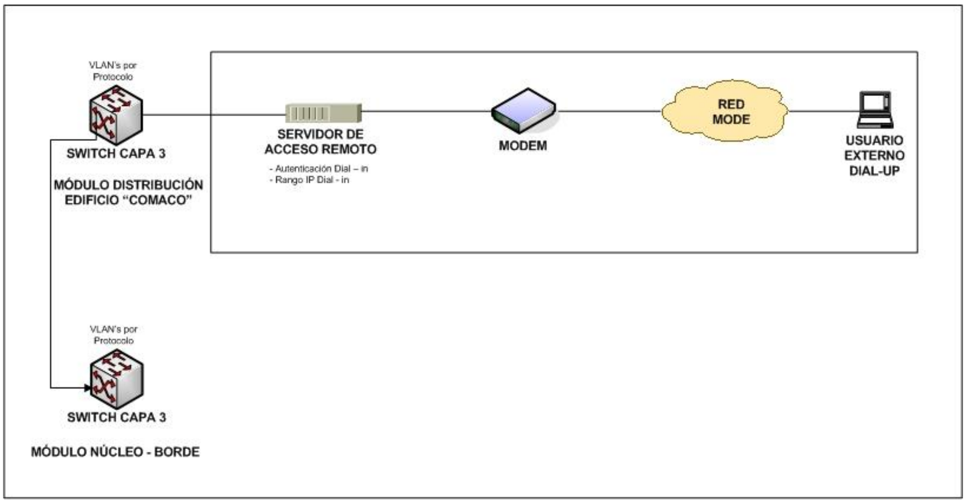


Figura 4.11 Módulo Acceso Remoto Propuesto

El objetivo principal del módulo Acceso Remoto es proteger la red LAN de los usuarios remotos que tengan acceso a ella. Para dichos usuarios se limitará el acceso a los servicios, únicamente podrán utilizar el Internet y el Correo, esta configuración se realizará en el switch de capa 3 ubicado en el segmento de Distribución del Edificio Propuesto.

La forma en que funciona actualmente el módulo de Acceso Remoto es adecuada, debido a que en el RAS Lucent Technologies MAX, se dispone de un protocolo que proporciona un mecanismo probado para autenticar a los usuarios remotos conectados a una red a través de una línea telefónica y que realica las tres funciones de seguridad AAA (Autenticación, Autorización, Auditoría). Una vez que los usuarios son autenticados asigna a sus conexiones un rango de direcciones IP's mientras mantiene la comunicación.

CAPÍTULO 5

DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD

5.1. INTRODUCCIÓN

Las políticas de seguridad informática establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que se desea proteger y el por qué de ello.

Para definir las Políticas de Seguridad en una Institución tan grande como es el Comando Conjunto de las Fuerzas Armadas "COMACO", se debe conocer las políticas existentes a nivel internacional, como ISO 17999:2005, para evaluar y adoptar las que satisfagan las necesidades de la Institución.

Existen sanciones para quienes no cumplan con lo definido en las políticas de seguridad, que pueden ser preventivas y correctivas, dependiendo del grado del delito, éstas pueden basarse en lo legal como: Ley De Comercio Electrónico, Ley de Propiedad Intelectual y Reglamentos Internos de las FF. AA.

5.2. DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD

5.2.1. Servidores y equipos de comunicación

a) Políticas de seguridad para Servidores y Estaciones de Trabajo

Los servidores deberán

- ✓ Funcionar 24 horas del día los 365 días del año.
- ✓ Recibir mantenimiento preventivo de software.
- ✓ Recibir mantenimiento mensual que incluya depuración de bitácoras.
- ✓ Recibir mantenimiento semestral que incluya la revisión de su configuración.
- ✓ Ser monitoreados por el Centro de Datos.
- ✓ La información de los servidores, así como su configuración y bitácoras deberá ser respaldada semanalmente.
- ✓ Los servidores deberán ubicarse en un área física que cumpla las recomendaciones para un Centro de Datos.
  - Acceso restringido.
  - Temperatura adecuada.
  - Protección contra descargas eléctricas.
  - Mobiliario adecuado que garantice la seguridad de los equipos.
- ✓ El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del Centro de Datos, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:
  - Cuando ésta sea una contraseña débil o de fácil acceso.
  - Cuando crea que ha sido violada de alguna manera.
- ✓ El usuario deberá notificar al Centro de Datos en los siguientes casos:
  - Si observa cualquier comportamiento anormal en el servidor.
  - Si tiene problemas en el acceso a los servicios proporcionados por el servidor.
  - Cuando deje de laborar o de tener una relación con la institución.
  - Si un usuario viola las políticas de uso de los servidores, el Centro de Datos podrá cancelar totalmente su cuenta de acceso a los servidores, notificando a las autoridades correspondientes.

- ✓ Los computadores de Comaco sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
- ✓ Los equipos de Comaco generalmente sólo deben usarse para actividades de trabajo y no para otros fines, tales como actividades comerciales privadas o para propósitos de entretenimiento y diversión. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de Comaco.
- ✓ Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática.
- ✓ No se permite fumar, comer o beber mientras se está usando un PC.
- ✓ Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- ✓ Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).
- ✓ Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- ✓ Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
- ✓ Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- ✓ No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de Comaco se requiere una autorización escrita.
- ✓ La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
- ✓ Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
- ✓ Si un PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- ✓ Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.
- ✓ Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- ✓ No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- ✓ Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de Comaco.
- ✓ A menos que se indique lo contrario, los usuarios deben asumir que todo el software de Comaco está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- ✓ Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de Comaco, sin la aprobación previa de la gerencia.
- ✓ No pueden extraerse datos fuera de la sede de Comaco sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan computadoras portátiles o están conectados a redes como Internet.
- ✓ Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.
- ✓ Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de Comaco.
- ✓ No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

- ✓ Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.
- ✓ Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.
- ✓ No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de Comaco a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- ✓ Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Comaco debe guardarse en otra sede, lejos del edificio.
- ✓ Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).
- ✓ La información de Comaco clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Gerencia de Informática.
- ✓ No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
- ✓ El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, proveedores y personal temporal.
- ✓ Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que se les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de Comaco.

