PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

TESIS DE GRADO PREVIO A LA OBTENCION DEL TÍTULO DE:

"MAGISTER EN REDES DE COMUNICACIONES"

TEMA:

"ESTUDIO DE LAS TECNOLOGIAS DE SEGURIDAD PERIMETRAL INFORMÁTICAS Y PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA LA AGENCIA NACIONAL DE TRÁNSITO"

DIEGO FRANCISCO CHICAIZA GARCIA

Quito, Junio 2014

RESUMEN

Este trabajo presenta, un estudio y análisis de las principales tecnologías de seguridad perimetral, para lo cual se revisará conceptos y características relacionados con la seguridad en redes; amenazas, vulnerabilidades, técnicas de ataque presentes en las redes. Luego a modo de ejemplo de diseño se analizará la red de la Agencia Nacional de Tránsito, tomando en cuenta aspectos como: servicios, aplicaciones, protocolos, acceso a Internet e Intranet, infraestructura existente, amenazas y vulnerabilidades a fin de realizar un diagnóstico sobre la seguridad actual y determinar los requerimientos de ésta red.

Posteriormente se presentará el plan de implementación del sistema de seguridad perimetral, considerando la tecnología más eficiente, de las analizadas y que se ajuste a los requerimientos de rendimiento y objetivos de seguridad, detallando sus características técnicas para la posterior adquisición e implementación en la Agencia Nacional de Tránsito.

DEDICATORIA

El presente trabajo, si bien ha requerido de esfuerzo y mucha dedicación de mi parte, no hubiese sido posible su finalización sin el apoyo total, cariño y comprensión de mi Esposa, quien ha sido mi soporte en todo momento.

AGRADECIMIENTO

Primero y antes que todo, quiero dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente.

A mi Esposa por brindarme su apoyo, confianza y sabiduría, compartiendo tanto alegrías como tristezas.

A los docentes de la Pontificia Universidad Católica del Ecuador quienes compartieron conmigo sus conocimientos y experiencias durante la maestría y la elaboración del proyecto de grado.

Al Director de Tecnologías de la Información y Comunicaciones que me permitió realizar este estudio en la Agencia Nacional de Tránsito.

Gracias a todos los que hicieron posible un triunfo más en mi vida.

DIEGO CHICAIZA

PRÓLOGO

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de información de una amplia variedad de amenazas como por ejemplo: acceso, uso, divulgación, interrupción o destrucción no autorizada. Su protección tiene como objeto asegurar la continuidad del negocio, minimizar los riesgos.

Por tal razón, se ha considerado realizar la investigación de las principales tecnologías que permiten minimizar riesgos derivados de vulnerabilidades informáticas.

En el capítulo 1 se detallan los objetivos y alcances del presente estudio.

El capítulo 2 expone conceptos y parámetros sobre seguridad de la información, políticas de seguridad, amenazas, vulnerabilidades y técnicas de ataque presentes en las redes.

El capítulo 3 describe las principales tecnologías de seguridad perimetral, sus características, arquitecturas, ventajas y desventajas.

El capítulo 4 realiza una descripción de la situación actual de la red de la Agencia Nacional de Tránsito a fin de determinar las vulnerabilidades presentes en ella.

En el capítulo 5 se realiza la propuesta de diseño del sistema de seguridad perimetral, exponiendo las especificaciones técnicas del equipamiento y el presupuesto referencial.

En el capítulo 6 se presentan las conclusiones y recomendaciones obtenidas a lo largo del presente estudio.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO DE TÉRMINOS Y LISTA DE SIGLAS, SÍMBOLOS Y ABREVIACIONES

LISTA DE SIGLAS, SÍMBOLOS Y ABREVIACIONES

AAA: Autenticación, Autorización y Contabilización.

ACL: Listas de Control de Acceso.

ANSI: Instituto Nacional Estadounidense de Estándares.

ANT: Agencia Nacional de Tránsito.

AP: Punto de Acceso.

BGP: Border Gateway Protocol.

CBIPS: Contenido de la Base IPS.

CD: Disco Compacto.

CNT: Corporación Nacional de Telecomunicaciones.

CPU: Unidad de Procesamiento Central.

CSO: Oficial de Seguridad Informática.

DCHP: Protocolo de Configuración de Host Dinámico.

DES: Estándar de Cifrado de Datos.

DMZ: Zona desmilitarizada.

