ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED QUITO MOTORS, UTILIZANDO TECNOLOGÍA UTM (UNIFIED THREAT MANAGEMENT)

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

DIANA VERÓNICA ALULEMA CHILUIZA
dianaalulema@yahoo.com

DIRECTOR: ING. FERNANDO FLORES
fflores@fie-epn.net

Quito, Junio 2008

DECLARACIÓN

Yo, Alulema Chiluiza Diana Verónica, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Alulema Chiluiza Diana Verónica

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Alulema Chiluiza Diana Verónica, bajo mi supervisión.

_____

Ing. Fernando Flores
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco de manera especial al Ing. Fernando Flores por su dirección y consejos para la realización del presente proyecto; además a los profesores de la Escuela Politécnica Nacional ya que contribuyen a la formación de personas integras que en el futuro constituyen parte importante de nuestra sociedad.

También expreso mi agradecimiento a la empresa Quito Motors S.A.C.I por la apertura y atención brindada.

DEDICATORIA

El presente trabajo va dedicado a todas las personas que me apoyaron de diferentes maneras y estuvieron día a día para lograr la exitosa culminación de este proyecto.

Para mi familia ya que son las personas que nunca fallan.
A mi padre y madre que se sacrifican por sus hijos con infinito amor.
A mis hermanos que me incentivan a seguir adelante en mis propósitos Alex, Raphael, Washington y Patricio.
Y Annabelle que se ha convertido en una nueva hermana y amiga.

Finalmente a mis amigos que forman parte importante de mi vida ya que son como una segunda familia.

CONTENIDO

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo abarca temas relacionados con la seguridad de la información, las redes y los sistemas en general.

La primera parte teórica contiene los conceptos, características, amenazas, vulnerabilidades y mecanismos relacionados con la Seguridad en Redes; también presenta consideraciones sobre los objetivos, desarrollo e implementación de las políticas de seguridad; adicionalmente expone las diferentes técnicas de ataques y tecnologías de protección que se utilizan en la actualidad para comprometer o brindar seguridad a la red de información; finalmente exhibe las consideraciones físicas que deben tomarse en cuenta para la seguridad integral de una red.

La segunda parte teórica, abarca el estudio de la tecnología UTM (Unified Threat Management) realizando un análisis de los módulos que la conforman y exponiendo soluciones de seguridad mediante esta tecnología de tres proveedores: Fortinet, Juniper y Cisco para finalmente realizar una comparación de las mismas.

Seguidamente se realiza el análisis de la red de Quito Motors, tomando en cuenta aspectos como la infraestructura, los servicios, los protocolos, las aplicaciones que maneja la red y la forma de acceso al Internet, a la Intranet y a la Extranet. También se analiza las amenazas y vulnerabilidades presentes en la red de Quito Motors para seguidamente hacer un diagnóstico sobre la seguridad actual de la misma y finalmente descubrir los requerimientos en torno a los temas de seguridad de red como a los asuntos relacionados con la funcionalidad del sistema en general.

Finalmente luego de estudiar, analizar y recopilar la información necesaria se realiza el diseño del sistema de seguridad perimetral para la presente red, considerando los problemas más urgentes, los objetivos de seguridad y rendimiento que se pretenden alcanzar. También se contemplan las directrices necesarias para el desarrollo de políticas que contribuyan con la administración eficiente del sistema. Seguidamente basados en el diagnóstico de la red, criterios de diseño y escenarios de seguridad se procede a dimensionar el dispositivo de seguridad, detallar sus características técnicas y evaluar las soluciones de los proveedores.

PRESENTACIÓN

El presente proyecto constituye un trabajo sobre los temas de seguridad en redes aplicados a una empresa de tipo comercial; de tal manera que engloba las tecnologías de protección y técnicas de ataques relacionados a la seguridad física y lógica en redes, con el cual se pretende contribuir a la protección de esta organización exponiendo las formas para hacerle frente a las amenazas que pueden dañar la información, funcionalidad y prestigio de la misma.

El material contenido en este proyecto busca dar a conocer el impácto que pueden causar los ataques en un sistema y determinar los activos informáticos más importantes de la presente empresa para seguidamente concientiza en los directivos y personal IT, sobre la importancia de la implementación de mecanismos de seguridad para la protección y proyección en temas de seguridad. Además de exponer los peligros asociados a la utilización del Internet pero su necesidad en las operaciones empresariales.

También se concentra en el análisis de las nuevas tecnologías y dispositivos de de seguridad en redes; a fin de presentar las potencialidades de los mismos y poner a consideración su uso en ambientes informáticos que requieran proveer seguridad a sus redes.
Finalmente se pretende como objetivo general, proporcionar a la empresa Quito Motors una visión del estado actual de sus redes y sistemas, para así conocer los requerimientos de la misma y sugerir una solución que permita mejorar la funcionalidad y seguridad de la presente Empresa.

CAPÍTULO I

Fundamentos Teóricos de Seguridad en Redes

1 FUNDAMENTOS TEÓRICOS DE SEGURIDAD EN REDES

Con el avance tecnológico experimentado en los últimos años, se han abierto nuevas formas de comprender al mundo, ya que la interconexión a diferentes redes y sistemas, permite la exploración de nuevos espacios fuera de los límites de una organización, lo cual conlleva al aparecimiento de nuevas amenazas inherentes a la expansión de una red aislada a una red compartida.

La seguridad de la información es un aspecto primordial en un sistema de red moderno, pero por ser considerado de forma errónea como un factor que no influye directamente en la productividad del sistema, no se proporciona la atención adecuada ni los recursos necesarios a esta labor.

Debido a que los datos constituyen recursos intangibles, el valor de los mismos gira en función de la importancia relativa que tienen para cada individuo, institución, empresa u entidad pertinente. Pero más allá del valor que alguien puede dar a la información, el problema real es el mal uso de la misma, ya que al exponerse a la red mundial puede ser interceptada o almacenada para realizar delitos informáticos y causar pérdidas económicas.

La inseguridad informática no se concentra solamente en el Internet, sino en toda forma de ataque electrónico como los accesos no autorizados, virus, falsificación y robo de información, violando las principales reglas de seguridad como lo es la integridad, privacidad y autenticidad.

A causa de los diferentes peligros a los que se exponen en la actualidad los sistemas informáticos, se considera necesario procedimientos que permitan el buen uso de recursos y contenidos, para garantizar la continuidad de operación y la seguridad de la información.

La seguridad es algo que comienza y termina en las personas, las mismas que son un componente importante dentro de un sistema; por tal motivo es importante inculcar los conceptos, usos y costumbres del manejo adecuado de los recursos informáticos a los usuarios; sin embargo esto requiere tiempo y esfuerzo.

1.1 SEGURIDAD INFORMÁTICA [1]

1.1.1 CONCEPTO

Es el estudio y aplicación de métodos y medios de protección para los sistemas de información y comunicación, contra revelación, modificación o destrucción de la información; o contra fallos de proceso, almacenamiento o transmisión que se lleva a cabo de forma accidental o intencional. [10]

1.1.1.1 Definición

Seguridad: “calidad de seguro”

Seguro: “libre de riesgo”

Información: “acción y efecto de informar”

Informar: “dar noticia de una cosa”

Redes: “El conjunto sistemático de caños o de hilos conductores o de vías de comunicación o de agencias y servicios o recursos para determinado fin”

Fusionando podemos concluir que la Seguridad en Redes es suministrar información y ofrecer servicios libres de riesgos para un determinado fin.

1.1.2 REQUISITOS [2] [3]

Son las características usadas para medir la seguridad de una red.

1.1.2.1 Identificación

Es el proceso de identificación de un individuo ante una entidad o la determinación de la identidad del individuo o entidad con la que se establece comunicación.

1.1.2.2 Autenticación

Es un proceso que sirve para probar que una entidad (persona, usuario o proceso) es quien dice ser, consiste en verificar la identidad de la misma, por medio de un computador o un

servicio adecuado, para así poder acceder a determinados recursos o ejecutar determinadas tareas.

1.1.2.3 Control de Acceso

Se refiere a la habilidad para controlar el nivel de acceso que los individuos o entidades tienen para una red o sistema y cuanta información pueden recibir, consiste en permitir el acceso a los recursos de un sistema a entidades plenamente identificadas y autorizadas.

1.1.2.4 Disponibilidad

Se refiere a si la red, sistema, hardware y software son fiables y pueden recuperarse rápida y completamente ante un evento de interrupción del servicio.

1.1.2.5 Confidencialidad

Consiste en la protección de la información ante revelaciones no autorizadas, mediante el acceso restringido o la encriptación.

1.1.2.6 Integridad

Es la habilidad para proteger la información, datos o transmisiones de alteraciones no autorizadas, no controladas o accidentales. También se refiere al correcto funcionamiento de una red, sistema o aplicación frente a ataques o desastres.

1.1.2.7 Responsabilidad

Consiste en seguir la pista o auditar lo que un individuo o entidad autorizada y no autorizada está haciendo en la red o sistema mediante el registro de funciones realizadas, accesos a archivos, información alterada.

1.1.2.8 No-Repudio

Es la habilidad de prevenir que individuos o entidades nieguen que la información, datos o archivos fueron enviados o recibidos, accedidos o alterados cuando de hecho lo fueron.

1.1.3 ELEMENTOS [6]

1.1.3.1 Hardware

Son los componentes materiales de un sistema informático, entre los más característicos tenemos: CPU, terminales (mouse, joystick, teclado), módem telefónico, monitor, impresora, unidades de disco (duro, CD-ROM, CD-RW, disquetes, flash, DVD), memoria (RAM, ROM).

1.1.3.2 Software

Son programas que contienen las instrucciones responsables de que el hardware realice determinadas tarea. Se clasifican en: software de sistema (sistema operativo, controladores de dispositivos, herramientas de diagnóstico, etc.), software de programación (editores de texto, compiladores, intérprete de instrucciones, enlazadores, debuggers, etc.), software de aplicación que permite realizar tareas a los usuarios finales y el software de red, que permite comunicarse a grupos de usuarios.

1.1.3.3 Datos

Son representaciones simbólicas (numéricas, alfanuméricas, etc.) de la información, manipuladas por el software y el hardware con el fin de cobrar sentido en el mundo informático.

1.1.4 AMENAZAS [1]

Es cualquier cosa que pueda alterar la operación, funcionalidad, integridad o disponibilidad de una red o sistema.

1.1.4.1 Formas de la Amenaza

1.1.4.1.1 Interrupción

Provoca que un objeto del sistema se pierda, quede inutilizable o no disponible, su detección es inmediata.

1.1.4.1.2 Interceptación

Cuando un elemento no autorizado consigue acceso a un elemento del sistema, su detección es difícil a veces no deja huellas.

1.1.4.1.3 Modificación

Cuando a más de conseguir el acceso, consigue modificar un objeto del sistema con el fin de obtener beneficios. Se considera también como la destrucción del objeto si el mismo queda inutilizable.

1.1.4.1.4 Generación

Cuando se crea o modifica un objeto con el fin de asemejarse a uno original, para pretender engañar al sistema, constituyen delitos de falsificación y su detección es difícil.

1.1.4.2 Tipos de Amenaza

1.1.4.2.1 Amenaza Pasiva

Atenta contra la confidencialidad de la información sin cambiar el estado del sistema. Consiste en el acceso no autorizado a la información protegida, mediante la escucha o monitoreo con el fin de obtener la información transmitida y así averiguar o utilizar información del sistema, sin afectar los recursos del mismo.

Estos ataques son muy difíciles de detectar, ya que no alteran los datos ni la funcionalidad del sistema; para impedir el éxito de estos se puede utilizar cifrado de datos. La defensa ante estos ataques se orienta a la prevención mediante cifrado, antes que a la detección.

- ***Divulgación del contenido.*** Consiste en publicar información de carácter sensible o confidencial.

- ***Análisis de tráfico.*** Consiste en estudiar la información (plana / cifrada) transmitida, para averiguar la naturaleza de la comunicación.

  Un atacante podría observar el patrón de los mensajes o las cabeceras de paquetes y así determinar la localización e identidad de los computadores, o la longitud y frecuencia de los mensajes; aun cuando la información viaje cifrada podría calcular la cantidad de

tráfico que circula por la red o que entra y sale de un sistema, para determinar la naturaleza de la comunicación.

1.1.4.2.2 Amenaza Activa

Provoca un cambio no autorizado y deliberado del estado del sistema; intenta alterar los recursos del sistema o influir en su normal funcionamiento; busca modificar el flujo de datos o crear flujos falsos.

Es difícil impedirlos de forma absoluta, para lograrlo sería necesario protección física permanente de todos los recursos y rutas de comunicación. La clave es la detección de ataques y la recuperación de interrupciones o retardos causados por estos; además la detección puede contribuir con la prevención.

- ***Enmascaramiento.*** Consiste en suplantar a una entidad, mediante la captura de secuencias de autenticación, y retransmisión de las mismas; con el fin de obtener privilegios adicionales dentro del sistema.

- ***Retransmisión.*** Consiste en la captura de datos y su posterior retrasmisión para provocar efectos no autorizados.

- ***Modificación de mensajes.*** Consiste en la modificación, retraso, reordenamiento de algún fragmento de un mensaje legítimo con el fin de provocar efectos no autorizados.

- ***Denegación de Servicio.*** Consiste en impedir el normal funcionamiento de equipos, redes y servicios de comunicación. Interrupción de un servidor o de toda una red, al deshabilitar el servidor o sobrecargarlo para degradar su rendimiento. Suprimir todos los mensajes dirigidos a un destino concreto, entonces si no hay petición no hay respuesta.[2]

1.1.4.3 Origen de las Amenazas

1.1.4.3.1 Humanas

Las personas son el eslabón más débil en la seguridad, ya que está en la naturaleza humana factores como la curiosidad, el bien y el mal que puede afectar a cualquier sistema de seguridad por más sofisticado que este sea.

- ***Personal.*** Son los integrantes de una organización, los mismos que se supone son confiables, pero pueden comprometer gravemente la seguridad del sistema de forma intencional o accidental; cuando los ataques son intencionados pueden causar efectos extremadamente dañinos, ya que el personal conoce los sistemas y sus debilidades mejor que cualquier persona externa a la organización y es frecuente también los accidentes causados por errores o desconocimiento de las normas básicas de seguridad.

- ***Ex empleados.*** Se trata de personas separadas de la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo por algún hecho que no consideran justo.

- ***Curiosos.*** Son los atacantes más habituales de un sistema; pues las personas son curiosas por naturaleza y con el amplio acceso a la tecnología que se tiene en la actualidad, potencialmente se convierten en profesionales y expertos de sistemas informáticos y telecomunicaciones, así exploran los sistemas en busca de mayores privilegios o accesos de los que ya tienen.

- ***Crackers.*** Son las personas que intentan de forma ilegal romper la seguridad de un sistema por diversión o interés. Su objetivo típico son los sistemas de seguridad media y redes generalmente abiertas. Mediante un escáner de seguridad detectan las vulnerabilidades de los sistemas para finalmente atacarlos.

- ***Hackers.*** Personas con altos conocimientos en informática, que crean programas que permiten eliminar limitaciones o candados y así desproteger programas y evitar pagar licencias de uso o comprarlos.

- ***Terroristas.*** Personas que atacan un sistema con el fin de causar algún tipo de daño.

- ***Intrusos remunerados.*** Constituyen el grupo más peligroso, ya que son personas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, pagados por una tercera parte (empresa de la competencia) para robar secretos o dañar la imagen de la entidad atacada.

- ***Script Kiddie.*** Persona inexperta, generalmente un adolescente que usa programas que descarga de Internet para atacar sistemas.

1.1.4.3.2 Amenazas Lógicas

Constituyen todo tipo de programas que de una forma u otra pueden dañar un sistema, creados de forma intencional (software malicioso) o errónea (bugs).

- ***Software incorrecto.*** Son los errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones, se los llama ***bugs*** y son explotados mediante programas llamados ***exploits***.

- ***Herramientas de seguridad.*** Son utilizadas para detectar fallos en los sistemas o redes, pero representan un arma de doble filo, ya que un administrador de red puede solucionar las falencias encontradas, mientras que un intruso puede explotar las mismas.

- ***Malware.*** Es cualquier software creado con la intención de molestar o dañar el normal funcionamiento de una computadora. Tenemos los virus, spywares, gusanos, etc.

1.1.4.3.3 Amenazas Físicas

Las catástrofes (naturales o artificiales) son la amenaza menos probable, sin embargo es importante tomar medidas básicas de protección, ya que si se produjeran generarían daños de gran impácto. Como ejemplos de catástrofes tenemos: terremotos, inundaciones, incendios, humo o atentados de baja magnitud.

También existe un subgrupo de catástrofes con posibilidad de ocurrencia mínima, denominados riesgos poco probables, por lo tanto no vale la pena tomar medidas de seguridad contra éstas, ya que el sistema de prevención resultaría costoso e inecesario.

1.1.5 VULNERABILIDADES [3]

Es una debilidad inherente al diseño, configuración o implementación de una red o sistema, que lo deja susceptible a ataques.

1.1.5.1 Diseño pobre

Se presenta en los sistemas hardware y software que contienen fallas de diseño que pueden ser explotadas, es decir que el sistema ha sido creado con huecos de seguridad.

1.1.5.2 Implementación pobre

Se presenta en los sistemas configurados incorrectamente y por lo tanto son vulnerables a un ataque; estos tipos de vulnerabilidades son el resultado de desconocimiento, inexperiencia, entrenamiento insuficiente o descuido en el trabajo.

1.1.5.3 Administración pobre

Son el resultado de procedimientos inadecuados, controles y verificaciones insuficientes. Las medidas de seguridad no pueden operar en un vacío, necesitan ser documentadas y monitoreadas.

1.1.6 MECANISMOS [1] [3]

La seguridad informática en las redes y sistemas requiere de un ciclo contínuo de protección, detección y respuesta.

1.1.6.1 Mecanismos de Prevención

Consiste en cerrar las brechas de seguridad para aumentan la fiabilidad de un sistema durante su funcionamiento normal, previniendo la ocurrencia de violaciones a la seguridad.

1.1.6.1.1 Mecanismos de autenticación e identificación

Permiten identificar entidades del sistema de una forma única para posteriormente autenticarlas (comprobar que la entidad es quien dice ser).

1.1.6.1.2 Mecanismos de control de acceso

Controlan todos los tipos de acceso sobre cada objeto por parte de cualquier entidad del sistema.

1.1.6.1.3 Mecanismos de separación

Se utilizan cuando un sistema maneja diferentes niveles de seguridad, para evitar el flujo de información entre objetos y entidades de diferentes niveles sin la exigencia de una autorización expresa del mecanismo de control de acceso. Tenemos mecanismos de separación física, temporal, lógica y criptográfica.

1.1.6.1.4 Mecanismos de seguridad en las comunicaciones

Se utilizan para garantizar la privacidad e integridad de los datos cuando se transmiten por la red. Algunos de estos mecanismos se basan en la criptografía como el cifrado de clave pública, de clave privada, firmas digitales, etc. Otros utilizan protocolos seguros como SSH, Kerberos, etc.

Los mecanismos de prevención se detallan más adelante en el subcapítulo Tecnologías de Seguridad Informática.

1.1.6.2 Mecanismos de Detección

Son aquellos que se utilizan para detectar violaciones a la seguridad o intentos de violación, ya que si no nos damos cuenta del ataque el daño va a ser mayor. Como ejemplo tenemos los programas de auditoría.

1.1.6.3 Mecanismos de Respuesta

Son aquellos que se aplican cuando una violación del sistema se ha detectado, ya que busca minimizar los efectos de un ataque o problema y finalmente retornar al sistema a su modo de trabajo normal. Como ejemplo tenemos las copias de seguridad o el hardware adicional (respaldos).

1.1.6.3.1 Mecanismo de análisis forense

Su objetivo es averiguar el alcance de la violación, las actividades del intruso en el sistema y la puerta utilizada para entrar; así se podrá prevenir ataques posteriores y detectar ataques a otros sistemas de nuestra red.

1.1.7 MODELOS DE SEGURIDAD [3]

1.1.7.1 Seguridad por Oscuridad

Consiste en esconderse o pasar desapercibido para protegerse, así si nadie conoce de la existencia de la red o sistema, entonces éste no estaría sujeto a ataques.

1.1.7.2 Perímetro de defensa

Consiste en cercar la red o sistema a proteger, generalmente mediante un firewall que separe la red protegida de la red no confiable.

1.1.7.2.1 A nivel de red

Busca proteger al sistema informático de los ataques de hackers, intrusiones o robo de información en conexiones remotas.

1.1.7.2.2 A nivel de contenidos

Busca proteger al sistema de amenazas como los virus, gusanos, troyanos, spyware, phishing y demás clases de malware, del spam o correo basura y de los contenidos web no apropiados.

1.1.7.3 Defensa en profundidad

Es el modelo más robusto y consiste en la protección y monitoreo de cada sistema aisladamente, dotándoles de la capacidad de defenderse por si mismos.

1.1.8 SEGURIDAD EN EMPRESAS [1]

Las redes y sistemas pertenecientes a empresas teóricamente son las que representan mayores ventajas en lo relativo a su protección ya que suelen ser muy aislables.

Las empresas disponen de una red LAN en el edificio donde están ubicadas, la misma que puede aislarse del exterior mediante un Firewall; pero si se ofrecen servicios hacia el exterior (correo electrónico y web), se pueden situar los servidores en una zona desmilitarizada entre el Router y la red interna. Además se tiene la conexión a Internet que brinda acceso hacia el exterior. Así la idealización de red aislada no sería posible con lo cual nos enfrentaríamos a los problemas de seguridad inherentes a esta apertura.

Las empresas cuentan con varias sucursales separadas geográficamente, para conectarlas tenemos dos opciones, hacerlo mediante una red propia (muy costoso) protegida por los técnicos de la misma compañía o mediante un enlace arrendado a través de una red de propósito general como base de comunicaciones (red telefónica, Internet, etc.), así la protección de la red ya no depende exclusivamente de la propia organización, entonces es

indispensable recurrir a VPN (Redes Privadas Virtuales), estableciendo canales de comunicación seguros dentro de redes inseguras.

El personal de las empresas cuenta con estaciones de trabajo móviles, las mismas que potencialmente pueden causar problemas de conectividad y seguridad, ya que una estación móvil puede entrar en contacto con ambientes inseguros y comprometer la información o infectarse, para seguidamente, introducirse en la organización y comprometer la seguridad de la misma.

Finalmente hay que considerar los ataques internos, que puede sufrir la organización por parte del personal propio de la empresa.

1.2 POLÍTICAS DE SEGURIDAD INFORMÁTICA [3] [4]

En la actualidad la gestión de la seguridad es algo crítico para cualquier organización, igual de importante que los sistemas de calidad o las líneas de producto que desarrolla.

Las políticas de seguridad son el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema, que indica lo que está y lo que no está permitido en el área de seguridad durante la operación general del sistema.

Sin una política de seguridad correctamente implantada en la organización no sirven de nada los controles de acceso (físicos y lógicos) implementados en la misma.

1.2.1 POLÍTICAS Y PROCEDIMIENTOS [3]

Las políticas y procedimientos de seguridad en una red o sistema sirven para asegurar la seguridad de la información, definen los niveles aceptables de seguridad de la información, mediante el planteamiento de aspectos como: ¿qué constituye la seguridad de la información?, ¿por qué es importante? y ¿cómo mantenerla?.

Para determinar el nivel de seguridad adecuado para cierta organización, se debe considerar los elementos de seguridad de la información: confidencialidad, integridad, disponibilidad, autenticación y control de acceso, de acuerdo a los requerimientos de la organización.

1.2.1.1 Políticas de seguridad

Son el conjunto de reglas y procedimientos que regulan cómo una organización administra, usa, protege y distribuye toda la información que directa o indirectamente le pertenece.

Las políticas deben estar orientadas a qué posesiones proteger y por qué necesitan ser protegidos, son amplias en su alcance y son diseñadas para fijar el tono y la dirección. Son documentos que exhiben el ***¿qué?*** y ***¿por qué?*** de la seguridad de la información para una organización, además deben ser simples de entender y fáciles de recordar.

1.2.1.2 Procedimientos de seguridad

El desarrollo de los procedimientos debe fluir desde las políticas de seguridad, estos deben ser más precisos y detallados, centrarse en las medidas específicas necesarias para proteger las posesiones de la organización. Son documentos que contienen el ***¿quién?***, ***¿cuándo?*** y ***¿cómo?*** de la seguridad de la información dentro de una organización.

1.2.2 OBJETIVOS DE LAS POLÍTICAS DE SEGURIDAD [3]

El desarrollo de políticas y procedimientos de seguridad para redes y sistemas de una organización proporciona beneficios directos como prevenir o detectar fraudes o disuadir hackers, también beneficios indirectos como proteger a la organización de potenciales responsabilidades o salvarla de posibles vergüenzas.

1.2.2.1 Administración de riesgos

Es casi imposible asegurar completamente el patrimonio informático de una organización, ya que los riesgos se pueden minimizar, pero nunca eliminarlos completamente.

Es necesario identificar los riesgos que enfrenta una organización y desarrollar medidas preventivas y de recuperación para minimizar el impácto de éstos.

1.2.2.2 Asegurar la continuidad del negocio

Las políticas y procedimientos deben asegura la reanudación del negocio mediante un esquema apropiado de las acciones necesarias en respuesta a un incidente o desastre.

1.2.2.3 Definición de responsabilidades, expectativas y comportamientos aceptables

Para que cualquier política o procedimiento sea eficaz, las personas involucradas con éstas deben entender, qué se requiere de ellas para cumplirlas. El acatamiento de una política se consigue llegando a un acuerdo de, qué constituye el acatamiento. Los empleados necesitan entender sus responsabilidades dependiendo de las circunstancias.

1.2.2.4 Cumplir con el deber fiduciario y obedecer los requerimientos regulatorios

La mayoría de las organizaciones están sujetas a reglas o regulaciones que controlan las responsabilidades de los oficiales corporativos y regulan la operación de la organización.

Si una compañía realiza comercio público, los oficiales corporativos tienen el deber de asegurar la solidez financiera de la organización ante el fisco, si fallan en este deber pueden ser responsabilizados directamente por las pérdidas incurridas.

Las organizaciones requieren adherirse a ciertos estándares (registros y libros de contabilidad) y regulaciones que requieren ciertas medidas para proteger las posesiones de la organización. Muchas organizaciones están sujetas a reglas y regulaciones respecto a la protección y revelación de la información perteneciente a los empleados y clientes.

La ausencia de políticas y procedimientos apropiados es considerada automáticamente como incumplimiento.

1.2.2.5 Proteger a la organización de la responsabilidad

La existencia de políticas y procedimientos son escenciales para demostrar que la organización no aprobó las acciones de un usuario final, o que un empleado actuó o no con la autorización de la organización.

1.2.2.6 Asegurar la integridad y confidencialidad de la información

La protección de los recursos informáticos de la organización constituye un componente clave de la seguridad de la información. Sin la integridad de la información la organización no puede tomar decisiones de negocios. Sin la confidencialidad de la información la organización perderá su ventaja competitiva por la pérdida de la información reservada de productos, clientes, compañeros, proveedores, etc.

1.2.3 DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD [3]

Para alcanzar los objetivos de seguridad mencionados se debe considerar ciertos elementos al momento de desarrollar las políticas y procedimientos de seguridad de la información para una organización.

Los siguientes elementos pueden ser considerados como claves para establecer con éxito las políticas y procedimientos de una organización ya que constituyen los peldaños para el proceso de desarrollo.

1. Identificar los recursos de la organización.
2. Definir los riesgos.
3. Definir la administración de los recursos informáticos.
4. Definir el acceso sobre los recursos informáticos.
5. Definir los procesos se usarán para la autenticación.
6. Definir clara y detalladamente, qué constituye el uso apropiado o no de los medios de comunicación electrónicos y servicios de la compañía.
7. Definir claramente, qué clase de información puede ser accedida y distribuida y por qué medios.
8. Definir, qué controles van a ser colocados.
9. Notificar a los usuarios de los procedimientos de auditoría, monitoreo, revelación de la información y las consecuencias del incumplimiento.
10. Identificar a aquellos responsables de la ejecución de seguridad y cómo las políticas y procedimientos se harán cumplir.
11. Desarrollar los pasos a seguir ante un evento de incumplimiento de la política, una brecha de seguridad o un desastre.

El primer paso es determinar responsabilidades para el desarrollo de las políticas de seguridad de la información, éstas deben ser un esfuerzo conjunto entre la unidad IT y todas las unidades de la organización.

Un factor decisivo para el éxito o fracaso de las políticas de seguridad es el apoyo por parte del gerente de la organización, los desarrolladores de la política de seguridad deben poseer la autoridad para implementar las medidas necesarias para proteger los recursos informáticos de la organización, caso contrario están destinadas al fracaso.

Es necesario inculcar una cultura de seguridad de la información en la organización y debe ser dirigida por el gerente para tener un mejor impácto.

1.2.3.1 Valoración del riesgo

Es un proceso que determina, ¿qué se quiere proteger?, ¿por qué se quiere proteger? y ¿de qué se necesita proteger?

1. Identificar y priorizar recursos.
2. Identificar vulnerabilidades.
3. Identificar amenazas y sus probabilidades.
4. Identificar contramedidas.
5. Desarrollar un análisis costo-beneficio.
6. Desarrollar las políticas de seguridad.

Las políticas y procedimientos implementados en una organización deben estar basados en el mundo real y no deben interferir con la operación de la organización; los procesos desarrollados no deben ser muy complicados.

1.2.4 IMPLEMETACIÓN DE LAS POLÍTICAS DE SEGURIDAD [3]

La implementación de las políticas de seguridad requiere de los siguientes procedimientos:

1. Desarrollar y escribir un manual de las políticas y procedimientos de seguridad.
2. Desarrollar un programa educacional para el conocimiento de los usuarios finales.
3. Desarrollar un proceso para la ejecución de las políticas y la puesta en práctica de los procedimientos.
4. Desarrollar un proceso para la evaluación y actualización periódica de las políticas y procedimientos.

1.2.4.1 Formato de la política de seguridad

1.2.4.1.1 Declaración de política

Esta sección muestra la política en forma general, contiene lo que la política dice y lo que implica.

1.2.4.1.2 Propósito

Esta sección debe decir por que se necesita la política de seguridad; puede detallar el efecto que la política tiene en la seguridad de la organización y sus empleados.

1.2.4.1.3 Alcance

Esta sección debe cubrir la extensión de la política. El alcance debe indicar las circunstancias bajo las cuales la política es aplicable, puede incluir el lapso de tiempo, hardware y software específico y/o eventos bajo los cuales la política es eficaz.

1.2.4.1.4 Acatamiento

Esta sección debe incluir una explicación detallada de lo que se debe y no se debe hacer para el cumplimiento de la política.

1.2.4.1.5 Penalidades

Esta sección debe explicar las consecuencias de no cumplir con la política de seguridad y listar las sanciones asociadas al no cumplimiento de las mismas. Las penalidades sirven como advertencias a los empleados.

1.2.4.2 Conocimiento de la política y educación

Una política no tiene valor si nadie conoce lo que dice. Los usuarios finales y el personal deben entender las expectativas de la administración y sus responsabilidades con respecto al cumplimiento de las políticas de una organización; también deben entender las consecuencias del no cumplimiento de las mismas.

Las organizaciones deben considerar obtener la confirmación escrita de usuarios finales y empleados diciendo que han leído, comprendido y aceptado las políticas de seguridad de información de la organización.

1.2.4.3 Ejecución de la política

El acatamiento de las políticas necesita hacerse cumplir. La única manera de asegurar el acatamiento es a través del monitoreo y la auditoría. Los responsables de hacer cumplir las políticas de seguridad deben tener el apoyo de la gerencia.

1.2.4.4 Administración de la política

Las políticas y los procedimientos son componentes importantes de un buen programa de seguridad, y la administración de políticas es igualmente importante ya que permite vigilar el cumplimiento de las mismas.

Sin embargo el sistema de administración de políticas podría no cubrir vulnerabilidades o configuraciones erróneas del software en el sistema o podría no garantiza que los usuarios revelen sus contraseñas a individuos no autorizados.

1.3 TÉCNICAS DE ATAQUES Y PROTECCIONES [3] [9]

1.3.1 AMENAZAS Y ATAQUES

1.3.1.1 Virus

Es código informático diseñado para replicarse, se adhiere a un programa o archivo para propagarse de un equipo a otro mediante la intervención humana (compartir un archivo, enviar un mensaje de correo), infecta a medida que se transmite y puede dañar hardware, software e información, puede causar desde leves molestias hasta la destrucción del sistema. [5]

1.3.1.2 Gusanos

Es un programa independiente, tiene la capacidad de propagarse automáticamente al tomar el control de las características del equipo que permiten transferir archivos o información, de esta manera puede viajar solo por el sistema en busca de otros sistemas conectados para infectarlos y seguir propagándose por la red. Un gusano puede consumir memoria o ancho de banda, bloqueando un equipo o una red, su poder de ataque radica en que puede replicarse en grandes números e independientemente. Para lograr detener a un gusano sería necesario apagar (reeboot) todos los sistemas infectados al mismo tiempo. [5]

1.3.1.3 Troyanos

Es un programa o fragmento de código que se esconde dentro de otro programa o se disfraza como un programa legítimo, aparenta ser software útil, pero realmente pone en peligro la seguridad y provoca daños ya que puede grabar información sensible o instalar

programas de puerta trasera. Se difunde cuando un usuario es engañado y abre un programa que aparenta venir de un origen legítimo. También pueden venir incluidos en software que se descargan gratuitamente.

1.3.1.4 Puertas traseras

Es una forma no documentada de ganar acceso al sistema construida por el diseñador, también puede ser un programa que ha sido alterado para permitir accesos privilegiados a un sistema o proceso.

1.3.1.5 Bombas lógicas

Es un programa o subsección de un programa diseñado con intenciones malignas, que es disparado cuando ciertas condiciones lógicas se presentan, tales como ausencia o presencia de ficheros, ejecución de un determinado usuario (root) o determinada fecha.

1.3.1.6 Escáner de puertos

Es una herramienta utilizada por un hacker para reunir información que puede utilizar después para atacar al sistema. Es un programa que escucha los números de puertos bien conocidos para detectar los servicios que se están ejecutando y pueden ser explotados, para así irrumpir en el sistema.

Las organizaciones pueden monitorear sus archivos log del sistema para detectar el escaneo de puertos como un preludio de ataque.

1.3.1.7 Spoofs

Buscan falsificar la identidad de alguien o enmascararse como algún otro individuo o entidad para ganar acceso a sistemas o redes y obtener información para propósitos no autorizados.

- ***IP Address Spoofing.*** Cada dispositivo tiene una dirección IP única en una red TCP / IP. Este ataque toma ventaja de sistemas y redes que confían en la dirección IP del sistema o dispositivo que se conecta para autenticarlo y permitir el acceso; pero si un hacker enmascara una dirección válida logrará acceso a la red interna.

- ***Sequence Number Spoofing.*** Las conexiones en redes TCP / IP usan números de secuencia, que son parte de cada transmisión y son intercambiados con cada transacción. Un hacker puede monitorear la conexión de red para registrar los números de secuencia intercambiados y predecir los números de secuencia futuros, lo cual le permitirá insertarse y adueñarse de la conexión de red o insertar información incorrecta.

- ***Sesión Highjacking.*** Un hacker se encarga de la conexión de sesión entre un cliente y un servidor, mediante la obtención de acceso a un router o dispositivo de red que actúe como gateway entre un usuario legítimo y el servidor.

- ***Man in the Middle Attack (MIM).*** Se lleva a cabo mediante el DNS spoofing o hyperlink sppoofing; consiste en registrar una URL que es muy similar a una URL existente. Así un hacker se inserta entre un programa cliente y un servidor en una red, para interceptar información ingresada por un cliente (números de tarjetas de crédito, contraseñas, información de cuentas), puede insertarse entre un browser y un servidor Web (Web Spoofing).

- ***DNS Poisoning.*** Explota una vulnerabilidad de bind, que permite ingresar entradas a la tabla de un servidor DNS con información falsa, así un hacker puede dirigir al usuario a una dirección IP incorrecta; haciendo que una URL legítima apunte al sitio web del hacker.

- ***Redirección.*** Es otro método de ataque DNS, consiste en comprometer links de una página web con links falsos, aparentemente estos enlaces son legítimos, pero re-direccionan al usuario a un sitio controlado por el hacker. También puede tratar de manipular el sistema de registro de nombres de dominio para alterar su funcionamiento normal, al transferir un nombre de dominio propietario a otra dirección IP provocando la re-dirección.

1.3.1.8 Ataque de repetición

Consiste en interceptar y almacenar una transmisión legítima entre dos sistemas y retransmitirla un tiempo después.

1.3.1.9 Password cracking

Son programas que descifran archivos de contraseña utilizando el mismo algoritmo usado para generar la contraseña cifrada, empleando un diccionario de palabras o frases conocidas y cifradas con el algoritmo de contraseña. Entonces comparan cada registro del archivo de contraseña con los registros del archivo diccionario hasta encontrar una coincidencia que revele la contraseña.

1.3.1.10 Ingeniería Social

Son métodos no técnicos que emplea un hacker para obtener acceso al sistema, pueden ser sorprendentemente efectivos; consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, como revelar información (contaseñas).

1.3.1.11 Sniffing

Consiste en monitorear los paquetes de una red en busca de información (contraseñas o direcciones IP) que pueda ser útil para un ataque; también el análisis de tráfico puede proveer información útil.

1.3.1.12 Modificación de sitios Web

Consiste en modificar los sitios web de alguna organización, se consigue mediante la explotación de configuraciones incorrectas y/o vulnerabilidades conocidas del software o sistema operativo del servidor Web. Para contrarrestar este ataque hay que actualizar las versiones del software y sistema operativo del servidor Web o implementar servidores caché de red que actualicen al servidor Web.

1.3.1.13 War Dialing

Es un método de fuerza bruta para descubrir puertas traseras en una red perteneciente a una organización, atenta de manera efectiva contra el perímetro de defensa; utiliza un sistema de marcado automático para llamar a cada número de teléfono de la organización en busca de conexiones de módem, para intentar irrumpir en el sistema al cual el módem está conectado y obtener acceso a la red.

1.3.1.14 Negación del servicio

Son diseñados para apagar o presentar inoperable un sistema, el objetivo es hacer a una red o sistema no disponible.

- ***Ping de la muerte.*** Ping es un comando TCP / IP que envía un paquete IP a una dirección IP específica para ver si existe respuesta y determinar si el host está en la red (está activo).

  Algunos sistemas operativos fueron o son vulnerables a paquetes ICMP más grandes de lo normal, entonces especificando un paquete grande en un comando ping se puede causar un desbordamiento interno en algunos sistemas dejándolos inhabilitados. Normalmente se requiere inundar de pings a un sistema para colapsarlo.

- ***Inundación de SYN.*** Explota la negociación de tres vías que TCP / IP utiliza para establecer una conexión, deshabilita un determinado sistema creando muchas conexiones entreabiertas.

  Consiste en inicializar una conexión a un servidor con el bit número SYN, sin embargo la dirección de retorno asociada con el SYN no es una dirección válida, entonces el servidor envía un SYN-ACK a una dirección no válida que no existe y no responde, por lo tanto permanece en espera del ACK de retorno. Así muchas conexiones entreabiertas no permiten el acceso de usuarios legítimos y también pueden colapsar el sistema.

- ***Spam.*** Es correo electrónico no deseado y para un servidor de correo puede representar un ataque de negación de servicio al inundar un determinado sistema con miles de mensajes de correo electrónico. El spam puede consumir el ancho de banda disponible en la red, sobrecargar CPUs, provocar el crecimiento desmedido de los archivos log, consumir todo el espacio de disco disponible del sistema y finalmente colapsarlo.

- ***Ataque smurf.*** Emplea paquetes ICMP ECHO_REQUEST falsificados, enviando como dirección IP origen la dirección IP de un determinado sistema (víctima) y la dirección destino de estos paquetes son direcciones IP de broadcast de red; de ésta manera las máquinas de la red responden e inundan al sistema apuntado, consecuentemente se degradará el rendimiento de la red que conecta a la red intermediaria con el sistema

víctima. Para contrarresta este ataque se puede configurar los dispositivos de red para no responder a ICMP ECHO_REQUEST y deshabilitar el broadcast IP directo.

1.3.1.15 Criptoanálisis

Se basa en la naturaleza del algoritmo y características del texto nativo o en pares de texto cifrado y su correspondiente texto nativo. Explota las características del algoritmo en busca de deducir un texto nativo específico o descubrir la clave secreta; si la clave es descubierta toda información cifrada con ésta se ve comprometida. [2]

1.3.1.16 Fuerza bruta

Radica en probar cada una de las posibles claves sobre el texto cifrado, hasta lograr un texto nativo coherente. [2]

TAMAÑO DE LA CLAVE (bits)	NÚMERO DE CLAVES ALTERNATIVAS	TIEMPO NECESARIO A 1 CIFRADO / µS	TIEMPO NECESARIO A 10^6 CIFRADOS / µS
32	232 = 4,3 × 109	231 µs = 35,8 minutos	2,15 milisegundos
56	256 = 7,2 × 1016	255 µs = 1.142 años	10,01 horas
128	2128 = 3,4 × 1038	2127 µs = 5,4 × 1024 años	5,4 × 1018 años
168	2168 = 3,7 × 1050	2167 µs = 5,9 × 1036 años	5,9 × 1030 años

Tabla 1.1: Tiempo promedio necesario para una búsqueda de clave exhaustiva. [2]

1.3.2 VULNERABILIDADES [7]

1.3.2.1 Sistemas operativos

1.3.2.1.1 Internet Explorer

Microsoft Internet Explorer es el navegador más popular usado para explorar la red y es instalado de forma predeterminada en los sistemas Windows.

Internet Explorer contiene muchas vulnerabilidades que pueden llevar a la corrupción de la memoria, spoofing y ejecución de secuencias de comandos arbitrarios. Los problemas más críticos son los que permiten la ejecución de código remoto sin ninguna interacción del usuario cuando se visita una página web maliciosa o se lee un correo electrónico. Además Internet Explorer ha sido utilizado para explotar vulnerabilidades en otros componentes de Windows como la ayuda HTML, motor de representación gráfica, control ActiveX.

Estos defectos han sido explotados extensamente para instalar spyware, adware y otro malware sobre los sistemas de usuarios.

1.3.2.1.2 Librerías Windows

Las aplicaciones de Windows se apoyan fuertemente en un gran número de librerías del sistema empaquetadas en archivos DLL. Estas librerías son utilizadas para tareas como ejecución de HTML, decodificación de formatos de imágenes, decodificación de protocolos, etc.

Aplicaciones accesibles tanto local como remotamente usan estas librerías; de ésta forma una vulnerabilidad crítica en una librería impácta un rango de aplicaciones de Microsoft y de terceros que recaen en la librería.

Librerías críticas afectadas:

- Graphics Rendering Engine.
- DirectShow.
- Color Management.
- HTML Help.
- Web View.
- Shell.
- Hyperlink Object.
- PNG Image Processing.
- Cursor e Icon Processing.
- Compressed Folder.
- JPEG Processing.

1.3.2.1.3 Microsoft Office

Microsoft Office es la herramienta de correo electrónico y productividad más utilizada en el mundo. Las aplicaciones incluyen Outlook, Word, PowerPoint, Excel, Visio, Frontpage y Access. Las vulnerabilidades en estos productos pueden explotarse a través de los siguientes vectores de ataque:

- El atacante envía el documento de Office malicioso en un mensaje de correo electrónico (virus).

- El atacante hospeda el documento en un servidor web o en una carpeta compartida, tentando al usuario a navegar en el sitio web o la carpeta compartida.

- El atacante ejecuta un servidor que envía respuestas maliciosas para disparar un buffer overflow en clientes de correo electrónico.

1.3.2.1.4 Servicios Windows

Los sistemas operativos Windows soportan una gran variedad de servicios, métodos de red y tecnologías, implementados con Service Control Program (SCP) bajo el control de Service Control Management (SCM), que se ejecutan como Service.exe.

Las vulnerabilidades de buffer overflow explotables remotamente continúan siendo el principal problema que afecta a los Servicios de Windows.

Diversos servicios del sistema proveen interfaces remotas a componentes de clientes mediante Remote Procedure Calls (RPC; Llamadas a Procedimiento Remoto), quedando expuestos mediante los extremos de pipes accesibles por medio del protocolo Common Internet File System (CIFS), puertos TCP/UDP conocidos y en ciertos casos puertos TCP/UDP efímeros. Muchos de estos servicios pueden ser explotados vía sesiones anónimas para ejecutar código arbitrario con privilegios de “SISTEMA”.

1.3.2.1.5 Debilidades de configuración de Windows

- ***Configuración de contraseñas de usuario.*** Las debilidades en la configuración de contraseñas ha adquirido importancia en los últimos años con la proliferación de gusanos, bots y otro malware que han mejorado su habilidad de propagarse por si mismos, mediante el abuso de contraseñas inadecuadas. Esta debilidad puede existir tanto en el directorio activo como a nivel local y puede ser explotado eficazmente tanto por malware como por amenazas internas. Además con el incremento de la autenticación centralizada de plataforma múltiple, el acuerdo de las credenciales de Windows puede resultar en el acuerdo de credenciales directamente para otras plataformas.

- ***Servicio para contraseñas de cuenta.*** Es muy común usar contraseñas cortas y publicables para las cuentas de usuario, esto es un problema cuando es usado sobre muchas máquinas ya que tienen privilegios altos y se cambian rara vez.

- ***Entrada en el sistema nula.*** Las credenciales nulas permiten establecer sesiones a usuarios anónimos.

1.3.2.1.6 MAC OS X

Contiene diferentes componentes que pueden tener fallas de seguridad.

- ***Safari.*** Es un navegador web, las vulnerabilidades en esta aplicación pueden permitir tomar el control completo del navegador o sesión del usuario.

- ***ImageIO.*** Es un controlador de imagen utilizado por el sistema y la mayoría de aplicaciones, las vulnerabilidades en ésta estructura podrían afectar a muchas aplicaciones ya que los archivos de imagen son considerados generalmente archivos seguros y son abiertos por defecto sin necesidad de confirmación.

- ***Unix.*** Muchas aplicaciones escritas para los sistemas operativos Unix corren en MAC OS X, las vulnerabilidades en estas aplicaciones pueden comprometer a este sistema.

- ***Inalámbrico.*** Se reportaron vulnerabilidades críticas en el subsistema de red inalámbrico, que permiten que atacantes físicamente próximos incluso sin formar parte de la misma red lógica, puedan conseguir un control completo del subsistema vulnerable; defectos adicionales se descubrieron en el subsistema de interfaz inalámbrico Bluetooth.

1.3.2.1.7 Debilidades de configuración de Unix

La mayoría de los sistemas UNIX / LINUX incluye en su instalación predeterminada un determinado número de servicios estándar, tales como CUPS (Common Unix Printing System), portmap (soporta RPC), sendmail (Mail Transport Agent) y sshd (servidor OpenSSH). Son de particular interés los ataques de fuerza bruta para adivinar contraseñas contra SSH, ftp y telnet.

1.3.2.2 Aplicaciones Multiplataforma

1.3.2.2.1 Aplicaciones Web

Aplicaciones como Content Management Systems (CMS), Wikis, portales, tablero de anuncios y foros de discusión, son usadas por pequeñas y grandes organizaciones; cientos de vulnerabilidades son reportadas y explotadas en estas aplicaciones web, por válidación insuficiente o errores lógicos de la aplicación.