- ✓ No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de Comaco.
- ✓ El personal que utiliza un computador portátil que contenga información confidencial de Comaco, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

5.2.2. Usuarios

A todos los empleados de Comaco, se les debe proporcionar adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la institución. Los usuarios son responsables de cumplir con todas las políticas de Comaco, relativas a la seguridad informática y en particular:

- ✓ Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- ✓ Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.
- ✓ No divulgar información confidencial de Comaco a personas no autorizadas.
- ✓ No permitir y no facilitar el uso de los sistemas informáticos de Comaco a personas no autorizadas.
- ✓ No utilizar los recursos informáticos (hardware, software o datos) para otras actividades que no estén directamente relacionadas con el trabajo realizado en Comaco.
- ✓ Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- ✓ Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- ✓ Reportar inmediatamente a su jefe inmediato o a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de Comaco y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.
- ✓ Los usuarios no deberán crear programas tendientes a alterar los sistemas institucionales académicos, administrativos o contables.

- ✓ No se debe hacer uso de huecos de seguridad o claves de acceso especiales para dañar los sistemas, ganar acceso no autorizado, o lograr información confidencial. En caso de encontrar un hueco de seguridad, éste se deberá reportar al Jefe del Centro de Datos.

a) Políticas de seguridad para las cuentas de usuarios

- ✓ La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
- ✓ No debe concederse una cuenta a personas que no sean empleados de Comaco a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- ✓ Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
- ✓ No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el período de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.
- ✓ Se prohíbe el uso de cuentas anónimas o de invitado (guest). Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.
- ✓ Toda cuenta queda automáticamente suspendida después de un cierto período de inactividad. El período recomendado es de 30 días.
- ✓ Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

- ✓ Cuando un empleado es despedido o renuncia a Comaco, debe desactivarse su cuenta antes de que deje el cargo.
- ✓ Queda prohibido para cualquier persona prestar su cuenta personal de red a alguien más, así como usar la cuenta personal de otro usuario.
- ✓ Está prohibido el tratar de abrir cuentas con datos falsos o presta nombres.
- ✓ Ninguna cuenta de usuario o de servicios administrativos podrá ser usada con propósitos ilegales o contrarios a la ética.
- ✓ Las cuentas de la red del personal serán inhabilitadas durante los períodos vacacionales.
- ✓ El Operador de Red no podrá remover información de cuentas individuales, así como tampoco eliminará la información de boletines electrónicos, a menos que la información involucrada sea ilegal o ponga en peligro, tanto los recursos de información de otros usuarios, como el buen funcionamiento de los sistemas computacionales.

b) Políticas de seguridad para las contraseñas y el control de acceso

- ✓ Una buena contraseña debe tener las siguientes cualidades: tener por lo menos ocho caracteres, estar hecha de caracteres, números y símbolos, ser única .
- ✓ Se deben evitar contraseñas que: sean palabras que se encuentran en el diccionario, tengan que ver con sus datos personales, no pueda ser escrita rápidamente.
- ✓ El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- ✓ Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- ✓ Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- ✓ La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- ✓ Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- ✓ Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

- ➢ **Clave de autorización de encendido**

Este es un recurso de protección disponible en todas las computadoras, se habilita al momento de configurar el equipo y es una clave que será solicitada como primer paso de inicialización después de encendida la computadora. Todo usuario que así lo solicite le será activado este passsword por el Centro de Datos. Cuando se activa esta protección se debe tener presente las siguientes consideraciones:

- ✓ No olvide su clave, su desactivación puede gastar tiempo valioso durante el cual la computadora no puede ser utilizada.
- ✓ Dé a conocer la clave a su jefe de departamento y/o sólo a aquellas personas que realmente deben encender y hacer uso del equipo.
- ✓ El sistema exigirá la modificación periódica de su clave.

- ➢ **Clave de acceso a la red**

Este es un recurso de protección disponible en todas las computadoras, se habilita al momento de configurar el equipo y es una clave que será solicitada para acceder a los recursos de la red. Todas las computadoras que están conectadas a la red cuentan con este passsword. Cuando se activa esta protección se debe tener presente las siguientes consideraciones:

- ✓ No olvide su clave, su desactivación puede gastar tiempo valioso durante el cual la computadora no puede ser utilizada.
- ✓ Dé a conocer la clave a su jefe de departamento y/o sólo a aquellas personas que realmente deben encender y hacer uso del equipo.

- ✓ El sistema exigirá la modificación periódica de su clave.
- ✓ Si le da ESC o CANCELAR no tendrá derecho a los recursos de la red.

- ➢ **Clave de acceso a los programas administrativos**

Todo usuario que requiera utilizar un programa administrativo debe de contar con un usuario y una clave para acceder a dicho recurso. Debe tener presente las siguientes consideraciones:

- ✓ No olvide su clave.
- ✓ No dé a conocer la clave a nadie, si alguien desea hacer uso de un programa administrativo debe solicitar su usuario y su clave al Centro de Datos.
- ✓ Es conveniente modificar periódicamente su clave.