DNS: Sistema de Nombres de Dominio.

DPI: Inspección Profunda de los Paquetes.

DVD: Disco de Vídeo Digital.

EIA: Electronics Industry Association.

ECC: Elliptical Curve Cryptography.

EGSI: Sistema Gubernamental de Seguridad de la Información.

EXE: Ficheros Ejecutables.

FTP: Protocolo de Transferencia de Ficheros.

GB: Gigabyte.

GNU/LINUX: Linux con el Sistema GNU.

HIDS: Sistemas de Detección de Intrusos para Hosts.

HIPS: IPS Basados en Host.

HTTP: Protocolo de Transferencia de Hipertexto.

HTTPS: Protocolo Seguro de Transferencia de Hipertexto.

IBM: International Business Machines Corporation.

ICMP: Protocolo de Mensajes de Control de Internet.

IMAP: Internet Message Access Protocol.

IP: Internet Protocol.

IPS: Sistema de Prevención de Intrusiones.

IPSec: Internet Protocol Security.

ISO: Organización Internacional de Estandarización.

ISP: Proveedor de Servicios de Internet.

IV: Vector de inicialización.

JVM: Máquina Virtual Java.

Kbps: Kilobits por segundo.

L2F: Reenvío de Capa Dos.

L2TP: Protocolo de Túnel de Capa Dos.

LAN: Red de Área Local.

MAC: Control de Acceso al Medio.

Mbit/s: Megabit por Segundo.

NAT: Conversión de Direcciones de Red.

NFS: Sistema de archivos de red.

NIDS: Sistemas de detección de intrusos para red.

NSA: Agencia de Seguridad Nacional.

P2P: Redes Entre Pares o Iguales.

PAT: Traslación de Direcciones Dinámico.

PDA: Asistente Digital Personal.

PEM: Correo Enriquecido con Carácter Privado.

PGP: Privacidad Bastante Buena.

PHP: Hypertext Preprocessor.

PIN: Número de Identificación Personal.

POE: Alimentación a través de Ethernet.

PPTP: Point to Point Tunneling Protocol.

PPTP: Protocolo para Paso de Punto a Punto.

PRTG: Paessler Router Traffic Grapher.

QOS: Calidad De Servicio.

RAM: Memoria de Acceso Aleatorio.

RFID: Identificación por Radio Frecuencia.

RIP: Ruteo Dinámico.

RPC: Protocolo de Llamada a Procedimiento Remoto.

S/MIME: Extensiones de Correo de Internet de Propósitos Múltiples/Seguro.

SAR: Servicio de Acceso Remoto.

SATA: Serial Advanced Technology Attachment.

SFP: Transceptor de Factor de Forma Pequeño Conectable.

SIP: Protocolo de Inicialización de Sesiones.

SLA: Acuerdo de Nivel de Servicio.

SMS: Mensaje Corto de Texto.

SMTP: Protocolo para la Transferencia Simple de Correo Electrónico.

SOHO: Pequeña Oficina - Oficina en Casa.

SPI: Inspección de Estado de los Paquetes.

SQL: Lenguaje de Consulta Estructurado.

SSL: Sapa de Conexión Segura.

TIA: Telecommunications Industry Association

TCI: Tarjeta con Circuito Integrado.

TCP: Protocolo de Control de Transmisión.

TIC: Las tecnologías de la información y la comunicación.

TLS: Seguridad de la Capa de Transporte.

UDP: Protocolo de Datagrama de Usuario.

UPS: Sistema de Alimentación Ininterrumpida.

URL: Localizador de Recursos Uniforme.

USB: Bus de Serie Universal.

UTM: Gestión unificada de Amenazas.

VPN: Red Privada Virtual.

WAN: Red de Área Amplia.

GLOSARIO DE TÉRMINOS

Amenaza: Situación o evento con que puede provocar daños en un sistema.

Análisis de vulnerabilidades: Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.

Ancho de Banda: En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado, se mide en millones de bits por segundo (Mbps).

Antivirus: Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos.

Aplicación engañosa: Aplicación cuya apariencia y comportamiento emulan a una aplicación real. Normalmente se utiliza para monitorizar acciones realizadas por atacantes o intrusos.

Ataque por interceptación: Estrategia de ataque en la que el atacante intercepta una comunicación entre dos partes, substituyendo el tráfico entre ambas a voluntad y controlando la comunicación.