- ***Inclusión de archivos remotos en las aplicaciones PHP.*** PHP es el lenguaje de aplicaciones web más utilizado, permite funciones de archivo para acceder a recursos en el Internet, usando una característica llamada “allow_url_fopen”, permite que un atacante ejecute o instale código a su elección en el servidor web vulnerable.

- ***Inyección SQL.*** Son posibles, debido a la mezcla de datos de usuario dentro de consultas dinámicas o procedimientos de almacenamiento mal formulados, permite a los atacantes crear, leer, actualizar o borrar arbitrariamente datos disponibles en la aplicación y en el peor de los casos comprometer el sistema de base de datos y los sistemas a su alrededor.

- ***Scripts de sitio cruzado (XSS).*** Permite que atacantes modifiquen sitios web, inserten contenido hostil, dirijan ataques de phishing, tomen el control del navegador usando malware JavaScript o forcen a los usuarios a dirigir comandos que no son de su elección.

- ***Falsificación de solicitud de sitio cruzado (CSRF).*** Fuerza a usuarios legítimos a ejecutar comandos sin su consentimiento, este tipo de ataque es sumamente difícil de prevenir.

- ***Directorio Transversal.*** Permite a los atacantes acceder a recursos controlados como archivos de contraseña, archivos de configuración, credenciales de base de datos, etc.

1.3.2.2.2 Software de Base de Datos

Las bases de datos son el elemento clave de muchos sistemas para almacenar, buscar o manipular grandes cantidades de datos. Debido a la valiosa información que almacenan

como detalles personales y financieros a menudo son blancos de ataque. Entre las vulnerabilidades más comunes en los sistemas de base de datos tenemos:

- Bases de datos ejecutándose en configuración predeterminada, con usuarios y contraseñas predeterminados.
- Buffer overflows en procesos que escuchan puertos TCP/UDP bien conocidos.
- Inyección SQL a través de la interfaz web de la base de datos.
- Bases de datos ejecutándose con contraseñas débiles para cuentas privilegiadas.

1.3.2.2.3 Aplicaciones para compartir archivos P2P

Las redes punto a punto consiste de una colección de computadoras o nodos que funcionan simultáneamente como cliente y servidor para conseguir un propósito común. Los nodos pueden intercambiar datos, compartir recursos, proveer servicios de directorio, soportar comunicaciones y proveer colaboración en tiempo real. Las aplicaciones punto a punto se utilizan para la descarga y distribución de contenidos tales como música, video, gráficos, texto, código fuente, etc.

Estas aplicaciones pueden ser mal usadas o explotadas para compartir ilegalmente material con derechos reservados, obtener datos confidenciales, exponer a los usuarios a pornografía no deseada, violencia o propaganda, distribuir o ejecutar malware (virus, spyware, bots, etc) y como resultado sobrecargar la red.

Gran parte de los programas P2P utilizan puertos predeterminados aunque pueden ser configurados para utilizar otros diferentes y así evadir la detección, el firewall o el filtrado saliente.

Las principales amenazas que surgen a partir del software P2P son:

- Aprovechamiento remoto de vulnerabilidades en aplicaciones P2P utilizadas para comprometer clientes o servidores P2P.
- Virus y bots que utilizan las carpetas compartidas P2P para propagarse mediante la copia de archivos maliciosos en dichas carpetas con nombres de archivo atractivos.

- El software P2P generalmente incorpora programas de tipo spyware y adware.
- Los atacantes pueden enmascarar archivos maliciosos como archivos legítimos de música o video; los usuarios al descargar estos archivos puedan llegar a infectar sus sistemas siendo estos utilizados como un bot.
- Los recursos compartidos P2P típicamente no cuentan con contraseñas o bien son débiles, esta falla puede ser aprovechada para infectar el recurso compartido.
- Una organización puede ser objeto de diferentes demandas como responsable de infracción de copyright.
- El tráfico P2P puede consumir el ancho de banda, provocando lentitud en otras aplicaciones críticas.

1.3.2.2.4 Mensajes Instantáneos

El amplio uso de los mensajes instantáneos (IM) continúa incrementando los riesgos de seguridad para las organizaciones e individuos que los usan; recientes ataques incluyen nuevas variaciones en el establecimiento y difusión de bots de red, y el uso de cuentas de mensajería instantánea comprometidas para obtener información sensible de los usuarios.

- ***Malware.*** Gusanos, virus y troyanos trasferidos mediante el uso de la mensajería instantánea; muchos bots son controlados mediante canales IRC (Internet Relay Chat).
- ***Información confidencial.*** La información transmitida vía mensajería instantánea puede estar sujeta a revelación.
- ***Red.*** Ataques de negación de servicio, utilización de la capacidad de red excesiva.
- ***Vulnerabilidades de la aplicación.*** Las aplicaciones de mensajería instantánea contienen vulnerabilidades que pueden ser explotadas para comprometer los sistemas afectados.

1.3.3 PROTECCIONES [3]

1.3.3.1 Secure Sockets Layer (SSL)

Fue desarrollado para brindar seguridad en la transmisión de información por Internet, ofrece confidencialidad al momento de ingresar o trasmitir datos por la Web. Se utiliza la encriptación asimétrica para preparar la sesión SSL y la encriptación simétrica para transmitir datos de forma segura sobre una red insegura.

1.3.3.1.1 https

Consiste en usar el servicio http sobre SSL, SSL establece una conexión segura mediante el uso de un túnel encriptado entre el cliente browser y el servidor Web, así los paquetes de datos viajan seguros. La integridad de la información se establece mediante algoritmos hash, la confidencialidad de la información es asegurada mediante la encriptación, la autenticación de las entidades se asegura mediante el uso de certificados digitales y encriptación asimétrica.

El proceso consiste en preparar una sesión SSL:

1. Ambos extremos intercambian números aleatorios.
2. El servidor envía su clave pública y un ID de sesión.
3. El cliente browser crea una clave denominada pre_master_secret, la cifra con la clave pública del servidor y la envía al servidor.
4. Ambos extremos generan una clave de sesión utilizando la pre_master_secret y los números aleatorios.
5. Utilizan la clave de sesión para trabajar con encriptación simétrica.

1.3.3.2 Seguridad E-mail

Consiste en no revelar el contenido del mensaje e-mail mediante el uso de encriptación; asegurar la integridad del mensaje mediante el empleo de algoritmos hashing o message digest; verificar la identidad del transmisor mediante el empleo de firmas digitales y finalmente verificar la identidad del receptor mediante el uso de encriptación de clave pública.

- ***Pretty Good Privacity (PGP).*** Es un programa de encriptación, usa encriptación simétrica para cifrar y descifrar el mensaje y encriptación asimétrica para cifra la clave secreta usada en la encriptación simétrica. Usa un sistema de anillo de claves en una Web de confianza, donde se exhibe la clave pública de los propietarios de las cuentas de correo electrónico.

- ***Privacy-Enhamsed Mail (PEM).*** Es un estándar que define el uso de encriptación de clave pública para asegurar la transmisión de e-mail por el Internet.

  Usa una organización jerárquica para la autenticación y la distribución de claves, para que la clave sea válida debe estar firmada por una AC.

- ***Secure MIME (S/MIME).*** Es un estándar que describe un método seguro para el envió de e-mail que usa el sistema de encriptación RSA, emplea certificados digitales con firmas digitales para identificar al transmisor, utiliza hashing para asegurar la integridad del mensaje y una combinación de encriptación simétrica y asimétrica para asegurar la confidencialidad.

1.3.3.3 Segmentación del tráfico LAN

Es el proceso de separar una red grande en varias redes pequeñas, así los paquetes permanecen dentro del segmento y no atraviesan la red entera, sirve para dos propósitos seguridad y rendimiento.

1.3.3.4 Sistemas Honeypot

Son sistemas de señuelo o carnada, que contienen servicios, archivos y aplicaciones farsantes, diseñadas para emular sistemas reales con vulnerabilidades bien conocidas. El objetivo es atrapar a los hackers, pues el administrador de seguridad puede seguir el rastro de estos.

1.3.3.5 Herramientas de seguridad [1] [11]

1.3.3.5.1 Exploración de vulnerabilidades

Constituye una parte importante de un buen programa de seguridad ya que ayudará a identificar los puntos de entrada potenciales para los intrusos.

Seguidamente debe implementarse medidas de seguridad a cada punto vulnerable identificado.

- ***Computer Oracle and Password System (COPS).*** Es un conjunto de herramientas usadas para examinar problemas de configuración comunes en los sistemas UNIX, como contraseñas débiles, sesiones ftp anónimas, sesiones tftp, permisos inapropiados.

- ***Security Administrator's Tool for Analyzing Networks (SATAN).*** Es una herramienta para sistemas UNIX, diseñada para reconocer problemas de seguridad relacionados con la red. SATAN identifica y genera un reporte de los problemas, explicando cada problema, la posible consecuencia y como arreglarlo.

- ***TITAN.*** Es un programa de auditoría automática para sistemas UNIX, que detecta problemas de seguridad en la máquina local.

1.3.3.5.2 Control y seguimientos de accesos

- ***TCPWrapper.*** Es un programa de monitoreo de seguridad de red UNIX, que permite observar y controlar las conexiones tftp, exec, ftp, rsh, telnet, rlogin y finger; filtra los accesos basándose en las direcciones IP.

1.3.3.5.3 Comprobación de la integridad del sistema

- ***Tripwire.*** Es un programa que comprueba la integridad de ficheros y directorios de sistemas Unix; compara un conjunto de archivos con información sobre los mismos almacenada previamente en una base de datos, y alerta al administrador en caso de que algo haya cambiado. Se crea un resumen de cada fichero o directorio importante para nuestra seguridad y se almacenan en un medio seguro, de forma que si alguno de los ficheros es modificado Tripwire alertará la próxima vez que se realice la comprobación.

1.4 TECNOLOGÍAS DE SEGURIDAD INFORMÁTICA [2] [3]

1.4.1 ENCRIPTACIÓN [3]

La encriptación es el proceso de mezclar el contenido de un archivo o mensaje para hacerlo incomprensible para cualquiera que no posea la clave requerida para descifrar el archivo o mensaje.

1.4.1.1 Encriptación Simétrica

Es un sistema para encriptación que utiliza una clave secreta (privada), las partes que intercambian información cifrada comparten el mismo algoritmo y clave secreta. La misma clave secreta sirve para cifrar y descifrar los mensajes.

La fortaleza de este sistema depende de la longitud de la clave privada y de mantenerla en secreto; su debilidad es la necesidad de compartir la clave secreta entre las partes.

VENTAJAS	DESVENTAJAS
Rapidez Seguridad relativa Ampliamente Difundido	Requiere compartir información secreta Administración compleja No autenticación No controla el No-repudio

Tabla 1.2: Ventajas y desventajas de la Encriptación Simétrica. [3]

1.4.1.2 Encriptación Asimétrica

Es un sistema para encriptación que utiliza una clave pública y una clave privada. Un mensaje cifrado con la clave privada solo puede ser descifrado con la correspondiente clave pública e inversamente un mensaje cifrado con la clave pública solo puede ser descifrado con la correspondiente clave privada.

La clave pública de un individuo o entidad es compartida a todos y la clave privada debe ser altamente protegida por cada individuo o entidad propietaria.

VENTAJAS	DESVENTAJAS
No necesita compartir información secreta Soporta autenticación Provee no-repudio Escalable	Más lento o computacionalmente intensivo Requiere una autoridad certificadora

Tabla 1.3: Ventajas y desventajas de la Encriptación Asimétrica. [3]

1.4.1.3 Localización de los dispositivos de cifrado [2]

- ***Cifrado de enlace.*** Cada enlace de comunicación vulnerable se equipa con dispositivos de cifrado en ambos extremos, para proteger todo el tráfico que circule por el enlace. Este esquema alcanza un alto nivel de seguridad, pero cuando un paquete entra en un nodo de conmutación es necesario descifrarlo para saber por donde encaminarlo y luego volver a cifrarlo, esto incrementa el tiempo de transmisión y la seguridad de la información se ve comprometida en nodos de conmutación inseguros.

- ***Cifrado de extremo a extremo.*** El proceso de cifrado se realiza en los dos sistemas finales. El terminal origen cifra los datos, los cuales se transmiten sin modificación a través de la red hasta el terminal destino; los terminales origen / destino comparten una clave para cifrar y descifrar. El terminal de origen cifra solamente los datos, ya que la información de cabecera es requerida en cada nodo de conmutación.

  Para incrementar la seguridad será necesario aplicar el cifrado de enlace y el extremo a extremo, de esta manera todo el paquete viaja seguro, excepto el intervalo de tiempo que reside en el conmutador de paquetes.

1.4.1.4 Relleno de tráfico [2]

Es una función que produce continuamente texto cifrado; cuando existe texto nativo lo cifra y transmite y cuando no genera un flujo de datos aleatorio los cifra y transmite, así proporciona seguridad en caso de análisis de tráfico, ya que un atacante no podría distinguir entre el flujo de datos verdaderos y el ruido, y consecuentemente no podría calcular la cantidad de tráfico.

1.4.1.5 Integridad de mensajes [2] [3]

Para conseguir uno alto nivel de confianza en la integridad de un mensaje o archivo, debe implementarse un proceso para prevenir o detectar alteraciones.

- ***Función Hash.*** Es un proceso usado para asegurar la integridad de un mensaje o archivo, toma un mensaje de cualquier longitud y calcula un valor de longitud fija denominado ***valor hash***, éste constituye un resumen criptográfico del mensaje original. Este resumen puede ser considerado como la huella digital del mensaje y usado para determinar si el mensaje o archivo ha sido modificado. Son usadas para crear firmas digitales.

  En el origen se transmite el mensaje junto con su correspondiente valor hash calculado, en el destino se calcula nuevamente el valor hash del mensaje recibido y se compra con el valor hash recibido, para determinar la integridad del mensaje al existir coincidencia o no.

  La función hash debe producir valores hash no reversibles y sin probabilidad de colisiones (dos mensajes diferentes produzcan un mismo valor hash).

ALGORITMO	VALOR HASH (bits)
MD4	128
MD5	128
SHA-1	160
RIPEMD	128, 160, 256

Tabla 1.4: Algoritmos Hashing.

1.4.1.6 Autenticación [2] [3]

Es usada para tener un alto nivel de confianza en la integridad de la información recibida por la red. Las partes involucradas en una transacción necesitan ser capaces de autenticar sus identidades mutuamente.

La falta de la autentificación segura ha sido un obstáculo muy importante para el desarrollo del comercio electrónico por Internet.

1.4.1.6.1 Firma Digital

Una firma digital es usada para asegurar la autenticación y la integridad de un mensaje.

Para el proceso de autenticación es necesario conocer la clave pública del transmisor mediante conocimientos previos o una tercera parte confiable.

El transmisor envía el mensaje cifrado con su clave privada y el valor hash del mensaje original, entonces el receptor descifra el mensaje con la clave pública del transmisor para calcular el valor hash del mensaje descifrado y compararlo con el valor hash recibido para determinar la coincidencia; si coincide se puede asegurar que el mensaje fue enviado por el transmisor correcto y que no fue modificado.

1.4.1.6.2 Certificado Digital

Es un método que permite asociar a un individuo o entidad con una clave pública. El certificado esta firmado digitalmente por una autoridad certificadora (CA), lo cual brinda una confirmación independiente de que el individuo o entidad es quien dicen ser y que la clave pública proporcionada en el certificado de estos les pertenece realmente.

La autoridad certificadora y la clave pública deben ser ampliamente conocidas, para que los certificados tengan valor. Se espera que los certificados sean legalmente aceptados como las firmas manuales notariadas.

Nombre: Individuo, Organización, Entidad.
Clave pública del propietario del certificado.
Fecha de expiración del certificado.
Número serial del certificado.
Nombre de la autoridad certificadora que lo emite.
Firma digital de la autoridad certificadora.

Tabla 1.5: Contenido básico de un Certificado Digital. [3]

Las limitaciones se presentan al momento de manejar los certificados expirados y revocados.

1.4.1.6.3 Autoridad Certificadora (AC)

Es una institución pública o privada, que trata de satisfacer la necesidad de una tercera parte en el comercio electrónico, emitiendo certificados digitales que dan fe de las identidades de los propietarios de los certificados. Para que este proceso funcione la clave pública de la AC debe ser confiable y bien conocida. La AC también debe llevar a cabo las diligencias necesarias para verificar que un individuo o entidad es quien dice ser antes de emitir el certificado.

1.4.1.6.4 Infraestructura de clave pública (PKI)

Esta infraestructura es necesaria para la autenticación de autoridades certificadoras y certificados digitales emitidos por las mismas. Una PKI es una red jerárquica de autoridades certificadoras. Una AC raíz certifica a autoridades certificadoras subordinadas.

1.4.2 FIREWALL [1]

Es un sistema o dispositivo de control de acceso que se utiliza para separar una red interna de una red externa, se encuentra en el límite entre el espacio protegido denominado perímetro de seguridad y la red externa denominada zona de riesgo, filtra tráfico de entrada y salida, y también esconde la configuración de la red hacia el exterior.

Configurados de manera apropiada, se convierten en dispositivos de seguridad indispensables.

Sin embargo no evitará que un atacante utilice una conexión permitida para atentar contra el sistema (ejemplo: un servidor web tiene permitido el acceso desde el exterior y es vulnerable a un ataque en contra de su software).

Tampoco protegerán a una organización de un usuario interno, ya que dicho usuario ya se encuentra en la red interna.

1.4.2.1 Características de diseño y configuración

Entre las características a considerar al momento de implementar un Firewall se tiene:

- Política de seguridad de la organización.
- Nivel de monitoreo, redundancia y control.

- Aspecto económico.

1.4.2.2 Componentes

1.4.2.2.1 Filtrado de paquetes

Se utiliza para implementar diferentes políticas de seguridad en una red, el objetivo es evitar el acceso no autorizado entre dos redes y presentar transparentes los accesos autorizados. El procedimiento consiste en analizar la cabecera de cada paquete y en función de reglas establecidas la trama es bloqueada o se le permite seguir su camino; estas reglas contemplan campos como:

- El protocolo utilizado (TCP, UDP, ICMP, etc.).
- Las direcciones fuente y destino (capa de red).
- El puerto destino (capa de transporte).
- Interfaz del router (arribo / reenvío).

Las reglas se expresan como una tabla de condiciones y acciones que se consulta en orden hasta encontrar una regla que permita tomar una decisión sobre el bloqueo o el reenvío de la trama. Es importante el orden de análisis de las tablas para poder implementar la política de seguridad de forma correcta, ya que la especificación incorrecta constituye uno de los problemas de seguridad en los sistemas de filtrado de paquetes; pero el mayor problema es la incapacidad de analizar datos situados por encima del nivel de red de modelo OSI.

- ***Filtrado de paquetes estático.*** Son reglas estáticas de filtrado que determinan si se niega o autoriza un paquete.

- ***Filtrado de paquetes dinámico.*** Las reglas de filtrado pueden ser modificadas de acuerdo a las necesidades.

1.4.2.2.2 Servidor Proxy

El proxy es una solución software que se ejecuta sobre el Firewall para permitir la comunicación entre dos redes de una forma controlada.

- ***Proxy a nivel de aplicación.*** Son aplicaciones software (servicios proxy) para bloquear o reenviar conexiones a servicios como finger, telnet, http, smtp o ftp; la máquina donde corren estas aplicaciones se denomina pasarela de aplicación.

  Los servicios proxy permiten únicamente la utilización de servicios para los que existe un proxy, además entiende el protocolo para el que fue diseñado lo que hace posible mayor capacidad de análisis y restricción; pero esto puede ser costoso, limitar el ancho de banda efectivo de la red o disminuir la funcionalidad de aplicaciones.

  La pasarela de aplicación permite un grado de ocultación de la estructura de la red protegida, ya que es el único sistema que se presenta hacia el exterior, todas las conexiones se originan y terminan en las interfaces del Firewall.

- ***Proxy a nivel de circuito.*** Crea un circuito entre un cliente y un servidor, sin interpretar la naturaleza de la petición pero requiere que el cliente corra una aplicación especial (SOCKS).

1.4.2.2.3 Monitoreo de la actividad

Es algo indispensable para la seguridad de todo el perímetro protegido, ya que facilitará la información sobre los intentos de ataque que esté sufriendo la red y la existencia de tramas sospechosas. La información que se registra es:

- Tipo de paquete recibido.
- Frecuencias.
- Direcciones fuente y destino.
- Puertos origen y destino.
- Nombre de usuario.
- Hora y duración.
- Intentos de uso de protocolos denegados.
- Intentos de falsificación de dirección (paquetes que llegan desde la red externa con una dirección de origen interno).
- Tramas recibidas desde routers desconocidos.

1.4.2.3 Arquitecturas

1.4.2.3.1 Screened Router

Consiste en utilizar un router como filtro de paquetes, explotando la característica de enrutado selectivo para bloquear o permitir el tránsito de paquetes mediante listas de control de acceso en función de ciertas características de las tramas.

1.4.2.3.2 Host Bastión

Es el sistema de red que se expone a la red externa y es usado para defender la red interna, ya que su función es permitir o no permitir el paso de tráfico.

1.4.2.3.3 Dual-Homed Host

Consiste en utilizar una máquina equipada con dos o más tarjetas de red en las que una de las tarjetas se suele conectar a la red interna a proteger y la otra a la red externa a la organización. El sistema de la máquina ejecutará servicios proxy para cada uno de los protocolos que se permita pasar a través del Firewall.

1.4.2.3.4 Screened Host

Consiste en combinar un router (filtardo de paquetes) con un host bastión (ejecuta los proxies de las aplicación).

1.4.2.3.5 Screened Subnet (DMZ)

Consiste en situar una subred (DMZ) entre la red externa y la red interna con el objeto de reducir los ataques exitosos al host bastión, éste es aislado en una red perimétrica de forma que un intruso que accede a esta máquina no consiga un acceso total a la subred protegida.

Es la arquitectura más segura, pero también la más compleja; se utilizan dos routers, denominados exterior e interior, conectados ambos a la red perimétrica que constituye el sistema cortafuegos.

La red perimétrica contiene al host bastión y también se puede incluir sistemas que requieran un acceso controlado, como módems, servidor web o servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red.

El router exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica.

1.4.3 VPN [8]

Es una red de datos privada creada a partir de una red de datos pública como Internet, transporta tráfico de una manera segura sobre una red insegura, mediante el uso de encriptación, autenticación y encapsulamiento (tunneling), con el fin de asegurar la integridad y privacidad de los datos. Existen varias razones para la implantación de VPNs:

- Bajo costo de implementación.
- Privacidad de los datos.
- Acceso desde todas partes.
- Flexibilidad.
- Escalabilidad.

1.4.3.1 Seguridad

1.4.3.1.1 Privacidad de los datos

- ***Modo Encriptación.*** Consiste en cifrar la porción de datos del paquete usando encriptación simétrica o asimétrica, la cabecera del paquete no es modificada.

- ***Modo Túnel.*** Todo el paquete de datos incluida la cabecera es encapsulado dentro de un nuevo paquete el mismo que es encriptado y finalmente se le añade una nueva cabecera, este modo es usado para transmitir protocolos no IP sobre el backbone IP o IP dentro de IP por razones de seguridad.

1.4.3.1.2 Integridad de los datos

Para asegurar la integridad de los datos las soluciones VPN utilizan los algoritmos hash.

1.4.3.1.3 Autenticación

Las soluciones VPN soportan varios esquemas de autenticación de usuarios como:

- User / Password.

- Autenticación vía token.
- Smartcards.
- Certificados X.509.

1.4.3.1.4 Autorización

Las soluciones VPN permiten definir perfiles de usuario con su correspondiente nivel de autorización y acceso.

1.4.3.1.5 Control de acceso

Las soluciones VPN proveen un control de acceso por razones de seguridad y auditoría basado en:

- UserID.
- HostID.
- IPaddress.
- Subnetwork address.

1.4.3.1.6 Auditoría

Las soluciones VPN definen un registro de actividad del usuario.

1.4.3.2 Rendimiento

El tiempo de respuesta entre una red segura y una red insegura deben ser semejantes, para brindar transparencia a la solución VPN, el trabajo adicional que acarrea el uso de VPNs incrementa la latencia y disminuye la velocidad efectiva de los datos. Entonces es importante considerar los siguientes parámetros al comprar o diseñar una solución VPN:

- Calidad de servicio (QOS).
- Acuerdos de nivel de servicio (SLAs).
- Soporte de múltiples protocolos.
- Confiabilidad y resistencia.

1.4.3.3 Facilidad de administración

Los sitemas VPN cuentan con características de monitoreo y control como:

- Administración centralizada de la seguridad y las políticas.
- Manejo de direcciones.
- Monitorear logs de eventos, auditorías y reportes.

1.4.3.4 Cumplimiento de estándares e interoperabilidad

Con el cumplimiento de estándares abiertos y estándares de facto se aumenta la interoperabilidad.

CAPA DE TRABAJO	TECNOLOGÍA UTILIZADA
Capa Aplicación	Proxy de aplicación
Capa Presentación	
Capa Sesión	SOCKSv5, SSL, TLS
Capa Transporte	
Capa de Red	IPSec, GRE
Capa Enlace	PPTP, L2F, L2TP, Frame Relay, ATM
Capa Física	

Tabla 1.6: Tecnologías para la formación de VPNs.

1.4.4 MODELOS DE AUTENTICACIÓN [1] [3]

Los sistemas de una organización deben tener la capacidad de restringir el acceso a sus diferentes recursos dependiendo de la identificación y autorización que posee el usuario.

1.4.4.1 Contraseñas

Cualidad que el individuo ***conoce***, las contraseñas brindan una seguridad débil ya que una contraseña puede ser adivinada, robada u obtenida.

1.4.4.2 Tarjetas inteligentes

Cualidad que el individuo ***tiene***, las tarjetas inteligentes proporcionan una seguridad mayor pero no completa, evitan el riesgo de que una contraseña sea descubierta, pero si una tarjeta es robada y constituye el único medio de autenticación una atacante explotará esta vulnerabilidad del sistema para tener acceso al mismo.

Las tarjetas inteligentes poseen un chip que puede implementar un sistema de ficheros cifrado y funciones criptográficas, además puede detectar activamente intentos no válidos de acceso a la información almacenada.

1.4.4.3 Biométrica

Cualidad que el individuo ***es***, costituye un mecanismo de seguridad muy confiable porque es un proceso que utiliza una característica física del individuo para autentificar su identidad.

Existen diferentes tipos de exploradores biométricos, para verificar los siguientes rasgos:

- Huellas digitales.
- Retina / iris.
- Huellas de las palmas.
- Geometría de las manos.
- Geometría facial.
- Voz.
- Escritura (firma).

Así como en otros métodos robustos de autenticación, para que el sistema biométrico sea efectivo el acceso al sistema debe ser intentado a través de una ruta de entrada única y correcta, si existen rutas alternativas para obtener acceso al sistema (vulnerabilidades), por más sofisticado que sea el sistema de autenticación, no será seguro.

1.4.5 SOFTWARE ANTIVIRUS [1] [5]

Son programas que escanean los virus, son muy efectivos contra virus conocidos, pero son incapaces de reconocer y adaptarse a nuevos virus.

Su funcionamiento radica en el reconocimiento de la ***firma*** de un virus conocido, el programa detecta un virus cuando encuentra una coincidencia entre los resultados escaneados y las firmas de virus almacenadas en la base de datos. La base de datos que contiene las firmas de virus debe ser actualizada regularmente caso contrario el programa antivirus se vuelve obsoleto rápidamente.

Constituye un componente necesario para una buena solución de seguridad, ya que si está implementado y configurado apropiadamente, puede reducir la exposición de una organización a programas mal intencionados.

Sin embargo no protegerá a una organización de un intruso que haga mal uso de un programa legítimo para obtener el acceso al sistema, tampoco si un usuario legítimo intenta obtener acceso a archivos a los que no tiene acceso.

1.4.6 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS) [1]

Constituyen sistemas administradores competentes que auditan y monitorean continuamente sus sistemas en busca de intrusiones. La detección de intrusiones es el arte de detectar actividades no autorizadas, inapropiadas o extrañas.

Los IDS son capaces de detectar ataques en progreso, generar alarmas en tiempo real y contrarrestar un ataque mediante el lanzamiento de un evento o la reconfiguración del router o Firewall.

Actúan como guardianes de seguridad o centinelas, constantemente están escaneando el tráfico de red o los logs de auditoría de un host.

1.4.6.1 Sistemas de detección de intrusos para host (HIDS)

Reside en el host y es capaz de monitorear y negar servicios automáticamente si una actividad sospechosa es detectada; usan los archivos log y los agentes de auditoría del sistema para realizar el monitoreo.

- ***Verificadores de integridad del sistema (SIV).*** Es un mecanismo encargado de monitorizar archivos de una máquina en busca de posibles modificaciones no autorizadas.

- ***Monitores de registros (LFM).*** Monitorizan los archivos de log generados por los programas de una máquina en busca de patrones que puedan indicar un ataque o una intrusión.

- ***Sistemas de decepción.*** Son mecanismos encargados de simular servicios con problemas de seguridad de forma que un pirata piense que realmente el problema se

puede aprovechar para acceder a un sistema, cuando realmente se está aprovechando para registrar todas sus actividades.

1.4.6.2 Sistemas de detección de intrusos para red (NIDS)

Monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador); éste analiza los siguientes elementos:

- Campos de fragmentación IP.
- Dirección origen y destino.
- Puerto origen y destino.
- Flags TCP.
- Campo de datos.

1.4.6.3 Detección de anomalías

La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía de nuestro sistema, estos modelos de detección conocen lo que es normal en nuestra red o nuestras máquinas a lo largo del tiempo, desarrollando y actualizando conjuntos de patrones contra los que se compararán los eventos que se producen en los sistemas, se tiene:

- Métodos estadísticos que determinan los perfiles de comportamiento habitual.
- Especificación de reglas que establecen los perfiles de comportamiento normal.

1.4.6.4 Detección de usos indebidos

El funcionamiento de los IDS basados en la detección de usos indebidos presupone que podemos establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones, este esquema se limita a conocer lo anormal para poder detectar intrusiones, se tiene:

- Sistemas expertos.
- Transición de estados.

- Comparación y emparejamiento de patrones.
- Detección basada en modelos.

1.5 SEGURIDAD FÍSICA DE RED [1]

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y detección contra las amenazas a los recursos y a la información confidencial. Éste suele ser un aspecto olvidado frecuentemente, lo cual motiva a los atacantes a explotar las vulnerabilidades físicas del sistema.

Entonces implementar cierta seguridad física es importante para garantizar la seguridad global de la red y los sistemas conectados a ella; pues se podría implementar un sistema sofisticado de seguridad lógica pero no serviría de nada si un intruso accede físicamente al sistema u ocurre una catástrofe que puede causar mucho más daño que una amenaza lógica.

Para establecer un sistema de seguridad física se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

1.5.1 PROTECCIÓN DEL HARDWARE

Las medidas encaminadas a asegurar la integridad del hardware son parte importante de la seguridad física de cualquier organización, ya que frecuentemente constituye el componente más caro de todo sistema informático.

1.5.1.1 Acceso Físico

Comprende la protección de zonas o elementos físicos que pueden comprometer la seguridad del sistema, es así que el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger, ya que se tendrán equipos bien protegidos dentro de la organización y otros ubicados en lugares de acceso casi público. La posibilidad de acceder físicamente a un sistema hace inútiles casi todas las medidas de seguridad que se hayan aplicado.

- ***Prevención.*** Consiste en implementar mecanismos de control de acceso, para prevenir un ingreso físico no autorizado. Los más adecuados para la seguridad física son los biométricos y los basados en algo que el individuo posee, así entre los más comunes tenemos videocámaras, geometría de la mano, huellas digitales, tarjetas inteligentes, control de las llaves que abren determinada puerta.

- ***Detección.*** Consiste en implementar mecanismos que permitan conocer la presencia de accesos no autorizados, entre los más comunes tenemos cámaras de vigilancia, alarmas o personal de la organización.

1.5.1.2 Desastres naturales

Son problemas poco habituales que amenazan la seguridad del sistema, pero que en caso de producirse puede acarrear gravísimas consecuencias, por lo tanto es necesario una prevención adecuada y razonable.

- ***Terremotos.*** Para saber que tipo de medidas debe tomarse ante esta amenaza, es necesario investigar la probabilidad e intensidad de movimientos sísmicos en la zona de ubicación geográfica de la organización. Sin embargo puede tomarse ciertas medidas de prevención de forma general, como colocar los equipos delicados en superficies no tan elevadas ni a ras del suelo, utilizar fijaciones para los elementos más críticos (CPUs, monitores, routers), no situar equipos cerca de las ventanas (para evitar accidentes de equipos o humanos). Se consideran las vibraciones amenazas potenciales (motor cercano a los equipos).

- ***Tormentas eléctricas.*** La caída de un rayo en el edificio que alberga los equipos del sistema o en la cercanía es poco probable pero no imposible. Los rayos que caen sobre la estructura metálica de un edificio pueden generar repentinas subidas de tensión infinitamente superiores a lo que pueda generar un problema en la red eléctrica, esto puede causar daños en los equipos ubicados en el mismo; o la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir hardware incluso protegido contra voltajes elevados. Para prevenir los posibles problemas que acarrea una tormenta eléctrica, se cuenta con mecanismos que atraen rayos de una forma controlada o se puede apagar y desconectar los equipos de la red eléctrica.

- ***Inundaciones y humedad.*** La humedad es un aspecto que requiere mantenerse equilibrado, ya que ambientes extremadamente secos generaría electricidad estática que pueden dañar el hardware y la información (circuitos sensibles); también niveles elevados de humedad son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados y provocar cortocircuitos, sobre todo en equipos sensibles.

  Puede implementarse alarmas que se activen al detectar condiciones ambientales desfavorables, especialmente en sistemas de alta disponibilidad.

  Las inundaciones generan problemas mayores, ya que cualquier equipo que entre en contacto con el agua resultará inutilizado, así es necesario tomar medidas preventivas como detectores de agua (para desconectar el sistema automáticamente) o pisos falsos.

1.5.1.3 Desastres del entorno

- ***Electricidad.*** Se pueden presentar los siguientes problemas con el sistema eléctrico que alimenta a los equipos: cortocircuitos, picos de tensión, bajas de tensión, cortes de flujo, que continuamente amenazan la integridad de hardware y los datos.

  Para contrarrestar estas amenazas puede implementarse tomas de tierra, acondicionadores de tensión o utilizar un SAI (Servicio de Alimentación Ininterrumpido) como los UPS o plantas generadoras de energía privadas.

  Para protegerse contra los problemas que puede causar la corriente estática se puede utilizar spray antiestático, o simplemente no tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el hardware o no mantener el entorno excesivamente seco.

- ***Ruido eléctrico.*** Es generado por motores, ordenadores u otros dispositivos, y puede perjudicar el normal funcionamiento de un equipo, para contrarrestarlo hay que situar los aparatos que causan ruido eléctrico un poco alejado de las instalaciones y equipos del sistema, caso contrario se puede instalar filtros en las líneas de alimentación y mantener alejados equipos emisores de ondas (teléfonos móviles, transmisores de radio, etc.).

- ***Incendios y humo.*** Pueden ser causados por problemas eléctricos (cortocircuitos o recalentamiento de equipos) debido a la sobrecarga de la red por el gran número de aparatos conectados al tendido. Para contrarrestar esta amenaza se puede colocar extintores adecuados (de dióxido de carbono) que se activen automáticamente al detectar humo o calor.

- ***Temperaturas extremas.*** Es recomendable evitar el frío intenso o el calor excesivo, tanto para los equipos como para las personas.

1.5.2 PROTECCIÓN DE LOS DATOS

La seguridad física también implica una protección a la información del sistema, tanto a la que está almacenada como a la que se transmite entre diferentes equipos.

- ***Interceptación***. Es un proceso mediante el cual un agente capta información (plana o cifrada) que no le pertenece. Mediante el sniffing un atacante puede capturar tramas que circulan por la red, para contrarrestar esta amenaza hay que evitar tener segmentos de red de fácil acceso o tomas de red libres y usar aplicaciones de cifrado para las comunicaciones o almacenamiento de la información (hardware de cifrado).

  También puede filtrarse la información (reuniones) mediante teléfonos fijos o móviles, para evitar esto se pueden desconectar los teléfonos fijos y bloquear la señal de los móviles mediante un sistema de aislamiento que bloquea cualquier transmisión en los rangos de frecuencias en los que trabajan las operadoras telefónicas.

- ***Backups***. Consiste en la protección de los diferentes medios donde residen las copias de seguridad, ya que contienen toda la información, hay que protegerlas igual que a los sistemas en si; se puede realizar backups cifrados y controlar más el acceso al lugar donde se guardan.

1.5.3 RADIACIONES ELECTROMAGNÉTICAS

Los dispositivos electrónicos emiten continuamente radiaciones a través del aire o de conductores, las mismas que con el equipo adecuado un atacante puede captar y reproducir remotamente. Las señales electromagnéticas que se interceptan más comúnmente son video, enlaces por radiofrecuencia o las de redes basadas en infrarrojos. Los mecanismos

implementados para dificultar el trabajo de un atacante pueden ser el salto en frecuencias, el espectro disperso, protocolos cifrados, definir un perímetro físico de seguridad (la solución es la distancia), hardware diseñado explícitamente para crear ruido electromagnético (la solución es la confusión) o usar dispositivos certificados que aseguran mínima emisión, así como instalaciones que apantallan las radiaciones.

La radiación electromagnética no es un riesgo importante en la mayoría de organizaciones ya que suele tratarse de un ataque costoso en tiempo y dinero, de forma que un atacante suele tener muchas otras puertas para intentar comprometer el sistema de una forma más fácil.

CAPÍTULO II

UTM
(Unified Threat Management)

2 UTM (UNIFIED THREAT MANAGEMENT)

2.1 ESTUDIO DE LA TECNOLOGÍA UTM [12]

Los avances de la tecnología y el desarrollo de amenazas cada vez más peligrosas y complejas, a determinado que las soluciones de seguridad perimetral evolucione a los sistemas de seguridad multi-amenazas, que constituyen la nueva generación de los sistemas de protección de red en tiempo real.

Los sistemas unificados de administración de amenazas (UTM) detectan y eliminan las más dañinas amenazas basadas en el contenido e-mail o tráfico web tales como virus, gusanos, intrusiones, contenido web inapropiado y más en tiempo real, sin degradar el rendimiento de la red.

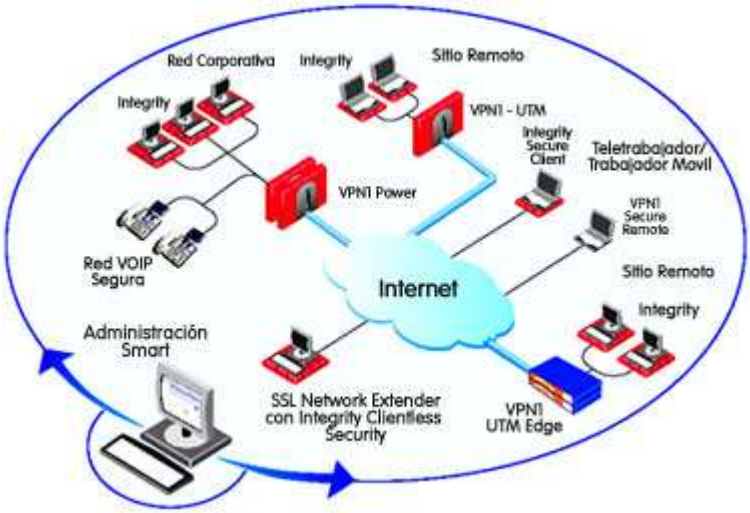


Figura 2.1: Características de los sistemas UTM. [13]

Un sistema de seguridad debe poseer varios componentes que trabajen conjuntamente con el fin de aproximarse a un sistema seguro, es así, que los sistemas UTM incorporan varias técnicas y componentes de seguridad para lograr el acercamiento a este objetivo.

Los sistemas reinantes actualmente como los Firewall, VPNs e IDS resultan efectivos proporcionando protección a nivel de red, sin embargo no cubren las necesidades de protección actual en los ámbitos telemáticos, ya que su capacidad permite el análisis de la cabecera de los paquetes pero no el análisis del contenido de los mismos.

Estos sistemas no pueden comprobar el contenido del paquete y procesarlo para identificar virus, gusanos u otras amenazas, por lo tanto son ineficaces contra ataques basados en contenido. Así los virus, gusanos, troyanos, etc, transmitidos por correo electrónico y tráfico http atraviesan fácilmente los Firewall, VPN o IDS.

Toda esta evolución de tecnología ha acelerado la necesidad de implantación de soluciones de defensa en profundidad a nivel de contenido. Aparentemente el reto de los fabricantes y proveedores de seguridad es la gestión eficiente de respuesta ante los nuevos ataques que nacen en el Internet y en proporcionar firmas actualizadas y efectivas para controlar dichos ataques.

Los sistemas UTM constituyen el software y hardware específico para la seguridad de redes, sus más comunes y principales características son el uso de tecnología ASIC (Application-Specific Integrated Circuit) y la integración de diferentes módulos de seguridad que garantizan la adecuada protección de la red sin degradar su rendimiento.

Finalmente para complementar la seguridad en entornos extremadamente críticos se incluye HIDS sistemas de seguridad en profundidad encargados de detectar y proteger a un sistema en particular de intrusiones; así se puede controlar de manera exhaustiva los datos, aplicaciones y accesos que se procesan en una determinada máquina.

Los dispositivos UTM combinan las funciones de diferentes dispositivos de seguridad, administración y análisis dentro de un solo ambiente más flexible lo cual permite desarrollar en forma integral múltiples características de seguridad (políticas de seguridad) en una sola plataforma.

Estos sistemas están ganando popularidad rápidamente debido al rendimiento que ofrecen en aplicaciones de seguridad, costo de operación e inversión de capital.

2.2 ANÁLISIS SOLUCIÓN 1: FORTINET [13]

Fortinet ofrece una completa gama de productos (software y hardware), servicios de subscripción y soporte que trabajan conjuntamente para proporcionar soluciones de seguridad de red amplias, rentables y manejables; cuenta además con certificaciones FIPS (Federal Information Processing Standards) e ICSA (International Computer Security

Association) y características NSS (Network Security Services) y EAL (Evaluation Assurance Level).

Los sistemas de seguridad multi-amenaza de Fortinet utilizan tecnología ASIC y constituyen la nueva generación de protección de red en tiempo real; detectan y eliminan las amenazas más perjudiciales de correo electrónico y tráfico web sin degradar el rendimiento de la red.

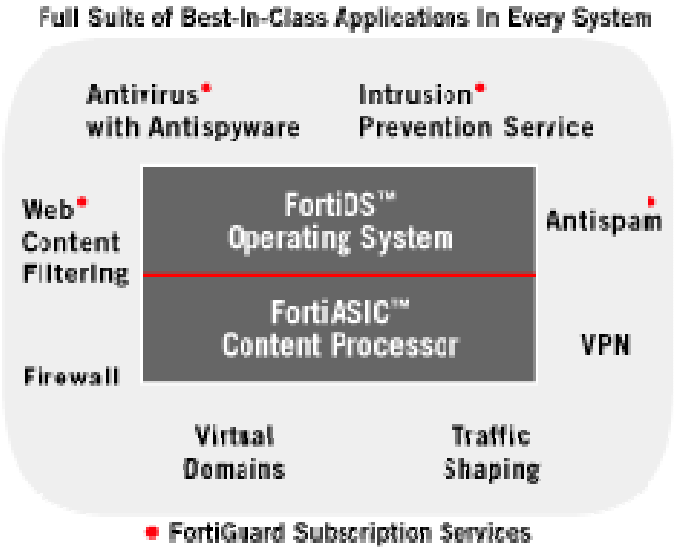


Figura 2.2: Tecnologías y ámbitos que envuelve Fortinet. [13]

2.2.1 FORTIGUARD DISTRIBUTION NETWORK (FDN)

Es una red mundial de servidores FortiGuard distribuidos que permite actualizar las definiciones de ataques.

La infraestructura FortiGuard de Fortinet asegura la rápida identificación de nuevas amenazas y el desarrollo de firmas de nuevos ataques. Los servicios de FortiGuard constituyen un valioso recurso para el cliente e incluye actualizaciones automáticas de virus, motores IPS y definiciones a través de la FDN.

2.2.1.1 FortiGuard Center

Presenta la base de datos de vulnerabilidades y amenazas, la misma que es mantenida y actualizada por el equipo mundial de respuesta de amenazas de Fortinet y provee cobertura de 24x7x365 sobre las más recientes amenazas globales.

2.2.1.1.1 Antivirus

- ***Radar de virus.*** Indica las amenazas de virus más comunes en las últimas 24 horas, 7 días y 30 días, las mismas que se actualizan diariamente.

- ***Escáner de virus en línea.*** Permite al cliente cargar o presentar archivos a Fortinet directamente, para luego notificar de forma instantánea si se detectan virus.

- ***Enciclopedia en orden alfabético.*** Permite la búsqueda de información sobre diferentes virus fácilmente.

- ***Test EICAR (European Institute for Computer Antivirus Research).*** Permite a los clientes probar sus defensas antivirus para HTTP y FTP.

2.2.1.1.2 IPS

- ***Advertencias de seguridad Fortinet.*** Proporciona a los clientes información de seguridad de naturaleza crítica sobre las posibles intrusiones que podría sufrir el sistema.

2.2.1.1.3 Filtrado Web

- ***Consulta URL.*** Consulta la base de datos URL de FortiGuard rápidamente, para clasificar la categoría a la que pertenece una determinada URL.

- ***Categorías y clases de URL.*** Son referencias para el cliente sobre las diferentes categorías de URLs y sus descripciones.

2.2.1.1.4 AntiSpam

Informa sobre el tráfico spam y los falsos positivos.

2.2.1.1.5 Servicios de subscripción FortiGuard

Son servicios de seguridad creados, actualizados y administrados por un equipo de profesionales de seguridad de Fortinet que trabajan continuamente para asegurar la detección y bloqueo de los más recientes ataques, antes de que dañen los recursos corporativos o infecten los dispositivos de computación del usuario final.

Estos servicios son creados con la más reciente tecnología de seguridad y diseñados para operar con el menor costo. Con la subscripción de servicios FortiGuard habilitada, los clientes pueden estar seguros que sus plataformas de seguridad FortiGate están funcionando óptimamente y protegiendo sus activos corporativos con la última tecnología de seguridad y con el mejor precio posible.

- ***Servicio Antivirus FortiGuard.*** Proporciona protección automática para el Firewall Antivirus de FortiGate y lo mantiene actualizado con las últimas defensas antivirus contra amenazas basadas en red.

- ***Servicio IPS FortiGuard.*** Proporciona a los clientes FortiGate las últimas defensas contra actividades de red maliciosas, sospechosas o secretas, provenientes de nuevas y desconocidas amenazas y vulnerabilidades mediante las cuales se pretende ganar acceso a la red, a sus aplicaciones importantes o a la información; este servicio toma medidas de precaución y responde a los ataques que se propagan rápidamente en la actualidad.

- ***Servicio de Filtrado Web FortiGuard.*** Regula y proporciona una valiosa comprensión de las actividades web, permitiendo a los clientes satisfacer las nuevas regulaciones gubernamentales, cumplimiento educacional, políticas de recursos humanos y políticas de uso de Internet corporativo; así previene el uso inapropiado de Internet que provoca bajas en la productividad, utilización inadecuada de los recursos empresariales, hostigamiento, deuda legal y demás cuestiones de recurso humanos.