5.2.3. Servicios de Red

a) Configuración del Servidor DNS

El servicio de DNS es crucial para la conexión a Internet. Sin embargo en muchas organizaciones no está configurado adecuadamente.

- ✓ Tener una versión actualizada del servidor de nombres, es conveniente actualizar a una versión actual del servidor. Las últimas versiones son más seguras y permiten establecer filtros y limitaciones en las transferencias de zonas, actualizaciones no solicitadas de datos, etc.
- ✓ Tener configurado el direccionamiento inverso, muchas instituciones no tienen establecido el direccionamiento inverso para los equipos, lo que dificulta muchas veces el acceso a determinados servicios o la monitorización en los logs.
- ✓ Denegar el acceso a las zonas a otros servidores, es conveniente que los servidores de DNS estén configurados para permitir las transferencias de zona solamente a los servidores que estén definidos como secundarios, así se evita el que se pueda obtener información sobre la topología y configuración de la red desde el exterior.
- ✓ No poner configuraciones de equipos en el DNS, es posible indicar en registros de DNS qué sistema operativo, arquitectura hardware, e incluso qué servicios se están ejecutando. Esta información se puede emplear para atacar desde fuera la organización.

- ✓ Configuración en los clientes, a nivel de filtrado de puertos con el tcp-wrapper o listas de acceso, emplear nombres cualificados por completo y no sólo el nombre del equipo, para evitar que un equipo de otra organización que se llama igual pueda tener acceso al sistema.
- ✓ Aspectos generales de configuración, como norma general, se debe cumplir:
  - No se deben configurar los servidores de DNS para que reenvíen las peticiones (forward) a equipos de Comaco.
  - No se deben configurar DNS como secundarios de otra organización, salvo autorización explícita de la otra parte.
  - Lo óptimo es tener dos servidores, primario y secundario, en una misma organización y tener definido ambos equipos como servidores de nombres en la configuración de los equipos.

b) Configuración del Servidor Web

Se debe considerar algunas medidas para evitar ataques a los servidores WWW, ya que éstos son susceptibles:

- ✓ Dimensionar el equipo adecuadamente, para evitar que se produzcan ataques de denegación de servicio (DoS).
- ✓ Instalar una versión actualizada del servidor WWW.
- ✓ Salvo que sea necesario, denegar el empleo de cgi-bin fuera de los empleados por los administradores, eliminar los cgi-bin de prueba, que suelen tener vulnerabilidades de seguridad, y no emplear extensiones (php, server-side include, server de java, etc.) salvo que sean necesarios.
- ✓ En caso de que los usuarios deban programar cgi's, advertirles de los fallos más comunes que pueden existir y como solucionarlos.
- ✓ No compartir las páginas de los servidores mediante un sistema de ficheros, emplear un sistema de mirror para realizar el intercambio de las páginas.

5.2.4. INTERNET CORPORATIVO

a) Políticas de seguridad del Router

- ✓ La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de Comaco y en tal sentido deben usarse las horas no laborables.
- ✓ Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que esté cifrada.
- ✓ La contraseña del ruteador debe estar de manera encriptada.
- ✓ El ruteador debe ser incluido en el módulo de administración de la red, con un punto de acceso específico.
- ✓ Cada ruteador debe estar debidamente identificado.
- ✓ Todos los ruteadores deben estar configurados sin la capacidad de redireccionar paquetes y sin tener activado el broadcast en las interfaces.
- ✓ Los ruteadores deben estar configurados para evitar ataques tipo smurf.
- ✓ Los ruteadores utilizados para la comunicación en la empresa deben tener la configuración anti-spoofing.
- ✓ Deshabilitar las siguientes opciones:
  - El ingreso hacia la red corporativa de paquetes con direcciones inválidas.
  - Servicios TCP y UDP que no son necesarios.
  - Gestión vía web del ruteador.

b) Políticas de seguridad del Correo

- ✓ Nunca se debe abrir o retransmitir archivos adjuntos de un origen desconocido, fuente sospechosa o poco fiable. Se deben anular y eliminar de la papelera de reciclaje.
- ✓ Enviar o reenviar mensajes no solicitados, “correo basura”, u otro material de publicidad a personan que no lo han pedido.
- ✓ No crear o remitir esquemas de cualquier tipo de “carta cadena”.
- ✓ Utilice como pie de firma: su nombre, cargo en la empresa, teléfono y extensión; solamente en los correos que sean de tipo comercial o de interés para la empresa. Caso contrario, solamente utilice como pie de firma su nombre.