Autenticación: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.).

Autorización: Acción de otorgar el acceso a usuarios, objetos o procesos. Basado en reglas: En detección de intrusiones, que utiliza patrones de actividad (generalmente ataques conocidos) para reconocer una intrusión.

Backup: En informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Base de reglas: Conjunto de reglas utilizadas para analizar los registros de datos. Caballo de Troya, troyano: Programa informático de aspecto inofensivo que

oculta en su interior un código que permite abrir una "puerta trasera" en el sistema en que se ejecuta. Capacidad de ser registrado: Habilidad de relacionar una determinada actividad o evento con la parte responsable.

Bug: Es un error o un defecto del software o hardware que hace que un programa funcione incorrectamente.

Cableado: Columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro. La reciente aparición de las redes inalámbricas ha roto el esquema tradicional al no utilizar ningún tipo de cableado.

Cifrado: Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.

Cliente.- Aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red. Sistema o proceso el cual le solicita a otro sistema o proceso la prestación de un servicio.

Composición: En seguridad informática, combinar un conjunto de componentes en un sistema para obtener los atributos de seguridad del sistema, según las propiedades de los componentes.

Comprobador de integridad: Herramienta de seguridad que utiliza funciones resumen basadas en algoritmos de cifrado para detectar alteraciones en objetos de sistema.

Conexión Remota.- Operación realizada en una computadora remota a través de una red de computadoras, como si se tratase de una conexión local.

Control de acceso discrecional: Política de acceso a los datos en la que el propietario del objeto, de forma voluntaria (discrecional), concede o deniega el acceso a éste a otros sujetos.

Control de acceso: Limitar el acceso a objetos de acuerdo a los permisos de acceso del sujeto.

Control de accesos obligatorio (MAC): Política de acceso a los datos en la que el sistema comparte de forma obligatoria tanto los objetos como los sujetos. A partir de dicha forma de compartir los elementos, se establecen unas reglas de acceso.

Cortafuegos: Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad mediante el uso de políticas de control de acceso de nivel de red.

Data center: Se denomina centro de procesamiento de datos a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Detección de intrusiones: Proceso de monitorizar los eventos de un sistema o red en busca de signos que indiquen problemas de seguridad.

Exploit: Es una pieza de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Gusano: Es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Hashing: Técnica que sirven para proteger la información. El hashing resume el texto en una pequeña huella que no puede descifrarse.

Housing: Consiste básicamente en vender o alquilar un espacio físico de un centro de datos para que el cliente coloque ahí su propia infraestructura.

Hosting: Consiste básicamente en vender o alquilar el espacio físico donde se van a almacenar los archivos que conforman su web, sus correos electrónicos y demás información.

Javascript: Es un lenguaje de programación utilizado para crear pequeños programitas encargados de realizar acciones dentro del ámbito de una página web.

Login: Es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario.

Logs: Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste.

Malware: También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

Pendrive: Es un dispositivo de almacenamiento que utiliza una memoria flash para guardar información.

Phishing: Es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Política de seguridad: 1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. 2. Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.

Puerta trasera: Mecanismo que permite a un atacante entrar y controlar un sistema de forma oculta. Suelen instalarse justo después de comprometer un sistema.

Puntos de acceso inalámbricos: Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. También puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Red privada virtual: Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

Router: Es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes.

Script: Es un pequeño código de programación que son típicamente interpretados y pueden ser tipeados directamente desde el teclado.

Sistema de prevención de intrusiones: Sistema que combina las capacidades de bloqueo de un cortafuegos y las de análisis de un IDS. Está diseñado para detener ataques antes de que tengan éxito.

Sniffing: Se trata de dispositivos que permiten al atacante “escuchar” las diversas comunicaciones que se establecen entre ordenadores a través de una red (física o inalámbrica) sin necesidad de acceder física ni virtualmente a su ordenador.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Spam: Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

Spoofing: Hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de o de investigación.

Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Switch: Es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI.

Troyano: Es software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo le brinda a un atacante acceso remoto al equipo infectado.

Virus: Son programas que tienen la característica de replicarse y propagarse por sí mismo, Algunos virus solo infectan, otros modifican datos y otros más destructivos, eliminan datos, pero los hay otros que solo muestran mensajes.

Vulnerabilidades: Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.

Zona desmilitarizada: Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar, y se utiliza para definir un área situada entre dos enemigos.