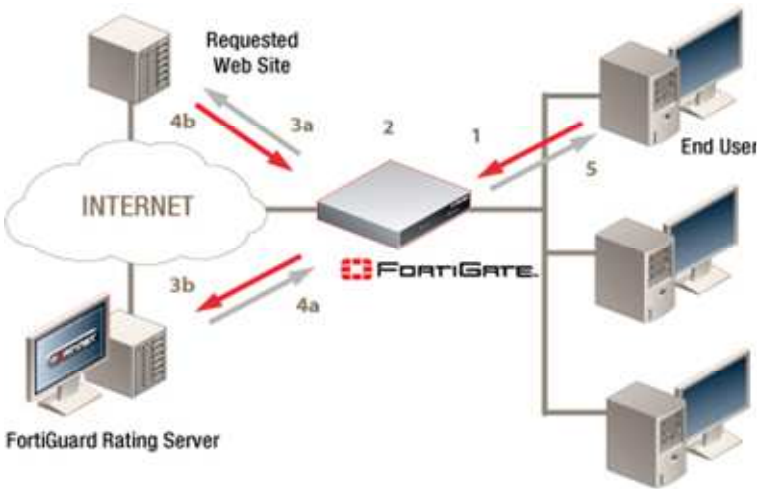


Figura 2.3: Servicio de Filtrado de Contenido Web FortiGuard. [13]

Presenta 56 categorías de contenido web, más de 30 millones de dominios clasificados y más de 2 billones de páginas web.

- ***Servicio FortiGuard AntiSpam.*** Brinda actualización automática a los sistemas FortiGate y FortiMail para reducir la cantidad de evidente spam en el perímetro de red; incrementa el índice de detección empleando tecnología dual scan para identificar rápidamente etiquetas o bloques de mensajes de evidente spam y eliminarlo antes de que afecte los recursos de red.

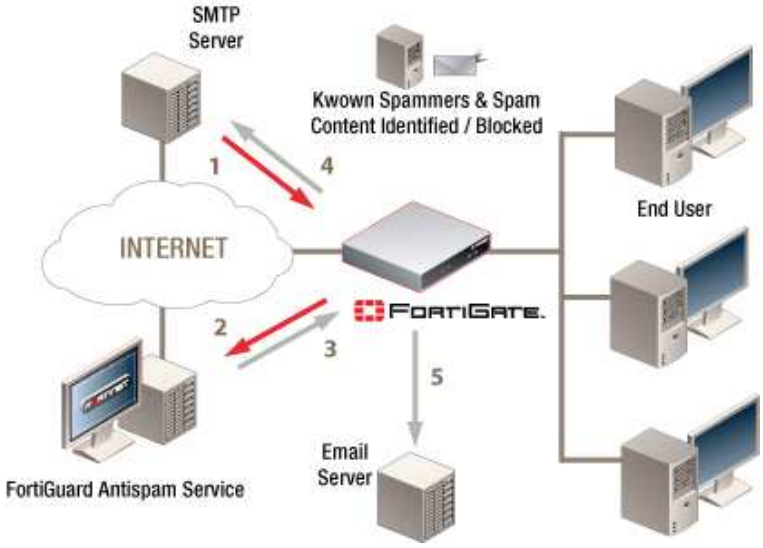


Figura 2.4: Servicio AntiSpam FortiGuard. [13]

2.2.2 FORTIGATE

Es un sistema de administración de amenazas unificado (UTM) que mejora la seguridad de red, reduce el mal uso y abuso de la red y ayuda a utilizar más eficientemente los recursos de comunicaciones sin comprometer el rendimiento de la red. Los sistemas UTM FortiGate cuentan con certificaciones ICSA para firewall, IPSec y Antivirus.

FortiGate es un dispositivo de seguridad dedicado y de fácil administración que ofrece un paquete completo de capacidades entre las cuales se incluye:

- ***Servicios a nivel de aplicación.*** Ofrecen protección contra virus y filtrado de contenido.

- ***Servicios a nivel de red.*** Ofrecen protección mediante firewall, detección / prevención de intrusiones, VPN y modelado de tráfico.

El sistema UTM FortiGate utiliza tecnología DTPS (Dynamic Threat Prevention System), que aprovecha los avances tecnológicos en:

- Diseño del chip.
- Red.
- Seguridad.
- Análisis de contenido.

La arquitectura basada en tecnología ASIC analiza el contenido y el comportamiento en tiempo real lo que permite que aplicaciones de seguridad claves sean desplegadas justo en el límite de red donde son más eficaces para la protección de la misma.

2.2.2.1 Estado del sistema

- ***Página de Estado.*** Expone información del sistema, información de licencias, recursos del sistema, consola CLI, estado de la interfaz, consola de mensajes de alerta, estadística de tráfico y protección.
- ***Información del sistema.*** Permite cambiar la hora, el nombre y el modo de operación para el VDOM.
- ***Firmware FortiGate.*** Permite actualizar a una nueva versión o regresar a una versión antigua del software FortiOS.
- ***Historial de operación.*** Permite visualizar seis gráficos que presentan los recursos del sistema y la actividad de protección.
- ***Definiciones FortiGuard.*** Permite actualizar las bases de datos de las diferentes herramientas FortiGuard:
  - Antivirus.

- Prevención de Intrusiones.
- AntiSpam.
- AntiSpyware.

- ***Visor de estadísticas.*** Muestra información sobre sesiones, archivos de contenido y actividad de protección de red.
- ***Visor de Topología.*** Permite diagramar y documentar las redes conectadas a la unidad FortiGate, para establecer un control y monitoreo de las mismas.

Figura 2.5: Pantalla de Estado del dispositivo FortiGate. [13]

2.2.2.2 Uso de Dominios Virtuales

Los dominios virtuales (VDOMs) permiten a la unidad FortiGate funcionar como múltiples unidades virtuales independientes; una sola unidad puede servir separadamente a varias redes y ser la base de la administración del servicio de seguridad.

Los VDOMs proporcionan diferentes dominios de seguridad que permiten separar zonas, autenticar usuarios, aplicar políticas de firewall / ruteo y configurar VPNs. Por defecto cada unidad tiene un VDOM llamado root, que incluye todas las interfaces físicas, sub interfaces VLAN, zonas, políticas de firewall, configuraciones router y VPN.

2.2.2.3 Configuración FortiGate

2.2.2.3.1 Modo NAT / Router

En este modo la unidad FortiGate es visible para la red, sus interfaces están en diferente subred. Se puede establecer políticas de firewall para controlar las comunicaciones a través de la unidad FortiGate que controla el tráfico basado en la dirección origen, dirección destino y servicio de cada paquete.

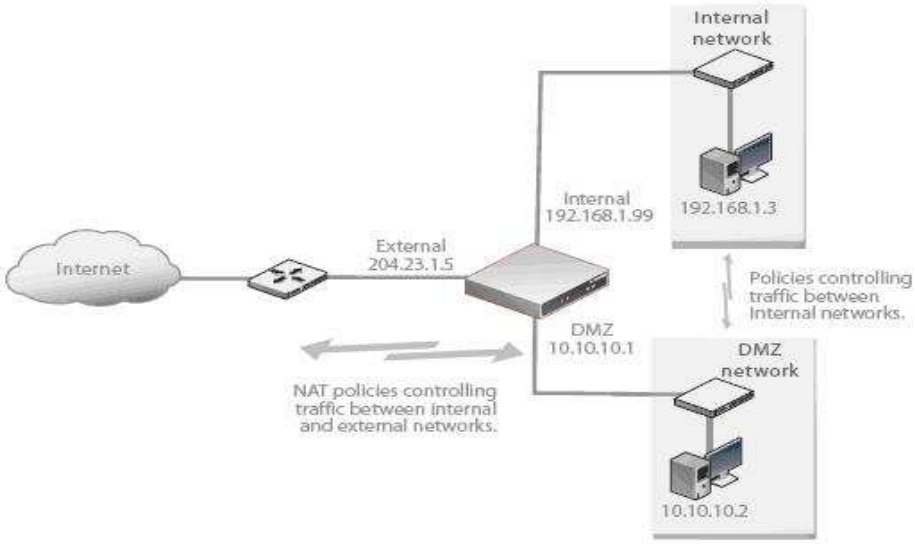


Figura 2.6: Configuración Modo NAT / Router. [13]

En el modo NAT FortiGate realiza la traducción de la dirección de red antes de enviar el paquete a la red destino; en el modo Router no hay traducción de dirección. Se usa el modo NAT/Router cuando la unidad FortiGate esta operando como un Gateway entre las redes pública y privada, se crean políticas de firewall en modo NAT para controlar el tráfico entre la red interna y la red externa y políticas de firewall en modo Router para controlar el tráfico entre las redes internas.

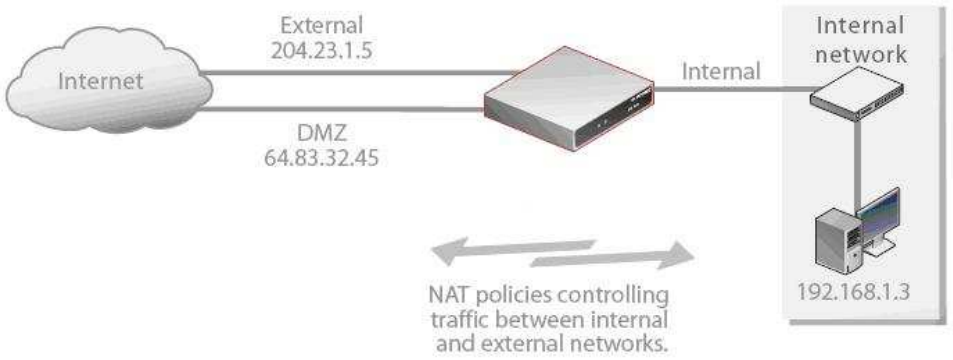


Figura 2.7: Configuración Modo NAT / Router con conexiones a Internet múltiple. [13]

2.2.2.3.2 Modo Transparente

En el modo transparente la unidad FortiGate no es visible para la red, su comportamiento es similar a un puente de red y todas las interfaces de la unidad deben estar en la misma subred; solamente se configura una dirección IP de administración para poder realizar cambios en la configuración, actualizar el antivirus y las amenazas.

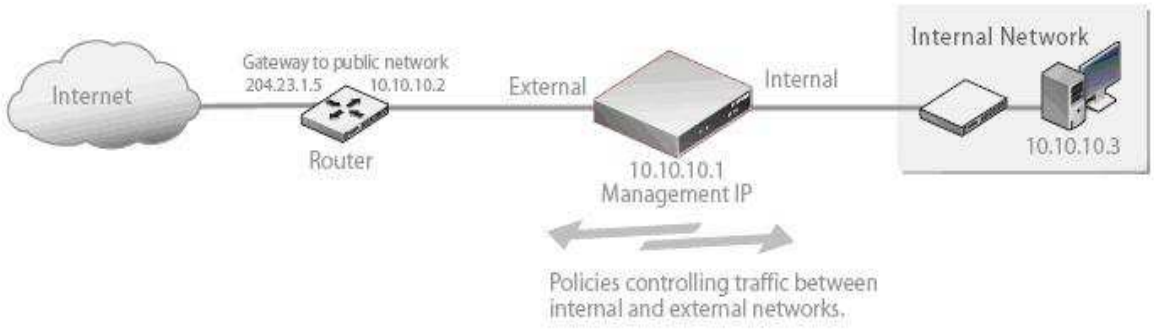


Figura 2.8: Configuración Modo Transparente. [13]

El modo transparente se usa en redes privadas detrás de un firewall existente o detrás de un router.

La unidad FortiGate realiza las funciones de firewall, IPSec VPN, escaneo de virus, filtrado web, IPS y filtrado Spam; pueden conectarse hasta doce segmentos de red a la unidad FortiGate para controlar el tráfico de red entre éstos.

2.2.2.4 Sistema de red

2.2.2.4.1 Interfaz

- ***Cambio de Modo.*** En el modo switch la interfaz interna es configurada como una interfaz compartida por todos los puertos.

  En el modo interfaz se puede configurar cada interfaz interna de forma separada, esto permite asignar diferentes subredes y máscaras de red a cada interfaz interna.

- ***Estándar IEEE 802.3ad.*** Permite agregar o combinar dos o más interfaces físicas para incrementar el ancho de banda o proporcionar redundancia de enlace.

- ***Configuración.*** Las interfaces de la unidad pueden ser configuradas para establecer enlaces ADSL, inalámbrico, PPPoE, PPPoA e IPSec, o para utilizar servicios como DHCP y DNS dinámico.

2.2.2.4.2 Zonas

Agrupan interfaces y sub interfaces VLAN relacionadas, con el fin de simplificar la creación de políticas que se aplicarán a las conexiones desde y hacia las zonas, mas no a las conexiones entre las interfaces de una misma zona.

2.2.2.4.3 Opciones de Red

- ***Servidor DNS.*** Varias funciones de la unidad FortiGate usan el servicio DNS, incluyendo las alertas e-mail y el bloqueo URL; se puede especificar la dirección IP del servidor DNS al cual se conecta la unidad.

- ***Detección del Gateway.*** Para confirmar la conectividad de red periódicamente se ejecutan pings hacia el servidor ping, que por lo general es el siguiente salto del router que se expone a la red externa o al Internet.

2.2.2.4.4 Tabla de ruteo estática

En el modo transparente se añaden rutas estáticas desde la unidad FortiGate hacia los routers locales.

2.2.2.4.5 Interfaz Módem

La interfaz módem puede ser usada como una interfaz de respaldo o como una interfaz independiente en el modo NAT/Route.

En el modo redundante, la interfaz módem automáticamente toma el control de la interfaz Ethernet no disponible (averiada).

En el modo independiente, la interfaz módem establece la conexión desde la unidad FortiGate hacia el Internet.

2.2.2.4.6 VLAN

Una VLAN es un grupo de PCs, servidores u otros dispositivos de red que se comunican como si estuvieran en el mismo segmento LAN, independientemente de donde se encuentren localizados; congrega dispositivos lógicamente antes que físicamente. Cada VLAN es tratada como un dominio de broadcast, así la comunicación entre dispositivos de una VLAN es independiente de la red física.

Una VLAN segrega dispositivos añadiendo etiquetas VLAN 802.1Q a todos los paquetes enviados y recibidos por los dispositivos en la VLAN.

La unidad FortiGate mediante el uso de VLANs puede proporcionar servicios de seguridad y control de conexiones entre múltiples dominios de seguridad. El tráfico de cada dominio de seguridad tiene un ID VLAN diferente, así cada unidad FortiGate puede reconocer las identificaciones y aplicar políticas para proteger la red y controlar el tráfico entre diferentes dominios de seguridad.

También puede aplicar autenticación, protección de perfiles y otras políticas de firewall para la red y el tráfico VPN que está permitido pasar entre dominios de seguridad.

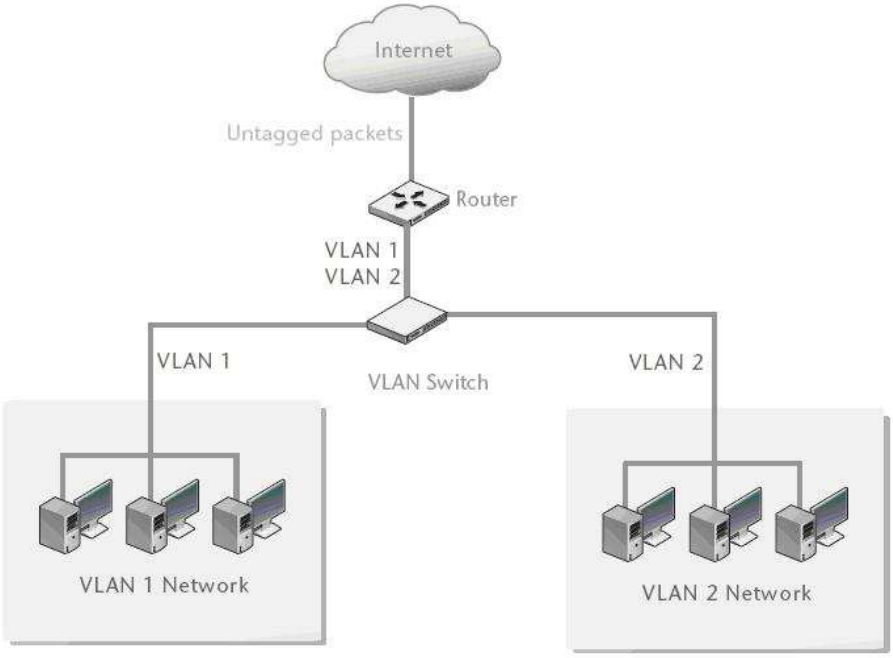


Figura 2.9: Topología VLAN básica. [13]

- ***VLAN en modo NAT / Route.*** La unidad FortiGate funciona como un dispositivo de capa 3 para controlar el flujo de paquetes entre VLANs; la unidad puede quitar las etiquetas VLAN de paquetes VLAN entrantes y retransmitir paquetes sin etiquetas a otras redes como Internet.

  La unidad FortiGate puede aplicar diferentes políticas para el tráfico entre cada VLAN que se conecta a la interfaz interna, en esta configuración se añaden sub interfaces VLAN a la interfaz interna de la unidad FortiGate que tienen IDs VLAN que se emparejan con los IDs VLAN de los paquetes; la unidad re direcciona los paquetes mediante los identificadores VLAN a las correspondientes sub interfaces.

  También se puede definir sub interfaces VLAN sobre todas las interfaces FortiGate, ya que puede añadir etiquetas VLAN a paquetes que dejan una sub interfaz VLAN o quitar las etiquetas de paquetes entrantes y añadir una etiqueta VLAN diferente para paquetes salientes.

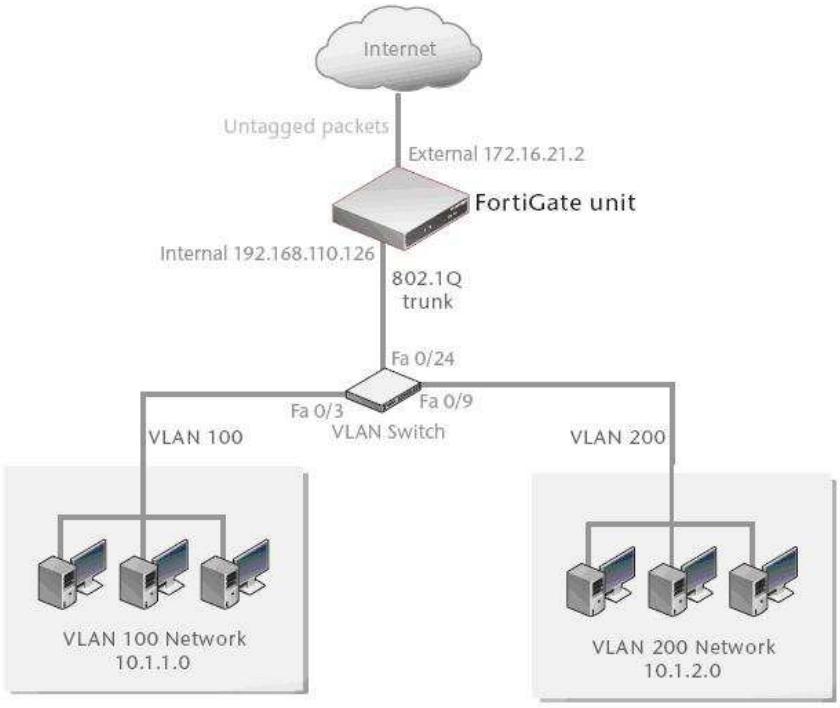


Figura 2.10: VLAN en Modo NAT / Router. [13]

- ***VLAN en modo transparente.*** En el modo transparente la unidad FortiGate puede aplicar políticas de firewall y servicios tales como autenticación, protección de perfiles y otras características para el tráfico VLAN.

  La interfaz interna de la unidad FortiGate acepta paquetes VLAN del tronco VLAN provenientes del switch o router VLAN conectado a las VLAN internas.

  La interfaz externa de la unidad FortiGate reenvía los paquetes etiquetados a través del tronco hacia un switch o router VLAN externo el cual puede estar conectado al Internet.

  La unidad FortiGate puede ser configurada para aplicar diferentes políticas para el tráfico de cada VLAN en el tronco.

  Para que el tráfico atraviese la unidad FortiGate debe configurarse sub interfaces VLAN tanto en la interfaz interna como externa de la unidad.

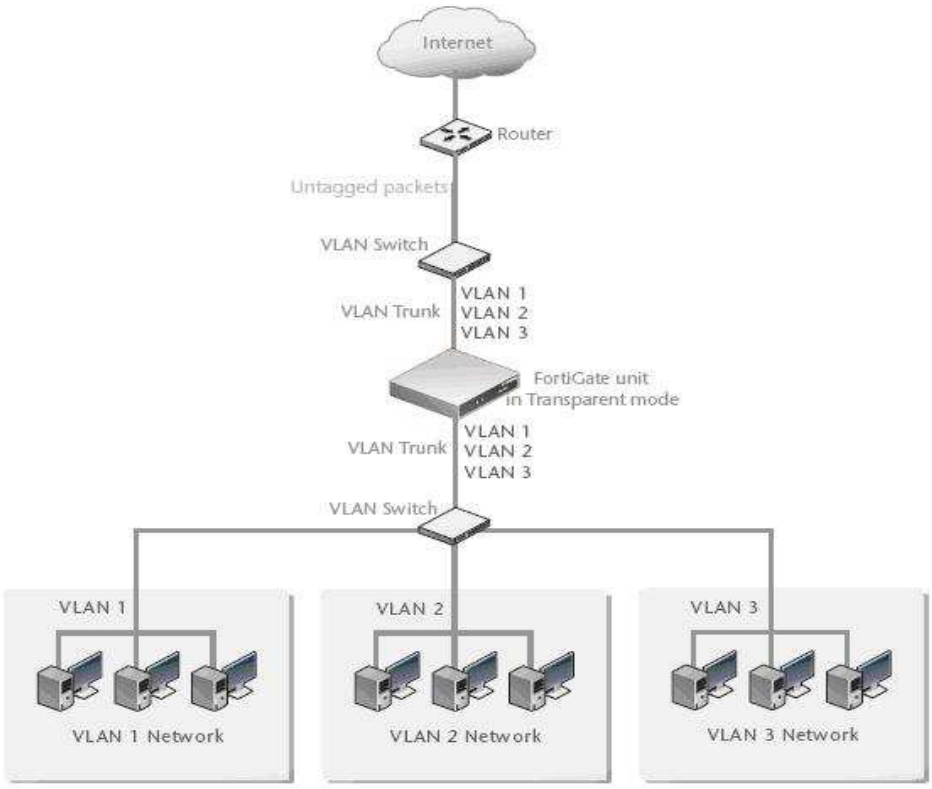


Figura 2.11: VLAN en Modo Transparente. [13]

Si la red usa IEEE 802.1 etiquetas VLAN para segmentar el tráfico de red, se puede configurar la operación de la unidad FortiGate en modo transparente para proporcionar seguridad al tráfico de red que atraviesa diferentes VLANs.

Para soportar tráfico VLAN en modo transparente se añaden dominios virtuales a la configuración de la unidad FortiGate. Un dominio virtual consiste de dos o más sub interfaces VLAN o zonas, una zona puede contener una o más sub interfaces VLAN.

Cuando la unidad FortiGate recibe un paquete VLAN etiquetado en una interfaz el paquete es dirigido a la sub interfaz VLAN con la cual coincide la identificación VLAN. La sub interfaz VLAN retira la etiqueta VLAN y asigna una interfaz destino al paquete basada en su dirección MAC destino. Las políticas firewall para las sub interfaces VLAN de origen y destino son aplicadas al paquete, si el paquete es aceptado por el firewall, la unidad FortiGate reenvía el paquete a la sub interfaz VLAN destino, el identificador VLAN destino es añadida al paquete por la unidad FortiGate y el paquete es enviado al tronco VLAN.

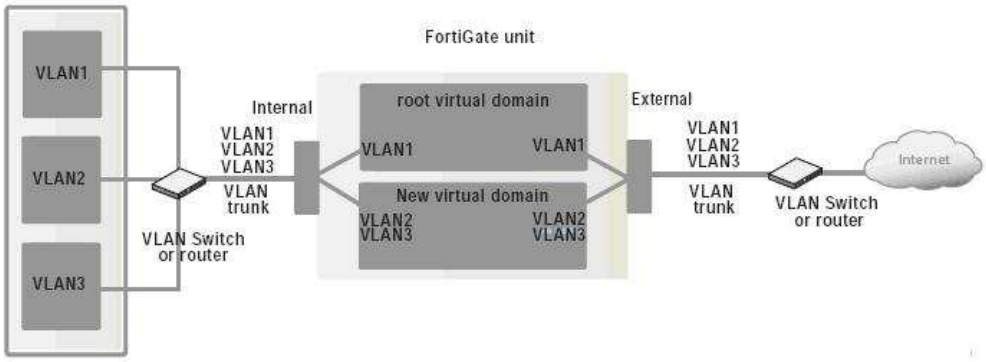


Figura 2.12: VLAN con dos Dominios Virtuales en Modo Transparente. [13]

2.2.2.4.7 Soporte IPv6

Se puede asignar direcciones IPv4 e IPv6 a cualquier interfaz de la unidad FortiGate, la interfaz funciona como dos interfaces una para paquetes con dirección IPV4 y otro para paquetes con dirección IPV6.

La unidad FortiGate soporta ruteo estático, informes periódicos de ruteo, políticas firewall y tunneling de tráfico con direccionamiento IPv6 sobre una red direccionada con IPv4.

2.2.2.5 Sistema Inalámbrico

- ***Interfaz LAN inalámbrica FortiWiFi.*** Ésta interfaz puede ser configurada para:
  - Proporcionar un punto de acceso al cual los usuarios con tarjetas de red inalámbricas pueden conectarse.
  - Conectar la unidad FortiWiFi a otra red inalámbrica.

Las unidades FortiWiFi soportan los siguientes estándares de red inalámbricas:

- IEEE 802.11a (Banda 5 GHz).
- IEEE 802.11b (Banda 2.4 GHz).
- IEEE 802.11g (Banda 2.4 GHz).
- WEP (Wired Equivalent Privacy).
- WAP acceso protegido Wi-Fi usando pre-shared key o servidor RADIUS.

- ***Filtro MAC inalámbrico.*** Permitir o niega el acceso a la red inalámbrica basándose en la dirección MAC de cada tarjeta inalámbrica.

2.2.2.6 Sistema DHCP

El protocolo DHCP habilita a los host para obtener automáticamente su dirección IP asignada, además pueden obtener el Gateway y servidor DNS.

Una interfaz FortiGate o sub interfaz VLAN pueden proporcionar los siguientes servicios DHCP:

- Servidores DHCP regulares para conexiones Ethernet regulares.
- Servidores DHCP IPSec para conexiones IPSec (VPN).
- Transmisión DHCP para conexiones Ethernet o IPSec.

2.2.2.7 Configuración del Sistema

2.2.2.7.1 Alta disponibilidad (HA)

Mejora la confiabilidad e incrementa el rendimiento, la unidad FortiGate puede unirse a un cluster de alta disponibilidad.

2.2.2.7.2 snmp

SNMP es un protocolo de administración simple que permite monitorear el hardware en la red; se puede configurar el hardware o el agente snmp de la unidad FortiGate para que reporte la información del sistema y envíe traps (alarmas o mensajes de eventos) al administrador SNMP. El administrador SNMP es una computadora corriendo una aplicación que puede leer las traps provenientes del agente y rastrear la información.

La implementación SNMP en FortiGate es de solo lectura, mediante la administración SNMP se puede tener acceso a las traps SNMP y a los datos de cualquier interfaz de la unidad FortiGate o sub interfaz VLAN configurada para el acceso de administración SNMP, lo que hace posible el monitoreo de la información de este sistema; pero para estar en capacidad de recibir traps FortiGate se debe compilar las MIBs propietarias de Fortinet así como las MIBs estándares soportadas por Fortinet en el administrador SNMP.

- ***Comunidad snmp.*** Una comunidad snmp consiste en la agrupación de equipos con el propósito de administrar la red, el administrador SNMP puede conectarse a la unidad FortiGate para observar la información del sistema y recibir traps SNMP; se puede añadir hasta tres comunidades SNMP y hasta ocho direcciones IP de administradores SNMP a cada comunidad.

- ***MIBs Fortinet.*** El agente SNMP de FortiGate soporta MIBs propietarias de Fortinet así como las MIBs estándar (RFC 1213 y RFC 2665); para comunicarse con el agente SNMP hay que compilar todas las MIBs estándar y privadas dentro del administrador SNMP.

- ***Traps FortiGate.*** El agente FortiGate puede enviar traps a los administradores SNMP que se agreguen a la comunidad SNMP; para recibir traps se debe cargar y compilar la MIB Fortinet 3.0 en el administrador SNMP. Las traps contienen el mensaje trap, el número serial de la unidad FortiGate y el Hostname.

2.2.2.7.3 Mensajes de reemplazo

La unidad FortiGate genera mensajes de reemplazo a una variedad de cadenas de contenido tales como mensajes e-mail infectados o bloqueados por spam, páginas web bloqueadas, sesiones FTP, etc, cuando detecta una amenaza.

2.2.2.7.4 Modo de operación y administración VDOM

Se puede cambiar el modo de operación de cada VDOM independientemente, así se puede combinar el modo de operación (NAT/Route o transparente) para cada una de las VDOMs de la unidad FortiGate; el acceso a la administración de cada VDOM puede ser restringida basándose en la interfaz y protocolo usado para la conexión con la interfaz.

2.2.2.8 Administración del sistema

2.2.2.8.1 Administradores

Existen dos niveles de cuentas de administradores:

- ***Administrador regular.*** Es asignado a una VDOM y no puede tener acceso a la configuración global o a la configuración de otro VDOM al cual no haya sido asignado.

- ***Administrador de sistema.*** Tiene acceso completo a la configuración de la unidad FortiGate.

2.2.2.8.2 Perfil de acceso

Cada cuenta de administrador pertenece a un perfil de acceso; el perfil de acceso separa en categorías el control de acceso a las características de la unidad FortiGate, se puede habilitar accesos de lectura y/o escritura.

2.2.2.8.3 FortiManager

La unidad FortiGate se comunica con el servidor FortiManager mediante un enlace IPSec VPN que es transparente y viene pre configurado en la unidad FortiGate.

2.2.2.9 Mantenimiento del sistema

2.2.2.9.1 Respaldo y Restauración

Se puede respaldar la configuración del sistema, incluyendo los archivos de contenido web y archivos de filtrado spam a la computadora que administra o a un disco USB; también se puede restaurar la configuración del sistema de archivos de respaldo descargados con anterioridad.

2.2.2.9.2 Centro FortiGuard

El centro FortiGuard configura a la unidad FortiGate para acceder a la red de distribución FortiGuard (FDN) y a los servicios FortiGuard.

La red de distribución FortiGuard proporciona actualización de antivirus, definiciones de ataques, lista negra de direcciones IP en línea, lista negra de URL y otras herramientas de filtrado spam.

La lista negra de direcciones IP contiene direcciones IP de servidores e-mail que se conoce son usados para generar spam.

La lista negra de URL contiene URLs de sitios web encontrados en e-mails spam; también proporciona cientos de millones de páginas web clasificadas en un amplio rango de categorías que el usuario puede permitir, bloquear o monitorear.

2.2.2.10 Ruteo estático

Una ruta proporciona a la unidad FortiGate la información necesaria para enviar un paquete a un destino particular en la red; una ruta estática hace que los paquetes se envíen a un destino diferente del configurado por defecto. Opcionalmente se pueden definir políticas de ruteo, que permiten especificar criterios adicionales para examinar las propiedades de los paquetes entrantes, mediante el uso de políticas de ruteo se puede configurar a la unidad FortiGate para que dirija paquetes basándose en la dirección IP de origen y/o destino, la interfaz por la cual el paquete fue recibido, el protocolo (servicio) y/o el puerto que está siendo usado para transportar el paquete.

2.2.2.11 Ruteo dinámico

Trabaja con protocolos dinámicos para enrutar el tráfico a través de redes grandes y complejas; los protocolos dinámicos habilitan a la unidad FortiGate para que comparta información de ruteo automáticamente con routers vecinos y aprenda sobre rutas y redes anunciadas por sus routers vecinos. La unidad FortiGate soporta los siguientes protocolos de enrutamiento dinámico:

- Routing Information Protocol (RIP).
- Open Shortest Path First (OSPF).
- Border Gateway Protocol (BGP).
- Protocol Independet Multicast (PIM).

2.2.2.12 Políticas Firewall

Las políticas firewall controlan todo el tráfico que pasa a través de la unidad FortiGate, son instrucciones usadas para decidir que hacer con una petición de conexión.

Cuando el Firewall recibe una petición de conexión en forma de paquete, éste es analizado para extraer la dirección origen, la dirección destino y el servicio (número de puerto), para ser evaluado con las políticas de firewall y tomar acciones sobre el paquete, como permitir

la conexión, negar la conexión, pedir autenticación antes de permitir la conexión o procesar al paquete como un paquete VPN IPSec.

2.2.2.13 Virtual IP - Firewall

2.2.2.13.1 Virtual IPs

Las direcciones IP virtuales pueden ser usadas para permitir conexiones a través de la unidad FortiGate usando políticas firewall de tipo NAT. Las IPs virtuales usan un proxy ARP para que la unidad FortiGate pueda responder a peticiones ARP pertenecientes a un servidor que actualmente está instalado en otra red; así la unidad FortiGate se presenta como el servidor y la red interna permanece oculta al público.

2.2.2.13.2 Pool de IPs

Son utilizadas para añadir políticas NAT que traduzcan dinámicamente direcciones origen de los paquetes salientes a direcciones aleatorias seleccionadas del pool IP antes que limitarse a la dirección IP de la interfaz de destino. Un pool IP define una dirección o un rango de direcciones IP que responden a las peticiones ARP en la interfaz a la cual ha sido asignado el pool IP.

2.2.2.14 Perfil de protección Firewall

El perfil de protección es un grupo de configuraciones que pueden modificarse para ajustarse a un propósito particular; se pueden usar perfiles de protección para cada tipo de tráfico que maneja una política firewall, se tiene:

- Configurar la protección antivirus para políticas HTTP, FTP, IMAP, POP3, SMTP e IM.
- Configurar el filtrado web para políticas HTTP y HTTPS.
- Configurar el filtrado web por categorías para políticas HTTP y HTTPS.
- Configurar el filtrado spam para políticas IMAP, POP3 y SMTP.
- Habilitar IPS para todos los servicios.
- Configurar el archivo de contenido para políticas HTTP, HTTPS, FTP, IMAP, POP3, SMTP e IM.

- Configurar filtrado IM y control de acceso para mensajería instantánea AIM, ICQ, MSN, Yahoo y SIMPLE.
- Configurar acceso P2P y control del ancho de banda para clientes punto a punto Bit Torrent, eDonkey, Gnutella, Kazaa, Skype, WinNY, Emule y Ares.
- Configurar cuales acciones del perfil de protección serán registradas.
- Configurar la capacidad para los protocolos VoIP, SIP y SCCP.

Mediante los perfiles de protección se puede personalizar los tipos y niveles de protección para diferentes políticas firewall.

La unidad FortiGate tiene pre-configurados cuatro perfiles de protección:

- ***Estricto.*** Aplica máxima protección al tráfico HTTP, FTP, IMAP, POP3 y SMTP.
- ***Escanear.*** Aplica escaneo de virus al tráfico HTTP, FTP, IMAP, POP3 y SMTP.
- ***Web.*** Aplica escaneo de virus y bloqueo de contenido web para el tráfico HTTP.
- ***No filtrado.*** No aplica escaneo, bloqueo o IPS.

2.2.2.15 vpn

2.2.2.15.1 IPSec (Internet Protocol Security)

La unidad FortiGate implementa el protocolo ESP (Encapsulated Security Payload), donde los paquetes encriptados aparecen como paquetes ordinarios que pueden ser enrutados a través de cualquier red IP, el procedimiento IKE (Internet Key Exchange) es realizado automáticamente basándose en pre-shared keys o certificados digitales X.509, aunque también se pueden especificar claves manualmente.

Cuando se define una ruta basada en un túnel IPSec, una interfaz IPSec virtual es creada automáticamente como una sub-interfaz en la interfaz física, agregada o VLAN de la unidad FortiGate esto es conocido como IPSec modo interfaz.

Una interfaz virtual IPSec es considerada en funcionamiento cuando puede establecer una conexión de fase 1 con un punto similar VPN o un cliente; sin embargo la interfaz virtual IPSec no puede ser usada para enviar tráfico a través de un túnel hasta pasar a la fase 2 de

definición; después de que una interfaz virtual IPSec ha sido asignada a un túnel, el tráfico puede ser enrutado a la interfaz usando métricas específicas tanto para rutas estáticas como para políticas de rutas, además se pueden crear políticas de firewall considerando a la interfaz virtual IPSec como la interfaz origen o destino.

Cuando el tráfico IP se origina detrás de la unidad FortiGate local busca una interfaz FortiGate de salida que actúe como el punto final local del túnel IPSec, el tráfico es encapsulado por el túnel y enviado a través de la interfaz física a la cual pertenece la interfaz virtual IPSec.

Cuando el tráfico encapsulado de un punto VPN remoto o de un cliente busca una interfaz física local de la unidad FortiGate, ésta determina si una interfaz virtual IPSec está asociada a la interfaz física a través de selectores en el tráfico; si el tráfico coincide con los selectores predefinidos, éste es des-encapsulado y enviado a la interfaz virtual IPSec.

En la dirección saliente, la unidad FortiGate realiza un lazo de ruteo para encontrar la interfaz a través de la cual debe enviar el tráfico para alcanzar el siguiente router, si la unidad encuentra una ruta a través de una interfaz virtual que está ligada a un túnel VPN específico, el tráfico es encriptado y enviado a través del túnel VPN.

En la dirección entrante, la unidad identifica un túnel VPN usando la dirección IP de destino y el SPI (Security Parameter Index) en el datagrama ESP, luego para completar la fase 2 se analiza la SA (Security Association); si una coincidencia SA es encontrada, el datagrama es des encriptado y el tráfico IP asociado es re direccionado a través de la interfaz virtual IPSec.

- ***Fase uno.*** En la fase 1 los dos puntos VPN se autentican uno al otro e intercambian claves para establecer un canal de comunicación segura entre ellos.

    - Intercambio de información de autenticación encriptado o no encriptado.
    - Uso de pre-shared key o certificados digitales para la autenticación de las entidades de los puntos VPN.
    - Uso de un identificador especial, un certificado de nombre distinguido o nombre de grupo para identificar el punto VPN remoto o cliente remoto.

- ***Fase dos.*** Los parámetros de la fase 2 definen los algoritmos que la unidad FortiGate puede usar para cifrar y transferir los datos por el resto de la sesión; durante la fase 2, las asociaciones de seguridad específicas de IPSec requeridas para implementar servicios de seguridad son seleccionadas y un túnel es establecido.

2.2.2.15.2 PPTP

La unidad FortiGate soporta PPTP para túneles con tráfico PPP entre dos puntos VPN, los clientes PPTP de Windows o Linux pueden establecer un túnel PPTP con una unidad FortiGate configurada para actuar como servidor PPTP, también se puede configurar la unidad para enviar los paquetes PPTP al servidor PPTP de la red detrás de la unidad FortiGate.

Las VPN PPTP son posibles solo en el modo NAT/Route y se permiten hasta 254 sesiones PPTP y L2TP.

2.2.2.15.3 SSL

La unidad FortiGate permite establecer sesiones SSL en el modo NAT/Route, para operaciones en modo túnel o modo web y si se requiere se puede habilitar el uso de certificados digitales para la autenticación de usuarios remotos.

2.2.2.16 Autenticación de usuarios

2.2.2.16.1 Servidor RADIUS

Si el usuario requiere autenticarse usando un servidor RADIUS, la unidad FortiGate envía las credenciales del usuario al servidor RADIUS para su autenticación; si el servidor RADIUS puede autentificar al usuario, el mismo es autentificado exitosamente con la unidad FortiGate, caso contrario la conexión es rechazada por la unidad FortiGate.

2.2.2.16.2 Servidor LDAP

Si el usuario requiere autenticarse usando un servidor LDAP, la unidad FortiGate contacta al servidor LDAP para la autenticación. Para autenticarse con la unidad FortiGate el usuario ingresa un nombre y contraseña, los mismos que son enviados al servidor LDAP, donde se realiza el procedimiento de autenticación, si el usuario es autenticado

positivamente obtiene el accesos a la unidad FortiGate, caso contrario la conexión es rechazada. Adicionalmente FortiGate LDAP soporta LDAP sobre SSL / TLS.

2.2.2.16.3 Autenticación PKI

Utiliza una biblioteca de certificados de autenticación, así los usuarios necesitan solamente un certificado válido para su autenticación.

2.2.2.16.4 Servidor AD de Windows

En las redes que usan servidores Windows Active Directory (AD) para la autenticación, la unidad FortiGate puede autenticar a los usuarios de forma transparente sin necesidad de preguntarles su nombre de usuario y contraseña, para lo cual se debe instalar FSAE (Fortinet Server Authentication Extensions) en la red y configurar la unidad FortiGate para recuperar información del servidor Windows AD.

2.2.2.16.5 Grupo de usuario

Es una lista de identidades de usuario, donde una identidad puede ser:

- Una cuenta de usuario local (nombre de usuario y contraseña) almacenado en la unidad FortiGate.
- Una cuenta de usuario local con una contraseña almacenada en un servidor RADIUS o LDAP.
- Un servidor RADIUS o LDAP (todas las identidades almacenadas en el servidor pueden ser autentificadas).
- Un grupo de usuarios definidos en un servidor Microsoft Active Directory.

En la mayoría de los casos la unidad FortiGate autentica a los usuarios mediante su nombre de usuario y contraseña, primero chequea las cuentas de usuarios locales, luego los servidores RADIUS o LDAP que pertenecen al grupo de usuario; la autenticación es exitosa cuando encuentra una coincidencia. Para el grupo de usuario de AD la autenticación se realiza cuando el usuario entra a la red mediante el agente de FSAE la unidad FortiGate recibe el nombre de usuario y la dirección IP.

2.2.2.17 AntiVirus

El procedimiento antivirus engloba varios módulos y motores que realizan tareas separadas; los elementos antivirus trabajan en secuencia para proporcionar un método de escaneo eficiente para los archivos entrantes; estos elementos trabajan para ofrecer a la red una protección antivirus incomparable.

Además para asegurar la mejor protección disponible, todas las definiciones y firmas de virus son actualizadas regularmente mediante los servicios antivirus FortiGuard.

2.2.2.17.1 Archivo patrón

Una vez que un archivo es aceptado, la unidad FortiGate aplica el filtro de reconocimiento de patrón de archivo y compara el archivo entrante con el patrón de archivo configurado, si el archivo tiene un patrón de bloqueo, éste es detenido y un mensaje de reemplazo es enviado al usuario final, además ningún otro nivel de protección es aplicado; pero si el archivo no es bloqueado entonces otros niveles de protección son aplicados.

El patrón de archivos sirve para bloquear archivos que constituyen una potencial amenaza y prevenir los ataques de virus; los archivos pueden ser bloqueados por nombre, extensión o cualquier otro patrón, así se proporciona la flexibilidad para bloquear potencial contenido dañino. La lista de archivos patrón está pre configurada con una lista por defecto de archivos patrón:

- Archivos ejecutables (*.bat, *.com y *.exe).
- Archivos comprimidos (*.gz, *.rar y *.tar, *.tgz y *.zip).
- Librerías de enlace dinámico (*.dll).
- Aplicaciones html (*.hta).
- Archivos Microsoft Office (*.doc, *.ppt y *.xl?).
- Archivos Microsoft Works (*.wps).
- Archivos Visual Basic (*.vb?).
- Archivos screen saver (*.scr).
- Archivos de información de programa (*.wps).

2.2.2.17.2 Escáner de virus

Si el archivo ha pasado el módulo archivo patrón, entonces se le se aplica el scanner de virus; las definiciones de virus son almacenadas y actualizada periódicamente a través de FDN. La unidad FortiGate usa las definiciones de virus para detectar y remover virus, gusanos, troyanos y otras amenazas de contenido.

La lista de virus muestra en orden alfabético las definiciones de virus FortiGuard actualizadas que se encuentran instaladas en la unidad FortiGate.

2.2.2.17.3 Grayware

Una vez que el archivo entrante ha pasado los módulos archivo patrón y escáner de virus, será chequeado por el módulo grayware.

Los programas grayware son software comercial no solicitado que se instalan en computadoras generalmente sin el conocimiento o consentimiento del usuario; estos programas son considerados una molestia ya que causan problemas en el rendimiento del sistema o son usados para fines maliciosos. La lista de categorías y contenidos grayware son añadidos o actualizados cuando la unidad FortiGate recibe los paquetes de actualización de virus.

Las categorías grayware que se pueden habilitar para que la unidad FortiGate los bloquee son:

- Adware.
- Dial.
- Download.
- Game.
- Hacker Tool.
- Hijacker.
- Joke.
- RAT (Remote Administration Tools).
- NMT (Network Management Tools).
- BHO (Block browser Helper Objects, son archivos dll).
- Keylog.
- Misc.
- P2P.
- Plugin.
- Spy.
- Toolbar.

2.2.2.17.4 Heurístico

Finalmente, luego de haber pasado los tres módulos anteriores, el archivo entrante es sometido al módulo heurístico. El motor heurístico de la unidad FortiGate realiza pruebas en el archivo para detectar virus basándose en indicadores de comportamiento o en virus conocidos, es así que se puede detectar nuevos virus pero también se pueden producir resultados falsos positivos.

2.2.2.17.5 Cuarentena

La unidad FortiGate con disco duro puede poner en cuarentena a archivos bloqueados e infectados para ver el nombre y la información de estado de éstos; además pueden ser cargados automáticamente al análisis Fortinet. Para las unidades FortiGate que no cuentan con disco duro, se puede configurar para que los archivos bloqueados e infectados sean enviados a la unidad FortiAnalyzer.

2.2.2.18 Protección contra intrusos

El sistema de prevención de intrusos (IPS) FortiGuard combina la detección de firmas y anomalías para descubrir y prevenir las intrusiones al sistema, con baja latencia y excelente confiabilidad. La unidad FortiGate puede grabar el tráfico sospechoso en logs, puede enviar alertas e-mail al sistema administrador y puede registrar, comunicar, soltar, restaurar y limpiar sesiones o paquetes sospechosos. También es posible habilitar o deshabilitar todas las firmas o anomalías en cada perfil de protección firewall.

2.2.2.18.1 Firmas

El IPS FortiGate compara el tráfico de red con los patrones contenidos en las firmas de ataques, las firmas de los ataques protegen la red de los ataques conocidos. La unidad FortiGate permite modelar nuevas firmas de acuerdo a las necesidades de la red además de las firmas predefinidas.

2.2.2.18.2 Decodificador de protocolo

El IPS FortiGate usa la detección de anomalías para identificar el tráfico de red que intenta tomar ventaja de debilidades conocidas.

2.2.2.18.3 Anomalías

El IPS FortiGate usa la detección de anomalías para identificar el tráfico de red que no encaja en los patrones de tráfico predefinidos o conocidos; identifica cuatro tipos de anomalías estadísticas para los protocolos TCP, UDP e ICMP:

- Flooding.
- Scan.
- Source session limit.
- Destination session limit.