- ✓ La empresa debe tener la capacidad de administrar, monitorear, y registrar el uso de servicios HTTP, FTP, SMTP y comunicaciones en Internet en general.
- ✓ Los servicios de Internet disponibles para los usuarios autorizados dentro de la empresa son HTTP, FTP, SMTP. Cualquier otro servicio fuera de los mencionados debe ser bloqueado.
- ✓ Se prohíbe navegar en sitios cuyo contenido sea obsceno, constituya pornografía infantil o aliente conductas que puedan convertirse en ofensas criminales.
- ✓ Al enviar un documento de texto a otro usuario a través de Internet, el archivo debe guardarse bajo la extensión rtf, que no contiene macros.
- ✓ Mantenga controlado el acceso al correo electrónico corporativo, implementando estrictos requerimientos como el cambio periódico de contraseñas.
- ✓ Implemente varias capas de seguridad en lo relativo al correo electrónico, usando una combinación de aplicaciones antivirus individuales en cada computadora, un antivirus a nivel de servidor, preferentemente de otro fabricante, aplicaciones de filtrado de contenido, y alguna aplicación para el manejo centralizado del SPAM mediante filtros a nivel del servidor o aplicaciones específicas.
- ✓ Debido a la cantidad de virus, y a la variedad de métodos utilizados por estos hoy día, un solo sistema de antivirus no llega a ser suficiente (tampoco lo es tener más de un antivirus monitoreando en una misma computadora). Sin embargo, es una posibilidad totalmente válida, disponer de varias capas de filtrado con diferentes productos, uno en cada computadora individual, y otro a nivel del servidor que conecta la Intranet de la empresa con Internet.
- ✓ También es importante mantener un estricto control de actualizaciones de los productos antivirus, que perfectamente podrían ser con chequeos automáticos cada 60 minutos a la Web del fabricante.
- ✓ Encripte las conexiones de correo electrónico mediante VPN (redes privadas virtuales) o Secure Sockets Layer (SSL). No deje nunca el sistema de correo electrónico corporativo abierto directamente a Internet, a pesar de la tentación que ello significa por su conveniencia.
- ✓ Cerciórese de que los usuarios con otra clase de acceso dentro de la empresa (conexiones inalámbricas, etc.), tengan el mismo nivel de seguridad que un usuario de computadora de mesa, sin comprometer su acceso a la red.
- ✓ Utilice antivirus en cada máquina, cortafuegos personales y conexión VPN. VPN es una red privada que protege, mediante un proceso de encapsulación y en ocasiones de

encriptación, los paquetes de datos enviados a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Las VPN pueden enlazar oficinas corporativas entre ellas, con usuarios móviles, etc.

- ✓ Monitoree su sistema de correo electrónico corporativo y prevea soporte a los usuarios 24x7 si ello fuera posible (las 24 horas del día los 7 días de la semana). Asegúrese de que los diferentes administradores están subscriptos a listas informativas (como VSAntivirus), y a foros de seguridad que los mantengan alertas y al día sobre los incidentes de seguridad más recientes, listas de vulnerabilidades descubiertas, amenazas víricas, etc.
- ✓ Evalúe los modelos de experiencia y seguridad para cualquier sistema o producto de correo electrónico que su compañía use. Pregunte sobre otros productos antivirus, antiespams, infraestructuras, redundancia de los recursos disponibles, almacenamiento de datos, política de respaldos, conectividad y encriptación.
- ✓ El correo electrónico de Comaco no se usará para envío masivo, materiales de uso no laboral o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, etcétera).
- ✓ Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de Comaco, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de Comaco sin la debida aprobación.
- ✓ Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

5.2.5. Físicas

El solo contar con buenos programas de mantenimiento preventivo de los equipos de computación, no garantiza totalmente su operación satisfactoria, ni eliminan los riesgos de desperfecto que como cualquier elemento electrónico puede presentar. Pero si este equipo cuenta además con los cuidados de instalación, limpieza, temperatura, humedad, eléctricos, se estará brindando un estado óptimo de trabajo con un mínimo de revisiones y reparaciones. Las siguientes recomendaciones, prolongarán la vida de los equipos:

- ✓ Ubique el equipo en un área donde no exista mucho movimiento de personal.
- ✓ No traslade la computadora sin la autorización y asesoría del Centro de Datos.
- ✓ Instale la computadora sobre escritorios o muebles estables o especialmente diseñados para ello.
- ✓ Ubique el equipo lejos de la luz del sol y de ventanas abiertas.
- ✓ La energía eléctrica debe ser regulada a 110 voltios y con polo a tierra. Asesórese debidamente para garantizar una buena toma eléctrica
- ✓ No conecte otros aparatos (radios, máquinas de escribir, calculadoras, etc.) en la misma toma de la computadora.
- ✓ Cada usuario, al momento de terminar las labores diarias, deberá apagar los equipos (Computadora, Impresoras, Escanners).
- ✓ Evite colocar encima o cerca de la computadora ganchos, clips, bebidas y comidas que se pueden caer accidentalmente dentro del equipo.
- ✓ No fume cerca del equipo, el alquitrán se adhiere a las piezas y circuitos internos del equipo.
- ✓ Mantenga libre de polvo las partes externas de la computadora y de las impresoras. Utilice un paño suave y seco. Jamás use agua y jabón.
- ✓ Mantenga la pantalla y el teclado cubiertos con fundas cuando no haga uso de ellos por un tiempo considerable o si planea el aseo o reparaciones de las áreas aledañas a la computadora.
- ✓ Utilice en la impresora el ancho del papel adecuado. El contacto directo de la cabeza de impresión sobre el rodillo puede estropear ambas partes. (Usuarios con impresoras de matriz de punto).
- ✓ Esta prohibido destapar y tratar de arreglar los equipos por su cuenta. En todos los casos asesórese del Centro de Datos o del encargado de esta operación.
- ✓ No preste los equipos o asegúrese que la persona que lo utilizara conoce su correcta operación.
- ✓ Todos los sistemas de comunicaciones estarán debidamente protegidos con infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones al equipo activo y los sistemas de cableado del Centro de Datos.
- ✓ Las visitas internas o externas podrán acceder al Centro de Datos siempre y cuando se encuentren acompañadas cuando menos por un responsable de la institución visitante, habiendo previamente solicitado el permiso de acceso a Comaco existiendo una razón

suficiente que amerite el acceso a las mismas. Así mismo Comaco deberá asignar a una persona que guiará dicha visita.