CAPÍTULO 1

INTRODUCCIÓN

1.1 DESCRIPCIÓN GENERAL DEL PROYECTO

1.1.1 Introducción

Teniendo como premisa la información como el recurso más valioso de una empresa, y considerando que en la actualidad la misma se enfrenta cada vez más a riesgos e inseguridades procedentes de una amplia variedad de fuentes que pueden causar daños importantes en los sistemas de información y poner en peligro la continuidad del negocio. Ante estas circunstancias es imprescindible que las empresas evalúen los riesgos asociados y establezcan las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

Ciudadanos y empresas son cada vez más dependientes de la informática tanto para la gestión de negocios como para el entretenimiento. Con el desarrollo de la Sociedad de la Información y la proliferación del uso de Internet y sus tecnologías asociadas, han aparecido los primeros inconvenientes traducidos básicamente en problemas de seguridad que pueden ser evitados.

Este trabajo presentará, un estudio y análisis de las principales tecnologías de seguridad perimetral, para lo cual se revisará conceptos y características relacionados con la seguridad perimetral en redes; amenazas, vulnerabilidades, técnicas de ataque presentes en las redes. Luego a modo de ejemplo de diseño se analizará la red de la Agencia Nacional de Tránsito, tomando en cuenta aspectos como: servicios, aplicaciones, protocolos, acceso a Internet e Intranet,

infraestructura existente, amenazas y vulnerabilidades a fin de realizar un diagnóstico sobre la seguridad actual y determinar los requerimientos de ésta red. Posteriormente se presentará el diseño del sistema de seguridad perimetral, considerando la tecnología más eficiente, de las analizadas y que se ajuste a los requerimientos de rendimiento y objetivos de seguridad, detallando sus características técnicas para la posterior adquisición e implementación en la Agencia Nacional de Tránsito.

1.2 JUSTIFICACIÓN

Las amenazas de seguridad que enfrentan las redes son suficientes para pensar en las posibles soluciones que disponemos en la actualidad para enfrentar dichas amenazas, esto nos plantea el problema de cuál es la mejor manera para resolver esta situación. Estas intrusiones no deseadas pueden ser detenidas siempre y cuando las organizaciones definan e implementen de una manera clara sus opciones en seguridad perimetral, esto en concordancia con las políticas de seguridad previamente establecidas.

En un alto porcentaje las organizaciones, carecen de profesionales y recursos en el tema de seguridad de redes y por tal razón permanentemente están expuestas tanto a amenazas internas por medio de sus empleados, como a amenazas externas generadas por terceras partes de forma intencionada, con el objeto de causar algún tipo de perjuicio u obtener un beneficio, generalmente económico, de los ataques producidos contra los sistemas de una organización a través de la red.

Para prevenir y contrarrestar una amplia gama de amenazas a las redes, es necesario conocer sus vulnerabilidades e identificar diversos tipos de ataques.

En este proyecto se desea investigar las tecnologías de seguridad perimetral más actuales y que son factibles de implementar en el contexto de las instituciones con una relación costo beneficio favorable a fin de diseñar un sistema de seguridad perimetral y considerando los componentes necesarios que detecten ataques maliciosos, infección involuntaria para poder analizarlos,

contrarrestarlos y a demás que garantice la seguridad y disponibilidad de los servicios e información.

La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de segurización en el perímetro externo de la red y a diferentes niveles. Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros [1].

La seguridad perimetral:

- No es un componente aislado: es una estrategia para proteger los recursos de una organización conectada a la red
- Es la realización práctica de la política de seguridad de una organización. Sin una política de seguridad, la seguridad perimetral no sirve de nada
- Condiciona la credibilidad de una organización en Internet

1.3 ANTECEDENTES

Durante los primeros años de internet, los ataques a sistemas informáticos requerían pocos conocimientos técnicos. Por un lado, los ataques realizados desde el interior de la red se basaban en la alteración de permisos para modificar la información del sistema. Por el contrario, los ataques externos se producían gracias al conocimiento de las contraseñas necesarias para acceder a los equipos de la red. [2]

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de las redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a internet. Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos. [3]