Las siguientes son las acciones de respuesta cuando se detecta un patrón de firma o una anomalía:

Action	Description
Pass	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall without further action. If logging is disabled and action is set to Pass, the signature is effectively disabled.
Drop	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The firewall session is not touched. Fortinet recommends using an action other than Drop for TCP connection based attacks.
Reset	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to both the client and the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.
Reset Client	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the client and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established, it acts as Clear Session.
Reset Server	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established, it acts as Clear Session.
Drop Session	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. For the remainder of this packet's firewall session, all follow-up packets are dropped.
Pass Session	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall. For the remainder of this packet's session, the IPS is bypassed by all follow-up packets.
Clear Session	When a packet triggers a signature, the FortiGate unit generates an alert and the session to which the packet belongs is removed from the session table immediately. No reset is sent. For TCP, all follow-up packets could be dropped. For UDP, all follow-up packets could trigger the firewall to create a new session.

Tabla 2.1: Respuestas ante amenazas detectadas por el dispositivo UTM. [3]

2.2.2.19 Filtro web

Los filtros web son aplicados en el siguiente orden:

1. URL de excepción.
2. URL bloqueada.
3. URL patrón bloqueada.
4. Categoría URL web bloqueada.
5. Contenido web bloqueado.
6. Filtro script.
7. Escaneo de virus.

2.2.2.19.1 Bloqueo de contenido

Controla el contenido web al bloquear palabras o patrones específicos; si se habilita en el perfil de protección, la unidad FortiGate busca las palabras o patrones en las páginas web solicitadas, una coincidencia es encontrada cuando los valores asignados a las palabras son totales, si el valor de umbral definido de un usuario es excedido, la página web es bloqueada.

2.2.2.19.2 Filtro URL

Permite o bloquea el acceso a URLs específicas, las cuales han sido añadidas a la lista de filtrado; se añaden los patrones usando texto o expresiones regulares (caracteres wildcard). La unidad FortiGate permite o bloquea páginas web comparándolas con las URLs o patrones especificados y despliega un mensaje de reemplazo a cambio indicando que la página no es accesible de acuerdo a las políticas de uso de Internet.

2.2.2.19.3 Filtro web FortiGuard

Es una solución de filtrado web administrada y provista por Fortinet que clasifica cientos de millones de páginas web dentro de un amplio rango de categorías que los usuarios pueden permitir, bloquear o monitorear.

La unidad FortiGate accede al punto de servicio FortiGuard - Web más cercano para determinar la categoría de una página solicitada, entonces continúa a la política firewall configurada por el usuario en la interfaz.

FortiGuard - Web abarca millones de valoraciones individuales de sitios web aplicándose a cientos de millones de páginas; las páginas son clasificadas y valoradas en 56 categorías que los usuarios pueden permitir, bloquear o monitorear; las categorías pueden ser añadidas o actualizadas según como el Internet evolucione.

La valoración de FortiGuard - Web es realizada mediante la combinación de métodos propietarios como análisis de texto, explotación de la estructura web y la intervención humana en la clasificación; los usuarios pueden notificar a los puntos de servicio FortiGuard - Web si piensan que una página no está categorizada correctamente además nuevos sitios son clasificados rápidamente.

Si se necesita acceder a un sitio web restringido se puede anular temporalmente la regla.

2.2.2.20 AntiSpam

Esta funcionalidad puede ser configurada para manejar e-mails comerciales no solicitados, mediante la detección de mensajes e-mail spam e identificación de transmisiones spam provenientes de servidores spam conocidos o sospechosos.

FortiGuard - AntiSpam es una de las características diseñadas para manejar el spam; incluye una lista negra de direcciones IP, una lista negra de direcciones URL y herramientas de filtrado spam.

El orden en el cual los e-mails entrantes pasan a través de los filtros AntiSpam de FortiGate está determinado por el protocolo usado para transferir el e-mail.

- ***Para SMTP:***

1. Verificación BWL (Black / White List) de la dirección IP con el último brinco IP.
2. Verificación RBL (Realtime Blackhole List) & ORDBL (Open Relay Database List), FortiGuard verifica la dirección IP, mediante HELO DNS lookup.
3. Verificación BWL de la dirección e-mail.
4. Verificación de la cabecera MIME (Multipurpose Internet Mail Extensions).
5. Verificación BWL de la dirección IP (para IPs extraídas de las cabeceras recibidas).
6. Verificación DNS de retorno de e-mails, verificación FortiGuard – AntiSpam (para IPs extraídas de las cabeceras recibidas y URLs en el contenido e-mail).

7. Verificación de palabras prohibidas en el asunto e-mail.
8. Verificación de palabras prohibidas en el contenido e-mail.

- ***Para POP3 e IMAP:***

1. Verificación BWL de la dirección e-mail.
2. Verificación de la cabecera MIME, verificación BWL de la dirección IP.
3. Verificación DNS de retorno de e-mails, verificación FortiGuard - AntiSpam, verificación RBL & ORDBL.
4. Verificación de palabras prohibidas en el asunto e-mail.
5. Verificación de palabras prohibidas en el contenido e-mail.

Para SMTP, POP3 e IMAP los filtros requieren preguntar a un servidor (servicio FortiGuard-AntiSpam, DNSBL/ORDBL) y una respuesta es ejecutada simultáneamente; para evitar retardos, las interrogantes son enviadas mientras otros filtros se están ejecutando, la primera respuesta a un trigger es una acción spam que toma efecto tan pronto como la respuesta es recibida. Cada filtro spam pasa el e-mail al siguiente filtro si no se encuentran coincidencias o problemas. Si la acción en un filtro es “Mark as Spam”, la unidad FortiGate etiquetará o desechará (solo en SMTP) el e-mail de acuerdo a las configuraciones del perfil de protección. Si la acción en un filtro es “Mark as Clear”, el e-mail estará exento de cualquier filtro restante. Si la acción en un filtro es “Mark as Reject”, la sesión e-mail es dada de baja. Los mensajes e-mail SMTP rechazados son substituidos con mensajes de reemplazo configurables.

2.2.2.20.1 Palabras prohibidas

El control spam por bloqueo de mensajes e-mail contiene palabras o patrones específicos, si se habilita en el perfil de protección, la unidad FortiGate busca palabras o patrones en el mensaje e-mail.

2.2.2.20.2 Lista Negra/Blanca

La unida FortiGate usa una lista de direcciones IP y una lista de direcciones e-mail para filtrar los e-mail entrantes; cuando se realiza la verificación en la lista de direcciones IP, la unidad FortiGate compara la dirección IP del que envía el mensaje con la lista de direcciones IP en forma secuencial, si se encuentra una coincidencia se toma la acción

asociada con la dirección IP caso contrario el mensaje pasa al siguiente filtro spam habilitado. Cuando se realiza la verificación en la lista de direcciones e-mail, la unidad FortiGate compara la dirección e-mail del que envía el mensaje con la lista de direcciones e-mail en forma secuencial, si se encuentra una coincidencia se toma la acción asociada con la dirección e-mail caso contrario el mensaje pasa al siguiente filtro spam habilitado.

2.2.2.21 IM, P2P & VoIP

La unidad FortiGate puede controlar y monitorear el uso de aplicaciones IM/P2P y protocolos VoIP (SIP y SCCP).

Fortinet reconoce que estas aplicaciones son parte de los negocios pero si se abusa de las mismas pueden degradar la productividad y el rendimiento de la red.

El sistema FortiGate permite configurar la lista de usuarios para permitir o bloquear el uso de este tipo de aplicaciones a más de asignar el ancho de banda a ser usado por las mismas.

2.2.3 SOFTWARE PARA PROTECCIÓN

2.2.3.1 FortiClient

Es un software para seguridad host, provee un ambiente de computación seguro para computadoras de escritorio y portátiles que corren el sistema operativo Microsoft Windows y brinda las siguientes funcionalidades:

- Creación de conexiones VPN con redes remotas.
- Configuración de protección en tiempo real contra virus.
- Protección contra la modificación del registro de Windows.
- Escaneo de virus.

2.2.3.2 FortiMail

Es una plataforma de mensajes segura, provee escaneo heurístico flexible e informa de la capacidad de entrada y salida del tráfico e-mail. La unidad FortiMail utiliza el escaneo DCC (Distributed Checksum Clearinghouse) y Bayesiano que brindan alto rendimiento y confiabilidad para la detección y bloqueo de anexos maliciosos.

Gracias a la tecnología FortiASIC y FortiOS, el antivirus FortiMail extiende las capacidades de inspección de contenido para detectar las amenazas de correo electrónico más avanzadas.

PUERTO	**SERVICIO**
Tráfico originado por FortiMail	
UDP 514 / TCP 514	Syslog
TCP 389	LDAP
TCP 1812	RADIUS
TCP 2049	NFS
TCP 21 / TCP 22	FTP / SFTP
TCP 25	SMTP
UDP 162	SNMP
UDP 53	DNS
UDP 123	NTP
TCP 443	Actualización Antivirus (download)
UDP 9443	Actualización Antivirus (upload)
UDP 8889	Clasificación AntiSpam
Tráfico que recibe FortiMail	
TCP 23	Telnet
TCP 22	SSH
TCP 80	HTTP
TCP 443	HTTPS
UDP 9443	Actualización Antivirus / IPS
TCP 25	SMTP
TCP 465	SMTP Seguro
TCP 110	POP3
TCP 995	POP3 Seguro
TCP 143	IMAP
TCP 993	IMAP Seguro
UDP 161	SNMP

Tabla 2.2: Tráfico y puertos asociados con FortiMail. [13]

2.2.3.3 FortiBridge

Estos productos son diseñados para proveer tráfico de red continuamente en caso de un corte de energía o un fallo en el sistema FortiGate; son productos fáciles de usar e implementar y se pueden personalizar las acciones a tomar en caso de fallos.

La unidad FortiBridge evita la unidad FortiGate para asegurarse que la red pueda continuar procesando tráfico.

2.2.3.4 FortiManager

Es un sistema diseñado para cubrir las necesidades de empresas grandes responsables de establecer y mantener las políticas de seguridad de varias instalaciones FortiGate dispersas.

Con este sistema se puede configurar múltiples dispositivos FortiGate y monitorear su estado, también se puede ver el historial de logs y logs en tiempo real, incluyendo la actualización de imágenes de los dispositivos FortiGate administrados. Este sistema es de fácil uso y se integra fácilmente a otros sistemas.

2.2.4 FORTIANALYZER

Es un dispositivo de red que provee herramientas para la obtención de reportes, ejecución de análisis de datos y recopilación integrada de logs. Los informes de log detallados proveen el análisis tanto histórico como en tiempo real del tráfico de red, e-mail, FTP, actividad web, actividad de virus, actividad spam y actividad de ataques de intrusión, para ayudar a identificar las cuestiones de seguridad y reducir el mal uso y abuso de la red.

Provee a los administradores de red una visión exhaustiva del uso de red y la información de seguridad, cubre las necesidades de empresas y proveedores de servicios responsables por descubrir y direccionar las vulnerabilidades a través de los sistemas FortiGate dispersos.

Los dispositivos FortiAnalyzer minimizan el esfuerzo requerido para monitorear y mantener políticas de uso aceptable, identificar patrones de ataques, enjuiciar a los atacantes, obedecer reglamentos gubernamentales respecto a la privacidad y develación de la información. Aceptan y procesan un amplio rango de registros (logs) proporcionados por los sistemas FortiGate, provee funciones de administración de seguridad avanzadas como

archivos en cuarentena, correlación de eventos, valoración de vulnerabilidades, análisis de tráfico y de archivos de contenido.

Los registros log de los sistemas FortiGate / FortiMail son transmitidos al sistema FortiAnalyzer usando túneles VPN encriptados para garantizar la seguridad en la transmisión de archivos log y archivos puestos en cuarentena. Su capacidad varía desde 250GB hasta 4.8TB de datos log y niveles RAID (Redundant Array of Inexpensive Disks) de 0, 1, 5, 10 y 50 que pueden ser seleccionados para soportar el nivel deseado entre capacidad y seguridad de los datos.

2.2.4.1 Características

FortiAnalyzer recibe los archivos log de varios dispositivos FortiGate, FortiMail, FortiManager, FortiClient y demás servidores syslog; además por su capacidad de reportes robusta puede monitorear el tráfico, los ataques y el mal uso de la red por parte de los usuarios.

2.2.4.1.1 Registros

La unidad FortiAnalyzer crea sus propios mensajes log del sistema en relación a su actividad, eventos de seguridad y negociaciones IPSec para la transmisión segura de los paquetes que contienen los mensajes log.

- ***Registros locales.*** Permite almacenar los mensajes log en el disco duro de la unidad FortiAnalyzer local.

- ***Registros para un host.*** Permite enviar los mensajes log de la unidad FortiAnalyzer a un servidor Syslog.

2.2.4.1.2 Reportes

- ***Análisis log y reportes.*** Analiza logs presentados por múltiples dispositivos y genera una variedad de reportes que hacen posible una seguridad de red proactiva, ya que permite conocer las amenazas que aparecen, evitar el abuso de red, administrar los requerimientos de ancho de banda y monitorear los sitios web visitados a fin de asegurar el uso apropiado de la red.

- ***Reportes de vulnerabilidades.*** Presenta las debilidades potenciales ante ataques que podrían existir para un dispositivo seleccionado. FortiAnalyzer consulta los puertos abiertos y la información sobre el servicio que se ejecuta, para dar a conocer las vulnerabilidades existentes para este servicio.

2.2.4.1.3 Significado de los datos

Permite fácil acceso a reportes simples para obtener información sobre los intentos de intrusión y el tipo de tráfico en la red. Los resúmenes de eventos de seguridad proporcionan una vista rápida del tráfico no deseado que intenta romper la seguridad del Firewall (virus, intrusiones y actividad sospechosa) y los creadores de tráfico excesivo en la red, mientras que los resúmenes de tráfico proporcionan una vista rápida del tráfico que atraviesa el Firewall e ingresa a la red.

2.2.4.1.4 Analizador de red

Actúa como un sniffer que captura datos del tráfico de red para almacenarlos en el disco duro o generar reportes en base a éstos.

El analizador de red usa un puerto dedicado de la unidad FortiAnalyzer que se conecta al switch, permite alcanzar áreas de red donde el Firewall de FortiGate no se esté utilizando o si no se tiene un FortiGate como Firewall.

2.2.4.1.5 Visor de Logs

El navegador de logs permite visualizar los mensajes log enviados al FortiAnalyzer desde los dispositivos registrados; permite ver cualquier mensaje o archivo log guardado en el disco duro. Todos los archivos y mensajes pueden ser explorados y filtrados para localizar información específica.

- ***Visor de logs en tiempo real.*** Provee registros en tiempo real de tráfico Web, FTP y correo electrónico mediante registros de contenido.

  El visor de contenidos ofrece una visualización en tiempo real de la información meta de los dispositivos registrados. La información meta incluye la fuente y el destino de la información, lo que permite seguir en tiempo real las tendencias de uso de la red.

- ***Visor del historial de logs.*** Permite visualizar la información log de un rango de tiempo específico y filtrarla para encontrar información de eventos específicos.

2.2.4.1.6 Agregación de Logs

Es un método que permite recopilar datos log de dispositivos FortiAnalyzer remotos u otros dispositivos de red que soporten el formato syslog a una unidad FortiAnalyzer central.

La unidad FortiAnalyzer actúa como cliente cuando envía logs a un servidor de agregación, y como servidor cuando recibe los logs de los clientes de agregación.

2.2.4.1.7 Cuarentena

Para los FortiGate que no tienen disco duro, FortiAnalyzer ofrece la habilidad de poner en cuarentena archivos sospechosos o infectados que entran en el ambiente de red. Mediante el explorador de cuarentena se puede observar los archivos para determinar si son peligrosos o no.

2.2.4.1.8 Almacenamiento en red

FortiAnalyzer actúa como un dispositivo NAS, se lo usa como un medio de respaldo para almacenar información importante en el espacio extra del disco duro, como un servidor de archivos o repositorio.

2.2.4.1.9 RAID

FortiAnalyzer utiliza múltiples discos duros para almacenar los datos log usando un arreglo RAID para ofrecer almacenamiento redundante, protección de los datos, rápido acceso al disco duro o una gran capacidad de almacenamiento.

2.2.4.1.10 LDAP

La unidad FortiAnalyzer usa LDAP para consultar al servidor Active Directory de Windows sobre los nombres usuarios o grupos para generar los reportes.

2.2.4.1.11 Análisis Forense

Proporciona un método de vigilancia y reportes sobre individuos o grupo de personas a cerca de su tráfico de red, correo electrónico y mensajes instantáneos; permitiendo al administrador reducir la información a determinados individuos o grupos de personas.

Además permite ejecutar reportes con información detallada sobre el acceso a sitios web, accesos web bloqueados, correo electrónico, FTP y mensajes instantáneos durante un periodo específico en la red.

2.2.4.1.12 Alertas

Informan sobre los asuntos que se originan en un FortiGate, en la red o en el mismo FortiAnalyzer, tales como fallas del sistema o ataques de red, permitiendo reaccionar inmediatamente ante el evento; puede enviar los mensajes de alerta a direcciones de correo electrónico, servidores syslog o como traps SNMP, para informar a los administradores sobre los sucesos y su origen.

2.2.4.1.13 Escáner de vulnerabilidades

La unidad FortiAnalyzer genera un informe de las vulnerabilidades de los host que están en riesgo ante los ataques de hackers y spyware.

El escáner de vulnerabilidades entra al host y escanea los puertos, el software y las aplicaciones instaladas; esta exploración revela posibles puntos de ataque que pueden ser explotados para acceder a la información del computador o afectar su operación. El informe de la vulnerabilidad provee la información sobre la gravedad de la amenaza de seguridad y los parches disponibles o las soluciones conocidas para eliminar la amenaza.

El escáner de vulnerabilidades usa conexiones Remote Vulnerability Scan (RVS) y un motor RVS que es actualizado a través de la red de distribución Fortinet (FDN).

2.2.5 FORTIREPORTER

Es un software de análisis de seguridad, que genera informes de fácil comprensión y puede recopilar logs de cualquier unidad FortiGate y de otros dispositivos de seguridad (otros vendedores).

FortiReporter revela el abuso de la red, administra el requerimiento de ancho de banda, monitorea el uso de web y asegura que los empleados usen la red apropiadamente; permite a los administradores IT identificar y responder a los ataques, incluso identificar las maneras para asegurar proactivamente sus redes antes de que las amenazas de seguridad aparezcan.

2.3 ANÁLISIS SOLUCIÓN 2: JUNIPER [14]

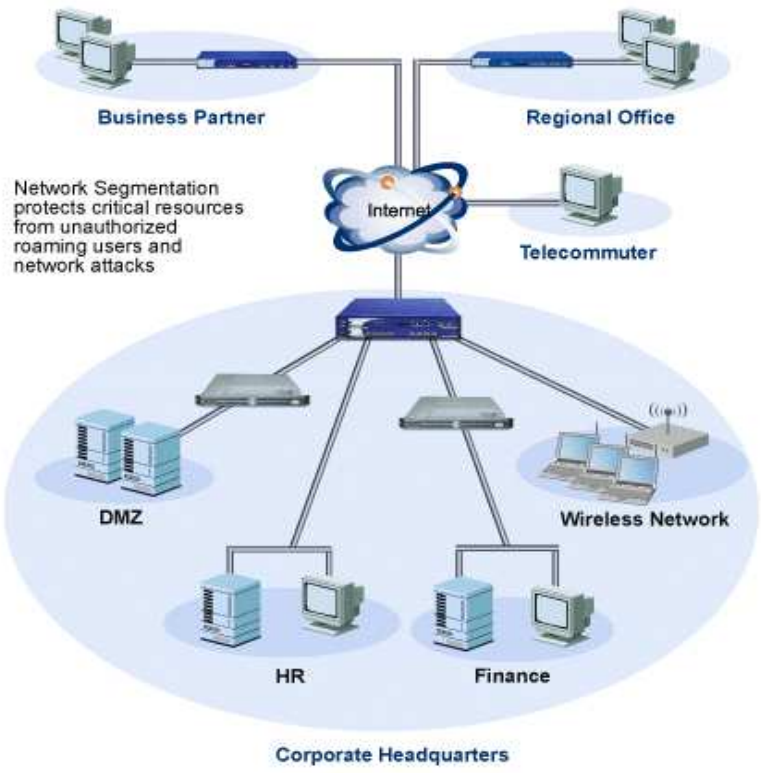


Figura 2.13: Solución de seguridad Juniper. [14]

Los dispositivos de seguridad Juniper, protegen aplicaciones, datos e infraestructura mediante el uso de capas de funciones de seguridad, que mitigan amenazas emergentes y controlan el acceso a la red tanto en forma externa como interna.

2.3.1 AAA Y 802.1X EN REDES JUNIPER

Ofrece una completa colección de productos de seguridad, para el acceso de red basados en RADIUS y en el estándar 802.1X; apropiado para redes de cualquier tamaño como empresas y proveedores de servicio de red tanto cableada como inalámbrica.

Esta colección de productos constituye un importante componente para el cumplimiento de las políticas de seguridad de forma uniforme, para todos los métodos de acceso a la red como WLAN, VPN/remota, dial up y cableadas con 802.1X.

Presenta también soluciones especializadas para proveedores de servicio que ofrecen autenticación de subscriptor, soporte y entrega rápida de nuevos servicios; con capacidad para manejar cualquier carga de tráfico y soporte para cualquier infraestructura de red con un buen rendimiento y confiabilidad.

2.3.1.1 Juniper Networks Steel-Belted Radius (SBR)

Es una familia completa de RADIUS / AAA y servidores de administración de políticas para empresas y proveedores de servicios, dispone de una variedad de factores que permiten cubrir cualquier requerimiento. El paquete de software desarrollado SBR disponible tanto para usuarios como para vendedores que quieran personalizar sus propias implementaciones SBR.

2.3.1.2 Juniper Networks Odyssey

Es una familia completa que provee seguridad de acceso 802.1X para clientes, provee autenticación fuerte y seguridad de la información mediante protección de datos y credenciales de red.

2.3.2 FIREWALL / IPSec WAN EN REDES JUNIPER

Ofrece soluciones de seguridad orientadas al uso de Firewall / VPN para empresas y proveedores de servicio; integra un conjunto de aplicaciones de seguridad para brindar la adecuada protección contra gusanos, troyanos, virus y otros tipos de malware.

Presenta múltiples tipos de administración como: CLI, WebUI o administración centralizada mediante el uso de Administración Segura NetScreen.

2.3.2.1 Características

- Dispositivos que brindan seguridad y rendimiento apropiado con conectividad WAN y ruteo.

- Unified Threat Management (UTM) incluye Firewall Stateful, IPSec VPN, IPS (Inspección a profundidad), Antivirus (AntiSpyware, AntiPhishing, AntiAdware), AntiSpam y Filtrado Web.

- Segmentación de red, ruteo dinámico y múltiples modos de desarrollo, simplifican la integración de red, el desarrollo de la seguridad interna o el desarrollo de múltiples dominios de seguridad.

- Dispositivos de seguridad que proporcionan alto rendimiento, seguridad y conectividad modular LAN/WAN.

- Desarrollado como un dispositivo de ruteo LAN/WAN y como Firewall para reducir IT CAPEX (Gastos de Capital) y OPEX (Gastos Operativos).

- Alto rendimiento del Firewall e integración de la plataforma IDP para proteger las redes de alta velocidad de los ataques a nivel de red y aplicación.

- La arquitectura modular de I/O brinda alta densidad y flexibilidad de interfaz, para varios requerimientos de conectividad.

- La solución de Firewall de estado y VPN de alta disponibilidad con respaldos para mantener la continuidad del negocio.

- La plataforma de alto rendimiento Firewall / VPN protege ambientes de alta velocidad como los centros de datos y proveedores de red.

2.3.3 PREVENCIÓN DE INTRUSIONES EN REDES JUNIPER

Ofrece soluciones IPS para redes de todo tamaño y de diferentes requerimientos de rendimiento, el rápido desarrollo de protección ante ataques en línea con configuraciones de alta disponibilidad, asegura protección de seguridad ininterrumpida; además permite a los administradores visualizar actividades a nivel de aplicación y de red para identificar el origen de los ataques.

Los productos para detección y prevención de intrusiones de las redes Juniper proveen protección adecuada y de fácil uso contra amenazas nuevas y actuales en las capas de red y aplicación; usa técnicas de detección y prevención de estado industrialmente

reconocidas, provee protección de día cero contra gusanos, troyanos, spyware, keyloggers y otros. Esta protección puede desarrollarse rápidamente y confidencialmente en línea para identificar y parar de forma efectiva los ataques antes de que causen daños, minimizando el tiempo y costo asociados a las intrusiones.

También provee información sobre aplicaciones o servidores maliciosos que pueden haber sido añadidos de forma desconocida en la red; así los administradores pueden tener un control granular de la red mediante una administración centralizada del comportamiento del sistema, facilitando la auditoría, los reportes y el análisis de logs.

2.3.3.1 Características

- Puertos dedicados de alta disponibilidad y administración.
- Bypass integrado para puertos de tráfico gigabit.
- Gateway de seguridad de alto rendimiento que integra prevención de intrusiones, Firewall e IPSec VPN; para brindar redes escalables y seguridad a nivel de aplicación.
- La presentación Gigabit + IDP ofrece seguridad mediante tecnología ASIC, microprocesadores de alta disponibilidad y módulos de seguridad adaptables que tiene su propio procesador y memoria.

2.3.4 CONTROL DE ACCESO UNIFICADO EN REDES JUNIPER

Consiste en un lazo de identificación del usuario, integridad del dispositivo e información de ubicación, mediante una política reforzada de sesión específica a lo largo de la red; habilita el control de acceso para invitados, contratistas y empleados; soporta infraestructuras 802.1X y estándares abiertos mediante conexiones de red confiables.

Esta solución combina la identidad del usuario y la información de estado de seguridad del dispositivo con la información de ubicación de red, para crear una política de control de acceso única por cada usuario. Se puede trabajar en capa 2 usando 802.1X para el control de admisión de red y en capa 3 para el control de acceso a los recursos.

2.3.4.1 Características

- Provee Host Checker e integra características de Odyssey Access Client.
- Integra características de Steel-Belted Radius.
- Plataforma de alto rendimiento para desarrollos grandes y complejos.
- Puede administrar al mismo tiempo miles de dispositivos finales.

2.3.5 ACCESO SEGURO SSL VPN EN REDES JUNIPER

Ofrece una plataforma de acceso remoto seguro para empleados y socios, así los usuarios puedan acceder a aplicaciones y recursos de la empresa mediante el establecimiento de seguridad en dispositivos de punto final, para un control de acceso granular, prevención y control de amenazas coordinado con IDP.

Dispositivos escalables permiten cubrir los requerimientos de acceso remoto / móvil y externo para compañías de todos los tamaños, además ofrece alta disponibilidad y escalabilidad para proveedores de servicios.

El acceso seguro SSL VPN en redes Juniper está basado en la plataforma IVE (Instant Virtual Extranet), la cual usa SSL. SSL elimina la necesidad de un software cliente, de cambios en los servidores internos y de costos de mantenimiento y soporte; además combina soluciones IPSec que brindan características de seguridad punto a punto.

2.3.5.1 Características

- Acceso seguro para empleados remotos / móviles, sin necesidad de un software cliente.
- Actualizaciones opcionales permiten el acceso desde cualquier PC y desde cualquier lugar.
- Desarrollos Plug and Play.
- Características de seguridad robustas.
- Acceso LAN, intranet y extranet seguro para empleados, socios y clientes.

- Tres métodos de acceso permiten a los administradores dar acceso de acuerdo al propósito.
- Administración dinámica de privilegios de acceso.
- Software avanzado permite funcionalidades sofisticadas como la administración centralizada.
- Certificados de Criterio Común, dispositivos FIPS (Federal Information Processing Standards) disponibles.
- Compresión y aceleración SSL para todo tipo de tráfico.
- Administración de privilegios de acceso dinámico mediante tres métodos de acceso.
- Plataforma de alto rendimiento para desarrollo de accesos grandes, complejos y seguros en ambientes intranet, extranet y LAN.
- Plataforma SSL VPN que permite habilitar interfaces virtuales para brindar servicios SSL VPN basados en red a múltiples empresas desde un solo dispositivo / cluster.
- No requiere instalación de software cliente y no presenta complicaciones de Firewall/NAT, así reduce el soporte e incrementa el ROI (Return On Investment).
- Oportunidad de rédito diferenciada con servicios como acceso extranet, recuperación ante desastres, seguridad LAN intranet y acceso de dispositivos móviles.
- Cubre requerimientos de escalabilidad, rendimiento y alta disponibilidad para proveedores de servicios.

2.3.6 SOPORTE A FUNCIONALIDADES EMPRESARIALES

El interés y reto actual de las empresas se centra en acelerar la entrega de aplicaciones convergentes que alimenten las interacciones y transacciones de alto valor operacional.

La aproximación de capas de servicio de Juniper, permite a las empresas visualizar e influenciarse con la inversión existente para desplegar nuevas funcionalidades en pasos, dependiendo de las necesidades de cada organización.

2.3.6.1 Aceleración de aplicación

Permite acelerar y optimizar la entrega de aplicaciones desde los centros de datos sobre conexiones punto a punto, para reducir el retardo y enviar / recibir más tráfico sobre enlaces de ancho de banda constante.

2.3.6.2 Oficina remota / sucursal

Asegura la operación de negocios en sucursales y sitios remotos, mediante la protección de los sistemas internos y la disponibilidad de las aplicaciones centralizadas.

2.3.6.3 Cumplimiento

Soporta el cumplimiento de las regulaciones concernientes a la seguridad de la información como integridad, privacidad y rendimiento; mediante el aseguramiento de datos tanto almacenados como transmitidos, el control de acceso, la disponibilidad y el monitoreo de los eventos de red.

2.3.6.4 Control de acceso

Provee seguridad de acceso basándose en la identidad del usuario, estado de seguridad del punto - final, ubicación de la información y políticas de cualquier ubicación de usuario (LAN / remoto) sin tener en cuenta su dispositivo, así incrementa la productividad del usuario y se protege los recursos y aplicaciones empresariales.

2.3.6.5 Centros de datos

Permite proteger la inversión de aplicación y consolidación de servidores en pequeños y grandes centros de datos, con capacidades integradas que defienden, aseguran, extienden y aceleran todo tipo de aplicaciones.

2.3.6.6 Aplicaciones Microsoft

El centro de recursos Microsoft de las redes Juniper provee demos, literatura, casos de estudio y herramientas para optimizar el rendimiento de las aplicaciones Microsoft centralizadas.

2.3.6.7 Control de Acceso Remoto

Permite a los usuarios remotos acceder a aplicaciones centralizadas como si se encontraran en la oficina central, mediante el chequeo de los host de punto - final, la autenticación dinámica y el control de acceso granular.

2.3.6.8 Seguridad

Protege la confidencialidad de los datos y los activos de cómputo, mediante el uso de capas de funciones de seguridad que mitigan amenazas emergentes y controlan el acceso a la red tanto en forma externa como en forma interna.

2.3.6.9 Administración de Amenazas

Asegura toda la red mediante una solución holística para proteger aplicaciones, datos e infraestructura tanto de amenazas externas como internas.

2.3.6.10 Voz sobre IP

Asegura que la infraestructura esté preparada para soportar alta calidad en voz y video; y al mismo tiempo que brinda protección contra amenazas y mal uso, asegura el adecuado rendimiento y disponibilidad del recurso.

2.3.6.11 Evolución VPN y WAN

Permite la migración hacia nuevas tecnologías como WAN con IP / MPLS, IPSec y SSL VPN, mediante plataformas que aceleren las aplicaciones para asegurar bajo costo y convergencia.

2.4 ANÁLISIS SOLUCIÓN 3: CISCO [15]

Cisco presenta un conjunto de productos y servicios de seguridad que constituyen una solución de Comunicación Segura de Cisco llamada Cisco Self-Defending Network.

Esta solución incorpora capacidades que buscan asegurar la red, los dispositivos finales, las aplicaciones y los mensajes.

2.4.1 SELF - DEFENDING NETWORK

Es una solución arquitectónica diseñada para cubrir los diferentes escenarios de seguridad; la empresa puede diseñar, implementar, operar y optimizar plataformas de red que protejan los procesos críticos del negocio contra ataques y rupturas; además permite brindar privacidad a los datos, soporte a las políticas y cumplimiento a los controles reguladores.

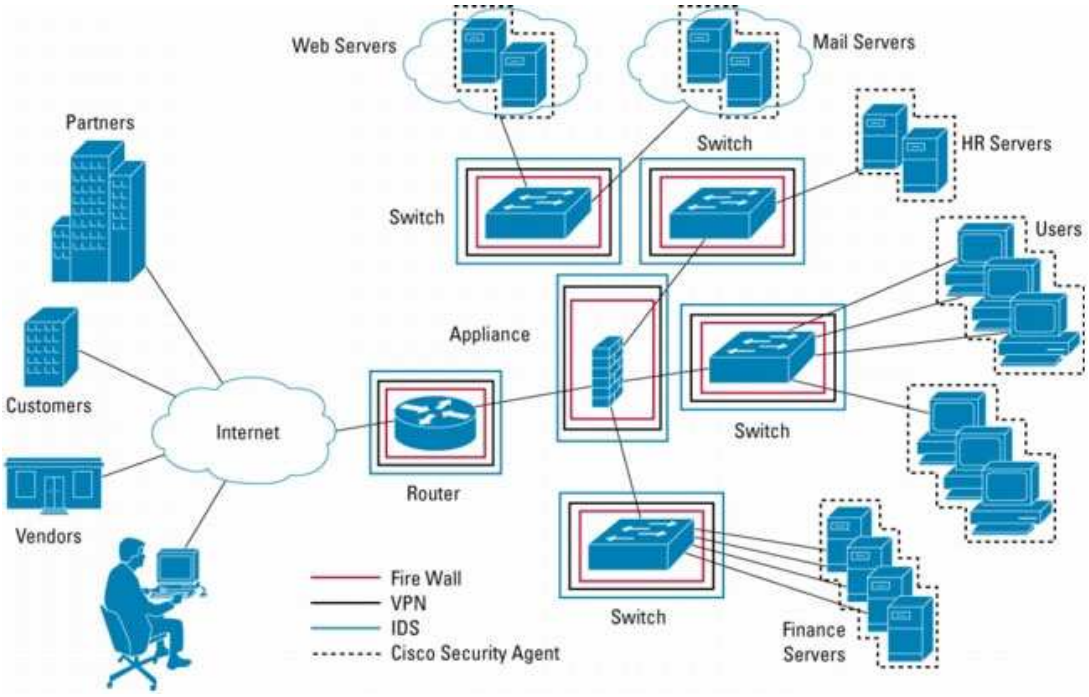


Figura 2.14: Solución de seguridad Cisco. [15]

Usando la red como plataforma se puede:

- Mantener los recursos humanos y tecnológicos seguros.
- Hacer a la organización más resistente y confiable.
- Conseguir el máximo beneficio del negocio de la inversión IT.
- Asegurar el cumplimiento de las regulaciones de seguridad.
- Proveer comunicaciones unificadas seguras y soluciones de movilidad.
- Brindar seguridad para el centro de datos y las sucursales.

2.4.1.1 Servicios de Seguridad

2.4.1.1.1 Control de Amenazas

Se encarga de controlar y contener activamente tanto amenazas conocidas como desconocidas. Esta solución de seguridad ofrece protección para la red mediante las siguientes características:

- Visión amplia de la red.
- Control simplificado de políticas.
- Protección proactiva del sistema.

Está diseñada específicamente para la protección de red, servidores, dispositivos finales e información; también regula el acceso de red, aísla los sistemas infectados, evita intrusiones y protege los activos críticos del negocio. Además contrarresta tráfico malicioso como gusanos, virus y malware antes de que el sistema sea afectado.

Todas estas actividades se llevan a cabo mediante políticas centralizadas, configuraciones adecuadas y la administración de eventos causados por las amenazas.

- ***Para dispositivos finales.*** Se encarga de defender al sistema contra las amenazas más comunes introducidas por el uso del Internet, tales como virus, spyware y otros contenidos maliciosos que podrían provocar la pérdida de datos y la degradación de la productividad.

- ***Para la Infraestructura.*** Salvaguarda la infraestructura de servidores y aplicaciones contra ataques e intrusiones, defendiendo al sistema contra intentos tanto internos como externos de penetración o ataque mediante la explotación de vulnerabilidades de sistemas operativos y aplicaciones.

- ***Para E-mail.*** Asegura la productividad del negocio, la disponibilidad de los recursos y la confidencialidad de la información mediante la detención de amenazas e-mail desde sus orígenes.

2.4.1.1.2 Cumplimiento de los Reglamentos

Se encarga de establecer los reglamentos correctos para cumplir con aspectos de seguridad como privacidad, integridad, disponibilidad y auditoría.

Ayuda a evitar multas, castigos, abogados, investigaciones y auditorías que la organización puede sufrir si ocurre una brecha de seguridad y si ésta se encuentra fuera del cumplimiento de la ley. Sin embargo el mayor impácto es la pérdida de prestigio de la organización en caso de presentarse problemas de seguridad.

2.4.1.1.3 Comunicaciones Seguras

El objetivo es proteger la privacidad y la integridad de la información que se maneja a través de las comunicaciones.

- ***Para Acceso Remoto.*** Mediante el establecimiento de acceso personalizado a la red corporativa y sus aplicaciones, utilizando túneles encriptados a través de Internet.

- ***Para Conexiones punto a punto.*** Brinda una infraestructura de red WAN basada en Internet para conectar oficinas en sucursales, oficinas en el hogar u oficinas de socios, a una porción de la red o a toda la red.

2.4.1.1.4 Control de Acceso de red

Se encarga de reforzar las políticas de seguridad en todos los dispositivos de comunicación mediante la búsqueda de accesos de red.

El Control de Admisión de Red Cisco (NAC), permite el acceso solamente a dispositivos finales confiables como PCs, servidores y PDAs internos a la red; y restringe el acceso a dispositivos no confiables; por consiguiente limita daños potenciales, minimiza el riesgo y controla las amenazas de seguridad que aparecen continuamente. Además NAC permite a la organización desarrollar métodos de acceso basados en roles para prevenir accesos no autorizados y mejorar la resistencia de la red.

Trabaja en aspectos como:

- Cumplimiento de las políticas de seguridad.

- Protección de la inversión existente.
- Mitigar riesgo de virus, gusanos y accesos no autorizados.

2.4.1.2 Aplicaciones de Seguridad

Constituyen software desarrollado para identificar nuevas clases de amenazas, mediante la inspección granular del tráfico de red, para así detener tráfico dañino antes de que se propague por la red.

2.4.1.3 Escenarios de Seguridad NAC

La seguridad Cisco se ha desarrollado para infraestructuras LAN, WAN, Wireless y de Acceso Remoto.

2.4.1.4 Componentes de Seguridad Cisco

Los dispositivos Cisco dependiendo del modelo pueden incluir los siguientes componentes de seguridad:

- Firewall.
- Prevención de Intrusiones y Ataques (IDS / IPS).
- Protección contra Virus y Spam.
- VPNs.
- Control de Acceso a la red.
- Administración de Seguridad.
- Seguridad Física.

2.5 COMPARACIÓN DE TECNOLOGÍAS UTM: FORTINET, JUNIPER Y CISCO

De acuerdo al estudio realizado previamente en el presente capítulo sobre las tecnologías mencionadas, el mismo que estubo orientado a las soluciones de seguridad que ofrece cada proveedor, se presenta el siguiente resumen comparativo.

La tecnología ofrecida por ***Fortinet*** se presenta como la más apropiada al momento de hablar sobre UTM, siendo este proveedor el que lidera actualmente el mercado.

Los UTM de Fortinet ayudan a frustrar ataques combinados[1], mediante una amplia variedad de funcionalidades y servicios de seguridad; además, soportan sólidamente aplicaciones exigentes, mediante sistemas hardware de alto rendimiento ya que utilizan microprocesadores ASIC, exclusivamente diseñados para soportar el análisis que requieren los temas de seguridad.

La tecnología ofrecida por ***Juniper*** se presenta como una alternativa de seguridad no muy enfocada a los UTM sino más bien a productos de seguridad aislados, pero constituye una tecnología enfocada al tema de seguridad en redes, por lo tanto posee al igual que Fortinet lo último en tecnología de seguridad como lo son los microprocesadores ASIC.

La tecnología ofrecida por ***Cisco*** se presenta como una alternativa de conectividad más que como una alternativa de seguridad; pero para cubrir el ámbito de seguridad en redes ha incorporado algunos servicios de seguridad en sus dispositivos de conectividad. Es así que este proveedor no tiene un enfoque exclusivo en temas de seguridad, y no presenta una solución enfocada a los UTM.

Finalmente de acuerdo a evaluaciones realizadas por IDC (International Data Corporation), se ubican en el siguiente orden los proveedores de seguridad de acuerdo a su liderazgo en el mercado y a su tecnología de desarrollo en temas de seguridad:

1. Fortinet.
2. Juniper.
3. Cisco.

En el capítulo IV se presenta en detalle la comparación de las soluciones de seguridad que ofrece cada proveedor, ya que se exponen las características y funcionalidades de los dispositivos de seguridad que permiten cubrir los requerimientos de la red Quito Motors.

[1] **Ataques Combinados**. Consiten en la agrupación de varias amenazas como: virus, gusanos, spam, spyware, etc; provenientes de una sola forma de infección o distribución. Ejemplo: Un correo electrónico indeseado (spam) que contiene archivos adjuntos (amenazas).

CAPÍTULO III

Análisis de la Situación Actual de la red de Quito Motors

3 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE QUITO MOTORS

3.1 INFRAESTRUCTURA DE LA RED DE DATOS

El crecimiento de la red de Quito Motors ha sido progresivo de acuerdo a las necesidades operacionales que rodean a esta empresa de tipo comercial.

Actualmente la organización se presenta como un grupo llamado Quito Motors S.A.C.I. que integra cinco asociaciones como se muestra en el siguiente gráfico:

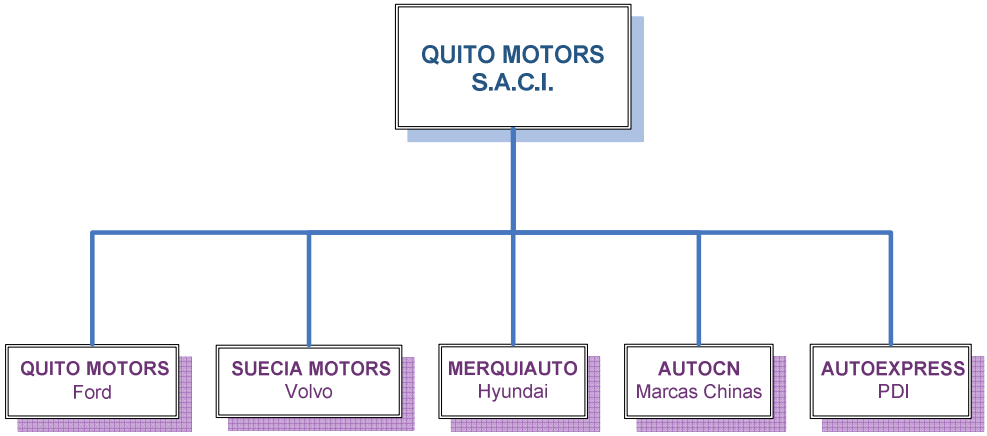


Figura 3.1: Esquema Organizacional de Quito Motors S.A.C.I.

Cada asociación cuenta con diferentes departamentos y sub-departamentos que forman parte de la red de Quito Motors como se muestra en el siguiente gráfico:

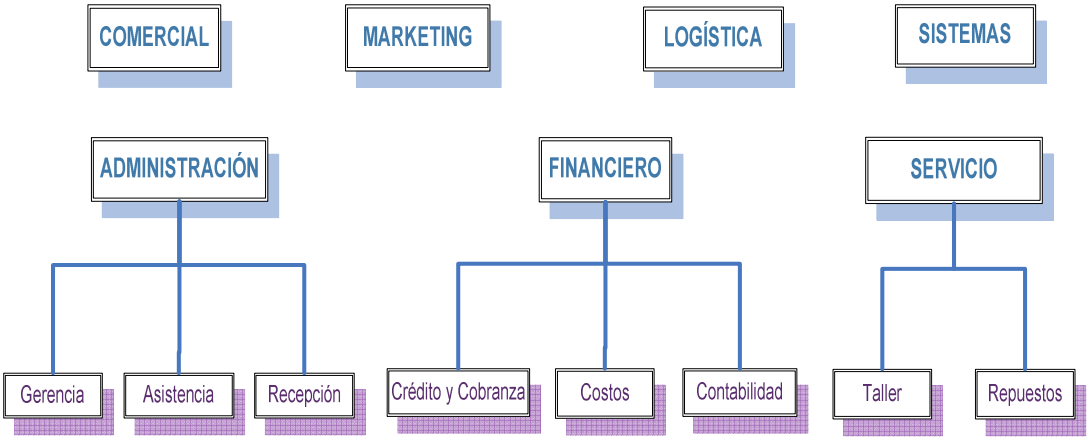


Figura 3.2: Esquema Departamental de Quito Motors S.A.C.I.

Esta organización cuenta con varias sucursales ubicadas a nivel nacional las mismas que se encuentran interconectadas y forman parte de la red de Quito Motors; a continuación se detalla su ubicación geográfica y la asociación a la que pertenecen:

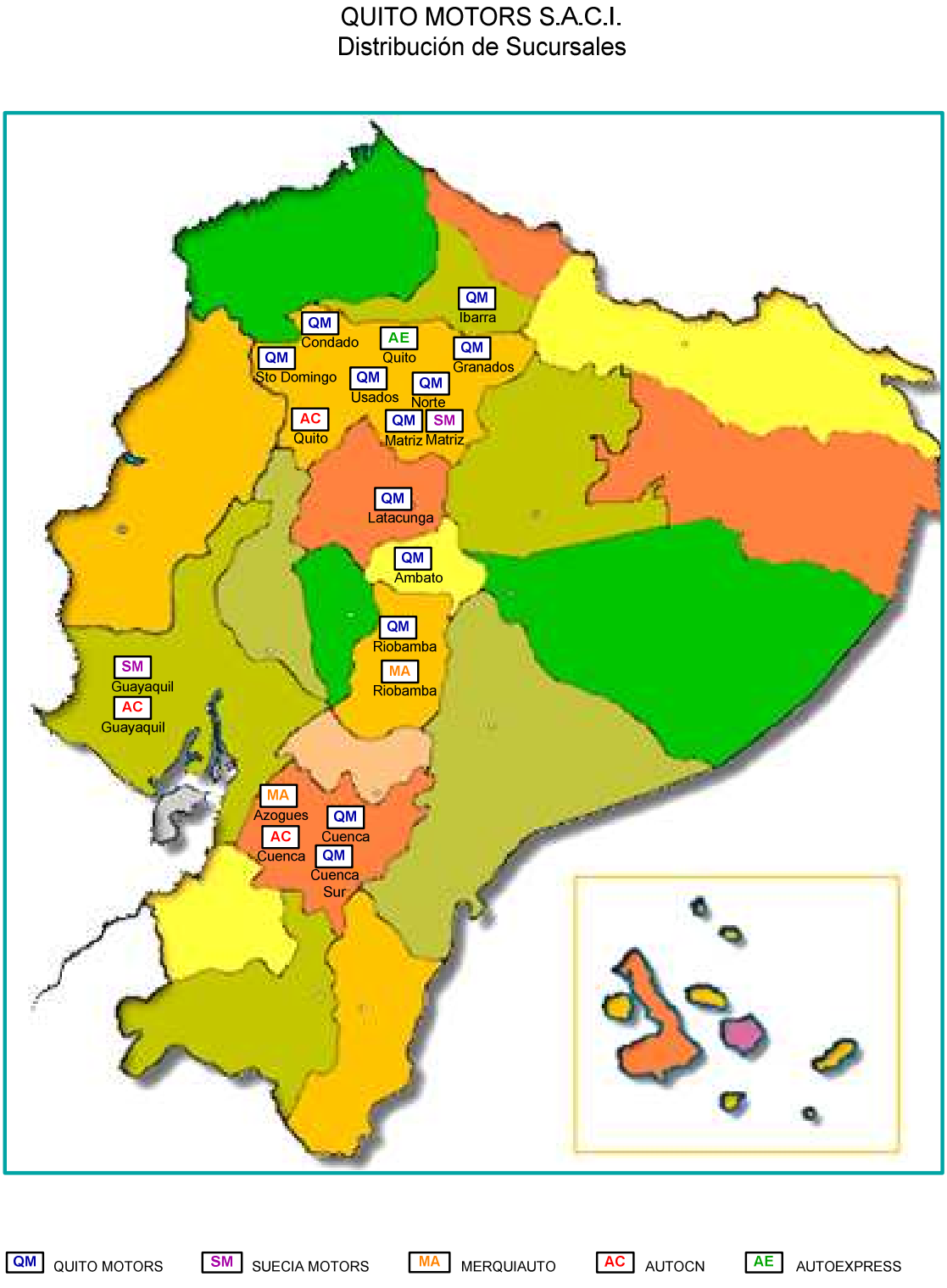


Figura 3.3: Ubicación Geográfica de las Sucursales.