- ✓ Se debe definir qué personal está autorizado para mover, cambiar o extraer equipo del Centro de Datos a través de identificaciones; y se debe informar de estas disposiciones a personal de seguridad de la Secretaría de Finanzas y Administración.
- ✓ Protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.
- ✓ Control de utilización de equipos de prueba de comunicaciones para monitorizar la red y el tráfico en ella.
- ✓ Prioridad de recuperación del sistema.
- ✓ Control de las líneas telefónicas.
- ✓ El equipo de comunicaciones ha de estar en un lugar cerrado y con acceso limitado.
- ✓ La seguridad física del equipo de comunicaciones debe ser la adecuada.
- ✓ Tomar medidas para separar las actividades de los electricistas y de cableado de líneas telefónicas.
- ✓ Las líneas de comunicación deben estar fuera de la vista.
- ✓ Se debe asignar un código a cada línea, en vez de una descripción física de la misma.
- ✓ Debe existir procedimientos de protección de los cables y las bocas de conexión para evitar pinchazos a la red.
- ✓ Revisar periódicamente la red, buscando pinchazos a la misma.
- ✓ El equipo de prueba de comunicaciones ha de tener unos propósitos y funciones específicas.
- ✓ Deben existir alternativas de respaldo de las comunicaciones.
- ✓ Con respecto a las líneas telefónicas, no debe darse el número como público y tenerlas configuradas con retro-llamada, código de conexión o interruptores.
- ✓ Los respaldos de la información crítica deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.

5.2.6. Políticas Antivirus

- ✓ Todos los servidores y pc's de Comaco, deberán tener instalada la Solución Antivirus.
- ✓ Mediante consolas de administración central, ubicadas en el Centro de Datos de Comaco, se implementará automáticamente la Solución Antivirus en las computadoras de los usuarios.

- ✓ Diariamente se realizará un rastreo automático mediante la Solución Antivirus para detectar y eliminar virus de documentos, archivos ejecutables, correos recibidos y páginas web, en todos los computadores.
- ✓ Semanalmente se hará el rastreo en los equipos de cómputo de Comaco, y se realizará la actualización automática de las firmas antivirus proporcionadas por el fabricante de la Solución Antivirus.
- ✓ En caso de contingencia con virus que la Solución Antivirus no haya detectado automáticamente, el Centro de Datos de Comaco:
  - Actualizará las firmas antivirus.
  - Se pondrá en contacto con el fabricante de la Solución Antivirus con el fin de determinar la estrategia más efectiva para eliminar el virus.
  - Generará las configuraciones necesarias para la detección del virus mediante los analizadores de redes de las dependencias.
- ✓ Si la Solución Antivirus no puede desinfectar un archivo con virus de manera automática, se aplicará el procedimiento de tratamiento de nuevos virus.
- ✓ Aunque existen tratamientos "vacunas", lo primordial es prevenir el contagio mediante la adopción de una política de "sano" procesamiento que el usuario debe seguir:
  - Utilizar únicamente software original legalmente adquirido y autorizado e instalado por el Centro de Datos.
  - No se debe instalar en la computadora software "pirata" ni de "juegos".
  - No se debe instalar "vacunas" sin la autorización del Centro de Datos. Estas aunque parezca irónico, pueden estar infectadas.
  - Estar atentos a los mensajes de alerta emitidos por la computadora. El Centro de Datos aplicará el detector de virus periódicamente.

5.2.7. Políticas sobre la utilización de software y hardware

El uso de Software no autorizado o adquirido ilegalmente, se considera como PIRATA y una violación a los derechos de autor, por lo tanto está estrictamente prohibido instalar software pirata. El uso de Hardware y de Software autorizado está regulado por las siguientes normas:

- ✓ No se permite el uso de ningún programa de cómputo que no cuente con la debida licencia.

- ✓ Queda prohibido borrar, modificar, dañar o alterar de cualquier manera los programas de cómputo contenidos en los discos duros de las computadoras o en el sistema de red. Solamente el personal del Centro de Datos tiene las facultades para hacerlo.
- ✓ Los miembros de la Institución podrán almacenar su información personal en los espacios destinados para ello (cuentas personales de red). El Centro de Datos garantiza la confidencialidad de esta información pero su integridad depende del usuario quien es responsable del respaldo de su información.
- ✓ La información de carácter institucional será respaldada por encargados del Centro de Datos, siempre y cuando se almacene en los sitios designados para ello.
- ✓ Todo departamento podrá utilizar únicamente el hardware y el software que el Centro de Computo le haya instalado.
- ✓ Tanto el hardware (computadoras, impresoras, scanners, etc.), software, y los datos, son propiedad de la Institución, su copia, sustracción o daño intencional o utilización para fines distintos a las labores propias de la Institución, será sancionada de acuerdo con las normas y reglamento interno.
- ✓ El Centro de Datos llevará el control del software instalado en cada equipo.
- ✓ La asignación de Ip's es responsabilidad del Centro de Datos y queda estrictamente prohibido cambiarlas.
- ✓ Periódicamente, el Centro de Datos efectuará visitas para verificar el software y configuración utilizada en cada Departamento. Por lo tanto, el detectar software no instalado por este Departamento, será considerado como una violación a las normas internas de la Institución.
- ✓ Toda necesidad de hardware y/o software adicional debe ser solicitada por escrito al Centro de Datos, quién justificará o no dicho requerimiento, mediante un estudio evaluativo.
- ✓ El Centro de Datos instalará el software en cada computadora y entregará al área usuaria los manuales pertinentes los cuales quedarán bajo la responsabilidad del Jefe del departamento respectivo.
- ✓ Los disquetes y/o Cd's que contienen el software original de cada paquete serán administrados por cada Departamento.
- ✓ El Centro de Datos auxiliará a cada departamento en caso de requerirse la reinstalación de un paquete determinado.
- ✓ La prueba, instalación y puesta en marcha de los computadores, serán realizadas por el Centro de Datos.

- ✓ Una vez entregados los equipos de computación y/o el software por el Centro de Datos, éstos serán cargados a la cuenta de activos fijos del área respectiva y por lo tanto, quedarán bajo su responsabilidad.
- ✓ Así mismo, el Centro de Datos mantendrá actualizada la información de los computadores de la Institución, en cuanto a número de serie y ubicación, con el fin que este mismo departamento verifique, por lo menos una vez al año su correcta destinación.
- ✓ El Centro de Datos hará las gestiones para actualizar el software comprado cada vez que una nueva versión salga al mercado, a fin de aprovechar las mejoras realizadas a los programas, siempre y cuando se justifique esta actualización.

5.2.8. Políticas de seguridad para copias y/o backups de respaldo

Así como se protege la información contra accesos no autorizados, es también importante mantener en lugar seguro, copias actualizadas de la información VITAL de cada departamento, con el fin de garantizar la oportuna recuperación de datos y programas en caso de pérdidas o daños en la computadora. Las siguientes pautas determinan una buena política de Backups aplicable en cada dependencia de Comaco.

- ✓ Determinar el grado de importancia de la información que amerite copias de seguridad.
- ✓ Comunicar al Centro de Datos para que éste elabore copias periódicas a través de la red.
- ✓ Indique cuanto tiempo se debe conservar esta información.
- ✓ Diseñar cierta codificación que sólo conozcan las personas responsables de las copias de seguridad, de forma que cada cinta vaya convenientemente etiquetada, pero sin conocer el código y este sea difícil de imaginar su contenido.

5.2.9. Políticas de Seguridad de Acceso Remoto

- ✓ Los números telefónicos utilizados para este tipo de conexión no deben ser publicados ni listados en los sistemas.

- ✓ Permitir que los módems vuelvan a la configuración estándar al inicio y final de cada llamada.
- ✓ Los módems deben tener la característica de módems silenciosos, los cuales no enviarán la señal característica de "conexión establecida" hasta que no se haya completado el inicio de sesión.
- ✓ Las conexiones dial-in deben ser controladas estrictamente, y debe usarse las funciones "AAA" para los usuarios que desean acceder a la red.
- ✓ Es responsabilidad de los usuarios con privilegios de acceso remoto acceder a la red corporativa siguiendo los lineamientos de seguridad de las conexiones locales.
- ✓ Los usuarios con privilegios de acceso remoto deben asegurarse de que cuando se encuentran conectados a la red corporativa, no se encuentren unidos al mismo tiempo a cualquier otra red, con excepción de las redes personales que se encuentran bajo el total control del usuario.
- ✓ Las sesiones abiertas para acceso remoto deben terminar cuando ya no se necesitan.
- ✓ El uso de acceso remoto será utilizando una autenticación de contraseñas, realizada por un dispositivo de propiedad de la empresa.
- ✓ Las reglas de acceso se van a añadir de acuerdo a los requerimientos de la empresa.
- ✓ Todas las computadoras conectadas a la red interna de la empresa mediante acceso remoto deben utilizar software antivirus actualizado.
- ✓ Los usuarios de acceso remoto serán desconectados automáticamente cuando hayan transcurrido 30 minutos de inactividad.
- ✓ No utilizar el derecho al acceso remoto para tareas fuera del interés de la empresa.

5.2.10. Políticas de Seguridad a nivel de Red

a) Filtrado de Paquetes en el Router

Es imprescindible el uso de filtros a nivel de red, que permitan a una organización restringir el acceso externo a los servicios. De esta forma, sólo aquellos servicios que deban estar accesibles desde fuera del área local serán permitidos a través de filltros en los routers. Además es importante que estos filtros determinen las condiciones de acceso a los servicios permitidos. Se recomienda que se filtren los siguientes servicios si no es necesario su acceso desde fuera de una organización concreta:

CHARGEN y ECHO Puertos 11 y 19 (TCP/UDP) Es muy importante para evitar ataques de denegación de servicio por puertos UDP, filtrar a nivel de router o firewall los servicios chargen y echo y en general todos los servicios UDP que operen por debajo del puerto 900 con excepción de aquellos que se necesiten implícitamente.

Transferencias de zona DNS Puerto 53 (UDP/TCP) Es necesario filtrar el acceso desde el exterior a todos los equipos excepto a los servidores de DNS primarios y secundarios establecidos en una organización.

TFTPD Puerto 69 (UDP) En general cualquier servicio UDP que responde a un paquete de entrada puede ser víctima de un ataque de denegación de servicio (DoS). Un acceso no restringido al servicio TFTP permite a sitios remotos recuperar una copia de cualquier fichero "word-readable", entre los que se pueden incluir ficheros críticos como ficheros de configuración de routers y ficheros de claves. Es por ello, que aquellas organizaciones que no necesiten usar este servicio deberán filtrarlo y aquellas que necesiten usarlo, lo configuren adecuadamente teniendo en cuenta las medidas de seguridad a nivel de aplicación.