3.1.1 ESTADO ACTUAL DE LA RED LAN / MAN / WAN

La red LAN / MAN / WAN de Quito Motors presenta una topología de red en Estrella a nivel físico, ya que todos los dispositivos que integran esta red se conectan de forma centralizada a Quito Motors – Matriz (centro de cómputo); y una topología de red en Bus a nivel lógico, ya que se trabaja sobre redes LAN Ethernet (IEEE 802.3) donde las tramas de información emitidas por un nodo (terminal o servidor) se propagan por la red utilizando el método de acceso CSMA / CD en busca del host destino.

El backbone y la granja de servidores de esta red se encuentran ubicados en el Centro de Cómputo; y constituyen los diferentes dispositivos que hacen posible la interconexión y operación LAN / MAN / WAN para la red de Quito Motors.

Para la implantación de la red LAN de Quito Motors – Matriz (core de la red Quito Motors) se utilizan los siguientes switch administrables: SWCISCO (Cisco Switch Catalys 2900), SW3COM1 (3Com Switch 4200G 48-Port) y SW3COM2 (3Com Switch 4200G 48-Port).

Para el establecimiento de la red MAN / WAN de Quito Motors (sucursales a nivel nacional) se utiliza una antena inalámbrica QM_MATRIZ y los siguientes routers: ANDINADATOS, ECUAONLINE, QMCENTRAL y UIO-GYE; éstos se encuentran ubicados en Quito Motors – Matriz y su correspondiente equipo (router, antena o módem) está ubicado en cada sucursal. Finalmente para el acceso a Internet se utiliza un dispositivo firewall: WATCHGUARD.

La red de la empresa utiliza la tecnología de red de Microsoft Windows, UNIX / Linux y Novell Netware; su funcionamiento está basado en el protocolo Netbeui (NetBIOS Extended User Interface), con el cual todos los miembros de la red local se conectan; para la comunicación a través de conmutadores o ruteadores se utilizan otros protocolos como TCP / IP o IPX, los mismos que encapsulan el protocolo Netbeui para integrar la red local dentro de una red más compleja, mediante el uso de direcciones IP e IPX.

La red LAN / MAN de Quito Motors trabaja bajo un esquema de Dominio NT[2] y las diferentes sucursales trabajan bajo el esquema de Grupo de Trabajo; de esta forma se establece la interconexión y comunicación que permite compartir recursos como aplicaciones, archivos e impresoras a fin de facilitar el trabajo diario de los funcionarios.

La empresa maneja un modelo centralizado de aplicaciones y servicios, es así que los funcionarios de cada una de las sucursales se enlazan con los servidores ubicados en la Matriz mediante conexiones remotas, utilizando el Terminal Service.

Los integrantes de esta red utilizan la salida a Internet en forma centralizada; existe un canal de interconexión a Internet entre Quito Motors – Matriz y el ISP de Satnet con capacidad de 1 Mbps; el mismo que abastece a todas las sucursales miembros de la red Quito Motors a nivel nacional y a Quito Motors – Matriz.

La red LAN de cada sucursal utiliza tecnología LAN Ethernet (IEEE 802.3) y Wi-Fi (IEEE 802.11g); utilizan par trenzado categoría 5e con conectores RJ45 y enlaces inalámbricos como medio de transmisión.

La red MAN que permite la integración de determinadas sucursales, se establece por medio de enlaces inalámbricos de banda ancha, provistos a través de antenas Motorola Canopy que utilizan tecnología Motowi4; éstas trabajan mediante una distribución punto – multipunto, transmiten en la banda 5,75 – 5,85 GHz con un radio de cobertura de 3Km y pueden manejar hasta 200 usuarios.

La red WAN de interconexión entre la Matriz y cada sucursal se establece mediante canales dedicados, se utiliza routers para encaminar el tráfico, módems como DTU (Data Terminal Unit), enlaces mediante cobre, microondas o fibra óptica para trasportar datos en diferentes tecnologías como Frame Relay y ATM (Asincronous Trasmision Mode).

La red Quito Motors está formada por un firewall, siete servidores, ciento cuarenta estaciones de trabajo, tres switch administrables, doce routers, cinco antenas y diferentes dispositivos como access point, hub, switch e impresora en cada una de las sucursales.

Para el detalle de la red observar los anexos A1, A2, A3, A4.

---

[2] **Dominio NT.** Es un método que permite establecer una red de trabajo, mediante la agrupación y autenticación de los usuarios dentro de un dominio; en este caso el servidor de dominio utiliza el sistema operativo Windows NT y el dominio se llama QUITO_M.

ANEXO A1: Diagrama de la Red Quito Motors.

ANEXO A2: Elementos Activos de Conectividad.

ANEXO A3: Enlaces de Interconexión entre la Matriz y las Sucursales.

ANEXO A4: Subredes de la Red Quito Motors.

El dispositivo WatchGuard se encuentra ubicado en el centro de cómputo y realiza NAT (Network Address Translation), lo que permite ocultar la red interna del exterior y así obtener salida hacia el Internet mediante una dirección pública.

Existen los siguientes servidores ubicados en el centro de cómputo: Servidor de Comunicaciones, Servidor Antivirus, Servidor de Correo Electrónico, Servidor Terminal, Servidor AS / 400, Servidor SQL y Servidor Novell.

Las estaciones de trabajo están distribuidas en la cada una de las sucursales mencionadas anteriormente y trabajan bajo una red tipo C.

Adicionalmente existen dos redes LAN inalámbricas con capacidad de 54 Mbps para brindar accesibilidad a lugares que requieren flexibilidad, como lo son:

- La sala de reuniones de Gerencia en Quito Motors – Matriz.
- El área de Taller en Quito Motors – Matriz.

3.1.2 RECURSOS INFORMÁTICOS

3.1.2.1 Computadores

Los computadores que forman parte de la red Quito Motors se encuentran distribuidos a nivel nacional en las diferentes sucursales, a continuación se detallan las principales características de los ejemplares existentes en la red:

ELEMENTO	**CARACTERÍSTICAS**
CPU	Desconocido[3], 2133 MHz

[3] **Desconocido.** El software AIDA32 v3.93, utilizado para obtener el reporte de las características de un computador resuelve el tipo de procesador como desconocido, debido a que se trata de un procesador clon (dispositivo genérico que constituye la copia de un dispositivo de marca).

	Desconocido, 3000 MHz Desconocido, 2000 MHz Desconocido, 2800 MHz Intel Pentium 4, 1600 MHz Intel Pentium 4E, 2800 MHz Intel Celeron 4A, 2000 MHz
Sistema Operativo	Microsoft Windows XP Professional Microsoft Windows 2000 Professional Microsoft Windows 98 Microsoft Windows 95
RAM	1024 MB; 512 MB; 256 MB
DISCO	40 GB, 7200 RPM 80 GB, 7200 RPM 40 GB, 5400 RPM
Tarjeta de red	Broadcom NetXtreme Gigabit Ethernet Intel(R) PRO/100 VE Network Connection Realtek RTL8139(A) PCI Fast Ethernet Adapter Realtek RTL8139/810x Family Fast Ethernet NIC CNet PRO200 PCI Fast Ethernet Adapter 108Mbps High Speed Wireless Network Adapter

Tabla 3.1: Características de los Computadores que conforman la red Quito Motors.

3.1.2.2 Servidores

Los servidores de la red de Quito Motors están localizados en el centro de cómputo (Quito Motors – Matriz), a continuación se detallan las principales características de los mismos:

1. AS / 400 Servidor Base de Datos, que contiene la información de Taller y Repuestos.	
CPU	Intel Celeron 4A, 2000 MHz
Sistema Operativo	OS 400

RAM	512 MB
DISCO	16 GB
Tarjeta de Red	Linksys NC100 Fast Ethernet 10/100
2. MAILSERV Servidor de Correo Electrónico, que permite administrar el correo interno y externo de la organización.	
CPU	Intel Pentium 4E, 3.0 GHz
Sistema Operativo	Linux Centos
RAM	512 MB
DISCO	80 GB
Tarjeta de Red	Ext: Intel Corporation 82801G LAN Controller Int: Linksys NC100 Fast Ethernet 10/100
3. SQLSERV Servidor de Base de Datos, que contiene información de Salarios, Ventas e Inventarios.	
CPU	Intel Pentium 4E, 2800 MHz
Sistema Operativo	Microsoft Windows 2000 Server
RAM	247 MB (128 MB) 256 MB
DISCO	76316 MB
Tarjeta de Red	Broadcom NetXtreme Gigabit Ethernet
4. COMSERV Servidor de Comunicaciones, que permite administrar la asignación de direcciones IP y el dominio.	
CPU	GenuineIntel x86 Family 6 Model 5 Stepping0, 300 MHz
Sistema Operativo	Microsoft Windows NT 4.0
RAM	256 MB
DISCO	4 GB
Tarjeta de Red	3 Com Etherlink III Adapter 10Base-T
5. TSSERV Sevidor de Conexiones Remotas, que permite compartir aplicaciones centralizadas.	

CPU	Intel Xeon-A, 3066 MHz (5.75 x 533)
Sistema Operativo	Microsoft Windows Server 2003, Standard Edition
RAM	3072 MB
DISCO	36 GB, 15000 RPM y 18 GB, 10000 RPM
Tarjeta de Red	Broadcom NetXtreme Gigabit Ethernet
6. SERVF – SEC Servidor de Seguridad, que permite administrar el sistema de protección F-Secure.	
CPU	Intel Pentium 4, 1.60 GHz
Sistema Operativo	Microsoft Windows 2000 Profesional
RAM	512 MB
DISCO	40 GB
Tarjeta de Red	3 Com EtherLink XL 10/100
7. NOVELL Servidor de Archivos de Red, que permite compartir recursos de almacenamiento.	
CPU	Intel Pentium 4, 1.60 GHz
Sistema Operativo	Netware 4.10
RAM	256 MB
DISCO	60 GB
Tarjeta de Red	NI00_1_E82 [Ethernet 802.2]

Tabla 3.2: Características de los Servidores de la red Quito Motors.

3.1.2.2.1 Servidor de Comunicaciones

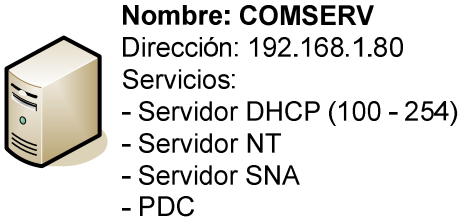


Figura 3.4: Servidor de Comunicaciones.

- ***Servicio DHCP (Dynamic Host Configuration Protocol).*** Es un protocolo de red que permite a los nodos de una red TCP / IP obtener sus parámetros de configuración automáticamente.

  El servidor DHCP está configurado para brindar servicio a la subred 192.168.1.0/24; las primeras cinco direcciones desde 192.168.1.1 hasta 192.168.1.5 se encuentran reservadas, las direcciones que van desde 192.168.1.6 hasta 192.168.1.99 se asignan de forma estática y las direcciones restantes desde la 192.168.1.100 hasta la 192.168.1.254 están configuradas de forma dinámica para que el servidor las asigne automáticamente a los clientes en forma permanente.

- ***Servicio NT (New Technology).*** Permite la agrupación y autenticación de los usuarios dentro de un dominio de trabajo denominado QUITO_M; el dominio está compuesto por un controlador primario y por estaciones de trabajo que actúan como clientes (usuario / ordenador) del dominio.

  Debido al gran número de ordenadores y de usuarios que trabajan en esta red, la estructura creada por el dominio aporta numerosas ventajas para el control administrativo de red, siendo la más importante la seguridad del dominio.

  El servidor NT mantiene la base de datos de los clientes del dominio, y válida al usuario mediante el PDC (Primary Domain Controller) a través de un canal seguro.

  El dominio posee una base de datos de usuarios y de equipos única y centralizada, a cada usuario se le asigna una cuenta que lo identifica en el dominio; la autenticidad del usuario está garantizada por el uso de su contraseña.

  El esquema de dominios permite crear grupos de usuarios, que facilitan la administración del dominio QUITO_M, se tiene los siguientes grupos de trabajo:

  - Administrador.
  - Restringido.

  El sistema de dominios simplifica la administración de servidores y estaciones de trabajo, ya que a medida que se añaden los equipos el administrador se encarga de

darlos de alta para que puedan comunicarse de forma segura con los demás miembros del dominio.

Al momento de instalar una estación de trabajo o servidor se escribe el nombre del dominio, el nombre de usuario y la contraseña, estos datos son validados por el controlador del dominio para permitir o negar el acceso al mismo, finalmente el programa de instalación configura automáticamente el sistema para que sea miembro del dominio.

El sistema de dominios simplifica la gestión de grandes redes, ya que los cambios introducidos en la configuración del dominio se reflejan automáticamente en todos los miembros del dominio.

- ***Servicio SNA (System Network Architecture).*** Es una arquitectura de red diseñada y utilizada por IBM para la conectividad con sus hosts o servidores. SNA define los estándares, protocolos y funciones usadas por los dispositivos para permitirles la comunicación entre ellos en las redes SNA.

  El servidor SNA funciona como un gateway entre una red SNA y una red TCP / IP; este servicio hace posible el trabajo entre el servidor AS / 400 (plataforma IBM) y los usuarios (plataforma Windows).

3.1.2.2.2 Servidor Terminal

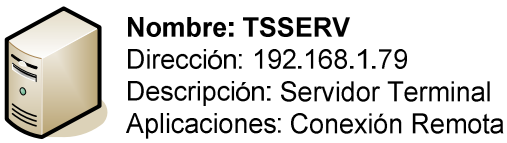


Figura 3.5: Servidor de Conexiones Remotas.

Este equipo está configurado como un servidor de conexiones remotas mediante la instalación del componente Terminal Server, que proporciona una implementación centralizada de las aplicaciones a compartir con los usuarios remotos.

Mediante este servidor los usuarios pueden ejecutar programas, guardar archivos y utilizar recursos de red desde una ubicación remota como si estuvieran instalados en sus propios equipos; al instalar programas en un servidor Terminal Server, se asegura que todos los usuarios utilicen la misma versión de un programa.

El servidor de licencias de Terminal Server se encuentra en éste mismo equipo, y permite la instalación de CALs (Client Access Licency).

Los accesos instalados en este servidor son:

- Vehículos.- Contiene información sobre el stock de vehículos.
- Cartera.- Contiene información financiera para la venta de vehículos.
- Materiales.- Contiene información sobre los materiales requeridos en los talleres.

3.1.2.2.3 Servidor SQL

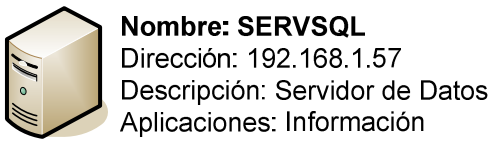


Figura 3.6: Servidor de Base de Datos SQL.

El sistema operativo instalado en este servidor es SQL Server 2000, éste permite gestionar y analizar datos para realizar las operaciones ágilmente.

Las aplicaciones que utilizan SQL son:

- ***Rol de pagos.*** Contiene toda la información relacionada a los salarios de los empleados.

- ***SIG (Sistema de Información Gerencial).*** Permite ejecutar reportes para gerentes, lo cual contribuye con la toma de decisiones en los siguientes ámbitos: Ventas de vehículos y repuestos, Servicio (trabajo en taller) e Inventarios.

- ***Hot Line.*** Es un aplicativo que brinda reportes relacionado a los pickings (repuestos) y OT (orden de trabajo) de la Matriz y de todas las sucursales, para así gestionar las importaciones de repuestos y el trabajo en talleres.

3.1.2.2.4 Servidor Novell

Nombre: NOVELL
Dirección: IPX
Descripción: Servidor Novell
Aplicaciones: Autenticación

Figura 3.7: Servidor de Archivos de Red.

Novell Netware es un sistema operativo de red, usado para establecer los accesos a los archivos compartidos en la red. En la empresa el Servidor Novell maneja los accesos a Vehículos, Materiales, Cartera y Home (datos del funcionario).

Luego de que un usuario se autentica se presentan los siguientes recursos de red:

RECURSO DE RED	ALMACENA	FORMATO	TOTAL	LIBRE
F: (\\QUITO_MOTORS_Q\SYS)	Vehículos Cartera Materiales	NWFS	43107 MB	42 %
G: (\\QUITO_MOTORS_Q\HOME)	Funcionario	NWFS	8410 MB	52 %

Tabla 3.3: Recursos de Red.

3.1.2.2.5 Servidor AS / 400

Nombre: AS / 400
Dirección: 192.168.1.2
Descripción: Servidor de Datos
Aplicación: Información

Figura 3.8: Servidor de Base de Datos AS / 400.

El servidor AS / 400 es un ordenador de IBM, se presenta como un sistema multiusuario con una interfaz controlada mediante menús y comandos CTL (Control Lenguaje), utiliza terminales y un sistema operativo basado en objetos y bibliotecas, trabaja con el sistema operativo OS / 400 y la base de datos DB2 / 400.

Este servidor maneja los siguientes aplicativos:

- Sistema Integrado de Gestión Administrativa (SIGA).
- Información de Taller.
- Información de Repuestos.

3.1.2.2.6 Servidor F-Secure

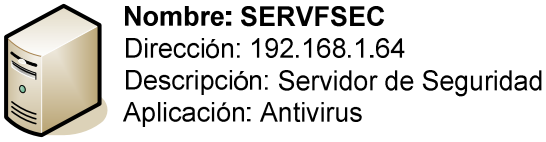


Figura 3.9: Servidor de Seguridad.

Es un computador normal que ejecuta el software F-Secure Policy Manager 6.0, este equipo acoge a todos los usuarios de la red, monitorea su actividad y actualiza el motor antivirus de las estaciones de trabajo donde se tiene instalado F-Secure cliente, para garantizar así su seguridad frente a números tipos de virus, gusanos, intrusos y otras amenazas.

3.1.2.2.7 Servidor Mail

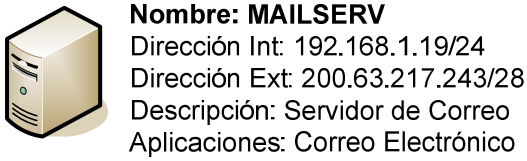


Figura 3.10: Servidor de Correo.

Es un servidor de correo electrónico con soporte LDAP desarrollado en la plataforma Linux, que permite manejar el correo electrónico interno de la organización y acoplarse con servidores de correo electrónico externos a la empresa.

3.2 SERVICIOS, PROTOCOLOS Y APLICACIONES DE LA RED LAN / MAN / WAN

3.2.1 SERVICIOS DE RED

La red Quito Motors ofrece servicios a nivel LAN / MAN / WAN de impresión, archivos y aplicativos, mediante el establecimiento físico (enlaces) y lógico (protocolos de red) de la red.

Otro servicio es el Internet a nivel LAN / MAN / WAN, logrado mediante la interconexión de las diferentes sucursales y la provisión centralizada de este servicio a través del dispositivo WatchGuard que actúa como un servidor Proxy y ejecuta NAT.

3.2.2 PROTOCOLOS DE RED

A continuación se presenta una tabla con los principales protocolos y tecnologías que utiliza la red Quito Motors:

CAPA	TECNOLOGÍAS Y PROTOCOLOS	SERVICIO
Nivel de aplicación	DNS	Resolución de nombres
	FTP	Descargar archivos
	HTTP	Navegación web
	HTTPS	Navegación web segura
	IMAP	Acceso al correo electrónico
	NFS	Acceso a archivos distribuido
	POP3	Acceso al correo electrónico
	SMB / CIFS	Compartir archivos e impresoras
	SMTP	Transferir correo electrónico
Nivel de presentación	ASN.1	Trabajo con dispositivos IBM
Nivel de Sesión	NETBIOS	Recursos básicos de red
	ONC RPC	Establecer sesiones remotas
	DCE / RPC	Establecer sesiones remotas
Nivel de Transporte	TCP	Transmisión de cadenas de datos

	UDP SPX	Transmisión de unidades de datos Transmisión de cadenas de datos
Nivel De Red	IP IPX	Asignar dirección de Red IP Asignar dirección de Red IPX
Nivel de Enlace	Ethernet Frame Relay ATM Wi-Fi Inalámbrica	Redes LAN Redes WAN Redes WAN Redes W-LAN Redes W-MAN
Nivel Físico	Cable de Fibra Óptica Cable de par trenzado Inalámbricas	Redes LAN / MAN / WAN Redes LAN Redes LAN / MAN

Tabla 3.4: Tecnologías y Protocolos utilizados en la red Quito Motors.

3.2.3 APLICACIONES DE RED

3.2.3.1 Microsoft Office

Constituye un paquete de software que permite realizar el trabajo funcional de la empresa, mediante diferentes herramientas como: Word, Excel, Outlook y PowerPoint.

3.2.3.2 Solomon

Constituye una solución para negocios de Microsoft y consiste en un conjunto de herramientas de software que sirven para el procesamiento de información e integración de datos financieros críticos; permite cinco sesiones para acceder concurrentemente a la información de todo el negocio.

Este paquete de software es utilizado para llevar la contabilidad de toda la empresa, realizar desde la cotización hasta la facturación y consultar artículos, disponibilidad, crédito, etc.

Entre sus características se tiene:

- Módulo central integrado a todas las áreas.

- Estados financieros parciales para cualquier día del mes.
- Prorrateo automático, pólizas recurrentes, consolidación bancaria.
- Administración de efectivo.
- Integración de flujos de efectivo.
- Cuentas por cobrar.
- Administración integral de la cartera.
- Integración con ventas y contabilidad.
- Cuentas por pagar.
- Administración integral de proveedores.
- Cheques, programación de pagos, compras.

3.2.3.3 Fox Pro 2.6

Fox Pro 2.6 es un lenguaje de programación que corre en MS-DOS, MS Windows, Mac OS y UNIX; Foxito[4] es una aplicación desarrollada en este lenguaje de programación, mediante la cual se puede brindar accesos (lectura, escritura y ejecución) a los sistemas de Vehículos, Cartera, Materiales, Clientes y Activos Fijos.

3.2.3.4 Sistema Integrado de Gestión Administrativa (SIGA)

Es un aplicativo que corre en la plataforma SQL y permite obtener informes gerenciales de las áreas de Taller y Repuestos.

3.3 ACCESOS

3.3.1 ACCESO AL INTERNET

Para el acceso a Internet se cuenta con un canal dedicado (clear channel) con capacidad de 1024 / 1024 Kbps contratado con el ISP Satnet, este canal se enlaza al puerto externo del dispositivo WatchGuard y brinda el servicio de Internet a toda la empresa.

---

[4] **Foxito.** Es una aplicación desarrollada por el Ing. Washington Pérez, jefe del Departamento de Sistemas – Quito Motors.

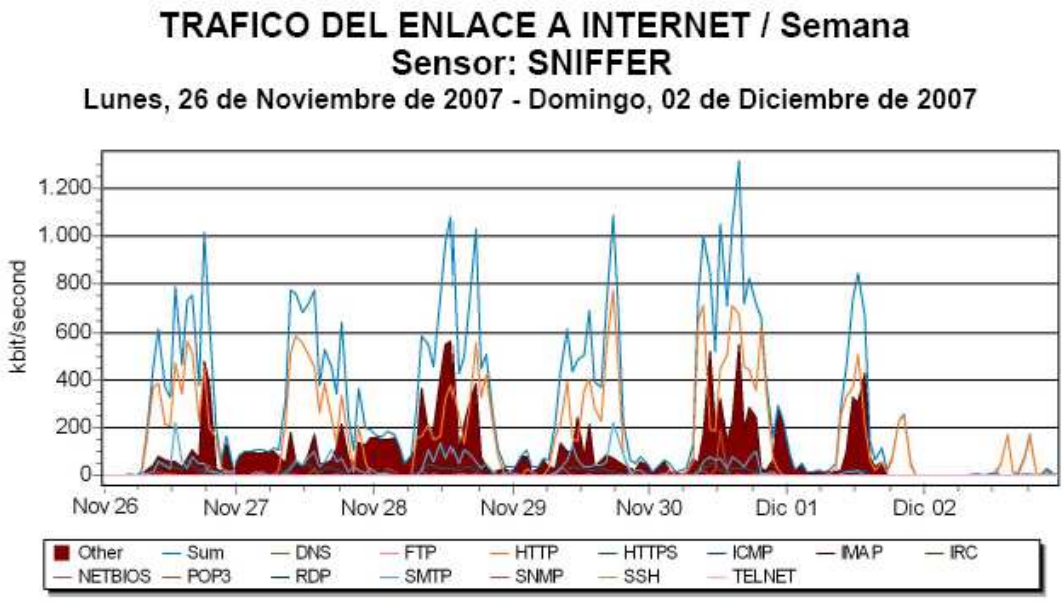


Figura 3.11: Tráfico de Internet.

De acuerdo a la figura la capacidad actual del canal es adecuada, ya que no hay saturaciones en el enlace; también muestra el comportamiento en el uso del Internet, siendo el viernes el día de mayor uso del canal. Adicionalmente se muestra a continuación en detalle el uso del ancho de banda por protocolo.

Toplist

	04/12/2007 9:00:00 - 04/12/2007 9:15:00		
	Channel	Volume	Trend (100%)
1	Other	69 megabytes	
2	HTTP	57 megabytes	
3	SMTP	3706 kbytes	
4	HTTPS	2344 kbytes	
5	POP3	1358 kbytes	
6	DNS	405 kbytes	
7	ICMP	146 kbytes	
8	NETBIOS	124 kbytes	
9	FTP	1134 bytes	
10	SSH	124 bytes	

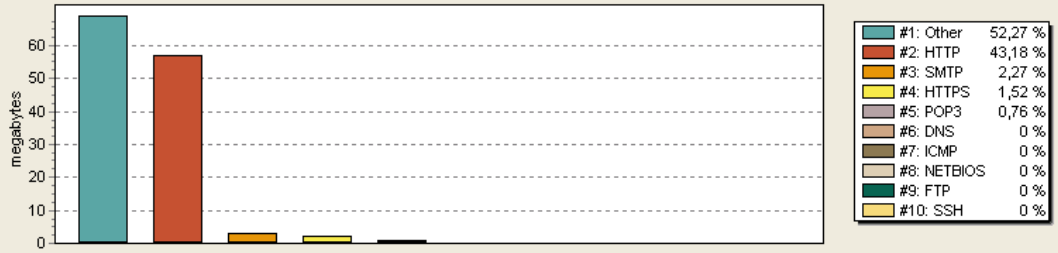


Figura 3.12: Estadística de los protocolos.

3.3.2 ACCESO A SUCURSALES

El acceso hacia Quito Motors – Matriz por parte de las sucursales Quito Motors – Granados, Quito Motors – Norte, Autocn – Quito y Autoexpress se establece mediante un enlace inalámbrico a nivel MAN; se usan las antenas instaladas en cada una de las sucursales mencionadas y una antena repetidora en el cerro Pichincha (propiedad de Quito Motors) para establecer los enlaces que cuentan con una capacidad de 512 Kbps para las sucursales y 1024 Kbps para el enlace entre Quito Motors – Matriz y el cerro Pichincha; la antena ubicada en la Matriz se conecta al puerto 5 del SWCISCO.

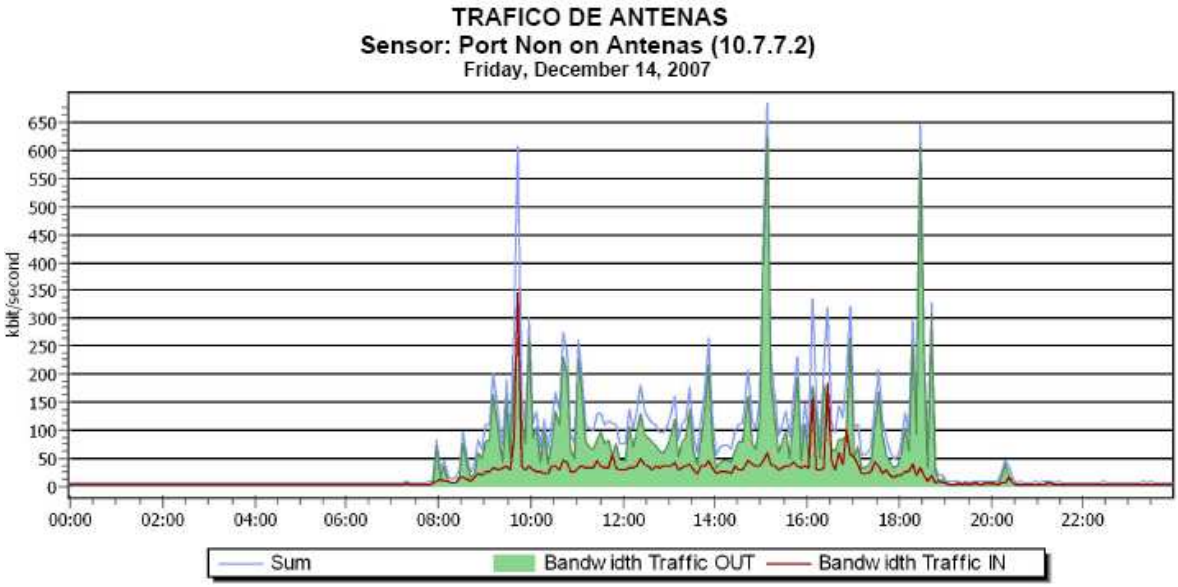


Figura 3.13: Tráfico de la antena ubicada en Quito Motors - Matriz.

De acuerdo a la figura la capacidad del canal es suficiente e incluso puede soportar mayor carga de tráfico (crecimiento futuro), ya que el pico es 680 Kbps y el canal tiene 1024 Kbps de capacidad, lo que le permite un crecimiento de 33.59%.

El acceso hacia Quito Motors – Matriz por parte de las sucursales Quito Motors – Condado y Quito Motors – Cuenca Sur se establece mediante un enlace ATM contratado con la empresa Ecuaonline, con capacidad de 128 Kbps para Quito Motors – Condado y 512 Kbps para Quito Motors – Cuenca Sur; el router ECUAONLINE ubicado en Quito Motors – Matriz se conecta al puerto 17 del SW3COM1.

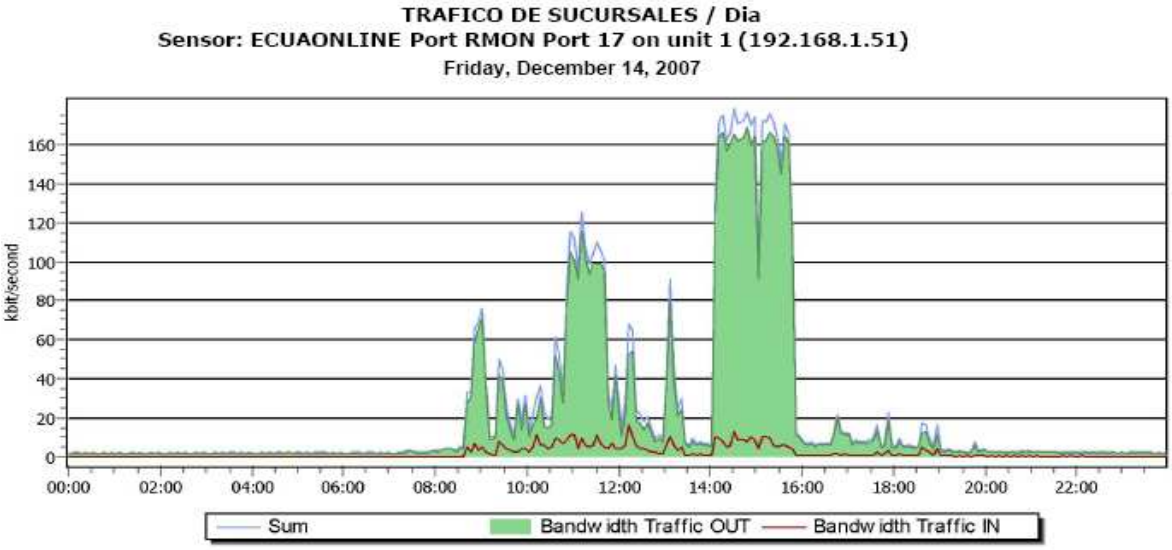


Figura 3.14: Tráfico del router ECUAONLINE.

De acuerdo a la figura el uso de la red por parte de estas sucursales es bajo, ya que el pico es 175 Kbps y en total se puede tener hasta 640 Kbps, por lo que se está ocupando el 27.34%.

El acceso hacia Quito Motors – Matriz por parte de las sucursales Quito Motors – Cuenca, Quito Motors – Ambato, Quito Motors – Ibarra, Quito Motors – Santo Domingo y Quito Motors – Riobamba se establece mediante un enlace Frame Relay contratado con la empresa Suratel, con capacidad de 384 Kbps para cada sucursal; el router QMCENTRAL ubicado en Quito Motors – Matriz se conecta al puerto 16 del SWCISCO.

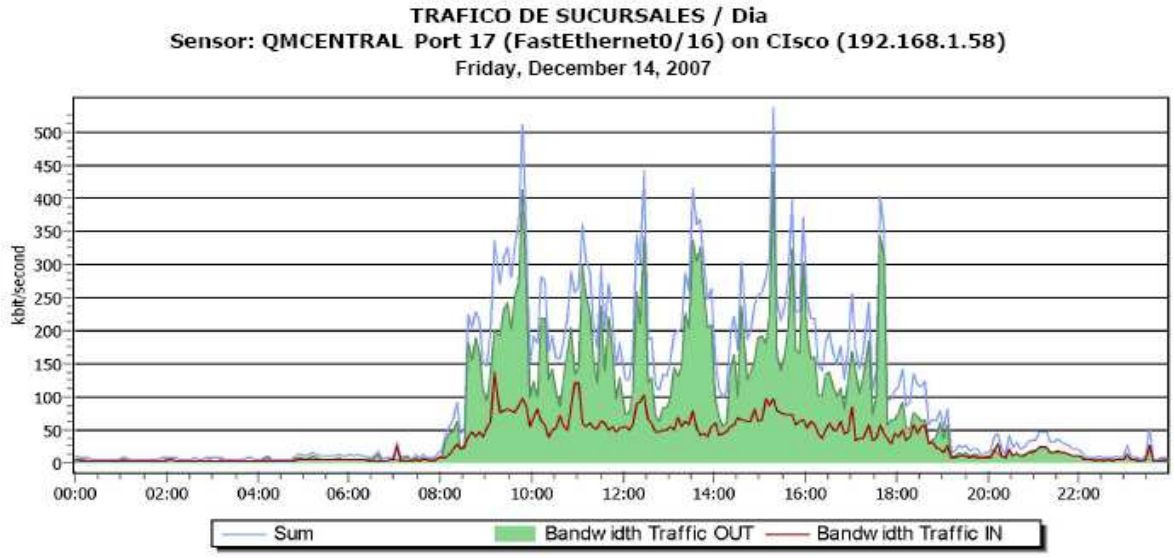


Figura 3.15: Tráfico del router QMCENTRAL.

De acuerdo a la figura el uso de la red por parte de estas sucursales sigue un patrón similar durante el horario de trabajo; además indica que la red está siendo utilizada a un 27.96%, ya que el pico es 537 Kbps y en total se puede tener hasta 1920 Kbps.

El acceso hacia Quito Motors - Matriz por parte de la sucursal Suecia Motors – Guayaquil se establece mediante un enlace Frame Relay contratado con la empresa Suratel, con capacidad de 384 Kbps; el router UIO – GYE ubicado en Quito Motors – Matriz se conecta al puerto 8 del SWCISCO.

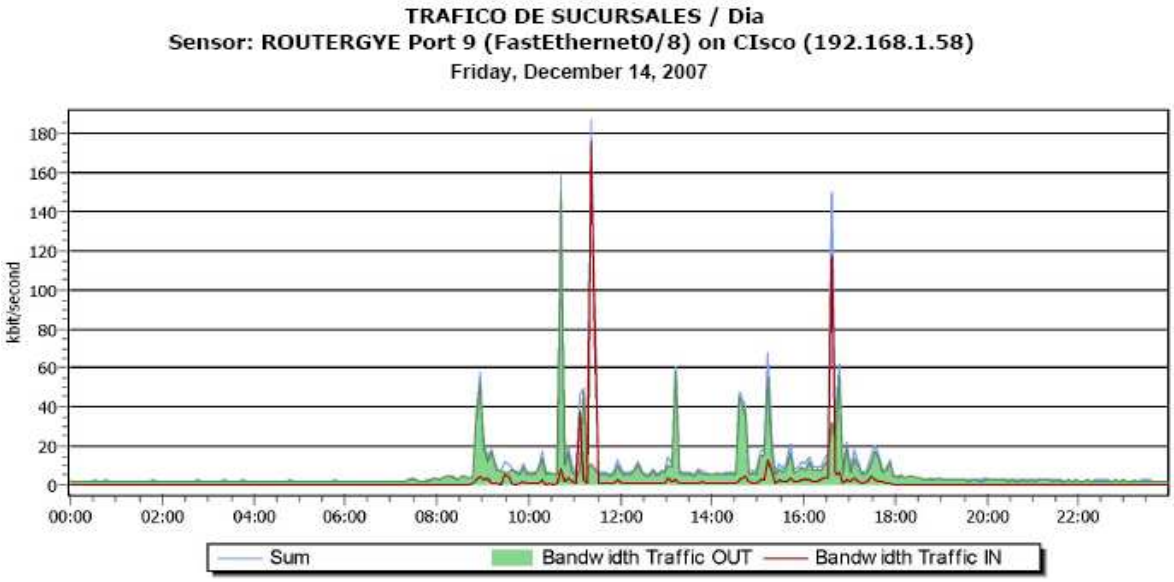


Figura 3.16: Tráfico del router UIO - GYE.

De acuerdo a la figura este canal presenta una demanda esporádica del ancho de banda; siendo el mayor pico 185 Kbps, lo que da un 48.17% de utilización del total posible 384 Kbps.

El acceso hacia Quito Motors – Matriz por parte de las sucursales MerquiAuto – Riobamba, Quito Motors – Usados y Quito Motors – Latacunga se establece mediante enlaces ADSL contratados con la empresa Andinadatos, con capacidad de 256 Kbps para MerquiAuto – Riobamba, 64 Kbps para Quito Motors – Latacunga y 128 Kbps para Quito Motors – Usados; el dispositivos ANDINADATOS se conecta al puerto 45 del SW3COM1.

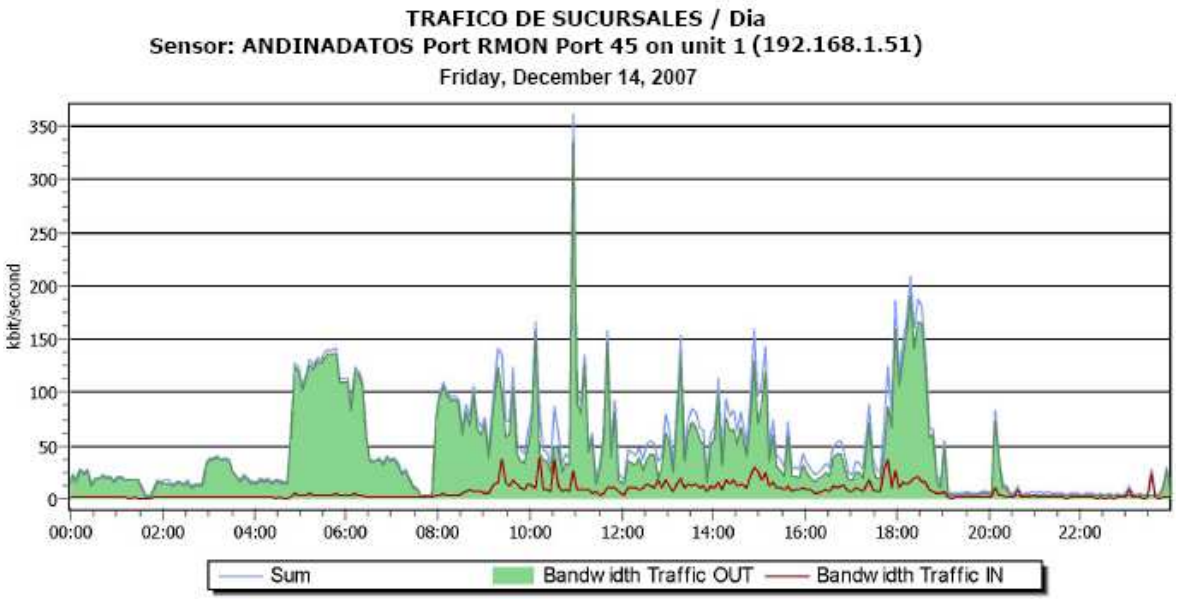


Figura 3.17: Tráfico del dispositivo ANDINADATOS.

De acuerdo a la figura este canal presenta una demanda similar del ancho de banda de 210 Kbps y un pico de 360 Kbps; así este enlace presenta un 80.35% de utilización del total posible 448 Kbps.

3.4 ADMINISTRACIÓN DE LA RED

La red Quito Motors carece de sistemas que permitan la administración y el monitoreo de la red, es decir no cuenta con herramientas que faciliten la presentación y el análisis de logs a fin de conocer sobre la existencia, cambios, errores en el sistema o modificaciones del hardware y software; también carece de herramientas que permitan administar de forma eficiente los asuntos relacionados con el Departamento de Sistemas en cuanto a componentes, usuarios y actividades de la red.

El mantenimiento de las máquinas es realizado manualmente por la empresa Asisnet y el personal de Sistemas, pero estas operaciones son muy precarias por lo que no cubren las expectativas requeridas por los usuarios y responsables de este campo; es así que no existe un adecuado mantenimiento y chequeo de elementos como cableado estructurado, elementos activos, servidores, computadores y demás dispositivos que integran la red.

3.4.1 GESTIÓN DEL SOFTWARE

La instalación del software para computadoras se realiza de forma manual e independiente en el departamento de sistemas; la información sobre licencias, paquetes, aplicaciones y otros, se ingresa manualmente en un archivo de Excel, ésto hace que las operaciones en el departamento de sistemas sean muy lentas, ya que se trata de una red grande que provoca una administración compleja.

3.4.2 GESTIÓN DEL HARDWARE

Los dispositivos son registrados manualmente en un archivo de Excel, pero debido al crecimiento experimentado por la empresa en los últimos tiempos, esta información presenta muchas deficiencias debido a la falta de actualización.

Cuando un dispositivo presenta deficiencias, es trasladado hasta Quito Motors – Matriz al departamento de sistemas, para ser revisado, arreglado o desechado; por lo general son arreglados o actualizados para luego enviarlos de regreso a su antigua localidad o almacenarlos en bodega hasta que sean requeridos por la organización.

La compra de dispositivos se lleva a cabo luego de la petición del funcionario y la autorización del departamento financiero; y adicionalmente se cuenta con un contrato de mantenimiento preventivo y correctivo con la empresa Asisnet.

3.4.3 GESTIÓN DE USUARIOS

La creación y administración de usuarios está a cargo del Administrador de la red, el mismo que maneja dos modelos de creación de cuentas y perfiles de usuario.

Cuenta:

- Basado en el cargo y sucursal de usuario.
- Basado en el usuario.

Perfil:

- Usuario Administrador.
- Usuario Limitado.

3.4.4 GESTIÓN DE ANTIVIRUS

El sistema de protección que utiliza la red Quito Motors es el antivirus F-Secure que se encuentra instalado en el servidor SERVF – SEC, éste se actualiza periódicamente por Internet de forma automática.

En las máquinas de los usuarios se encuentra instalada la versión cliente del software F-Secure, éstas actualizan sus bases de datos con el servidor SERVF-SEC.

3.4.5 GESTIÓN DEL ESPACIO DE ALMACENAMIENTO

El espacio de almacenamiento se encuentra de la siguiente forma:

- Centralizado en el servidor de archivos NOVELL, en el disco del Administrador y en el servidor SQL.

RECURSO DE RED	FORMATO	TOTAL	LIBRE
F: (\\QUITO_MOTORS_Q\SYS)	NWFS	43107 MB	42 %
G: (\\QUITO_MOTORS_Q\HOME)	NWFS	8410 MB	52 %
E: (\\Jramirez)	NTFS	152625 MB	12 %
K: (\\Servsql)	NTFS	76316 MB	88 %

Tabla 3.5: Recursos de Almacenamiento de la red Quito Motors.

- Individual en cada estación de trabajo con una o dos particiones de disco:
    - Partición C: Sistema Operativo.
    - Partición D: Datos de Usuario.

Debido al manejo centralizado de la información y a las aplicaciones que se manejan en esta red, la capacidad de almacenamiento tanto para sistema operativo como para datos de usuario es suficiente en la actualidad.

3.4.6 MONITOREO DE LA RED

La presente red carece de un sistema que permita el monitoreo y análisis de red, por lo que este trabajo se lo realiza de forma precaria a través de la interfaz de línea de comandos tanto para sistemas Windows como para sistemas Linux; por lo tanto el departamento de

sistemas no cuenta con información sobre los parámetros de funcionamiento de la red, las aplicaciones utilizadas por los usuarios o el conocimiento de forma oportuna sobre la causa de problemas relacionados con los dispositivos que integran la red.

3.5 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES EN LA RED DE DATOS

3.5.1 SEGURIDAD FÍSICA

En Quito Motors – Matriz los principales equipos como la granja de servidores y los dispositivos activos de conectividad que hacen posible la interconexión de red y las operaciones empresariales, se encuentran ubicados en el centro de cómputo, el mismo que cuenta con un sistema de ventilación, un extintor en caso de incendios, un detector de humo y un sistema de acceso protegido por una contraseña.

El centro de cómputo cuenta con un rack que alberga dos patch panels (uno para datos y otro para telefonía) y diferentes dispositivos de conectividad; la capacidad de este rack se encuentra agotada, por lo que el espacio físico en el mismo representa un problema potencial; por esta razón se han implementado dos soportes en la pared para poder ubicar los dispositivos de conectividad restantes y aun así el espacio físico es insuficiente tanto para los dispositivos de conectividad (DTUs y routers) como para los servidores y los UPS.

También existen equipos como los access points, switches y hubs que se encuentran ubicados en diferentes departamentos exentos del control del personal de Sistemas, algunos de éstos se exponen a condiciones extremas en ambientes abiertos, ya que no poseen ninguna seguridad o restricción, por lo que pueden ser objeto de ataques o sufrir daños debido a las condiciones ambientales a las que se exponen principalmente en los Talleres.