Comandos r de BSD UNIX Puertos 512, 513 y 514 (TCP) Los comandos r incrementan el peligro de que sean interceptados passwords en texto plano cuando se presenta un ataque utilizando sniffers de red, pero lo más importante es que son una fuente bastante frecuente de ataques y vulnerabilidades. Filtrando los puertos 512, 513 y 514 (TCP) a nivel de red se evitará que personas ajenas a su organización puedan explotar estos comandos, pero no lo evitará a personas de su propia organización. Para ellos, aconsejamos el uso de otras herramientas como el ssh, uso de versiones seguras de los comandos "r" (WietseVenema'slogdaemon), uso de tcp wrapper para proporcionar una monitorización del acceso a estos servicios, etc.

SunRPC y NFS Puertos 111 y 2049 (TCP/UDP) Filtrar el tráfico NFS evitará que sitios ajenos a su organización accedan a sistemas de archivos exportados por máquinas de su red, pero como ocurría en el caso anterior, no se evitará que se realicen ataques desde dentro del área local. La mayoría de las implementaciones NFS emplean el protocolo UDP, por lo que es posible, en algunos casos, el envío de peticiones NFS falsificando la dirección origen de los paquetes (IP-spoofing), es por tanto aconsejable la instalación de las últimas versiones actualizadas de los servidores y clientes NFS que tienen en cuenta estas características.

SMTP Puerto 25 (TCP) Es importante configurar el router de manera que todas las conexiones SMTP procedentes de fuera de una organización pasen a una estafeta central y que sea desde ésta desde donde se distribuya el correo internamente. Este tipo de filtros permitirán, que no existan puertos 25 descontrolados dentro de una organización que suelen ser foco de importantes problemas de seguridad, además de un logueo centralizado de información, que podrá ayudar a la hora de detectar el origen de intentos de ataque. El administrador del sistema o el responsable de seguridad sólo se tendrá que preocupar de tener actualizado este servidor para evitar ataques aprovechando vulnerabilidades o fallos bien conocidos en los mismos.

NetBios. Puertos 137, 138 y 139 (UDP/TCP) Estos puertos, son los empleados en las redes Microsoft (Windows para trabajo en Grupo, Dominios NT y LANManager), tanto para la autentificación de usuarios como para la compartición de recursos (impresoras y discos). Es frecuente el permitir el acceso global a uno de estos dispositivos, ignorando que es posible el acceso a estos recursos desde cualquier dirección de Internet.

SNMP Puerto 161 (UDP/TCP) Muchos equipos disponen en la actualidad de gestión SNMP incorporada. Dado que estas facilidades de gestión no suelen necesitar accesos externos, se deben establecer filtros a nivel de router que eviten que se pueda obtener información sobre los dispositivos (routers, hubs, switches) desde el exterior o incluso se gestionen los equipos en remoto.

Filtros de datagramas IP Para prevenir los ataques basados en bombas ICMP, se deben filtrar los paquetes de redirección ICMP y los paquetes de destino ICMP inalcanzables. Además, y dado que actualmente el campo de opciones de los paquetes IP no son casi utilizados se pueden filtrar en la mayoría de las organizaciones los paquetes de origen enrutado.

En la entrada a la interface interna de una organización se deberán filtrar los bloques de paquetes con las siguientes direcciones:

- ✓ Redes Broadcast, para evitar que su organización sea utilizada como intermediaria en un ataque de denegación de servicio de tipo smurf, es necesario bloquear el tráfico ICMP a las direcciones de broadcasts (bits dedicados a hosts todos a uno) y de red (bits dedicados a hosts todos iguales a cero).
- ✓ Su área local.
- ✓ Números de red privada reservados, no se debe recibir tráfico desde hacia las siguientes direcciones a través de los routers puesto que se trata de redes privadas reservadas:
  10.0.0.0 - 10.255.255.255 10/8 (reservada)
  127.0.0.0 - 127.255.255.255 127/8 (loopback)
  172.16.0.0 - 172.31.255.255 172.16/12 (reservada)
  192.168.0.0 - 192.168.255.255 192.168/16 (reservada)

b) Configuración de las pilas TCP/IP en equipos finales

Se debe revisar la configuración de “reenvío de datagramas IP" (ip-forwarding), que permite que un sistema funcione como un router, así como deshabilitar el empleo de datagramas IP con el campo de enrutamiento fuente activado, ya que gran parte de los ataques de denegación de servicio (DoS) se producen debido a fallos en las implantaciones de las pilas TCP/IP en los sistemas operativos, dentro de los cuales se destacan: los ataques de denegación de servicio mediante el envío de datagramas IP con información ICMP errónea, que provocan el reseteo del equipo, o los ataques mediante SYN y FIN flood, impidiendo el normal funcionamiento de los servidores.

c) Monitorización de router y equipos de acceso

- ✓ Tanto los equipos de acceso (servidores de pools de módems, router de acceso, etc) como los routers de interconexión y cualquier dispositivo (switch, etc.), deben estar monitorizados mediante syslogs.
- ✓ Los syslogs deben configurarse para enviar los mensajes de la consola a un equipo central donde se almacena durante un período de tiempo, de forma que se puedan comprobar los intentos de conexión no autorizados y las caídas que se producen en estos equipos.

- ✓ En instalaciones con mucho equipamiento de red puede ser recomendable el empleo de alguna herramienta de monitorización SNMP de los equipos, de forma que las incidencias que vayan ocurriendo sean notificadas en tiempo real a los administradores de la red.
- ✓ Es necesaria la instalación de versiones recientes de los sistemas operativos de estos equipos, puesto que muchas instalaciones disponen de versiones antiguas susceptibles a ataques de denegación de servicio que pueden ser fácilmente evitables si se actualizan periódicamente los sistemas.

d) Separación de las redes y filtros anti-sniffing

Gran parte de los ataques que se producen son debidos a la obtención de las claves empleando un programa de sniffing en una red ethernet.

- ✓ En muchas ocasiones, la separación de las redes y el empleo de switches y routers es necesario para permitir una mayor descongestión del tráfico interno de una organización, pero además es necesario para lograr una mayor seguridad dentro de esta.
- ✓ Los equipos que necesiten el empleo de sistemas inseguros de transmisión de claves deben estar separados mediante puentes o switches del resto de la red, para evitar que se puedan obtener, mediante sniffers, passwords de acceso de otros grupos de usuarios.
- ✓ Hay que considerar además las posibilidades de gestión y consola remota que disponen muchos hubs, routers y switches, hay que cambiar las claves por defecto que suelen tener estos equipos y deshabilitar la gestión remota de estos si no se va a hacer uso de ella. (snmp, consolas remotas, servidores de HTTP).
- ✓ Existen versiones de sniffer para los sistemas Windows, siendo posible la obtención de password de acceso a sistemas de ficheros remotos de Netbios, pudiendo modificar fácilmente cualquier aplicación existente en estos servidores. Además en muchos servidores samba el password de conexión de Windows coincide con la clave del usuario, por lo que estas medidas anti-sniffing se deben aplicar a cualquier protocolo que circule por la red.

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- El análisis de los conceptos básicos de seguridad, proporcionaron las pautas iniciales para el desarrollar este proyecto.

- La seguridad absoluta no es posible de conseguir, ya que con la evolución del Internet, a pesar de que se utilice los equipos con tecnología de punta, aparecen nuevas amenazas.

- Se realizó el análisis de la situación actual de la red de datos de COMACO, el mismo que sirvió de guía para definir las políticas de seguridad y diseñar el modelo de una red segura.

- No fue posible la implementación de una herramienta que realice el mapeo de puertos y las pruebas de penetración a la red de datos de COMACO, debido a que la información es confidencial.

- La infraestructura de la red de datos de la Institución dispone de una variedad de hardware y sistemas operativos que no permiten unificar configuraciones que faciliten tareas de monitoreo y administración de cada uno de los dispositivos de la red.

- Las técnicas de protección estudiadas son soluciones eficientes a los problemas de seguridad, ya que son una combinación de Hardware y Software capaces de detectar, prevenir y atenuar cualquier situación de peligro para el sistema.

- La instalación de la red OOB (Fuera de Banda) puede ser aprovechada para obtener los respaldos de los dispositivos y servidores, sin que esto afecte el tráfico de la red de producción.

- Al configurar una red OOB (Fuera de Banda), el tráfico de la administración no congestiona a la red de producción.

- La implementación de una red fuera de banda evita el tráfico que puede generar la gestión de los equipos de comunicación y los servidores en la red de producción.

- El switch de capa 3 a diferencia del de capa 2, proporciona enrutamiento, calidad de servicio y características de seguridad.

- El modelo SAFE propuesto por Cisco Systems, Inc. permite agrupar a los componentes de la red de acuerdo a su funcionalidad, este modelo ha guiado el desarrollo del diseño de una red segura para el Comando Conjunto.

6.2 RECOMENDACIONES

- Considerar este proyecto como documento habilitante para la implementación de la red segura, puesto que propone un diseño funcional que responde a la problemática real de la Institución.

- Debe darse mucha importancia a la "seguridad física" del sistema ya que si no se analizan los factores físicos que puedan ocurrir, todos los esfuerzos por asegurar un sistema serían estériles.

- Se recomienda que COMACO obtenga versiones corporativas existentes en el mercado para las actualizaciones del software antivirus.

- Se recomienda que el HUB que realiza la función del módulo de Distribución del Edificio sea cambiado por un switch de capa 3, por que en el hub no se puede configurar características de seguridad.

- Se recomienda que el documento de políticas de seguridad sea difundido a todo el personal que trabaja en las instalaciones de COMACO, para minimizar el riesgo de la violación a la seguridad de la red.

- Considerar la creación de una Intranet para que todo el personal esté informado de la misión y visión de la Institución, así como también eventos sociales a realizarse, la información del directorio telefónico, etc.

- Tomar en cuenta la adquisición de un contrato de mantenimiento para tener acceso a las últimas actualizaciones de los sistemas operativos de los equipos de comunicación, así como de los servidores, cada uno de ellos con sus respectivos parches.

- Unificar a un solo sistema operativo, todas las estaciones de trabajo para facilitar el manejo y control de las mismas.

- Reemplazar los hubs por los switches, porque los hubs producen cuellos de botella, mientras que en los switches se puede obtener varios dominios de colisiones.

- Considerar una cadena de seguridad para todas las computadoras personales (laptops) que existan en la Institución evitando la sustracción de las mismas.

- Se recomienda llevar un control inventariado de todos los equipos que sea actualizado periódicamente.

- Se recomienda que el personal técnico encargado de las seguridades en la Red de COMACO sea capacitado periódicamente.

- Se recomienda que COMACO desarrolle una verdadera cultura de seguridad, en todos sus niveles y estamentos.