El cableado estructurado está implementado de acuerdo a los estándares y recomendaciones ANSI / EIA / TIA, pero presenta falencias en torno a la recomendación de etiquetado en puntos de red, patchcords y patchpanel; además no existe un control y documentación veraz sobre la asignación de puntos de red y puertos de conexión (en switches y hubs) de los diferentes usuarios.

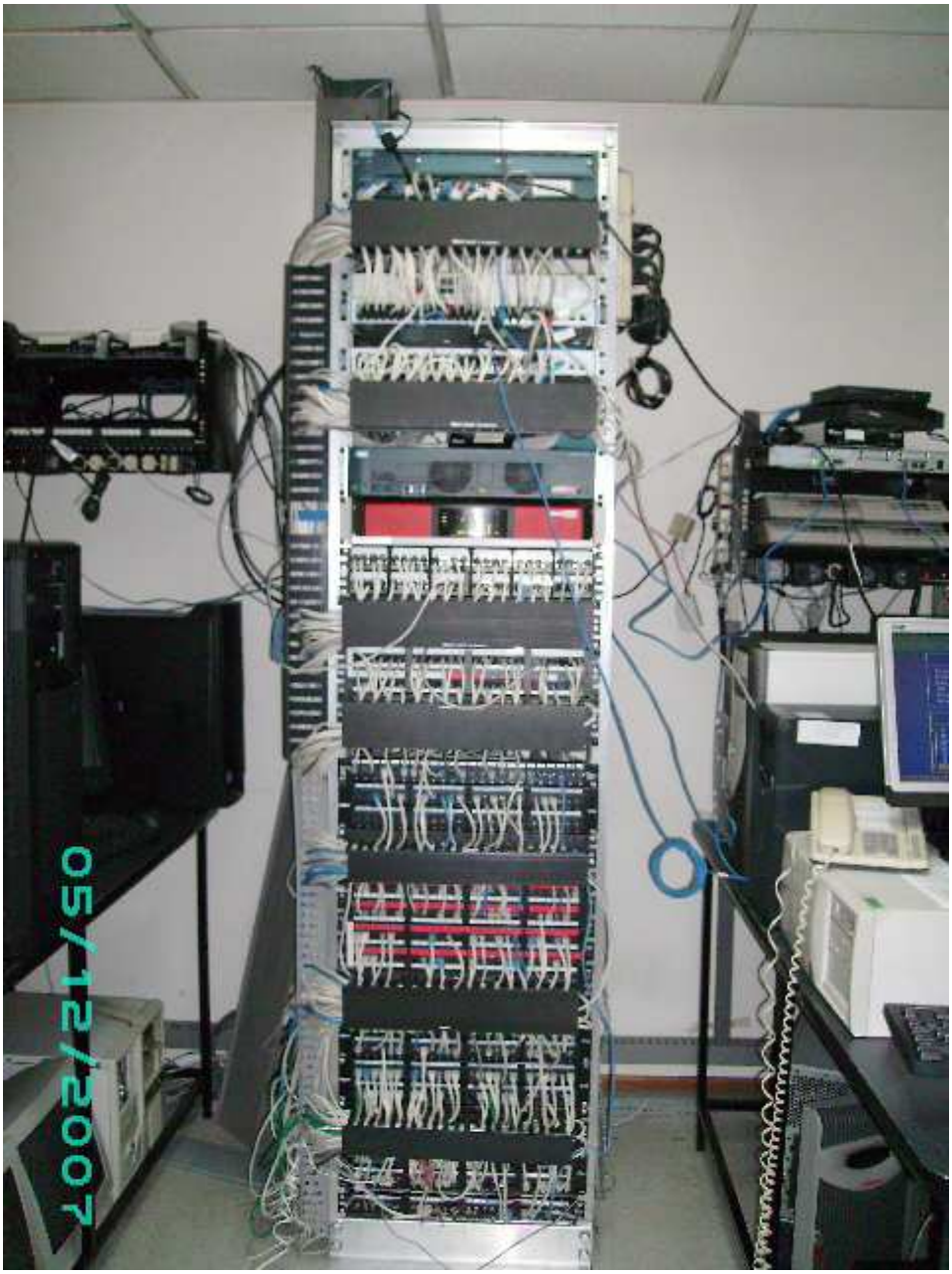


Figura 3.18: Centro de Cómputo

En caso de cortes de energía se cuenta con nueve UPS ubicados en el centro de cómputo, los mismos que abastecen de energía a los dispositivos más críticos de la red como servidores, elementos de conectividad y usuarios importantes; este sistema provee en promedio quince minutos de energía, tiempo en el cual se debe guardar la información y apagar los dispositivos correctamente, la deficiencia en el presente sistema es que este respaldo de energía no cubre íntegramente a todos los computadores de la red LAN de Quito Motors - Matriz.

La empresa cuenta también con una planta generadora de energía eléctrica propia, que entra a funcionar en caso de cortes de energía prolongados, ésta abastece a Quito Motors – Matriz alrededor de 1 hora.

Finalmente Quito Motors – Matriz cuenta con guardias de seguridad, sistemas de alarma que se activan al movimiento y sistemas de control que restringen el acceso a lugares importantes.

Los recursos informáticos importantes como CDs (software) se encuentran almacenados una parte en el centro de cómputo y otra en estantes cerrados en el Departamento de Sistema, las licencias de uso de software se encuentran almacenadas en una bodega de acceso restringido y la información documentada se encuentra almacenada en gavetas de libre acceso en el Departamento de Sistemas.

3.5.2 SEGURIDAD DEL SOFTWARE

El Departamento de Sistemas ha elaborado un documento que posee políticas de seguridad en forma general, en lo que respecta al uso de recursos de red como el espacio de almacenamiento, el acceso a Internet, el correo electrónico, el software de terceros y la propiedad de la información, las mismas que por la carencia de control son incumplidas frecuentemente.

Para el control de amenazas que atenten contra la integridad de la información y el normal funcionamiento de los sistemas se utiliza el sistema antivirus de F-Secure. Esta medida de protección ha permitido controlar gran variedad de amenazas, ya que actualiza sus bases de datos constantemente; sin embargo hubo amenazas que no pudo contrarrestar, las mismas que causaron inconvenientes en algunas máquinas. Adicionalmente hay problemas con máquinas que no están en red y tienen que ser actualizadas manualmente.

Los respaldos de la información se realizan de la siguiente manera:

RECURSO DE RED	FORMATO	TOTAL	LIBRE
F: (\\QUITO_MOTORS_Q\SYS)	NWFS	43107 MB	42 %
G: (\\QUITO_MOTORS_Q\HOME)	NWFS	8410 MB	52 %
M: (\\QUITO_MOTORS_Q\HOME\ACCT\COMMN)	NWFS	8410 MB	52 %
N: (\\QUITO_MOTORS_Q\HOME\ACCT\DB)	NWFS	8410 MB	52 %

O: (\\QUITO_MOTORS_Q\HOME\ACCT\LG)	NWFS	8410 MB	52 %
P: (\\QUITO_MOTORS_Q\HOME\ACCT\PROG)	NWFS	8410 MB	52 %
Q: (\\QUITO_MOTORS_Q\HOME\ACCT\TEMP)	NWFS	8410 MB	52 %
R: (\\QUITO_MOTORS_Q\HOME\ACCT\ESI)	NWFS	8410 MB	52 %
Z: (\\QUITO_MOTORS_Q\SYS\PUBLIC)	NWFS	8410 MB	52 %
E: (\\Jramirez\discos)	NTFS	152625 MB	12 %
H: (\\Jramirez\qmail2)	NTFS	152625 MB	12 %
K: (\\Servsql\Aplicaciones)	NTFS	76316 MB	88 %
L: (\\Servsql\BACKSQL)	NTFS	76316 MB	88 %
S: (\\Servsql\DATA)	NTFS	76316 MB	88 %

Tabla 3.6: Recursos de la red Quito Motors a ser respaldados.

INFORMACIÓN	**ALMACENAMIENTO**	**FRECUENCIA**	**DURACIÓN**
Recurso F: Vehículos y Caja **Recurso G:** Funcionario **AS / 400:** Taller y Repuestos **SERVSQL:** Roll de Pagos y SIG	Disco Externo (40 GB) Cinta	1 día 1 dia	1 día 1 semana
Correo Electrónico Disco de Gerentes	Disco del Administrador (150 GB) Cinta	7 días 7 días	1 semana 1 semana

Tabla 3.7: Respaldos de Información.

La granja de servidores no recibe un mantenimiento adecuado en temas relacionados a la seguridad, ya que no se realiza un control o ajuste adecuado de acuerdo a las necesidades de cada uno de éstos en torno a temas de seguridad; es así que no se ha tomado en cuenta un análisis de las brechas de seguridad para la configuración de los mismos, por lo que funcionan con configuraciones predeterminadas, provocando que los servidores presenten servicios mal configurados (accesos ilimitados) y puertos abiertos innecesariamente.

Para suplir de alguna manera las falencias de los sistemas operativos, en cada servidor se encuentra configurada la actualización automática.

No se realiza un análisis de logs adecuado a fin de estar en conocimiento de las actividades sospechosas que se sucitan en la red, estas revisiones se realizan solamente cuando se presentan problemas graves.

Finalmente el tratamiento de contraseñas establecido para el uso de los recursos de red presenta las siguientes deficiencias:

- ***Creación.*** El esquema que se sigue para la creación de contraseñas no es tan resistente o fuerte, ya que se basa en características del departamento, del cargo, del funcionario o de la fecha; por lo que se presentan como un formato estándar fácil de descifrar al momento de querer romper una contraseña.

- ***Distribución.*** La contraseña es entregada al usuario personalmente (muy seguro), por medio de terceros (seguro / inseguro) y por línea telefónica (muy inseguro).

- ***Conocimiento.*** Todo el Departamento de Sistemas tiene acceso y conocimiento de toda la información que éste maneja, los archivos carecen de contraseñas y la documentación no cuenta con un acceso restringido, por lo que se ve comprometida información sensible como contraseñas y configuraciones.

3.6 DIAGNÓSTICO DE LA SEGURIDAD EN LA RED DE DATOS

Para el diagnóstico de la seguridad en la presente red, se ha utilizado la herramienta de software GFI LANGuard Network Security Scanner[5], la misma que provee la siguiente información:

- Exploración de puertos del sistema.

- Vulnerabilidades encontradas en el sistema.

    - SANS (SysAdmin Audit Network Security).
    - OVAL (Open Vulnerability Assessment Language).

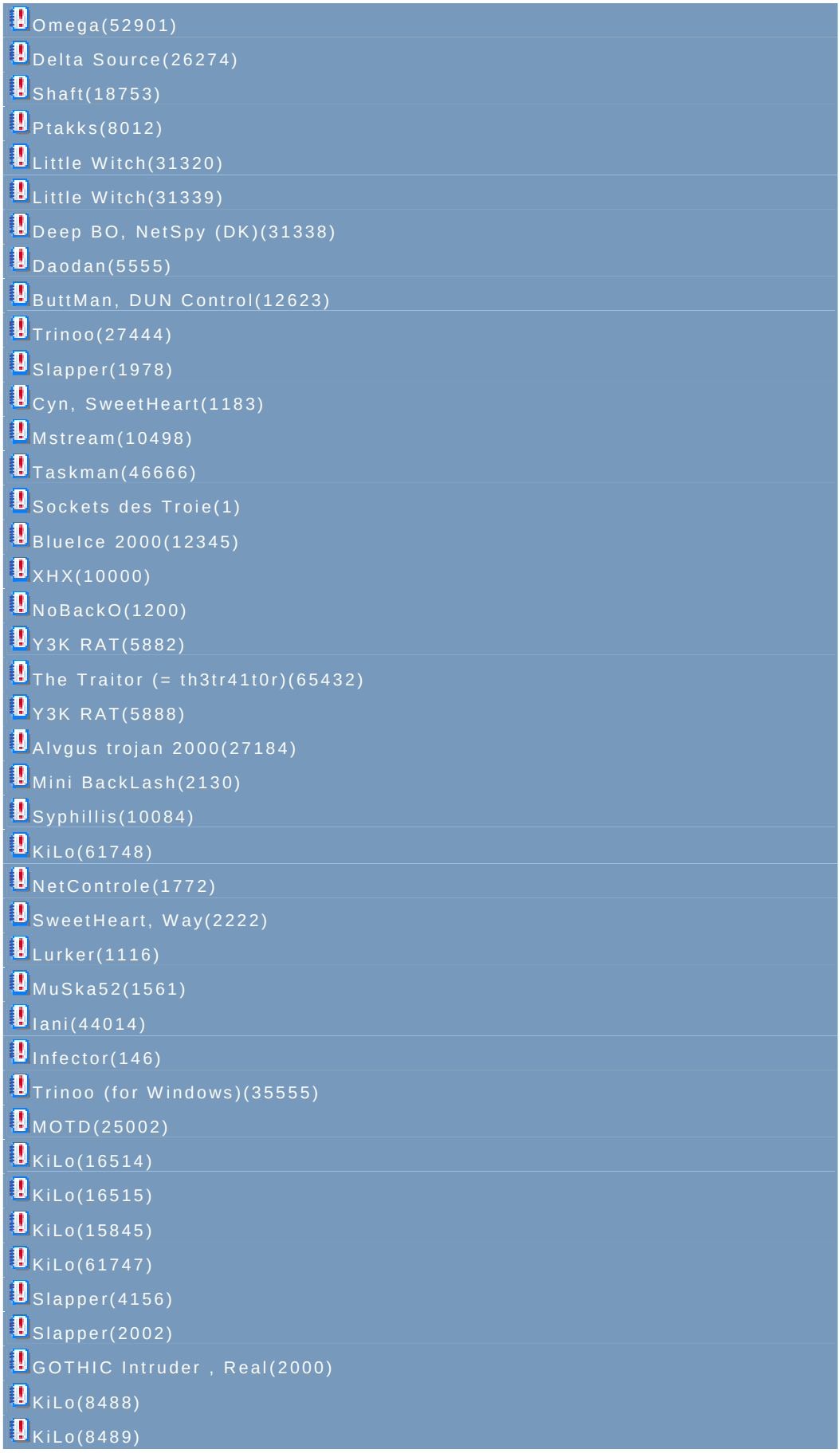
A continuación se presentan las vulnerabilidades más importantes encontradas mediante el software GFI en los principales equipos de la presente red.

DISPOSITIVO: WATCHGUARD

[5] **GFI LANGuard Network Security Scanner:** http://www.gfi.com/lannetscan/

- High security vulnerabilities - 84
  - Backdoors - Open ports commonly used by trojans - 84

Ambush(10666)	top
Remote Anything(3996)	
KiLo(50829)	
Donald Dick(23476)	
Daodan(3333)	
UDP remote shell backdoor server(15210)	
NetSphere(30103)	
Last 2000, Singularity(1122)	
Penrox(80)	
Remote Administration Tool - RAT(2989)	
RedShad(4128)	
School Bus(44767)	
KiLo(49698)	
DarkSky(5419)	
Slapper(10100)	
KiLo(47785)	
Mstream(7983)	
KiLo(43720)	
Hack a Tack(31791)	
KiLo(29589)	
KiLo(6667)	
Lithium(31416)	
KiLo(15486)	
Deep Throat , Foreplay , Mini BackLash(3150)	
Shaft(20433)	
Singularity(7788)	
9_119, Chonker(8127)	
Aphexs Remote Packet Sniffer(8090)	
Fenster(49683)	
Protoss(12321)	
Host Control(7424)	
Trinoo (for Windows)(34555)	
Hack a Tack(31789)	
Mstream(6838)	
Cyn(11225)	
Mstream(9325)	
XHX(3215)	
Black Diver(1985)	
KiLo(6766)	


Omega(52901)
Delta Source(26274)
Shaft(18753)
Ptakks(8012)
Little Witch(31320)
Little Witch(31339)
Deep BO, NetSpy (DK)(31338)
Daodan(5555)
ButtMan, DUN Control(12623)
Trinoo(27444)
Slapper(1978)
Cyn, SweetHeart(1183)
Mstream(10498)
Taskman(46666)
Sockets des Troie(1)
BlueIce 2000(12345)
XHX(10000)
NoBackO(1200)
Y3K RAT(5882)
The Traitor (= th3tr41t0r)(65432)
Y3K RAT(5888)
Alvgus trojan 2000(27184)
Mini BackLash(2130)
Syphillis(10084)
KiLo(61748)
NetControle(1772)
SweetHeart, Way(2222)
Lurker(1116)
MuSka52(1561)
Iani(44014)
Infector(146)
Trinoo (for Windows)(35555)
MOTD(25002)
KiLo(16514)
KiLo(16515)
KiLo(15845)
KiLo(61747)
Slapper(4156)
Slapper(2002)
GOTHIC Intruder , Real(2000)
KiLo(8488)
KiLo(8489)

Delta Source(47262)

KiLo(61746)

Low security vulnerabilities - 3

Services vulnerabilities - 3

Trivial FTP service running

Unrestricted tftp access allows remote sites to retrieve a copy of any world-readable file. You should remove this service, unless you really need it.

Service running: FTP

If this is not a FTP server, the FTP service is most likely unnecessary. FTP is very problematic and insecure service, use HTTP, HTTPS or SFTP instead.

Service running: DNS

If this is not a internet domain name server, the DNS service is most likely unnecessary.

TCP open ports top

21**[Description: FTP, If this service is not installed beware could be trojan: ADM, KWM, WinCrash, The Flu and others / Service: Unknown]**

113**[Description: identd, If this service is not installed beware could be trojan: ADM, Alicia, Cyn, DataSpy, Dosh / Service: Unknown]**

9001**[Description: Cisco XRemote Service / Service: Unknown]**

9000**[Description: Netministrator / Service: Unknown]**

UDP open ports top

520 **[router => Router routed RIPv.1, RIPv.2]**

1512 **[wins => Microsoft Windows Internet Name Service]**

1900 **[ssdp => Simple Service Discovery Protocol]**

61747 **[KiLo]**

2702 **[SMS Remote Control, If this service is not installed beware could be trojan: Black Diver]**

1028 **[LSASS, If this service is not installed beware could be trojan:KiLo, SubSARI]**

1032 **[ismserv.exe, If this service is not installed beware could be trojan:Akosch4]**

1031 **[BBN IAD, If this service is not installed beware could be trojan:Xot]**

1025 **[RPC, Scheduled tasks, If this service is not installed beware could be trojan: KiLo, and others]**

1026 **[Messenger, If this service is not installed beware could be trojan:Remote Explorer 2000]**

1029 **[MSMQ(mqsvc), If this service is not installed beware could be trojan:SubSARI]**

1104 **[HP Lexmark spooler, If this service is not installed beware could be torjan: RexxRave]**

1201 **[dnscache.dll , If this service is not installed beware could be trojan: NoBackO]**

1111 **[WinLogon, If this service is not installed beware could be trojan:Daodan]**

1561 **[MuSka52]**

1042 **[MS Exchange, NTFRS, If these services are not installed beware could be trojan:BLA trojan]**

1044 **[MSNMsgr, If this service is not installed beware could be trojan:Ptakks]**

2001 **[spoolsv.exe, If this service is not installed beware could be trojan: Scalper]**

Computer top

MAC address : 00-90-7F-00-49-CD ("WatchGuard Technologies, Inc.")
Time to live : 64(64)

DISPOSITIVO: AS / 400

192.168.1.2 [ ] Windows 9x

Vulnerabilities - 5 top

High security vulnerabilities - 1

Backdoors - Open ports commonly used by trojans - 1

Chode, Nimda(137)

Low security vulnerabilities - 4

Services vulnerabilities - 4

Service running: FTP

If this is not a FTP server, the FTP service is most likely unnecessary. FTP is very problematic and insecure service, use HTTP, HTTPS or SFTP instead.

Service running: Telnet

If this is not a Telnet server, this service is most likely unnecessary. Telnet is an obsolete and insecure service, use SSH instead.

Service running: POP3

If this is not a POP mail server, the POP3 service is most likely unnecessary.

Service running: SAMBA NMB

TCP open ports top

21**[Description: FTP, If this service is not installed beware could be trojan: ADM, KWM, WinCrash, The Flu and others / Service: Unknown]**

23**[Description: Telnet, If this service is not installed beware could be trojan: ADM, AutoSpY, Pest and others / Service: Unknown]**

110**[Description: Pop3, If this service is not installed beware could be trojan: ADM worm / Service: Unknown]**

139**[Description: Netbios-ssn, If this service is not installed beware could be trojan: Chode, Nimda, Qaz, Fire HacKer / Service: Unknown]**

515**[Description: printer spooler, If this service is not installed beware could be trojan: MscanWorm, Ramen / Service: Unknown]**

137**[Description: Chode, Nimda / Service: Unknown]**

Is trojan port

UDP open ports top

137 **[Netbios-NS => Netbios Name Service]**

138 **[Netbios-DGM => Netbios Datagram Service]**

Computer top

MAC address : 00-06-29-DC-37-BF (IBM CORPORATION)
Time to live : 64(64)
Network role : Server

DISPOSITIVO: MAILSERV

192.168.1.19 [ ] probably Unix

Vulnerabilities - 9 top

Medium security vulnerabilities - 1

Miscellaneous vulnerabilities - 1

SSH server accepts Version 1.x connections

SSH protocol Version 1 has various vulnerabilties, this should be disabled and only version 2 clients should be allowed to connect.

Low security vulnerabilities - 8

Mail vulnerabilities - 1

SMTP server allows relaying

The mail server on this machine is configured to allow email relaying (which allows remote possibly unauthorized users to send emails through it). This configuration is often abused by spammers and hackers to avoid email protection systems. You can configure your server to disable Email Relaying. Consult your mail server manual on how to disable it.

Services vulnerabilities - 7

Service running: HTTP

If this is not an web server, the HTTP service is most likely unnecessary.

Service running: SSH

If this computer is not administered via secure shell, the SSH service is most likely unnecessary.

Service running: SMTP

If this is not a SMTP mail server, the SMTP service is most likely unnecessary.

Service running: HTTPS

If this is not a secure web server, the HTTPS service is most likely unnecessary.

Service running: POP3

If this is not a POP mail server, the POP3 service is most likely unnecessary.

Service running: IMAP4

If this is not an IMAP mail server, the IMAP4 service is most likely unnecessary.

Service running: MySQL

If this is not a database server, the MySQL service is most likely unnecessary.

Potential Vulnerabilities - 5

top

Information based vulnerability checks - 5

Perl module running (web server)

mod_perl is installed on this web server.

PHP module running (web server)

PHP is installed on this web server.

SSL enabled (web server)

SSL is designed to encrypt and thus secure data in transit between a client and a server. However SSL does not eradicate vulnerabilities on the web server. These servers are vulnerable to the same attacks that compromise other non-SSL web servers.

SSL module running (web server)

SSL is designed to encrypt and thus secure data in transit between a client and a server. However SSL does not eradicate vulnerabilities on the web server. These servers are vulnerable to the same attacks that compromise other non-SSL web servers.

IMAP4 server banner provides information to attacker

Imap banners with information such as server versions and types should be omitted where possible. Instead you can change them to something more generic that will hide such information from potential intruders.

TCP open ports

top

22**[Description: SSH, If this service is not installed beware could be trojan: InCommand, Shaft, Skun / Service: SSH (Remote Login Protocol)]**

25**[Description: SMTP, If this service is not installed beware could be trojan: Antigen, Barok, BSE, Nimda and Others / Service: SMTP (Simple Mail Transfer Protocol)]**

80**[Description: HTTP, If this service is not installed beware could be trojan: Bluefire, AckCmd, Nimda and Others / Service: HTTP (Hyper Text Transfer Protocol)]**

110**[Description: Pop3, If this service is not installed beware could be trojan: ADM worm / Service: POP3 (Port Office Protocol 3)]**

111**[Description: SunRPC, If this service is not installed beware could be trojan: ADM Worm, MscanWorm / Service: Unknown]**

143**[Description: imap, If this service is not installed beware could be trojan: ADM Worm / Service: IMAP (Internet Message Access Protocol)]**

389**[Description: LDAP => Light Directory Access Protocol / Service: Unknown]**

443**[Description: Secure HTTP, If this service is not installed beware could be trojan: Slapper / Service: HTTP (Hyper Text Transfer Protocol)]**

3306**[Description: MySQL / Service: Unknown]**

UDP open ports top

111 **[RPC => SUN Remote Procedure Call]**

Computer top

MAC address : 00-19-DB-86-2D-0B ()
Time to live : 64(64)

DISPOSITIVO: COMSERV

192.168.1.80 [COMSERV] Windows NT 4.0

Potential Vulnerabilities - 182 top

Shares - 15 top

TCP ports - 7 open ports top

42**[Description: NameServer => WINS Host Name Server / Service: Unknown]**

135**[Description: epmap => DCE endpoint resolution / Service: Unknown]**

139**[Description: Netbios-ssn, If this service is not installed beware could be trojan: Chode, Nimda, Qaz, Fire HacKer / Service: Unknown]**

3389**[Description: Terminal Services / Service: Unknown]**

1028**[Description: LSASS, If this service is not installed beware could be trojan: DataSpy Network X, Dosh and others / Service: Unknown]**

1031**[Description: InetInfo, If this service is not installed beware could be trojan: KWM, Little Witch, Xanadu, Xot / Service: Unknown]**

1034**[Description: ISA Server(mspadmin), If this service is not installed beware could be trojan: KWM / Service: Unknown]**

UDP ports - 7 open ports top

42 **[Name => Name Server]**
67 **[bootps => Bootstrap Protocol Server]**
68 **[bootpc => Bootstrap Protocol Client]**
135 **[epmap => DCE endpoint resolution]**
137 **[Netbios-NS => Netbios Name Service]**
138 **[Netbios-DGM => Netbios Datagram Service]**
1032 **[ismserv.exe, If this service is not installed beware could be trojan:Akosch4]**

Computer top

MAC address : 00-A0-24-4E-3E-FF (3COM CORPORATION)
Time to live : 128(128)
Network role : PDC (Primary Domain Controller)

DISPOSITIVO: SERVFSEC

192.168.1.64 [SERVFSEC] Windows

TCP ports - 4 open ports top

80**[Description: HTTP, If this service is not installed beware could be trojan: Bluefire, AckCmd, Nimda and Others / Service: HTTP (Hyper Text Transfer Protocol)]**

135**[Description: epmap => DCE endpoint resolution / Service: Unknown]**

139**[Description: Netbios-ssn, If this service is not installed beware could be trojan: Chode, Nimda, Qaz, Fire HacKer / Service: Unknown]**

445**[Description: Microsoft-Ds, If this service is not installed beware could be trojan: Nimda / Service: Unknown]**

UDP ports - 3 open ports top

137 **[Netbios-NS => Netbios Name Service]**

138 **[Netbios-DGM => Netbios Datagram Service]**

445 **[Microsoft CIFS => Common Internet File System]**

Computer top

MAC address : 00-04-75-73-45-FB (3 Com Corporation)
Time to live : 128(128)

DISPOSITIVO: TSSERV

192.168.1.79 [TSSERV] Windows

TCP open ports top

135**[Description: epmap => DCE endpoint resolution / Service: Unknown]**

139**[Description: Netbios-ssn, If this service is not installed beware could be trojan: Chode, Nimda, Qaz, Fire HacKer / Service: Unknown]**

427**[Description: SLP => Service Location Protocol / Service: Unknown]**

3389**[Description: Terminal Services / Service: Unknown]**

1031**[Description: InetInfo, If this service is not installed beware could be trojan: KWM, Little Witch, Xanadu, Xot / Service: Unknown]**

UDP open ports top

123 **[NTP => Network Time Protocol]**

137 **[Netbios-NS => Netbios Name Service]**

138 **[Netbios-DGM => Netbios Datagram Service]**

161 **[SNMP => Simple Network Management Protocol]**

1026 **[Messenger, If this service is not installed beware could be trojan:Remote Explorer 2000]**

1029 **[MSMQ(mqsvc), If this service is not installed beware could be trojan:SubSARI]**

Computer top

MAC address : 00-0C-76-FC-8C-C7 ("MICRO-STAR INTERNATIONAL CO., LTD.")
Time to live : 128(128)

DISPOSITIVO: SERVSQL

192.168.1.57 [SERVSQL] Windows 2000

Potential Vulnerabilities - 4

top

Information based vulnerability checks - 4

Administrator account exists

It is recommended to rename this account

User IUSR_SQLSERV never logged on

It is recommended to remove this account if not used

User TsInternetUser never logged on

It is recommended to remove this account if not used

Microsoft SQL server

Microsoft SQL server is installed on this computer.

TCP open ports

top

80**[Description: HTTP, If this service is not installed beware could be trojan: Bluefire, AckCmd, Nimda and Others / Service: HTTP (Hyper Text Transfer Protocol)]**

135**[Description: epmap => DCE endpoint resolution / Service: Unknown]**

139**[Description: Netbios-ssn, If this service is not installed beware could be trojan: Chode, Nimda, Qaz, Fire HacKer / Service: Unknown]**

427**[Description: SLP => Service Location Protocol / Service: Unknown]**

443**[Description: Secure HTTP, If this service is not installed beware could be trojan: Slapper / Service: Unknown]**

445**[Description: Microsoft-Ds, If this service is not installed beware could be trojan: Nimda / Service: Unknown]**

1433**[Description: Microsoft SQL server, If this service is not installed beware could be trojan: Voyager Alpha Force / Service: Unknown]**

1028**[Description: LSASS, If this service is not installed beware could be trojan: DataSpy Network X, Dosh and others / Service: Unknown]**

1032**[Description: InetInfo, If this service is not installed beware could be trojan: Akosch4, Dosh, KWM / Service: Unknown]**

1030**[Description: MSMQ,inetinfom tpcsvcs.exe, If this service is not installed beware could be trojan: Gibbon, KWM / Service: Unknown]**

UDP open ports

top

137 **[Netbios-NS => Netbios Name Service]**

138 **[Netbios-DGM => Netbios Datagram Service]**

445 **[Microsoft CIFS => Common Internet File System]**

1434 **[ms-sql-m => Microsoft SQL Monitor]**

1029 **[MSMQ(mqsvc), If this service is not installed beware could be trojan:SubSARI]**

Computer

top

MAC address : 00-11-85-11-AC-C9 (Hewlett Packard)
Time to live : 128(128)
Network role : Member Server

Luego de realizadas las pruebas de diagnóstico a los principales sistemas, se descubren diferentes deficiencias que dan como resultado potenciales amenazas para la seguridad de dispositivos importantes; es así que entre las potenciales amenazas al sistema se encuentran:

- Backdoors que constituyen puertos abiertos usados por los troyanos.
- Servicios levantados innecesariamente.
- Puertos TCP / UDP abiertos innecesariamente por donde pueden atacar los troyanos.
- El uso del protocolo SSH versión 1 puede comprometer las conexiones seguras.
- El uso del servicio SMTP se encuentra mal configurado, ya que permite ***e-mail relayin***, posibilitando el uso no autorizado del mismo y exponiéndose así a sufrir un ataque de Third Party E – mail Relay and Spam.
- Acceso a los dispositivos mediante cuentas predeterminadas y con perfil de uso privilegiado.
- Archivos que contienen información sensible compartida en la red de forma predeterminada, permitiendo el acceso y modificación de los mismos a todos los usuarios.
- Cuentas habilitadas que no se encuentran en uso.

Un troyano es una aplicación disfrazada de un programa útil, el ***Servidor*** es el encargado de abrir un puerto en el dispositivo (computador) al que se quiere tener acceso y dejar un puerto a la escucha para poder establecer la conexión; el ***Cliente*** es el programa que se conecta al puerto que el Servidor dejó abierto, éste establece la conexión y solicita usa o daña la información o los recursos del sistema como:

- Lista de las contraseñas que se encuentran en caché (contraseñas que el usuario escribió recientemente).
- Archivos importantes.
- Recursos compartidos.
- Conversaciones en tiempo real.
- Borrar archivos fundamentales, como el archivo COMAND.COM, con lo cual puede dejar al dispositivo víctima sin poder arrancar.
- Desconexión de Internet del equipo remoto.

- Cuelgue del módem.
- Cambio de resolución de la pantalla.
- Contraseñas de la conexión telefónica a redes (contraseña de Internet), etc.

Son utilizados como una herramienta de administración remota, que permite manipular el sistema a distancia, generalmente usada como una herramienta para hackear, permitiendo penetrar a un sistema informático sin acceso autorizado.

De ésta manera cualquier persona con una conexión (pública / privada) puede espiar lo que hace otra persona conectada al Internet o a su red privada.

Además los puertos que se dejan a la escucha generalmente son altos por arriba del número 500 o 1000, para así garantizar que ningún otro programa pueda estar usándolos y se pueda cancelar la conexión del troyano.

Algunos de los síntomas para detectar la presencia de un troyano son:

- Aparición y/o desaparición de archivos.
- Deficiencia en el rendimiento del sistema (lentitud).
- Aparición de archivos temporales sin justificación.
- Bloqueo continuo del PC.
- Reinicio continuo del PC.
- Inicialización / Finalización de programas sin justificación.
- La bandeja del CD se abre / cierra sin motivo alguno.
- El teclado deja de funcionar.
- Actividad en el módem cuando no se está realizando ningún tipo de comunicación.
- El servidor de Internet no reconoce nuestro nombre y contraseña o indica que ya está siendo utilizado, lo mismo sucede con el correo.
- Ejecución de sonidos sin justificación.
- Presencia de ficheros TXT o sin extensión en el disco duro (normalmente en C:\), en los que se puede reconocer palabras, frases, conversaciones, comandos, que se han escrito anteriormente (captura del teclado por parte del atacante).
- Presencia de archivos y/o carpetas con caracteres extraños, como por ejemplo: |î, ìäñòó, càïóñêà; o paths extraños como: %windir%\patch.exe%windir%\.

- Aparición de una ventana con un mensaje tipo: "TE HE METIDO UN TROYANO".

A continuación se presenta los detalles de algunos troyanos:

REMOTE ANYTHING[6]

Name: Remote Anything
Aliases: RA, Backdoor.RA, Remote-Anything
Ports: 1025, 1025 (UDP), 3996, 3996 (UDP), 3997, 3999, 4000
Files: Slave.exe -
Actions: Remote Access
Registers: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\
Notes: Works on Windows 95, 98, ME, NT, 2000 and XP. This is a commercial software and cost $ 49
Country: Written in China
Program: Written in Visual C++

SLAPPER[7]

Es un gusano de red que se propaga en las máquinas Linux que corren el servidor web Apache con OpenSSL habilitado, usando una falla descubierta en las librerías OpenSSL. Este gusano contiene código para crear un ataque de red punto a punto, así las máquinas infectadas pueden ser instruidas remotamente para lanzar una amplia variedad de ataques DDOS (Distributed Denial of Service).

El proceso de enlace trabaja mediante la entrega de la lista de computadoras disponibles a cada computadora, para luego usando la técnica llamada segmentación de broadcast combinada con las funcionalidades de TCP, se asegure que otra computadora en la red reciba el paquete de broadcast, y realice el mismo proceso nuevamente, hasta inundar la red y afectar a todos sus host. Esta técnica puede ser usada para soportar hasta 16 millones de computadoras conectadas simultáneamente.

Su operación básica es similar a la del gusano Code Red que infectó más de 350.000 sitios web que corrían Microsoft IIS (Internet Information Service) en Julio del 2001. Se ejecuta y comienza a escanear las redes clase A en busca de máquinas vulnerables que mantengan

[6] **REMOTE ANYTHING :** http://www.mdsnetworks.co.uk/tr_data/y2759.html

[7] **SLAPPER:** http://www.f-secure.com/v-descs/slapper.shtml

abierto el puerto 80 mediante el servidor httpd; también contiene una puerta trasera en el puerto UDP 2002 y puede ser controlado remotamente con la habilidad de cagar y ejecutar programas en los host infectados, además contiene funcionalidades para ejecutar varios ataques de negación de servicio.

Este gusano se hace visible en el sistema infectado como un proceso llamado ".bugtraq" y los archivos creados en el directorio temporal: /tmp/.uubugtraq; /temp/.bugtraq.c; /temp/.bugtraq.

Una variante es Slapper.B crea un bash scrip en el directorio temporal /tmp/.cinik.go, y un proceso llamado ".cinik" usado para recopilar la información de configuración del sistema que luego es enviada al creador del virus vía mail, éste usa el puerto UDP 1978 para realizar la conexión. Adicionalmente el gusano se añade al archivo **crontab** para poder reiniciarse cada hora en caso de ser terminado.

Otra variante es Slapper.C que utiliza el puerto UDP 4156, crea un proceso "httpd" y el archivo /tmp/.unlock, éste envía direcciones IP de host infectados vía mail al escritor del virus (probablemente).

NIMDA[8]

Nombre técnico:	W32/Nimda
Peligrosidad:	Alta
Alias:	W32/Nimda.A, W32/Nimda@mm, W32/Nimda.A@mm, W32/Nimda.htm, Nimda.htm
Tamaño:	57.344 Bytes
Tipo:	Gusano
SubTipo:	Troyano
Efectos:	Infecta ficheros con extensión EXE, comparte y da acceso a todas las unidades de disco, pudiendo llegar a agotar el espacio libre de las mismas.

Plataformas que infecta: Windows XP/2000/NT/ME/98/95

País origen: CHINA. (Según MessageLabs, el primer mensaje interceptado con el virus, provenía de Corea).

[8] **NIMDA:** http://www.vsantivirus.com/nimda-desinf.htm

Nimda es un gusano peligroso, altamente contagioso y difícil de reconocer; afecta los siguientes ámbitos:

- *Páginas web:* aprovecha la vulnerabilidad Web Directory Traversal Exploit de los servidores web IIS, modificando las páginas escritas en lenguaje HTML, incluyendo un script en las mismas.

- *Mensajes de correo electrónico:* con un fichero adjunto llamado README.EXE. Nimda aprovecha una vulnerabilidad del navegador Internet Explorer (versiones 5.01 y 5.5), que le permite realizar su infección con la simple visualización.

- *Redes de ordenadores basadas en el sistema operativo Windows 2003/XP/2000/NT/Me/98/95*, en las que Nimda es capaz de compartir unidades de disco y propagarse a todas ellas. Proporciona acceso a todas las unidades de disco locales (Windows 2003/XP/2000/NT) y todas las unidades de disco disponibles (Windows Me/98/95) compartidas en una red informática.

- Infecta todos los ficheros con extensión EXE que encuentra y se activa cuando el usuario abre los programas Word y Wordpad.

Explota las siguientes vulnerabilidades:

- Vulnerabilidad que afecta al navegador Internet Explorer, versiones 5.01 y 5.5, que permite la ejecución automática de los ficheros adjuntos de los mensajes de correo.

- Vulnerabilidad que afecta a los servidores web IIS, llamada Web Directory Traversal Exploit. Nimda emplea esta vulnerabilidad para modificar las páginas web albergadas en dichos servidores, de modo que cuando un usuario las visite, quede afectado por Nimda.

- Comparte todas las unidades de disco disponibles, y se propaga a todas ellas. Para conseguirlo, crea un nuevo usuario (guest) en los ordenadores con Windows 2003/XP/2000/NT. La creación de este usuario le permite a Nimda compartir las unidades de disco disponibles, sin asignar ninguna contraseña en ordenadores con Windows Me/98/95.

- Nimda crea los siguientes ficheros:

  RICHED20.DLL en el directorio de sistema de Windows y se activa siempre que se trabaja con algún programa que utiliza esta DLL (Word y Wordpad).

  LOAD.EXE en C:\WINDOWS\SYSTEM en Windows Me/98/95, y C:\WINNT\SYSTEM32 en Windows 2003/XP/2000/NT.

  README.EML en C:, el mismo que es una copia del mensaje de correo original, y contiene el fichero README.EXE.

  ADMIN.DLL en C:, D: y E: (si son accesibles); crea una gran cantidad de archivos con extensiones EML y NWS.

  Crea otras copias de sí mismo en el directorio temporal de Windows: MEP*.TMP.EXE o MEP*.TMP.

- Modifica los siguientes archivos:

  MMC.EXE, que es un archivo de la aplicación Management Console Application, en el directorio de Windows.

  SYSTEM.INI, incluyendo en él la siguiente línea: Shell = Explorer.exe Load.exe –dontrunold.

  WININIT.INI, en el que incluye la siguiente línea: NUL = C:\ Windows\ temp\ mep52b0.tmp.exe.

- Modifica las siguientes entradas en el Registro de Windows: HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Advanced\ HideFileExt.

  HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Advanced\ Hidden.

  HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Explorer\ Advanced\ ShowSuperHidden.

- Elimina la siguiente entrada en el Registro de Windows:

  HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services\.

  lanmanserver\ Shares\ Security.

  Con ello desactiva la seguridad de los recursos compartidos en ordenadores con Windows 2000 Pro y Windows NT.

- Para infectar los servidores Web IIS (Internet Information Server), modifica las páginas Web, insertando un script infectado en ellas:

  INDEX.HTML, INDEX.HTM, INDEX.ASP, README.HTML, README.HTM, README.ASP, MAIN.HTML, MAIN.HTM, MAIN.ASP, DEFAULT.HTML, DEFAULT.HTM, DEFAULT.ASP.

- Cuando el usuario abre alguna de las páginas mencionadas, se abre una nueva ventana del navegador en la que se visualizará el archivo README.EML.

- Utiliza los siguientes métodos de propagación: Correo electrónico, Servidores web IIS, Redes de ordenadores con estaciones Windows 2003/XP/2000/NT. Nimda falsifica la dirección que aparece como remitente del mensaje de correo que provoca la infección; envía el archivo infectado ADMIN.DLL a cada servidor IIS vulnerable que encuentra, mediante TFTP, y luego lo ejecuta, localiza el archivo MMC.EXE en el servidor IIS y sobrescribe el contenido de éste con su código de infección (Microsoft Management Console); en ordenadores con Windows 2000 Pro/NT, Nimda crea el usuario “guest” y lo incluye en el grupo de administradores.

- Comparte las unidades de disco como %$ (letra de la unidad de disco compartida) en ordenadores con Windows Me/98/95 comparte todas las unidades de disco disponibles, sin ninguna contraseña de acceso, el objetivo es detectar las unidades compartidas y copiarse en ellas como un archivo de extensión EML.

KILO[9]

Nombre: W32/Kilo

[9] **KILO:** http://www.hacksoft.com.pe/virus/w32_kilo.htm

Alias: Backdoor.Kilo
Tipo: Troyano
Tamaño: 325,120 Kbits
Origen: Internet
Destructivo: SI
Detección y eliminación: The Hacker 5.4.

Descripción: W32/Kilo, es un troyano que permite el acceso remoto y no permitido de un intruso a la computadora infectada, éste utiliza el IRC para comunicarse con su creador, abre los puertos 6711 y 6718 del computador infectado. Cuando se ejecuta se copia a sí mismo en: C:\WINDOWS\SYSTEM\Njgal.exe; además crea la siguiente entrada en el registro para poder ejecutarse en cada reinicio del sistema: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Boot Manager"="C:\WINDOWS\SYSTEM\Njgal.exe". Finalmente crea el archivo Boot.dat, el cual no contiene rutinas maliciosas en C:\WINDOWS\SYSTEM\Boot.dat.

Cuando el troyano se instala queda a la espera de órdenes remotas de su creador, las órdenes podrían realizar las siguientes acciones:

- Enviar información de la computadora y de la red a su creador.
- Editar el registro del sistema.
- Finalizar procesos.
- Manipula los archivos del sistema.
- Descargar Archivos.
- Ejecuta programas.
- Realiza ataques Distribuidos de Denegación de Servicios (DDoS).

Se han descubierto vulnerabilidades ante gusanos y troyanos en los dispositivos de la red, de los cuales se han descrito los más importantes, cabe recalcar que los nuevos troyanos que se lanzan continuamente son variantes de troyanos representativos como NIMDA, SLAPPER, SLAMMER, CODE RED; y adicionalmente que en su funcionalidad son similares los ataques que pueden causar como los descritos en la parte teórica de este proyecto y en los troyanos arriba mencionados.

3.7 REQUERIMIENTOS DE SEGURIDAD

De acuerdo al análisis del sistema realizado en el presente capítulo se considera necesario establecer mecanismos de seguridad para diferentes aspectos, además de contemplar requerimientos generales para incrementar la funcionalidad de la red y prever su crecimiento futuro.

Entre los principales requerimientos descubiertos se tiene:

- Elaboración de políticas de seguridad más detalladas, que se ajusten a los requerimientos del usuario y de la empresa.
- Mecanismos de seguridad que permitan implementar políticas de seguridad puntuales.
- Mecanismos de seguridad que permitan proteger de forma integral al sistema en contra de antiguas y nuevas amenazas ya que éstas evolucionan continuamente.
- Mecanismos de seguridad que permitan brindar protección a datos sensibles e importantes que maneja la empresa, tanto para el almacenamiento como para la transmisión (intranet / extranet) de la información.
- Mecanismos de monitoreo y administración del sistema que permitan tener un conocimiento continuo del estado de la red, analizar problemas y auditar el cumplimiento de las diferentes políticas implementadas.

En los siguientes ítems se detalla más a profundidad los requerimientos del sistema.

3.7.1 FÍSICOS

La empresa Quito Motors posee una protección física aceptable, ya que cuenta con vigilancia las 24 horas, alarmas, cámaras de seguridad ubicadas en lugares específicos y zonas de acceso restringido protegidas por llaves o claves de seguridad. Sin embargo se requiere un control más exhaustivo para lugares específicos como se detalla a continuación:

- En el Departamento de Sistemas se requiere mayor control y seguridad sobre la información documentada que maneja.

- Para los dispositivos ubicados en lugares abiertos se requiere protección contra efectos dañinos del medio ambiente.

- El centro de cómputo ubicado en el Departamento de Sistemas cuenta con un adecuado sistema de protección, la falencia de éste es el espacio físico que actualmente se presenta insuficiente para albergar a los dispositivos existentes; es así que considerando el crecimiento futuro se requiere la adquisición de un rack adicional, además de una mejor distribución y organización de los diferentes dispositivos.

- En lo concerniente al cableado estructurado, se necesita realizar un mantenimiento que permita etiquetar y probar todos los puntos de red existentes.

- Finalmente es necesario implementar una política de respaldo para los principales dispositivos de conectividad del sistema, como switches que constituyen el backbone de la red y routers que permiten la comunicación con las diferentes sucursales.

3.7.2 DATOS

Es necesario proteger de forma integral, eficiente y efectiva los datos del sistema; es así que se requiere tecnologías de seguridad en redes que permitan brindar una protección integral y a profundidad contra las más sofisticadas amenazas que se lanzan a la red mundial continuamente.

Adicionalmente para la seguridad de los datos se requiere mecanismos que permitan implementar aspectos de seguridad como confidencialidad e integridad de la información sensible que maneja la empresa, mediante el uso de herramientas en Hardware o Software que permitan:

- Encriptación / Des – encriptación de la información.
- Trabajar con certificados digitales tanto internamente como externamente.

3.7.3 SOFTWARE

Se requiere desarrollar un plan que permita un control adecuado para los equipos que constituyen el núcleo del sistema, como son los servidores y elementos de conectividad, en

lo relacionado a la seguridad lógica (configuraciones del sistema), actualización de sistema operativo y parches de seguridad.

Además es importante implementar un sistema de administración y monitoreo de red, a fin de determinar continuamente las brechas de seguridad y anomalías presentes en el sistema.

Otro requerimiento urgente es el desarrollo e implementación de un software que permita documentar las tareas administrativas de la red y realizar inventarios del Hardware y Software; ya que se trata de una red considerablemente grande y el trabajo manual que se desarrolla en la actualidad no cubre las expectativas.

También se requiere el desarrollo y establecimiento de una correcta, organizada y fuerte política de contraseñas.

Finalmente se torna necesaria la implementación de un mecanismo que permita deshabilitar el puerto USB, ya que los dispositivos de almacenamiento masivo permiten almacenar y manipular la información libremente.

3.7.4 HARDWARE

Se requiere implementar un dispositivo que brinde adecuada seguridad al sistema en torno a todos los asuntos concernientes a su seguridad; es decir que cuente con los siguientes módulos de seguridad: Firewall, Antivirus, AntiSpyware, AntiSpam, IDS, IPS y VPN.

A fin de mantener una correcta y completa seguridad integral para la presente red y estar preparados para enfrentar las diferentes amenazas de seguridad como virus, spam, spyware, gusanos, mal uso de recursos y demás amenazas que pueden comprometer al sistema.

3.7.5 SERVICIOS

Desarrollo de un sistema de mensajería instantánea propietario para no comprometer la seguridad de la información y de la red al utilizar software gratuito, además un servidor FTP a fin de proveer mayor flexibilidad y funcionalidad al sistema.

CAPÍTULO IV

Diseño del Sistema de Seguridad Perimetral para la red de Quito Motors

4 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE QUITO MOTORS

4.1 PLANTEAMIENTO DEL PROBLEMA

La situación actual en cuanto a temas de seguridad y funcionalidad de la red Quito Motors presenta los siguientes problemas:

La carencia de control frente al acceso a Internet representa el mayor problema de ésta red en la actualidad, problema que se presenta debido a la ausencia de Políticas de Seguridad implementadas en hardware o software, necesarias para establecer un control efectivo; esta situación provoca el uso inadecuado e innecesario de diferentes recursos de Internet, que no contribuyen con el trabajo productivo de los empleados y pueden comprometer diferentes dispositivos de trabajo e información confidencial.

La ausencia de políticas de seguridad que restrinjan el acceso a Internet permite a los funcionarios la libre navegación por la red mundial, exponiendo al sistema a diferentes amenazas como virus, spyware, spam, etc; lo cual puede provocar serios daños en aspectos de seguridad como disponibilidad, privacidad, confidencialidad e integridad.

Los enlaces que proporcionan la conectividad con las diferentes sucursales son provistos por diferentes empresas (carrier), siendo así la información que atraviesa por éstos, vulnerable ante amenazas que comprometan aspectos de seguridad como privacidad, confidencialidad e integridad de los datos; a excepción de los enlaces MAN que utilizan antenas propiedad de Quito Motors, sin embargo ésto no garantiza la seguridad.

Además con el incremento en la demanda de redes LAN inalámbricas, debido a su flexibilidad, se torna preocupante el acceso a la red por parte de personas no autorizadas, por ende se requiere un mayor control de acceso en éstas.

Otro aspecto negativo en la presente red, debido a su crecimiento en los últimos tiempos y complejidad actual, es la deficiencia existente en la administración del sistema en asuntos relacionados con la auditoría y el monitoreo de Hardware, Software, Usuarios, Eventos y Amenazas de Seguridad.

En la actualidad se trabaja con redes clase C, que van desde la red 192.168.1.0 hasta la red 192.168.12.0, las mismas que son asignadas a cada sucursal; siendo la red 192.168.1.0 la más poblada, ésto provoca una deficiencia en el rendimiento de la misma, debido a que todos los equipos de esta red trabajan en un mismo dominio de colisión, por lo que comparten el ancho de banda y el dominio de broadcast; es así que se presenta la necesidad de organizar de mejor manera la distribución y asignación de las direcciones IP.

También resulta preocupante, la situación que enfrentaría esta red ante un desastre que involucre, el daño de los principales dispositivos que constituyen el núcleo del funcionamiento de este sistema, como son los servidores y los dispositivos de conectividad ya que no todos cuentan con los respaldos necesarios.

Finalmente debido a la cantidad de información que maneja esta empresa, y a la necesidad de su distribución y disponibilidad hacia las diferentes sucursales, resulta poco práctico la manera como se realiza en la actualidad ya que dependiendo de la información q se necesite ésta es compartida en la red por el administrador, pero el trámite que ésto conlleva provoca retrasos altamente significativos en las operaciones comerciales que deberían ser ágiles para cumplir con las expectativas del mundo actual.

Para solucionar los problemas presentes en la red Quito Motors se plantean las siguientes soluciones:

- Desarrollar e implementar Políticas de Seguridad que permitan proteger a la red en contra de las diferentes amenazas de seguridad físicas y lógicas, para de esta manera prever posibles incidentes y reaccionar de forma eficiente ante los mismos.

- Implementar los módulos de seguridad necesarios como Firewall, Antivirus, IDS / IPS, VPN, etc, que permitan la ejecución de las políticas de seguridad.

- Usar VPNs (Virtual Private Network) para la transmisión de información importante, tanto para el trabajo dentro de sucursales como entre sucursales y la utilización de mecanismos de cifrado / descifrado para el almacenamiento de la información sensible.

- Establecer un plan de monitoreo, que permita el análisis de los diferentes eventos suscitados en el sistema y desarrollar un software que permita la administración adecuada de los activos que maneja el Departamento de Sistemas.

- Desarrollar un plan que permita la adecuada organización y asignación de los diferentes dispositivos, funcionarios y direcciones IP; para lo cual se contempla la creación de VLANs, que permitan separar los diferentes departamentos y así balancear el tráfico de redes saturadas.

- Elaborar un plan de contingencia para los principales dispositivos que hacen posible el normal funcionamiento operacional de la empresa.

- Finalmente se plantea la implementación de un servidor FTP y un servidor HTTP que permitan, almacenar y presentar la información que requiere estar disponible para los usuarios de las diferentes sucursales y de Internet, con sus respectivos niveles de seguridad.

Todas estas contemplaciones serán hechas desde el punto de vista actual y con miras a un crecimiento futuro proyectado a diez años.

4.2 POLÍTICAS DE SEGURIDAD PARA LA RED DE DATOS

Las políticas de seguridad constituyen una valiosa herramienta para la correcta administración y control de los sistemas informáticos, ya que permiten desarrollar procedimientos y documentos que describen:

- La administración correcta de los recursos del sistema.
- Las responsabilidades y derechos de los usuarios del sistema.
- Los activos del sistema que se van proteger.
- Las amenazas de las que se va ha proteger al sistema.
- La auditoría y actualización continua del sistema de seguridad.
- La importancia de la seguridad en el sistema.

Estas políticas se desarrollan para cubrir las necesidades de seguridad desde varios ámbitos como la prevención, detección y recuperación; de esta manera se establecen reglas, responsabilidades y procedimientos a seguir para minimizar los riesgos existentes sin interrumpir el normal y adecuado funcionamiento del sistema en general.

4.2.1 OBJETIVOS

El desarrollo y creación de las políticas de seguridad sirve para:

- Identificar los riesgos que enfrenta la organización.
- Desarrollar medidas preventivas y de recuperación que permitan minimizar los daños frente a incidentes.
- Elaborar y dar a conocer de manera formal las políticas y procedimientos.
- Asignar responsabilidades para asegurar la reanudación de las operaciones luego de un incidente.
- Cumplir con regulaciones para desligar de responsabilidades judiciales a la organización.

4.2.2 JUSTIFICACIÓN

Debido a la naturaleza comercial de organización en estudio, se descubre que los principales aspectos o elementos de seguridad a considerarse son:

- ***Disponibilidad***, debido a que los procesos operacionales son centralizados y requieren su ejecución eficiente de manera que se cumplan las expectativas y necesidades operacionales tanto de empleados como de clientes.

- ***Integridad y Confidencialidad***, debido a la sensibilidad de la información (económica, empresarial, personal y de productos) que se maneja, ya que constituye información de carácter privado, que en caso de revelación sobre todo por parte de las empresas que constituyen la competencia, puede provocar la pérdida de fortaleza de la empresa; además es muy importante la integridad de los datos ya que esta organización maneja negocios que involucran miles de dólares y un cambio en la consistencia de los datos podría provocar pérdidas económicas y toma de decisiones equivocadas.

Las políticas de seguridad son necesarias en esta organización para cubrir los requerimientos de seguridad mencionados y así evitar pérdidas económicas, degradación de la confianza y prestigio de la organización y pérdida de clientes o negocios, por no tener

un sistema funcional y seguro. Además son necesarias para brindar protección adecuada al activo informático más importante en la actualidad, la información y el conocimiento.

Si el sistema no cuenta con políticas que establezcan seguridades lógicas y físicas adecuadas no se puede garantizar la seguridad de los usuarios, equipos e información; además éstas son necesarias para saber, cómo actuar frente a una posible conmoción en el sistema y así retornar a un normal funcionamiento lo más pronto posible.

La carencia de políticas puede causar el deficiente o mal funcionamiento del sistema ya que no existen estándares y procedimientos expresamente documentados y publicados que obliguen la procedencia correcta por parte de los usuarios en lo referente a la funcionalidad y seguridad del sistema.

4.2.3 ALCANCE

La creación de políticas y desarrollo de procedimientos permitirá establecer un sistema más confiable y funcional; pero los detalles de los procedimientos que involucra la creación y ejecución de las políticas de la organización, se revelarán el momento que se desarrollen e implementen los mecanismos de protección en la práctica, ya que determinarán las especificaciones necesarias para cada ámbito que involucre la política en cuestión.

4.2.4 RESPONSABLES

Para que las políticas de seguridad alcancen el éxito deseado es necesario definir las personas responsables de cada actividad y confirmar su correspondiente conocimiento y aceptación en el apoyo de las mismas.

Para la presente organización se definen los siguientes grupos de personas involucradas en este propósito, destinadas a desarrollar, acatar y cumplir o hacer cumplir las políticas de seguridad.

- ***Altos Directivos*** (Gerentes y Jefes de Departamentos), ya que es vital contar con su apoyo para establecer medidas preventivas y de recuperación para el sistema.

- ***Departamento de Sistemas*** (Jefe y Personal), ya que es el organismo encargado de llevar a cabo el procedimiento de investigación, desarrollo, implementación y control de las políticas de seguridad.

FUNCIONES PARA EL DEPARTAMENTO DE SISTEMAS	
Persona	**Actividad**
Jefe	Delegar tareas de elaboración, ejecución y actualización
	Establecer plazos y metas de ejecución
	Supervisar el avance
Asesor	Trabajar con el equipo de seguridad
Administrador	Elaborar y actualizar las políticas
	Liderar actividades de prevención y recuperación
	Dirigir mecanismos de actualización
Asistentes	Elaborar y actualizar las políticas
	Controlar (supervisar y monitorear) el cumplimiento

Tabla 4.1: Planificación para el establecimiento de las Políticas de Seguridad.

Usuarios del sistema de la empresa Quito Motors S.A.C.I en general, ya que son las personas responsables del acatamiento (conocimiento, aceptación, predisposición y ejecución) de las normas de seguridad en lo que respecta a la correcta utilización de los recursos IT; es necesario el trabajo en conjunto de toda la empresa para el cumplimiento de las políticas de seguridad y por ende el alcance de los objetivos planteados, para así obtener beneficios del establecimiento y ejecución de éstas en el sistema.

4.2.5 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad son medidas que se toman para establecer los procedimientos adecuados en pro de mejorar la seguridad del sistema; mediante la ejecución de auditorías y monitoreo se puede buscar cambios y adaptaciones requeridas, para conocer el grado de riesgo y verificar el cumplimiento de las normas de seguridad, así se puede determinar si es necesaria la actualización de los procedimientos de seguridad.

Estas medidas deben ser el resultado del consenso entre usuarios y administradores del sistema, en pro de minimizar los riesgos de seguridad asociados con el trabajo cotidiano que involucra a la Tecnología de la Información.

4.2.5.1 Seguridad Lógica

Mediante la seguridad lógica del sistema se establece que el acceso a los archivos, datos y programas sólo se permita a personal expresamente autorizado, ésta involucra los siguientes puntos:

- Uso de software y sistemas.
- Protección de los datos, procesos y programas.
- Acceso ordenado y autorizado de los usuarios a la información.
- Prevención y seguimiento de errores en los procesos.

4.2.5.1.1 Control de acceso

- ***Identificación***.

1. Implementación de una herramienta para el control y administración del acceso a los datos, procesos y programas.
2. Elaboración de un documento formal (política de seguridad) para el control de acceso, detallando el nivel de confidencialidad y sensibilidad de los datos, el procedimiento para la obtención de cuentas (claves) de acceso al sistema y los estándares a seguir para la identificación y autenticación de un usuario.
3. La activación de una cuenta (acceso) para dar de alta a un usuario, requiere de un procedimiento formal por escrito que regule y exija el ingreso de los siguientes datos:
    - Identificación del usuario (único).
    - Contraseña.
    - Nombres y Apellidos completos.
    - Cargo que desempeña.
    - Grupo de usuarios al que pertenece.
    - Fecha de creación de cuenta.
    - Fecha de expiración de la contraseña.

- Autorizaciones y accesos requeridos.

4. Asignación de permisos mínimos, de acuerdo a la función que realiza en el sistema.
5. Ejecución de mecanismos que permitan el monitoreo de los accesos y modificaciones en el sistema.
6. Establecimiento de horarios definidos de acceso.
7. Revisión de las cuentas de usuarios cada mes.
8. Comunicación formal mediante documento escrito o correo electrónico por parte de recursos humanos o jefes de departamento, sobre los cambios asociados con los usuarios y los recursos del sistema; este documento debe contener la información necesaria para reflejar los cambios realizados en el sistema de forma adecuada.
9. La desactivación de una cuenta (acceso) para dar de baja a un usuario, requiere de un procedimiento formal por escrito que solicite la disgregación del usuario, para así retirar permisos e información al mismo de forma paulatina (política de desvinculación) dependiendo de la información que disponga; este documento debe detallar la siguiente información:
    - Nombres y Apellidos completos.
    - Motivo del retiro.
    - Fecha de anulación de cuenta.
    - Plazos para la separación del funcionario.
10. Finalización de la sesión interactiva luego de trascurridos cinco minutos, para dar lugar a la ejecución de un procedimiento que solicite la autenticación nuevamente (protector de pantalla con contraseña).
11. Eliminación de perfiles de usuarios genéricos, privilegiados u obsoletos, excepto en casos especiales, sin embargo hay que tratar de minimizar los perfiles privilegiados.
12. Bloqueo de perfiles de usuario que no hayan accedido al sistema por el lapso de un día, salvo excepciones.
13. Disposición de una sola sesión por aplicación desde cada puesto de trabajo o usuario.
14. Asignación de responsabilidades para cubrir el funcionamiento correcto de estas normas.

15. Control periódico de las cuentas para conocer el estado de utilización, accesos de lectura, escritura y/o ejecución realizados sobre la información.

- ***Autenticación***.

La autenticación busca probar la identidad de una persona, y así en función de los resultados permitir o denegar diferentes niveles de acceso al sistema; para ésto se debe ejecutar un proceso con las siguientes características:

1. Desplegar un interfaz de autenticación que:
    a. Solicite el nombre de usuario y permita el ingreso de la información en texto visible, ejemplo: dalulema.
    b. Solicite la contraseña y permita el ingreso de la información en formato ilegible, ejemplo: **********.
    c. No proporcione información confidencial de la organización.
    d. Sea resistente a intentos de desvió o salto (bypass) del proceso de autenticación.
2. Disponer de una aplicación que permita administrar los datos de usuario, para validarlos en el proceso de autenticación.
3. Encriptación de los datos de usuario proporcionados en el proceso de autenticación, ya que tiene que transmitirse por la red para llegar al dispositivo que evaluará la información.
4. Desplegar la siguiente información luego de que el usuario ha logrado su autenticación en el sistema:
    a. Nombre del usuario.
    b. Nivel de acceso.
    c. Fecha y localización de la última conexión.
    d. Cantidad de intentos fallidos.
    e. Observaciones de amenazas de seguridad o anomalías.

- ***Cuenta y contraseña.***

El establecimiento de cuentas y contraseñas debe seguir las siguientes reglas y características:

1. La lógica a seguir para la creación de cuenta y contraseña debe ser documentada.
2. La contraseña del usuario debe seguir las siguientes normas y recomendaciones:
    - Debe contener de 8 – 10 caracteres alfanuméricos.
    - Tiempo de expiración 6 meses.
    - En lo posible no debe estar formada por información característica, como nombre de usuario, organización, cargo o palabras reservadas (características o comunes).
    - Bloquear al usuario luego de cinco intentos de ingreso de contraseña fallidos.
    - El usuario puede modificar su contraseña pero con notificación al administrador y los niveles de seguridad requeridos.

4.2.5.1.2 Asignación de funciones

Las tareas a cargo del personal del departamento de sistemas en lo referente al centro de cómputo y asuntos relacionados con la Tecnología de la Información, deben ser clasificadas y agrupadas en tareas que se puedan asignar al personal encargado de este campo, además planificar la rotación de tareas entre el personal con el objeto de medir el rendimiento y aportación de cada uno en las diferentes funciones.

4.2.5.2 Seguridad de Comunicaciones

La seguridad en comunicaciones involucra la protección y disponibilidad de los datos (información perteneciente a la organización) que se transmiten en las redes LAN / MAN / WAN tanto públicas como privadas para asegurar que la información pueda ser vista o modificada únicamente por individuos, entidades y procesos explícitamente autorizados, es así que se concentra en aspectos de seguridad como: Confidencialidad, Integridad, Control de acceso y Disponibilidad.

4.2.5.2.1 Topología de red

1. Garantizar la transmisión segura de los datos mediante el uso de mecanismos que provean confidencialidad e integridad.
    - Usar mecanismos de cifrado / descifrado.
    - Usar firmas digitales (X.509).

2. Documentar la red mediante diagramas, ubicación e información de importancia.
3. Implementar medios de transmisión alternativos que permitan restablecer lo más pronto posible las comunicaciones ante posibles incidentes, mediante el uso de mecanismos que provean disponibilidad.
    - Utilización de módems para la transmisión sobre la red telefónica pública (PSTN / ISDN).
    - Contratación de enlaces dedicados de respaldo.

4.2.5.2.2 Conexiones externas

1. Las conexiones que vienen desde redes públicas y arrendadas (Internet y sucursales) deben estar bajo un estricto monitoreo y control de las actividades.
    - Definición e implementación de mecanismos y procedimientos más fuertes para la autenticación de las conexiones provenientes de las sucursales e Internet.
    - Uso de encriptación para proteger los datos que se trasmiten por las conexiones remotas.
    - Utilizar protocolos y estándares adecuados para el proceso de autenticación y cifrado / descifrado.
2. Establecimiento del servicio de Internet bajo explícita solicitud de la gerencia o jefe del departamento, previo el conocimiento y aceptación por parte del usuario sobre las políticas de uso correcto de este recurso.
    - Utilizar el recurso para propósitos empresariales.
    - No descargar ni instalar software ajeno a la organización o sin el consentimiento y supervisión del personal encargado de los asuntos IT.
    - No utilizar el recurso para actividades de entretenimiento como descargas (música, video, etc), juegos, chat, navegación improductiva y demás actividades que no corresponden al trabajo operacional del sistema.
3. Realizar la capacitación correspondiente a los usuarios de Internet para concienciar sobre la funcionalidad, riesgos y medidas de seguridad que se deben adoptar para el uso correcto y eficiente de esta herramienta.

4. Ejecución de un monitoreo continuo de todo el tráfico que se intercambian entre la red pública y la red privada.
    - Todo el tráfico debe estar controlado por un dispositivo de seguridad que permita analizar los protocolos y los datos que tansitan por la red, además este dispositivo debe brindar capacidades de filtrado que faciliten el análisis de los eventos suscitados.
    - Prohibir el tráfico que no se encuentre autorizado.
5. Elaborar un documento que describa los servicios y actividades que están permitidos o restringidos a través del Internet, su funcionalidad y los responsables del su uso.
    - No publicar datos personales o empresariales.
    - Especificar el uso de la información monitoreada, para que el administrador pueda ver el contenido del tráfico en circunstancias necesarias, así se declara y establece el derecho para examinar los datos.

4.2.5.2.3 Conexiones inalámbricas

Debido a la gran demanda de redes inalámbricas en la actualidad este medio de comunicación se ha tornado en una amenaza potencial cuando la red inalámbrica no cuenta con las seguridades adecuadas.

- Implementar un mecanismo de control de acceso fuerte, para los usuarios que acceden al sistema vía medios inalámbricos.
- Controlar y monitorear los accesos (identificación, autorización y actividad) al sistema mediante conexiones inalámbricas.

4.2.5.2.4 Configuración lógica de red

La red debe ser organizada respetando aspectos básicos de seguridad como el establecimiento de la separación entre la red interna y la red externa, implementando una configuración que permita establecer el anonimato deseado de la red privada, debido al riesgo que involucran las redes externas.

1. Ocultar la red interna mediante el uso de mecanismos NAT, que permitan salir hacia el exterior usando direcciones públicas; así la red Quito Motors permanece aislada de la red mundial.
2. Establecer que los recursos físicos y lógicos como puestos de trabajo e información confidencial no sean visibles o accesibles para el exterior.
3. Establecer que los recursos necesarios como servidores especiales entren en contacto de forma controlada con redes externas, mediante el uso de mecanismos o dispositivos que permitan ofrecer el servicio y proteger al mismo tiempo (DMZ).
4. Establecer mecanismos que permitan restringir o permitir el uso de aplicaciones, dependiendo de la contribución de las mismas al trabajo empresarial.
    - Restringir: Chat, P2P, Navegación improductiva, etc.
    - Permitir: Navegación productiva.

Ver el anexo B1, para observar los detalles del esquema de seguridad.

4.2.5.2.5 Correo electrónico

1. Creación de cuenta de correo electrónico bajo petición formal.
2. Establecimiento de un procedimiento formal para dar de alta o de baja una cuenta de correo.
3. Interacción con servidores de correo externos y públicos.
4. Uso de diferentes dominios para cada asociación de Quito Motors S.A.C.I.
5. Establecimiento de seguridad para los aplicativos de correo electrónico.
    a. Uso de mecanismos que permitan controlar el spam.
    b. Uso de mecanismos que permitan scanear la información que cursa por el servidor de correo, para el control de amenazas lógicas (virus, gusanos, troyanos, etc).
    c. Uso de mecanismos que permitan realizar un análisis de contenido, para seguidamente aprobar, denegar o poner en cuarentena un correo.
6. Fomentar el reconocimiento de los mensajes de correo electrónico empresarial como documentos formales.

7. Establecer las sanciones pertinentes ante el uso inapropiado del lenguaje.
8. Prohibir el uso del correo electrónico para la propagación de cadenas de mensajes.
9. Permitir la asignación de prioridad a los correos electrónicos.
10. Permitir el uso de mecanismos de encriptación para mensajes que contengan información confidencial y sensible.
11. Asignar a cada cuenta de correo una capacidad de almacenamiento de 10 MB y establecer la reasignación de capacidad bajo petición formal.

4.2.5.2.6 Antivirus

1. Establecer un mecanismo que permita la protección de los equipos e información del sistema contra amenazas lógicas como virus, spyware, gusanos, etc.
2. Establecer un mecanismo de alta protección (IDS / IPS) contra amenazas lógicas, para equipos representativos como los servidores.
3. Implantación de un plan de actualización del mecanismo de protección de la forma más efectiva y funcional.
    - Implementación del mecanismo de protección en todos los dispositivos del sistema.
    - Permitir que el mecanismo de actualización sea automático o manual.
4. Establecer de forma obligatoria la ejecución de un escaneo periódico al sistema de forma automática o manual.
    a. Escaneo del sistema (espacio residente del Sistema Operativo o directorios especiales como C:\WINDOWS\system), cada semana.
    b. Escaneo del disco total cada mes.
5. Desarrollo y documentación del procedimiento formal ante la presencia de un virus en el sistema.
    a. Dar notificación al departamento de sistemas.
    b. No ejecutar ni borrar el archivo que contiene al virus.
    c. Ejecución del antivirus.

4.2.5.2.7 Firewall

1. Desarrollo e implementación de las políticas de prohibición y permisión para el establecimiento del tráfico que se intercambia entre la red interna y externa o entre diferentes subredes internas.
    - Establecer protocolos y servicios permitidos y prohibidos.
    - Utilizar una política de prohibición a todo y habilitación solo de servicios y protocolos requeridos.
2. Prohibir el paso de paquetes que provengan del exterior con direcciones de origen internas, para evitar spoofing.
3. Establecer la habilitación temporal selectiva de protocolos y servicios requeridos.
4. Establecer el monitoreo y control periódico de la configuración de los servicios de red.
5. Establecer los procedimientos necesarios para obtener una falla controlada ante un incidente de seguridad, mediante el bloqueo de los accesos desde y hacia redes inseguras.

4.2.5.2.8 Ataques de red

1. Establecimiento de enlaces de respaldo ante posibles incidentes de corte de enlace.
2. Encriptación de la información (sensible y confidencial) para su transmisión por redes.
3. Desarrollar y documentar el procedimiento formal a ser adoptado frente a los ataques de red más comunes.
4. Establecimiento de un mecanismo de control y protección (IDS / IPS) para detectar intrusiones y reaccionar ante éstas.
5. Establecer un mecanismo de monitoreo continuo que permita detectar cuando se produce un ataque a la disponibilidad del sistema (DoS).
6. Establecer un plan de segmentación física y lógica para las diferentes áreas de la organización, con objeto de reducir el riesgo de sniffing y realizar una administración de carga de tráfico.
    a. Utilizar switch en lugar de hubs.

b. Implementar redes LAN virtuales y subredes.

7. Establecer mecanismos de protección (encriptación) para los mensajes y archivos que contienen las contraseñas ya sea en transmisión o almacenamiento.
8. Realizar mediciones periódicas de la utilización del ancho de banda.

4.2.5.3 Seguridad de Aplicaciones

4.2.5.3.1 Software

1. Establecer el uso de un sistema operativo fuerte[10] para los equipos servidores.
2. Presentar características y procedimientos de seguridad fuertes.
   - Identificación y autenticación.
   - Acceso confiable.
   - Operación fiable.

4.2.5.3.2 Control de aplicaciones en computadores

1. Establecer el uso de estándares de configuración para los puestos de trabajo de cada funcionario que utilice un computador.
   - Seguridad.
   - Acceso.
   - Disponibilidad.
2. Definir un procedimiento formal que especifique, que tipo de aplicaciones se deben instalar dependiendo del perfil del usuario.
3. Definir procedimientos para la actualización de la versión de la aplicación.
   a. Funcionalidad de cada versión.
   b. Migración segura de datos.
   c. Respaldo de la configuración actual.
   d. Modos de emergencia en caso de incidentes.
   e. Documentación de los procesos realizados.
4. Establecer los procedimientos adecuados ante la presencia de un nuevo usuario.

---

[10] **Sistema Operativo fuerte.** Es un Sistema Operativo desconocido, es decir que el código del sistema no sea público, de esta manera no puede ser analizado y comprometido.

- Notificación formal.
- Conocimiento y aceptación.
- Prohibida la instalación de software que no provenga del Departamento de Sistemas.

5. Establecer un monitoreo frecuente a los equipos en busca de programas instalados sin autorización o innecesarios.

4.2.5.3.3 Control de datos en las aplicaciones

1. Controlar los datos de entrada y de salida procesados por las aplicaciones.
   - Integridad.
   - Exactitud.
   - Validez.
   - Eficacia.
2. Establecer controles lógicos para dar permisos de acceso (lectura, escritura y ejecución) a los datos.

4.2.5.4 Seguridad Física

4.2.5.4.1 Equipos de trabajo

1. Establecer la documentación formal sobre el cuidado físico que se debe proporcionar a los dispositivos que conforman el sistema.
   - No exponer al equipo a substancias dañinas como agua, polvo, etc.
   - No exponer al equipo a eventos dañinos como variaciones de voltaje, golpes, etc.
2. Asignar personal responsable a cada dispositivo.

4.2.5.4.2 Acceso a equipos

Establecer mecanismos que permitan proteger a los equipos del acceso físico, que puedan comprometer la privacidad de la información.

- Diskettes.
- CD / DVD.

- Dispositivos de almacenamiento masivo (USB, Ipod, etc).
- Red cableada y/o inalámbrica.

4.2.5.4.3 Dispositivos del sistema

Los principales dispositivos que hacen posible las operaciones del sistema (dispositivos de conectividad y servidores) deben contar con las condiciones adecuadas para su funcionamiento correcto.

- Acondicionar la temperatura y humedad adecuada.
- Proporcionar extintor de fuego.
- Establecer un mecanismo de alarma contra accesos no autorizados.
- Proporcionar fuentes de energía emergentes (generadores, UPS).
- Establecer un mecanismo que proporcione luz para casos de emergencia.
- Utilizar estabilizadores de tensión, para proteger a los equipos de las variaciones bruscas de energía.
- Utilizar un adecuado sistema de conexión a tierra para todo el edificio y para el centro de cómputo.
- Evaluar periódicamente la capacidad de protección de los mecanismos implementados.
- Contar con un control general para cortar la energía en su totalidad en casos extremos.
- Establecer un manual de procedimiento personal en caso de emergencias que contenga actividades a realizarse y responsabilidades.
- Realizar capacitación y pruebas de simulación.

4.2.5.4.4 Acceso físico a dependencias sensibles

Establecer controles de acceso físico en áreas específicas (entradas) para proteger dependencias sensibles, del acceso no autorizado por parte de personal ajeno a la organización o extraño (sospechosos).

1. Establecer procedimientos de identificación y autenticación para controlar el acceso físico a diferentes dependencias de la organización.

    - Departamento de sistemas.

- Centro de cómputo.

2. Utilizar mecanismos manuales y/o automáticos para ejecutar los procedimientos de identificación, autenticación y autorización.
    - Puertas / llaves.
    - Puertas / contraseñas.
    - Mecanismos biométricos.
    - Guardias.
3. Establecer horarios de autorización de acceso para los diferentes perfiles de personas.
4. Realizar pruebas de los procedimientos adoptados para la protección física.

4.2.5.4.5 Estructura del edificio

En lo que concierne al ambiente adecuado para la localización del centro de cómputo se establece las siguientes características.

- Ubicación en un piso superior (segundo piso).
- Establecer protecciones con el propósito de no permitir la visualización exterior.
- Protección contra radiaciones electromagnéticas.

4.2.5.4.6 Cableado estructurado

1. Utilizar las normas que se establece para el cableado estructurado en organizaciones como la del caso de estudio, TIA / EIA – 568 – B.
2. Establecer cableado redundante para abastecer a un crecimiento futuro.
3. Realizar mediciones de interferencia periódicamente, y tomar medidas correctivas en casos necesarios.

4.2.5.4.7 Respaldos

La información que se respalda debe ser almacenada de forma segura, evitando eventos o condiciones que puedan comprometerla.

1. Almacenar los discos o cintas de respaldo en lugares que cuenten con las condiciones de temperatura y humedad adecuadas.

2. Establecer un balance entre la disponibilidad de los respaldos y su nivel de seguridad.
3. Realizar pruebas de recuperación de información.
4. Definir la periodicidad de respaldo requerida por cada tipo de información o datos.

4.2.5.4.8 Usuarios

1. Evitar la exposición prolongada a radiaciones producidas por equipos como impresoras, monitores, CPU, copiadoras, etc.
2. Establecer las sanciones pertinentes ante el incumplimiento de las normas de seguridad.

4.3 OBJETIVOS DE SEGURIDAD Y RENDIMIENTO

El presente estudio realizado tanto el teórico que trabaja con temas de seguridad, como el análisis de la situación real de la empresa Quito Motors S.A.C.I y la propuesta de seguridad que se creará tiene por objetivos:

- Incrementar la seguridad actual del sistema de forma integral utilizando tecnología de última generación (UTM).
- Diseñar la propuesta de seguridad para el sistema considerando aspectos como:
    - Funcionalidad.
    - Rendimiento.
    - Flexibilidad.
    - Proyección a futuro.
- Establecer una protección al sistema que sea beneficiosa tanto para los intereses de la empresa como para las expectativas de los usuarios.
- Asegurar los activos informáticos de la organización.
- Proporcionar una visión de la evolución en los productos de seguridad sus beneficios y funcionalidad integral aplicada a un sistema real.

4.4 CRITERIOS DE DISEÑO Y ESCENARIOS DE SEGURIDAD

Para proveer a la red de seguridad se plantea la utilización de los diferentes dispositivos y tecnologías que se detallan a continuación.

Se ha elegido desarrollar el diseño de seguridad para la presente red mediante la tecnología UTM, por presentar las mejores características de seguridad y funcionalidad en la actualidad para redes como las del caso de estudio.

Como se analizó en el capítulo II esta tecnología puede satisfacer las diferentes necesidades de seguridad, pero en el presente diseño se pondrá especial atención en los requerimientos definidos luego del análisis de la situación actual de la red.

4.4.1 CRITERIOS DE DISEÑO

El dispositivo que se ubica entre la red pública y la red privada, debe presentar las siguientes características:

- Los puertos necesarios para conectar los dispositivos que pertenecen a la red interna, manejar una DMZ (zona desmilitarizada) para los servicios públicos que ofrece el sistema y un acceso para Internet de alta capacidad.

- La capacidad de operación de 10/100/1000 Mbps debido a la existencia de dispositivos que trabajan con estas capacidades de transmisión.

- Un dispositivo de control e inspección completa integrado por un Firewall, Motor de detección y prevención de intrusiones (IDS / IPS), Motor de Antivirus, Mecanismos para el Filtrado de contenido y Filtrado Web, Tecnología para la creación de redes privadas virtuales (VPN) mediante el uso de tecnologías difundidas (IPSec, SSL, etc) con características de encriptación de alta velocidad y capacidad para creación de VLANs para segmentación de redes por protección y balanceo de carga de tráfico.

- El dispositivo debe cubrir los requerimientos actuales y futuros, para manejar la carga de usuarios (servidores y funcionarios) que alberga el sistema como se detalla en los anexos del capítulo III.

- El sistema operativo debe contar con una fortaleza tanto en aspectos de seguridad como funcionalidad, es así que debe ser preferentemente un sistema operativo propietario y presentar alta capacidad de procesamiento.

- Contar con la tecnología necesaria para administrar conexiones inalámbricas con las respectivas consideraciones de seguridad y funcionalidad.

Ver el anexo B1, para observar los detalles del esquema de seguridad.

4.4.2 ESCENARIOS DE SEGURIDAD

4.4.2.1 Seguridad Física

1. Control del acceso físico al sistema.
2. Uso de cableado estructurado certificado.
3. Ingreso de personal autorizado al centro de cómputo.
4. Adecuación del medio ambiente para el centro de cómputo y las diferentes áreas de trabajo.
5. Ubicación adecuada de los dispositivos y activos informáticos del sistema.
6. Contratar un seguro para los equipos más importantes.

4.4.2.2 Seguridad de Datos

1. Utilizar mecanismo de Antivirus resistente y actualizado.
2. Realizar los respaldos de información en tiempo real, diariamente y/o semanalmente de acuerdo al requerimiento de la misma.
3. Realizar las actualizaciones del sistema operativo y parches de seguridad periódicamente.
4. Utilizar software de monitoreo, análisis y administración para evitar brechas de seguridad en puertos y servicios abiertos innecesariamente o servicios mal configurados.
5. Establecer perfiles para el uso de los servicios.
6. Documentar las tareas administrativas de la red y mantener un control y actualización permanente del inventario de hardware, software y usuarios del sistema.

4.4.2.3 Seguridad de Acceso al Sistema

1. Control de accesos realizados por los usuarios, mediante herramientas como:

- ***Active Directory.*** Es utilizado por Microsoft para implementar el servicio de directorio en una red distribuida de computadores, usa distintos protocolos como: LDAP, DNS, DHCP, Kerberos; su estructura jerárquica permite manejar usuarios, grupos de usuarios, permisos, asignación de recursos y políticas de acceso.

- ***LDAP en Linux.*** Es una estructura de servicio de directorio que permite combinar varios sistemas como: autenticación NT, autenticación LINUX, información de ruteo, información de servicios / protocolos / hosts, libros de direcciones de red, etc.

2. Uso de contraseñas fuertes[11] para el proceso de autenticación.

4.4.2.4 Seguridad en el Diseño de la Red

1. Utilización de dispositivos y tecnologías que provean todas las características de seguridad actuales (mecanismos de protección antiguos y actuales).

- ***Firewall*** para implementar una barrera de protección entre la red externa y la intranet para ejecutar políticas de seguridad (filtros IP, URL, servicios, aplicaciones, protocolos, etc).
- ***Antivirus*** para proteger a la red de amenazas lógicas existentes y de continua aparición.
- ***IDS / IPS*** para analizar las intrusiones (amenazas) que puedan dañar el normal funcionamiento de la red y reaccionar con medidas de protección ante las mismas.
- ***VPN*** para encapsular el tráfico que contiene información sensible.
- ***Proxy*** para brindar el servicio de Internet a toda la intranet.
- ***Inspector de contenido*** para proteger al sistema de tráfico no deseado e innecesario.
- ***AntiSpam*** para proporcionar protección al sistema de correo electrónico.

2. Organizar la topología de la red de acuerdo a diferentes aspectos como definición organizacional, dispositivos de conectividad y dispositivos de servicio, mediante la

[11] **Contraseña fuerte.** Es una contraseña con mínimo 8 caracteres alfanuméricos, y que no revele información del usuario, del cargo o de la empresa.

implementación de VLANs y subredes para administrar de mejor manera el ancho de banda y la separación de la información de acuerdo a grupos de trabajo en común.

- Granja de servidores.
- Enlaces con Sucursales.
- Departamentos.

Para el diseño de la seguridad de la presente red se considera todas las protecciones disponibles en el mercado presentadas por los proveedores que se analizan en el presente proyecto.

Pero una solución de seguridad casi completa resultaría muy costosa y su implementación sería muy poco probable o por completo improbable en ambientes reales como la presente empresa, ya que conseguir el apoyo económico de la alta gerencia para soluciones de seguridad (compra de equipos y servicios) tan sofisticadas resulta un trabajo muy difícil.

Además hay que mantener un equilibrio entre el costo de las soluciones de seguridad, el costo de los activos informáticos a proteger y la probabilidad de ocurrencia de las amenazas potenciales, para presentar la viabilidad de cada solución.

Son éstas las razones por las cuales para empresas como la del presente proyecto se utilizará en el diseño dispositivos UTM que resultan una solución muy conveniente ya que cuentan con los módulos necesarios para desarrollar un ambiente de seguridad muy bueno en la actualidad.

ANEXO B1: Diagrama del diseño de seguridad para la Red Quito Motors.

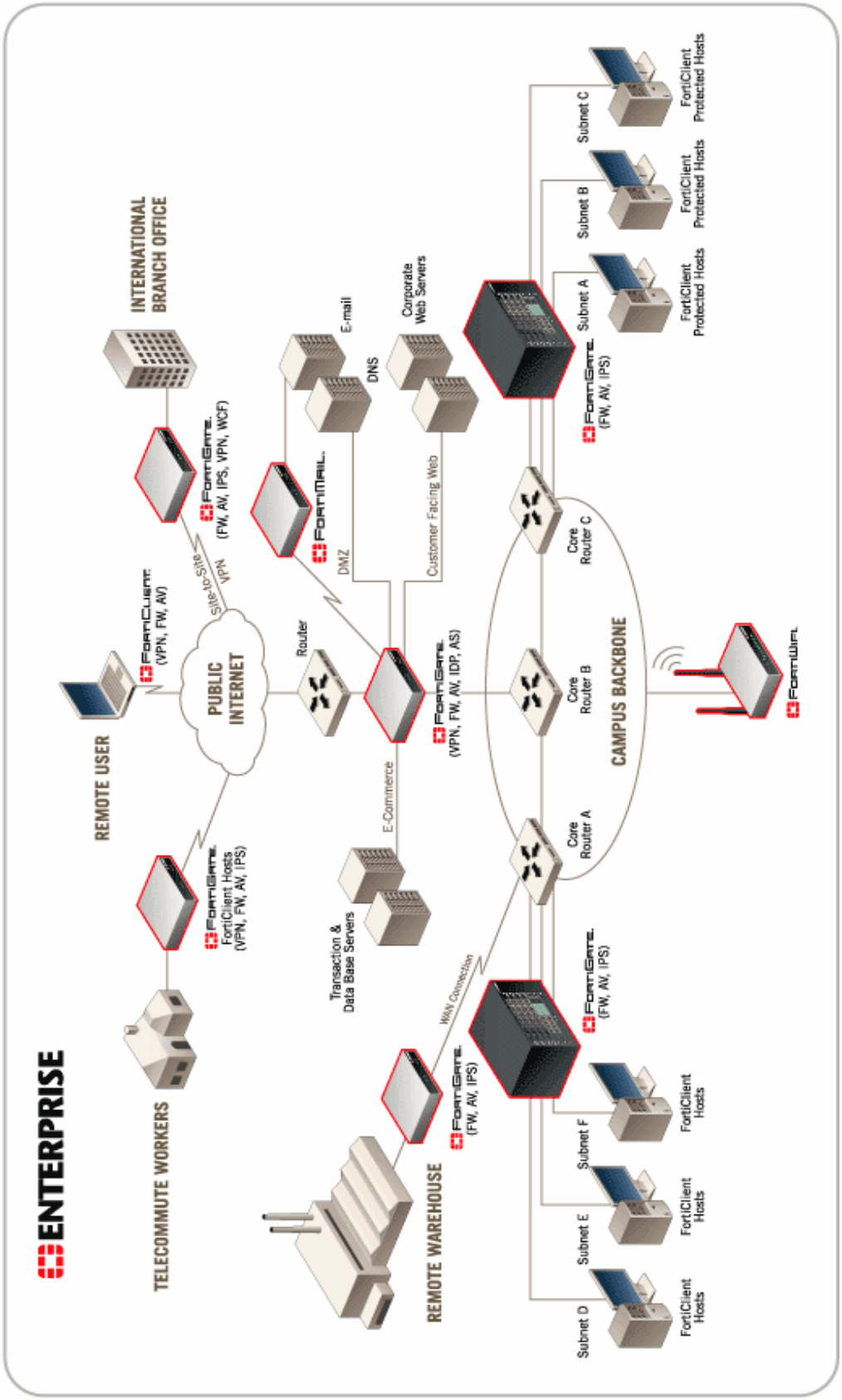


Figura 4.1: Solución de seguridad presentada por Fortinet. [13]

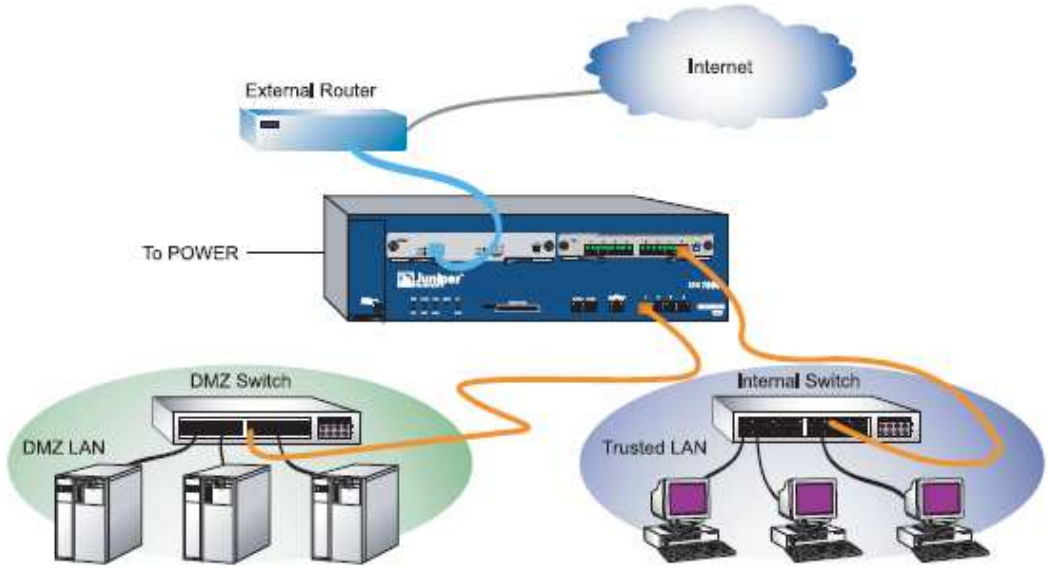


Figura 4.2: Solución de seguridad presentada por Juniper. [14]

Figura 4.3: Solución de seguridad presentada por Cisco. [15]

Las soluciones de seguridad presentadas por los proveedores, cuentan con diferentes características que permiten brindar una protección adecuada a la presente red, mediante diferentes dispositivos o herramientas propias para cada caso específico como: VPN, DMZ, Firewall, Antivirus, IPS, AntiSpam.

4.5 DIMENSIONAMIENTO, ESPECIFICACIONES TÉCNICAS Y EVALUACIÓN DEL DISPOSITIVO UTM

Las características de los dispositivos para proveer seguridad a la red de Quito Motors, deben cubrir los requerimientos actuales y proyectarse a crecimientos futuros de la presente red además de poseer características específicas para los requerimientos de seguridad de la misma.

4.5.1 DIMENSIONAMIENTO Y ESPECIFICACIONES TÉCNICAS

A continuación se detallan las características que debe cumplir el dispositivo UTM:

4.5.1.1 Características generales

1. Memoria RAM mínimo de 1024 MB.
2. Interfaces al menos seis con capacidad de 10 /100 / 1000 Mbps.
3. Capacidad de manejo de ancho de banda por interfaces.
4. Conexiones simultáneas al menos 400.000 sesiones.
5. Capacidad de servicio para 200 usuarios.
6. Disco duro al menos de 40 GB.
7. Soporte para VLANs (802.1Q) en sus interfaces.
8. Mantenimiento al menos 5x8 del fabricante.
9. Incluya capacitación al menos a dos personas.
10. Garantía del equipo al menos dos años.
11. Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc).
12. Soporte autenticación mediante certificados X.509v3 (PKI, IKE).
13. Interfaz para administración y configuración vía web, telnet y/o CLI.
14. Certificación ICSA Labs y/o EAL4.
15. Actualización automática de servicios de seguridad: IDS / IPS, AntiSpam, Antivirus (mínimo cada hora) y Lista de URLs.

16. Costo anual del las subscripciones a los servicios de seguridad.
17. Soporte técnico mensual.

4.5.1.2 Funcionalidades

4.5.1.2.1 Firewall

1. Throughput al menos de 1 Gbps.
2. Firewall de inspección completa en cada aplicación que maneje paquetes (Stateful Inspection).
3. Arquitectura de proxy que soporte reglas personalizadas para protocolos como CIFS, DNS, FTP, H.323, HTTP / SSL, UDP / TCP, NTP, ping para el tráfico ICMP, SMTP, POP, Telnet, RCMD, STP, etc. Además que soporte la creación de protocolos personalizados para aplicaciones puntuales.
4. Capacidad para aplicar, añadir, borrar o editar reglas del firewall en línea.
5. Filtrado de fragmentos IP y selección de paquetes.
6. Filtrado de paquetes con anomalía de protocolo.
7. Capacidad para bloquear tráfico P2P e IM.
8. Soporte para protocolos de enrutamiento RIP v1 y v2.
9. Soporte para NAT transversal H.323.
10. Autenticación a nivel de usuario basada en bases de datos locales, LDAP, RADIUS, Active Directory y Novell Directory.
11. Asignación selectiva de permisos basados en tiempo.
12. Alertas ante incidentes.

4.5.1.2.2 VPN

1. Throughput de almenos 100 Mbps.
2. Capacidad para creación de VPN sitio a sitio al menos 15.
3. Soporte para encapsulamiento IPSec y SSL.
4. Capacidad para filtrar paquetes dentro del túnel VPN basándose en dirección origen, dirección destino y protocolo.

5. Soporte VPN para encriptación DES, 3DES, AES-128, AES-256.
6. Soporte VPN para autenticación SHA-1, MD5.
7. Soporte cliente VPN sobre varias plataformas Windows XP, Windows Vista, Linux, Unix.

4.5.1.2.3 IDS / IPS

1. Throughput IDS / IPS al menos 500 Mbps
2. Capacidad de análisis y detección de segmentos específicos de red.
3. Capacidad de definición de políticas para el análisis de amenazas, basándose en el tráfico de cada segmento de red.
4. Capacidad de detectar ataques en base a:
   - Anomalías del protocolo.
   - Anomalías del tráfico.
   - Firmas y/o patrones.
5. Protección de amenazas de día cero.
6. Prevención, monitoreo y recolección de actividad maliciosa, tráfico y protocolos.
7. Capacidad para ejecutar notificación al administrador o bloqueo inmediato del tráfico.
8. Capacidad para prevenir violación de protocolos.

4.5.1.2.4 Antivirus

1. Throughput Antivirus al menos 100 Mbps.
2. Control de paquetes con virus y códigos malignos, tráfico SMTP, POP3, HTTP/HTTPS, FTP.
3. Capacidad de definir políticas individuales para cada protocolo.
4. Bases de datos con más de 80.000 firmas de virus.
5. Mínimo dos motores de antivirus.
6. Chequeo de archivos comprimidos, protegidos, imágenes, textos.
7. Detección de virus polimorfos (mediante encriptación).
8. Capacidad AntiSpyware y AntiAdware.
9. Detección de ficheros comprimidos.

10. Detección y eliminación de virus de macro.
11. Detección de ActiveX, Java, Flash.

4.5.1.2.5 Filtrado web

1. Filtrado de contenido por categorías de URLs, la base maestra debe tener más de 30 millones de sitios y más de 50 categorías; con capacidad de personalización.
2. Capacidad de filtrado basado en tamaño, extensiones, contenido, asuntos.
3. Aplicación de reglas por direcciones IP, redes / subredes, usuarios, grupos de usuarios.
4. Permitir la generación de más categorías por parte del administrador.

4.5.1.2.6 AntiSpam

1. Revisión de correos para evitar spam para SMTP, POP3.
2. Chequeo de URLs.
3. Bloqueo de mensajes vía RBL (Real-time Blackhole List).
4. Soporte para los diferentes agentes de transferencia de correo electrónico (MTA) Exchange, Sendmail, Lotus Domino, Exim.
5. Análisis de mensajes multimedia (JPG, MP3, etc).
6. Filtrado por cadenas de texto (asunto, cabecera, contenido).
7. Detección de código fuente.
8. Capacidad para aplicar reglas AntiSpam por redes o dominios.
9. Soporte para aplicación de controles mediante withlist y blacklist.
10. Análisis basado en palabras.
11. Análisis basado en extensiones de archivos adjuntos.
12. Control de atributos formales, dirección de envió, dirección de destinatario, dirección IP de origen.
13. Filtrado por tamaño máximo de mensaje.
14. Capacidad para poner en cuarentena, rechazar, notificar o borrar, los correos detectados como spam.

4.5.1.2.7 Reportes

1. Generación de reportes administrativos.
2. Reportes de tipo de tráfico que atraviesa por el equipo de seguridad (SMTP, http, MSN, P2P, otros).
3. Reporte de uso de hardware.
4. Reporte de tráfico por interfaces.
5. Reporte diario de páginas visitadas, porcentaje de uso por página y por usuario.
6. Reporte diario de páginas bloqueadas por usuario.
7. Reporte diario de páginas más visitadas.

4.5.1.2.8 Logs

1. Filtros en los logs para facilitar la visualización de problemas.
2. Logs en tiempo real de los diferentes servicios firewall, vpn, antivirus, antispam, otros.
3. Medios para notificación interactiva (administrador).

4.5.2 EVALUACIÓN DEL DISPOSITIVO UTM

4.5.2.1 Fortinet

FortiGate™-800 Series

HARDWARE SPECIFICATIONS

Total 10/100 Interfaces	4
Switch Interfaces	n/a
Configurable Ports	4
Fixed WAN / DMA Ports	n/a
Total 10/100/1000 Interfaces (Copper)	4 (FG-800 only)
1Gb SFP Interfaces (Fiber)*	4 (FG-800F only)

SYSTEM PERFORMANCE

Firewall Throughput	1 Gbps
VPN 3DES Throughput	200 Mbps
Antivirus Throughput	150 Mbps
IPS Throughput	600 Mbps
Dedicated IPSec VPN Tunnels	3,000
Unlimited User Licenses	Yes
Concurrent Sessions	400,000
New Sessions/Second	10K
Policies	20,000

CERTIFICATIONS ICSA Labs: Firewall, IPSec, SSL, Antivirus, IPS

Figura 4.4: Especificaciones Técnicas del dispositivo Fortinet. [13]

FIREWALL
ICSA Labs Certified (Enterprise Firewall)
NAT, PAT, Transparent (Bridge)
Routing Mode (RIP v1 & v2, OSPF, BGP, & Multicast)
Policy-Based NAT
Virtual Domains (NAT/Transparent mode)
VLAN Tagging (802.1Q)
User Group-Based Authentication
SIP/H.323 NAT Traversal
WINS Support
Customized Protection Profiles

VIRTUAL PRIVATE NETWORK (VPN)
ICSA Labs Certified (IPSec & SSL)
PPTP, IPSec, and SSL
Dedicated Tunnels
DES, 3DES, and AES Encryption Support
SHA-1/MD5 Authentication
PPTP, L2TP, VPN Client Pass Through
Hub and Spoke VPN Support
IKE Certificate Authentication
IPSec NAT Traversal
Dead Peer Detection
RSA SecurID Support

INTRUSION PREVENTION SYSTEM (IPS)
ICSA Labs Certified (NIPS)
Protection From Over 3000 Threats
Protocol Anomaly Support
Custom Signature Support
Automatic Attack Database Update

ANTIVIRUS
ICSA Labs Certified (Gateway Antivirus)
Includes AntiSpyware and Worm Prevention
HTTP/SMTP/POP3/IMAP/FTP/IM and Encrypted VPN Tunnels
Automatic "Push" Virus Database Update
File Quarantine Support
Block by File Size or Type

WEB FILTERING
URL/Keyword/Phrase Block
URL Exempt List
Content Profiles
Blocks Java Applet, Cookies, Active X
FortiGuard Web Filtering Support

ANTISPAM
Real-Time Blacklist/Open Relay Database Server
MIME Header Check
Keyword/Phrase Filtering
IP Address Blacklist/Exempt List
Automatic Real-Time Updates From FortiGuard Network

TRAFFIC SHAPING
Policy-based Traffic Shaping
Differentiated Services (DiffServ) Support
Guarantee/Max/Priority Bandwidth

NETWORKING/ROUTING
Multiple WAN Link Support
PPPoE Support
DHCP Client/Server
Policy-Based Routing
Dynamic Routing (RIP v1 & v2, OSPF, BGP, & Multicast)
Multi-Zone Support with Routing Between Zones
Route Between Virtual LANs (VDOMS)

MANAGEMENT/ADMINISTRATION OPTIONS
Console Interface (RS-232)
WebUI (HTTP/HTTPS) and Command Line Interface
Telnet / Secure Command Shell (SSH)
Role-Based Administration
Multi-language Support
Multiple Administrators and User Levels
Upgrades and Changes Via FTP and WebUI
System Software Rollback
Central Management via FortiManager (optional)

LOGGING/MONITORING
Internal Logging
Log to Remote Syslog/WELF server
Graphical Real-Time and Historical Monitoring
SNMP
Email Notification of Viruses And Attacks
VPN Tunnel Monitor
Optional FortiAnalyzer Logging

USER AUTHENTICATION OPTIONS
Local Database
Windows Active Directory (AD) Integration
External RADIUS/LDAP Integration
IP/MAC Address Binding
Xauth over RADIUS for IPSEC VPN
RSA SecurID Support

VIRTUAL DOMAINS (VDOMs)
Separate Firewall/Routing domains
Separate Administrative domains
Separate VLAN interfaces
10 VDOMs (standard)

HIGH AVAILABILITY (HA)
Active-Active, Active-Passive
Stateful Failover (FW and VPN)
Device Failure Detection and Notification
Link Status Monitor
Link failover

INSTANT MESSENGER / PEER-TO-PEER ACCESS CONTROL

AOL-IM	Yahoo	MSN	
ICQ	Gnutella	BitTorrent	
WinNY	Skype	eDonkey	KaZaa

Figura 4.5: Características de Seguridad del dispositivo Fortinet. [13]

FORTIGATE	**FortiGate - 800**
Características Requeridas	***Características Ofrecidas***
Características Generales	
Memoria RAM Mínimo 1024 MB	1024 MB
Interfaces al menos 6, Ethernet de 10 /100 / 1000 Mbps	- 4 Interfaces Ethernet 10/100/1000 Mbps - 4 Interfaces Ethernet 10/100/ Mbps - 4 Puertos configurables
Manejo de ancho de banda por interfaces	Si.
Conexiones simultáneas al menos 400.000	400.000 sesiones
Servicio para al menos 200 usuarios	Ilimitado
Disco duro al menos 40 GB	80 GB
Soporte para VLANs en sus interfaces	Si, Dominios Virtuales (VDOMS)
Autenticación certificados X.509v3 (PKI, IKE)	Si
Interfaz para administración: web, telnet y/o CLI	Si
Certificación al menos ICSA Labs y/o EAL4	ICSA Labs, NSS Labs, Common Criteria, FIPS 140-2
Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc)	RS-232, HTTPS, SSH
Características y Servicios de Seguridad	
Firewall	
Throughput Firewall al menos de 1 Gbps	1 Gbps
Capacidad de Stateful Inspection	Si
Capacidad de Arquitectura proxy	Si
Soporte para protocolos RIP v1 y v2	RIP v1 & v2, OSPF, BGP & Multicast
Soporte para NAT transversal H.323	Si
Autenticación basada en LDAP, RADIUS, Active Directory y Novell Directory	LDAP, RADIUS, Active Directory
Capacidad para bloquear tráfico P2P, IM	Si
VPN	
Throughput VPN al menos 100 Mbps	200 Mbps (3DES)
Capacidad para creación de VPN al menos 15	……
Soporte encriptación DES, 3DES, AES-128, AES-256	DES, 3DES, AES
Soporte VPN para autenticación SHA-1, MD5	SHA-1/MD5
Soporte para encapsulamiento IPSec, SSL	PPTP, IPSec, SSL
Soporte cliente VPN sobre Windows XP, Windows Vista, Linux, Unix	FortiClient
IDS / IPS	
Throughput IDS / IPS al menos 500 Mbps	600 Mbps (IPS)

Antivirus	
Throughput Antivirus al menos 100 Mbps	150 Mbps
Filtrado web	Si
AntiSpam	Si
Reportes y Logs	Si

Tabla 4.2: Evaluación del producto Fortinet.

4.5.2.2 Juniper

SSG 500 Series

Maximum Performance and Capacity

Minimum ScreenOS version support*	ScreenOS 5.4
Firewall performance (Large packets)	1+ Gbps
Firewall performance (IMIX)(2)	1 Gbps
Firewall Packets Per Second (64 byte)	600,000 PPS
AES256+SHA-1 VPN performance	500 Mbps
3DES+SHA-1 VPN performance	500 Mbps
Maximum concurrent sessions	256,000
New sessions/second	15,000
Maximum security policies	4,000
Maximum users supported	Unrestricted
Convertible to JUNOS 8.0 or higher	SSG 550M Only

Network Connectivity

Fixed I/O	4x10/100/1000
Physical Interface Module (PIM) Slots	6 (4 ePIM/uPIM/PIM + 2 uPIM/PIM)
WAN interface options (PIMS)	Serial, T1, E1, DS3, E3, ADSL/ADSL2/ADSL2+, G.SHDSL
LAN interface options (ePIMS and uPIMS)	10/100, 10/100/1000, and SFP

External Flash

Additional log storage	USB 1.1
Event logs and alarms	Yes
System configuration script	Yes
ScreenOS Software	Yes

Figura 4.6: Especificaciones Técnicas del dispositivo Juniper. [14]

Firewall

Network attack detection	Yes
DoS and DDoS protection	Yes
TCP reassembly for fragmented packet protection	Yes
Brute force attack mitigation	Yes
SYN cookie protection	Yes
Zone-based IP spoofing	Yes
Malformed packet protection	Yes

Unified Threat Management [3]

IPS (Deep Inspection firewall)	Yes
Protocol anomaly detection	Yes
Stateful protocol signatures	Yes
IPS/DI attack pattern obfuscation	Yes
Antivirus	Yes
Signature database	200,000+
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP, IM
Anti-spyware	Yes
Anti-adware	Yes
Anti-keylogger	Yes
Instant message AV	Yes
Anti-spam	Yes
Integrated URL filtering	Yes
External URL filtering[4]	Yes

Voice over IP (VoIP) Security

H.323 ALG	Yes
SIP ALG	Yes
MGCP ALG	Yes
SCCP ALG	Yes
NAT for VoIP protocols	Yes

IPSec VPN

Concurrent VPN tunnels	1,000
Tunnel interfaces	300
DES (56-bit), 3DES (168-bit) and AES (256-bit)	Yes
MD-5 and SHA-1 authentication	Yes
Manual key, IKE, IKEv2 with EAP, PKI (X.509)	Yes
Perfect forward secrecy (DH Groups)	1,2,5
Prevent replay attack	Yes
Remote access VPN	Yes
L2TP within IPSec	Yes
IPSec NAT traversal	Yes
Auto-Connect VPN	Yes
Redundant VPN gateways	Yes

User Authentication and Access Control

Built-in (internal) database - user limit	1,500
Third-party user authentication	RADIUS, RSA SecureID, LDAP
RADIUS Accounting	Yes – start/stop
XAUTH VPN authentication	Yes
Web-based authentication	Yes
802.1X authentication	Yes
Unified access control enforcement point	Yes

PKI Support

PKI Certificate requests (PKCS 7 and PKCS 10)	Yes
Automated certificate enrollment (SCEP)	Yes
Online Certificate Status Protocol (OCSP)	Yes
Certificate Authorities supported	VeriSign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape) Baltimore, DoD PKI
Self-signed certificates	Yes

Virtualization

Maximum number of security zones	60
Maximum number of virtual routers	8
Bridge groups*	Yes
Maximum number of VLANs	150

Routing

BGP instances	15
BGP peers	16
BGP routes	20,000
OSPF instances	8
OSPF routes	20,000
RIP v1/v2 instances	256
RIP v2 routes	20,000
Static routes	20,000
Source-based routing	Yes
Policy-based routing	Yes
ECMP	Yes
Multicast	Yes
Reverse Path Forwarding (RPF)	Yes
IGMP (v1, v2)	Yes
IGMP Proxy	Yes
PIM SM	Yes
PIM SSM	Yes
Multicast inside IPSec tunnel	Yes

Encapsulations

PPP	Yes
MLPPP	Yes
MLPP max physical interfaces	12
Frame Relay	Yes
MLFR (FRF .15, FRF .16)	Yes
MLFR max physical interfaces	12
HDLC	Yes

IPv6

Dual stack IPv4/IPv6 firewall and VPN	Yes
IPv4 to/from IPv6 translations and encapsulations	Yes
Syn-Cookie and Syn-Proxy DoS Attack Detection	Yes
SIP, RTSP, Sun-RPC, and MS-RPC ALG's	Yes
RIPng	Yes

Mode of Operation

Layer 2 (transparent) mode[5]	Yes
Layer 3 (route and/or NAT) mode	Yes

Address Translation

Network Address Translation (NAT)	Yes
Port Address Translation (PAT)	Yes
Policy-based NAT/PAT	Yes
Mapped IP	6,000
Virtual IP	32
MIP/VIP Grouping	Yes

IP Address Assignment

Static	Yes
DHCP, PPPoE client	Yes
Internal DHCP server	Yes
DHCP relay	Yes

Traffic Management Quality of Service (QoS)

Guaranteed bandwidth	Yes - per policy
Maximum bandwidth	Yes - per policy
Ingress traffic policing	Yes
Priority-bandwidth utilization	Yes
DiffServ marking	Yes - per policy

High Availability (HA)	
Active/Active - Transparent & L3 mode	Yes
Active/Passive - Active/Passive - Transparent & L3 mode	Yes
Configuration synchronization	Yes
VRRP	Yes
Session synchronization for firewall and VPN	Yes
Session failover for routing change	Yes
Device failure detection	Yes
Link failure detection	Yes
Authentication for new HA members	Yes
Encryption of HA traffic	Yes
System Management	
WebUI (HTTP and HTTPS)	Yes
Command line interface (console)	Yes
Command line interface (telnet)	Yes
Command line interface (SSH)	Yes v1.5 and v2.0 compatible
NetScreen-Security Manager	Yes
All management via VPN tunnel on any interface	Yes
Rapid deployment	No
Administration	
Local administrator database size	20
External administrator database support	RADIUS, RSA SecureID, LDAP
Restricted administrative networks	6
Root Admin, Admin and Read Only user levels	Yes
Software upgrades	TFTP, WebUI, NSM, SCP, USB
Configuration rollback	Yes
Logging/Monitoring	
Syslog (multiple servers)	Yes - up to 4 servers
Email (two addresses)	Yes
NetIQ WebTrends	Yes
SNMP (v2)	Yes
SNMP full custom MIB	Yes
Traceroute	Yes
VPN tunnel monitor	Yes

Figura 4.7: Características de Seguridad del dispositivo Juniper. [14]

JUNIPER	**Juniper Networks SSG 550M**
Características Requeridas	***Características Ofrecidas***
Características Generales	
Memoria RAM Mínimo 1024 MB	1024 MB
Interfaces al menos 6, Ethernet de 10/100/1000 Mbps	4 puertos 10/100/1000 Mbps

Manejo de ancho de banda por interfaces	Si
Conexiones simultáneas al menos 400.000	256.000 sesiones
Servicio para al menos 200 usuarios	Ilimitado
Disco duro al menos 40 GB	80 GB
Soporte para VLANs en sus interfaces	Virtualización, 150 VLANs
Autenticación certificados X.509v3 (PKI, IKE)	VeriSing, Entrust, Microsoft, RSA Keon, Baltimore, DoD PKI
Interfaz para administración: web, telnet y/o CLI	Si
Certificación al menos ICSA Labs y/o EAL4	EAL4, EAL4+, ICSA (Firewall y VPN)
Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc)	VPN, SSH, HTTPS
Características y Servicios de Seguridad	
Firewall	
Throughput Firewall al menos de 1 Gbps	1 Gbps
Capacidad de Stateful Inspection	Si
Capacidad de Arquitectura proxy	Si
Soporte para protocolos RIP v1 y v2	RIP v1 & v2, OSPF, BGP & Multicast
Soporte para NAT transversal H.323	Si
Autenticación a nivel de usuario basada LDAP, RADIUS, Active Directory y Novell Directory	LDAP, RADIUS, RSA SecurID
Capacidad para bloquear tráfico P2P, IM	Si
VPN	
Throughput VPN al menos 100 Mbps	500 Mbps
Capacidad para creación de VPN al menos 15	300
Soporte encriptación DES, 3DES, AES-128, AES-256	3DES, AES-256
Soporte VPN para autenticación SHA-1, MD5	SHA-1, MD-5
Soporte para encapsulamiento IPSec, SSL	L2TP, IPSec
Soporte cliente VPN sobre Windows XP, Windows Vista, Linux, Unix	……
IDS / IPS	
Throughput IDS / IPS al menos 500 Mbps	No especifica
Antivirus	
Throughput Antivirus al menos 100 Mbps	No especifica
Filtrado web	Si
AntiSpam	Si
Reportes y Logs	Si

Tabla 4.3: Evaluación del producto Juniper.

4.5.2.3 Cisco

Cisco ASA 5550 Firewall Edition Bundle Includes: 8 Gigabit Ethernet interfaces + 1 Fast Ethernet interface, 4 Gigabit SFP interfaces, 5000 IPsec VPN peers, 2 SSL VPN peers, 3DES/AES license	• 1.2 Gbps Firewall • 425 Mbps IPsec VPN

Figura 4.8: Especificaciones Técnicas del dispositivo Cisco. [15]

CISCO	**Cisco ASA 5550**
Características Requeridas	***Características Ofrecidas***
Características Generales	
Memoria RAM Mínimo 1024 MB	4096 MB
Interfaces al menos 6, Ethernet de 10 /100 / 1000 Mbps	- 8 Interfaces Ethernet 10/100/1000 Mbps - 4 SPF Fiber - 1 10/100 Mbps
Manejo de ancho de banda por interfaces	Si
Conexiones simultáneas al menos 400.000	650.000 sesiones
Servicio para al menos 200 usuarios	Ilimitado
Disco duro al menos 40 GB	No especifica
Soporte para VLANs en sus interfaces	250 VLANs
Autenticación certificados X.509v3 (PKI, IKE)	Certificados X.509, soporte CRL (Certificate Revocation List)
Interfaz para administración: web, telnet y/o CLI	Si
Certificación al menos ICSA Labs y/o EAL4	…….
Soporte de mecanismos seguros para el acceso (SSH, HTTPS, etc)	……
Características y Servicios de Seguridad	
Firewall	
Throughput Firewall al menos de 1 Gbps	1.2 Gbps
Capacidad de Stateful Inspection	Si, …….Insector de Contenidos
Capacidad de Arquitectura proxy	Si
Soporte para protocolos RIP v1 y v2	RIP v1 & v2, OSPF, BGP & Multicast
Soporte para NAT transversal H.323	Si
Autenticación basada en LDAP, RADIUS, Active Directory y Novell Directory	AAA, no especifica
Capacidad para bloquear tráfico P2P, IM	……..
VPN	
Throughput VPN al menos 100 Mbps	425 Mbps

Capacidad para creación de VPN al menos 15	No especifica
Soporte encriptación DES, 3DES, AES-128, AES-256	3DES, AES
Soporte VPN para autenticación SHA-1, MD5	No especifica
Soporte para encapsulamiento IPSec, SSL	PPTP, IPSec, SSL
Soporte cliente VPN sobre Windows XP, Windows Vista, Linux, Unix	Software disponible en la página de Cisco
Dispositivos Cisco Adicionales	**Cisco IPS 4255 / Cisco ASA 5520**
IDS / IPS	
Throughput IDS / IPS al menos 500 Mbps	500 Mbps
Antivirus	
Throughput Antivirus al menos 100 Mbps	450 Mbps
Filtrado de Contenido	Si
AntiSpam	Si
Reportes y Logs	Si

Tabla 4.4: Evaluación del producto Cisco.

4.5.2.4 Análisis de los Dispositivos UTM presentados

Los dispositivos analizados cumplen con la mayoría de requerimientos técnicos; a excepción de:

- Número de conexiones simultáneas que ofrece cada uno: Fortinet con 400.000, Juniper con 256.000 y Cisco con 650.000; con lo que se tendría una degradación en el rendimiento con Juniper, las mejores características con Cisco y un punto intermedio que además cumple con los requerimientos con Fortinet.

- Número de puertos disponibles en el equipo: Fortinet dispone de 12 puertos, Cisco disponen de 8 puertos y Juniper dispone de 4 puertos que no cubren los requerimientos, pero posee la capacidad de añadir más puertos en 6 slots disponibles.

- Juniper no cubren el requerimiento de la funcionalidad de encapsulamiento SSL, el cual es necesario para la para interacción segura con la web.

A continuación se presenta la potencialidad de los Servicios de Seguridad que presenta cada dispositivo:

Servicios de Seguridad	Fortinet	Juniper	Cisco

VPN			
Túneles IPSec VPN	3.000	1.000	5.000
Firewall			
Paquetes / segundo	No Especifica	600.000	
Antivirus			
Análisis IM	No Especifica	si	
Firmas de virus		200.000+	
Capacidad de análisis	- AntiSpyware - Prevención de Gusanos - Túneles VPN - HTTP/SMTP/POP3/ IMAP/FTP/IM	- Anti-spyware - Anti-adware - Anti-keylogger - POP3/HTTP/SMTP/ IMAP/FTP/IM	- Antivirus - AntiSpyware - File Blocking - AntiPhising - HTTP/SMTP/FTP/ POP3/HTML/ICMP/ DNS/RPC/NETBIOS/ GRE
Filtrado web			
Bloqueo	- URL - palabra clave - frase - Java Applet - Cookies - Active X	Filtrado web integrado en Anti-Spam	- URL - Active X - Java Applet - VBScript
IDS / IPS			
Amenazas	3.000+		
Soporte anomalía de protocolo	si	si	si
Soporte patrón de firma	si	si	No Especifica
Soporte anomalía de aplicaciones	No Especifica	No Especifica	si
AntiSpam			
Capacidad	- Lista Negra en tiempo real - Lista Negra de IP - Análisis cabecera MIME - Filtra frases/palabras	Filtra URLs	Detecta spam mediante tecnología heurística

Tabla 4.5: Servicios de Seguridad de los dispositivos.

Finalmente se presentan características adicionales que posee cada dispositivo:

Características Adicionales	Fortinet	Juniper	Cisco
Hardware y Rendimiento			
Slots PIM	----------	6	----------
Interfaz WAN (PIMS)	----------	serial, E1, T1, DS3, E3, ADSL, ADSL2, G.SHDSL	----------
Interfaz LAN (PIMS)	----------	10/100, 10/100/1000, SPF	----------
Flash Externo	----------	USB1.1	----------
Nuevas sesiones/segundo	10.000	15.000	28.000
Políticas	20.000	4.000	100.000
Funciones	Modelado de tráfico	Administración del tráfico (QoS)	Optimizador del ancho de banda: PacketShaper 7500
	Networking/Routing	Routing	Routing
	Administración	Administración	Administración
	Monitoreo/Registro	Monitoreo/Registro	Monitoreo/Registro
	Autenticación de usuarios	Autenticación de usuario y Control de Acceso	----------
	Dominios Virtuales	Virtualización	
	Alta Disponibilidad	Alta Disponibilidad	HA: activo/activo; activo/pasivo
	Control P2P e IM	----------	----------
	----------	Seguridad VoIP	H.323, SIP
	----------	Encapsulación: FR/HDLC	Encapsulación: FR/HDL/PPP/L2TP/ATM
	IPv6	IPv6	IPv6

Tabla 4.6: Características adicionales de los dispositivos.

Finalmente luego del análisis y las comparaciones técnicas realizadas entre los proveedores, se concluye que tanto el dispositivo Fortinet como el Juniper cumplen con el objetivo del presente proyecto que es realizar el diseño de seguridad mediante un dispositivo UTM, que permita cubrir los requerimientos de seguridad más importantes; en el caso de Cisco se requieren dispositivos adicionales para brindar una seguridad íntegra, por lo que con este proveedor se desvía de la idea de mantener un solo dispositivo que

trabaje como un UTM; sin embargo es el que mejores capacidades y facilidades presenta al momento de acoplarse debido a que está orientado a la interoperabilidad.

Es así que Juniper y Fortinet se presentan como la mejor opción al momento de recomendar un dispositivo que proteja la red, sin embargo cabe indicar que el dispositivo Juniper posee mayor capacidad tanto en procesamiento como en crecimiento futuro, además de poseer características adicionales como se indican en las tablas arriba descritas.

No obstante las características del dispositivo Fortinet son las más adecuadas y suficientes para brindar la seguridad requerida por la presente empresa.

Por lo tanto se concluye que la mejor opción técnica para este caso específico tiene el siguiente orden:

1. Fortinet
2. Juniper
3. Cisco

4.6 PLAN DE CONTINGENCIAS PARA LA RED DE DATOS

El plan de contingencias es un instrumento de gestión para afrontar los incidentes que pueden afectar a los asuntos relacionados con las Tecnologías de la Información y las Comunicaciones; ya que permiten asegurar la continuidad de las operaciones en el menor tiempo posible, minimizar el impácto económico, solucionar el desconocimiento de las medidas a tomarse y resguardar los activos e información importantes, mediante el desarrollo de un plan de recuperación para restaurar las operaciones a su funcionamiento normal.

Este plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de la compañía, debe contener los siguientes puntos:

- Estrategia de recuperación.
- Establecer las actividades para antes, durante y después del incidente y designar los respectivos responsables de las mismas.
- Documentar las actividaes realizadas, las actualizaciones y planificaciones.

A continuación se presentan los aspectos a los que debe enfocarse el plan de contingencia en orden de importancia:

Respaldos		
Dispositivos	**Información**	**Otros**
1. Servidores 2. Routers 3. Switch 4. Access Point	1. Operacional 2. Departamental 3. Personal	1. Cableado Estructurado 2. Equipos de trabajo

Tabla 4.7: Esquema para respaldar la información.

4.7 ANÁLISIS DE COSTOS DEL SISTEMA DE SEGURIDAD PERIMETRAL

El análisis de costos que se presenta a continuación contiene el detalle de los precios relacionados con el Hardware, Software, Servicios de Subscribción (licencias), Redundancia y Adicionales (instalación, configuración y capacitación), de cada una de las soluciones estudiadas y ofertadas en el presente proyecto; para seguidamente realizar una comparación de aspectos como precios, funcionalidad y vialbilidad; y así finalmente recomendar la mejor solución de seguridad tanto en características técnicas como en aspectos económicos requeridos por la empresa en cuestión.

La información económica de los dispositivos ofertados se obtubo de la lista de precios publicada por cada proveedor en el Internet, por lo que pueden estar sujetas a costos adicionales inherentes al envío e impuestos de aduana.

4.7.1 COSTO DE LA SOLUCIÓN PRESENTADA POR FORTINET

CANTIDAD	ELEMENTO	COSTO
UTM FortiGate: Hardware		
	FortiGate-800	
1	FG-800-US / FortiASIC	**$11,995**
UTM FortiGate: Software		

	FortiOS: Incluido en el dispositivo UTM	
	FortiClient: Licencia para 5 clientes por 12 meses	
1	FHB-15-C1001-053-10-12	**$250**
UTM FortiGate: Servicios y Soporte (por 12 meses)		
	FortiGate-800 **Paquete BDL** ***Protección*:** Anti-Virus, IPS, Content Filtering y Anti-Spam ($2,149) ***Soporte:*** 8X5 Hardware Return / Replace (3 days), Firmware Upgrades y 8X5 Phone Support ($1,200)	
1	FC-10-00800-901-02-DD	**$3,349**
UTM FortiGate: Redundancia		
	FortiGate-800	
1	FG-800-US / FortiASIC	**$11,995**
UTM FortiGate: Adicionales		
	- Instalación y Configuración ($1,210) - Capacitación ($3,200)	**$4,410**
COSTO TOTAL DE LA SOLUCIÓN:		**$31,999**
COSTO CRÍTICO:		**$19,754**

Tabla 4.8: Presupuesto referencial de la solución presentada por Fortinet.

4.7.2 COSTO DE LA SOLUCIÓN PRESENTADA POR JUNIPER

CANTIDAD	ELEMENTO	COSTO
UTM: Hardware		
	SSG 550M	$10,500
1	SSG-550M-SH	**$10,500**
UTM: Software		
	JUNOS: Incluido en el dispositivo UTM	
UTM FortiGate: Servicios y Soporte (por 12 meses)		
	SSG 550M **Protección:** Anti-Virus Juniper-Kaspersky, NS-K-AVS-SSG550 ($3,150) Anti-Spam, NS-SPAM-ISG1000 ($5,000) Web Filtering, NS-WF-SSG550 ($2,300) Deep Inspection, NS-DI-SSG550 ($1,050) **Soporte:** J-Care Support Services, SVC-COR-SSG550M ($750)	**$12,250**
UTM: Redundancia		

	SSG 550M	
1	SSG-550M-SH	**$10,500**
UTM: Adicionales		
	- Instalación y Configuración ($950) - Capacitación ($2,050) 3 dias	**$3,000**
COSTO TOTAL DE LA SOLUCIÓN:		**$36,250**
COSTO CRÍTICO:		**$25,750**

Tabla 4.9: Presupuesto referencial de la solución presentada por Juniper.

4.7.3 COSTO DE LA SOLUCIÓN PRESENTADA POR CISCO

CANTIDAD	ELEMENTO	COSTO
Firewall: Hardware		
	Cisco ASA 5550	
1	ASA5550-BUN-K9	**$12,132**
IPS: Hardware		
	Cisco IPS 4255	
1	IPS-4255-K9	**$15,166**
Inspector de Contenidos: Hardware		
	Cisco ASA 5520	
1	ASA5520-CSC20-K9	**$10,069**
Software		
	CISCO OS: Incluido en el dispositivo Hardware	
Servicios y Soporte (por 12 meses)		
	Cisco IPS 4255 CON-SNTE-IPS-4255 Smartnet 8x5x4	**$3,114**
	Cisco ASA 5520 (Inspector de Contenidos) ASA 5500 CSC SSM20 Plus Lie, Spam/URL/Phish ($1,821) CON-SNTE-AS2C20K9 Smartnet 8x5x4 ($1,574)	**$3,395**
UTM: Redundancia		
1	**Cisco ASA 5550**	**$12,132**
1	**Cisco IPS 4255**	**$15,166**
1	**Cisco ASA 5520**	**$10,069**
UTM: Adicionales		

	- Instalación y Configuración ($1,400) - Capacitación ($2,250) 98 horas / 5 personas	**$3,650**
COSTO TOTAL DE LA SOLUCIÓN:		**$84,893**
COSTO CRÍTICO:		**$47,526**

Tabla 4.10: Presupuesto referencial de la solución presentada por Cisco.

SOLUCION DE SEGURIDAD			
Elemento	***Fortinet***	***Juniper***	***Cisco***
Hardware y Software	$11,995	$10,500	$37,367
Servicio y Soporte	$3,349	$12,250	$6,509
Redundancia	$11,995	$10,500	$37,367
Adicionales	$4,410	$3,000	$3,650
Total	**$31,999**	**$36,250**	**$84,893**
Total Crítico	**$19,754**	**$25,750**	**$47,526**

Tabla 4.11: Costos comparativos de las soluciones presentadas.

Luego de haber expuesto las características, los alcances, las plataformas, las garantías de los equipos y servicios que ofrece cada una de las Soluciones de Seguridad analizadas, se puede concluir que las presentadas por Fortinet y por Juniper se ajustan a los objetivos de este proyecto; ya que ofrecen la tecnología requerida y necesaria para este caso específico de protección perimetral para la red de Quito Motors, debido a que constituyen soluciones de seguridad basadas en la tecnología UTM y cubren las necesidades de esta empresa de tipo comercial, que prefiere un solo equipo de fácil administración y de bajo costo; en tanto que la solución presentada por Cisco requiere de dispositivos adicionales para cubrir las expectativas de una protección integral, alejándose así de la idea de un solo dispositivo que protega por entero a la red.

Es así que las tecnologías Fortinet y Juniper constituyen la mejor opción, mientras que la tecnología Cisco quedaría relegada.

Seguidamente se concidera los costos del dispositivo, de la implementación y del mantenimiento para determinar cual es la solución más viable.

En cuanto a Hardaware, la tecnología Cisco es la más costosa debido a que su solución requiere de varios dispositivos, luego tenemos a Fortinet y Juniper con precios similares.

En lo relacionado a costos de Subscripción a los servicios de seguridad y soporte que ofrecen; la solución de Fortinet es la que ofrece una protección adecuada y de menor costo, con una diferencia muy significativa con Juniper; además hay que considerar que estos costos no son solamente iniciales sino anuales; por lo que tanto a corto como a largo plazo la solución de Juniper representa la opción más costosa. Es así que el costo asociado a los servicios de seguridad y soporte, permiten visualizar la mejor opción para el desarrollo e implentación de seguridad para esta red.

En orden de prioridad y viabilidad se tiene a Fortinet seguido por Juniper y finalmente a Cisco, por lo que se recomienda optar por la solucion de Fortinet.

Para finalizar se hace hincapié en la importancia de brindar una adecuada protección a la red, ya que la seguridad puede evitar pérdidas mayores y muy importantes en comparación a la inversión que se realice.

CAPÍTULO V

Conclusiones y Recomendaciones

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

La seguridad de la información en la actualidad, y en el ámbito comercial como es el caso de la empresa analizada no se encuentra entre los temas vitales dentro de las actividades operacionales o asuntos relacionados con las Tecnologías de la Información; este fenómeno de gran riesgo se presenta debido a que el personal IT se concentra únicamente en la funcionalidad de la red y no en su seguridad, debido al desconocimiento o falta de apoyo por parte de los altos directivos.

Esta situación ocurre debido a que los beneficios de la seguridad de una red no se perciben como un rédito o ganancia visible que es para lo que son creadas las empresas; sino mas bien como un gasto adicional sin mucha trascendencia, esta percepción herrada por parte de los altos directivos que desconocen los peligros asociados a la inseguridad de la red y los beneficios de una red protegida son la causa para que este tipo de redes sean muy vulnerables y por ende se encuentren expuestas a ataques contra la confidencialidad, integridad y disponibilidad de la información.

Otro problema que se vuelve más visible e impactante al enfrentar el crecimiento experimentado por la presente organización es la falta de mecanismos adecuados que permitan controlar, administrar y mejorar la funcionalidad del sistema en general. Es así que el presente sistema expone deficiencias tanto en el rendimiento de los empleados como en el rendimiento del sistema debido a la falta de administración y control del mismo.

Otra realidad en nuestros días es la fuerte presencia de la red pública mundial (Internet) en diferentes instituciones, organizaciones, empresas y personas en general ya que constituye una herramienta que brinda diferentes funcionalidades y que ha evolucionado de tal manera que ha llegado a posesionarse fuertemente, convirtiéndose en una herramienta de uso obligatorio gracias a las funcionalidades que se desarrollan continuamente y a la tecnología que avanza cada vez mas rápido. Es así que se convierte en una herramienta necesaria para las operaciones empresariales en este caso específico, pero al mismo tiempo por ser una red totalmente expuesta y pública que carece de controles adecuados se clasifica como una red altamente insegura a pesar de los esfuerzos que se realizan por dar seguridad a ésta, las dimensiones de la misma hacen de esta tarea un trabajo imposible, es

por eso que cada ente por si mismo debe concienciar sobre la protección que se requiere al entrar a formar parte de este sistema, ya que ofrece beneficios pero también alberga potenciales peligros y riesgos que pueden causar importantes daños económicos, de prestigio y personales. De ahí la necesidad de establecer mecanismos de protección que permitan hacer uso correcto, eficiente y seguro de esta herramienta que brinda grandes capacidades. También el incremento en la demanda de las comunicaciones inalámbricas de área local debido a su flexibilidad constituyen un importante campo a considerase para el establecimiento de la seguridad integral en un sistema.

En la actualidad la Red Quito Motors presenta un nivel de seguridad bajo, debido a que como medida de seguridad solamente utiliza el antivirus F-Secure en las estaciones de trabajo, sin embargo hay falencias en torno a la transferencia de información entre sucursales y a través de Internet, ya que no se utiliza ninguna herramienta de encriptación que permita dar confidencialidad a la información; adicionalmente no cuenta con un firewall que permita establecer un control de acceso adecuado desde y hacia el Internet.

Adicionalmente las direcciones IP se encuentran distribuidas de forma ineficiente e insegura, ya que no se realiza subneteo o VLANs que permitan organizar la asignación de direcciones y separar las diferentes áreas de trabajo.

La red de Quito Motors posee mecanismos de seguridad como el antivirus, el mismo que constituye una herramienta muy fuerte para la protección del sistema, pero carece de controles adicionales como:

- Una barrera de protección entre la red pública y privada con reglas de configuración correctas.
- Mecanismos de protección contra el spam, las intrusiones, los spywares y demás amenazas que evolucionan continuamente en el Internet.
- Mecanismos que permitan examinar el contenido del tráfico que se intercambia entre la red pública y la red privada.
- Controles sobre los sitios web que permitan discriminar entre los sitios que representan confianza y los que representan inseguridad y peligro.
- Finalmente carece de mecanismos que permitan controlar, administrar y monitorear las operaciones y eventos que se suscitan en la red, lo cual conlleva a la ineficiencia e inseguridad del sistema.

Todos estos mecanismos y consideraciones de seguridad son necesarios para brindar una seguridad aceptable a la organización, y mediante la tecnología UTM es posible establecer un nivel de seguridad coherente a las necesidades de empresas comerciales como la de este caso en particular, ya que permite cubrir los asuntos de seguridad más importantes.

Las soluciones de seguridad planteadas mediante el uso de dispositivos UTM, ayudarán a proteger de manera más profunda los activos informáticos y el personal de la empresa; además permitirá brindar seguridad a las comunicaciones entre sucursales y con el Internet; también contribuirá en la implementación de aplicaciones seguras para el desarrollo del comercio electrónico.

Los costos de las soluciones presentadas requieren una inversión razonable (económica), ya que se toma en cuenta los beneficios para la protección de la red y la baja disponibilidad de los altos directivos para la inversión en equipos de seguridad.

Sin embargo debemos estar concientes, que no hay un sistema que brinde seguridad por completo, pero es mejor establecer algo o mucho de protección antes que no hacer nada; es así que no se puede depositar toda la confianza ante un solo equipo de seguridad.

Otro punto importante es que éste constituiría un único punto de protección y de falla, donde vulnerado el mismo la red quedaría expuesta, es por eso que se deben considerar mecanismos de respaldo para proveer una protección y funcionalidad básica al sistema en caso de incidentes que ameriten la entrada en funcionamiento de los mismos.

Una vulnerabilidad que abarca al sistema completamente es la carencia de políticas de seguridad que contribuyan al manejo eficiente de los asuntos relacionados con las Tecnologías de la Información.

Finalmente el personal encargado del manejo de la red no es especializado, así la implementación y mantenimiento de sistemas y redes recae en terceros (proveedores).

5.2 RECOMENDACIONES

La principal recomendación para las empresas en general es concienciar y aceptar la importancia de la seguridad tanto para la institución como para las personas, con el objeto de prevenir incidentes y estar preparados para los retos tecnológicos que se presentan continuamente.

Desarrollar un programa de seguridad que permita establecer un nivel de protección y funcionalidad aceptable para la empresa Quito Motors S.A.C.I, tanto para los sistemas como para el personal de la misma.

Establecer mecanismos de protección como:

- Un firewall para restringir o permitir las conexiones y servicios de forma especifica.
- Encriptación para proteger la información sensible en transito mediante el uso de VPN y en almacenamiento.
- Filtros web que manejen listas de confianza para así discriminar entre sitios confiables y sitios riesgosos a fin de consentir o no el acceso a los mismos.
- Sistemas de detección de intrusos que permitan reaccionar ante posibles incidentes que puedan afectar la normal operación del sistema.
- Antivirus, antispam, antispyware y demás mecanismos que permitan hacerle frente a las amenazas contra la seguridad del sistema.

Implantar mecanismos que permitan monitorear al sistema para mejorar la administración y control del mismo.

Finalmente inculcar buenas prácticas de seguridad en el personal de la empresa mediante la capacitación y la implementación de mecanismos que permitan brindar protección de los asuntos relacionados con la Tecnología de la Información.

Desarrollar e implementar políticas de seguridad que ayuden al correcto funcionamiento de la organización en general, en especial a los asuntos relacionados con la seguridad de la información y las redes; mecanismos que permitan ejecutar un control, administración y monitoreo de los asuntos relacionados con las Tecnologías de la Información eficiente, ya que la planificación de los mecanismos y procedimientos incrementan la probabilidad de éxito en el manejo de un sistema.

Establecer un plan de auditoria y actualización de los mecanismos que hacen posible el funcionamiento del sistema empresarial tanto para la funcionalidad de las aplicaciones y servicios como para los asuntos relacionados a la seguridad del sistema.

REFERENCIAS BIBLIOGRÁFICAS

CAPÍTULO I

[1]	VILLALÓN HUERTA, Antonio. "*Seguridad en Unix y Redes*". Versión 2.1. Julio 2002. Disponible en Web: http://www.rediris.es/cert/doc/unixsec/unixsec.pdf Capítulo 1: Introducción y conceptos previos. Pag. 1-16. Capítulo 15: Cortafuegos: Conceptos teóricos. Pag. 253-264. Capítulo 18: Sistemas de detección de intrusos. Pag. 313-325. Capítulo 21: Algunas Herramientas de Seguridad. Pag. 363-386.
[2]	STALLINGS, William. "*Comunicaciones y Redes de Computadores*". 7ma Edición. Prentice Hall. New Jersey. 2004. Capítulo 21: Seguridad en redes. Pag. 724-759.
[3]	CANAVAN, John. "*Fundamentals of Network Security*". Artech House. United States of America. 2001. Capítulo 1: Basic Security Concepts. Pag. 1-19. Capítulo 2: Threats, Vulnerabilities, and Attacks. Pag. 25-48. Capítulo 3: Encryption, Digital Signatures, and Certification Authorities. Pag. 55-72. Capítulo 5: Encryption on the World Wide Web. Pag. 80-83. Capítulo 6: E-Mail. Pag. 100-114. Capítulo 8: LAN Security. Pag. 170. Capítulo 14: Policies and Procedures. Pag. 239-245.

[4]	ARGENTINA. ArCERT. "*Manual de Seguridad en Redes*" [en línea]. 1999. Disponible en Web: http://www.arcert.gov.ar/ Capítulo 2: Políticas Generales de Seguridad. Pag. 17-18
[5]	MICROSOFT. Centro de Protección. "Virus y Gusanos" [en línea]. aaaa. Disponible en Web: http://www.microsoft.com/latam/athome/security/viruses/virus101.mspx#EPC
[6]	MICROSOFT. "*Enciclopedia Encarta*" [CD-ROM]. 2005. Temas: Hardware, Software, Datos.
[7]	SANS. "*Top-20 Internet Security Attack Targets*" [en línea]. Versión 7.0. Noviembre 2006. Disponible en Web: http://www.sans.org/top20/2006/?portal=dfc6f97e508c58aee728d21214a2a34a
[8]	KAUSTUBH, Phaltankar. "*Practical Guide for Implementing Secure Intranets and Extranets*". Artech House. United States of America. 2000. Capítulo 6: Virtual Private Network. Pag. 183-191
[9]	MAIWALD, Eric. "*Fundamentos de seguridad de redes*". Segunda Edición. McGraw-Hill. 2005. Capítulo: Fundamentos de seguridad de la información. Pag. 3-89
[10]	INTECO (España) Centro de Alerta Temprana sobre Virus y Seguridad Informática. "*Criterios Generales de Seguridad*" [en línea]. Disponible en Web: http://alerta-antivirus.inteco.es/seguridad/ver_pag.html?tema=S&articulo=2&pagina=0

[11]	RedIRIS. "*Herramientas de Seguridad*" [en línea]. 2004. Disponible en Web: http://www.rediris.es/cert/tools/

CAPÍTULO II

[12]	SECURE COMPUTING. "Unified Threat Management". 2007. Disponible en Web: http://www.securecomputing.com/index.cfm?skey=1477
[13]	FORTINET. "FortiGate Unified Threat Management" [en línea]. Disponible en Web: http://www.fortinet.com/ http://www.fortinet.com/products/fortigate_overview.html http://www.fortinet.com/doc/FGT1000-3800DS.pdf
[14]	JUNIPER. "Juniper Networks Firewall/IPSec VPN" [en línea]. Disponible en Web: http://www.juniper.net/ http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/index.html http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/isg_series_slash_gprs/
[15]	CISCO. "Cisco ASA 5500 Series Firewall" [en línea]. Disponible en Web: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd8048dba8.html