Los intentos de fraude tradicionalmente identificados tienen también presencia en el mundo de Internet, en el que nuevas herramientas y posibilidades de comunicación están también a disposición del timador. El acceso a servicios que requieren una especial confidencialidad, como es la banca electrónica, el comercio electrónico o los portales que facilitan los trámites con la administración, aumentan cada día y nos permiten realizar casi cualquier tipo de operación a través de Internet, pero constituyen también un objetivo para colectivos con intenciones deshonestas. Por todo ello, es necesario prestar una atención especial a las condiciones de seguridad con las que accedemos a estos servicios y así evitar ser víctima de cualquier intento de fraude. [4]

Con la aparición de grupos de hackers activistas quienes han realizado ataques masivos a portales web de instituciones públicas como la Presidencia, Ministerio de Telecomunicaciones, Vicepresidencia, Alcaldía de Quito, Corporación Nacional de Telecomunicaciones entre otras y el creciente aumento de los cyber delitos, vemos la necesidad de contar con la infraestructura de seguridad y políticas bien definidas para solventar las vulnerabilidades a las que está expuesta la información. Un ejemplo de estos grupos de hackers es Anonymous que ha saboteado programas en todo el mundo. La página web de la presidencia de Colombia fue intervenida por este grupo, y han hecho lo propio en España, Perú, Chile, entre otros países. Uno de sus últimos golpes fue a las páginas del FBI y a la compañía de ciberseguridad ManTech, que se encarga de guardar información confidencial. También han ingresado en otros organismos del gobierno de los Estados Unidos. [5]

La Agencia Nacional de Tránsito es el ente encargado de planificar, regular y controlar la gestión del Transporte Terrestre, Tránsito y Seguridad Vial en el territorio nacional, a fin de garantizar la libre y segura movilidad terrestre, prestando servicios de calidad que satisfagan la demanda ciudadana; coadyuvando a la preservación del medio ambiente y contribuyendo al desarrollo del País, en el ámbito de su competencia. [6]

La situación del desarrollo tecnológico de la Agencia Nacional de Tránsito ha experimentado una serie de modificaciones y cambios con respecto a las leyes y reglamentos, así como a definiciones operativas y técnicas, y de talento humano.

La decisión de adquirir y poner en producción el nuevo sistema de tránsito se apalanca en acciones políticas y en cambios tecnológicos en los que se tienen que realizar inversiones en corto y mediano plazo.

1.4 OBJETIVOS

1.4.1 General

Analizar las principales tecnologías de seguridad perimetral informática y propuesta de un plan de implementación para la Agencia Nacional de Tránsito, tomando en cuenta las características técnicas y económicas.

1.4.2 Específicos

- Conocer los conceptos, características, amenazas, vulnerabilidades y mecanismos relacionados con la Seguridad en Redes.

- Estudiar las principales tecnologías de seguridad perimetral realizando un análisis de las mismas para comprender de mejor manera su funcionamiento y poder utilizarlas de una forma más eficiente en el presente trabajo investigativo.

- Analizar la red de la Agencia Nacional de Tránsito para determinar las amenazas y vulnerabilidades presentes en la misma.

- Determinar la tecnología de seguridad perimetral más eficaz, para finalmente diseñar el sistema de seguridad perimetral y los dispositivos de seguridad, detallando sus características técnicas.

CAPÍTULO 2

ESTADO DEL ARTE

2.1 SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de información de una amplia variedad de amenazas como por ejemplo: acceso, uso, divulgación, interrupción o destrucción no autorizada. Su protección tiene como objeto asegurar la continuidad del negocio, minimizar los riesgos (combinación de la probabilidad de ocurrencia de un evento y sus consecuencias) y maximizar el retorno de la inversión y las oportunidades del negocio. [7]

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 o empresa. 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 seguridad informática puede dividirse en tres disciplinas: seguridad física, seguridad ambiental y seguridad lógica, las cuales deben actuar coordinadamente evaluando y tratando los riesgos para implementar medidas con el fin de minimizar el impacto ante un incidente de seguridad de la información (Indicado por uno o serie de eventos de seguridad de la información no deseados o no esperados que pueden tener una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información). [7]

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 vital 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.

2.1.1 Definición

La seguridad de la información, es un conjunto de reglas, planes y acciones que permiten asegurar la información manteniendo las propiedades de confidencialidad, integridad y disponibilidad. [8]

2.1.2 Requisitos

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. [9]

Las técnicas para llegar a una correcta organización están basadas en 5 pilares fundamentales que hacen que la información se encuentre protegida. Estos pilares se ocupan principalmente de proteger cinco aspectos de la información [14]:

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Autenticación.
- No repudio.

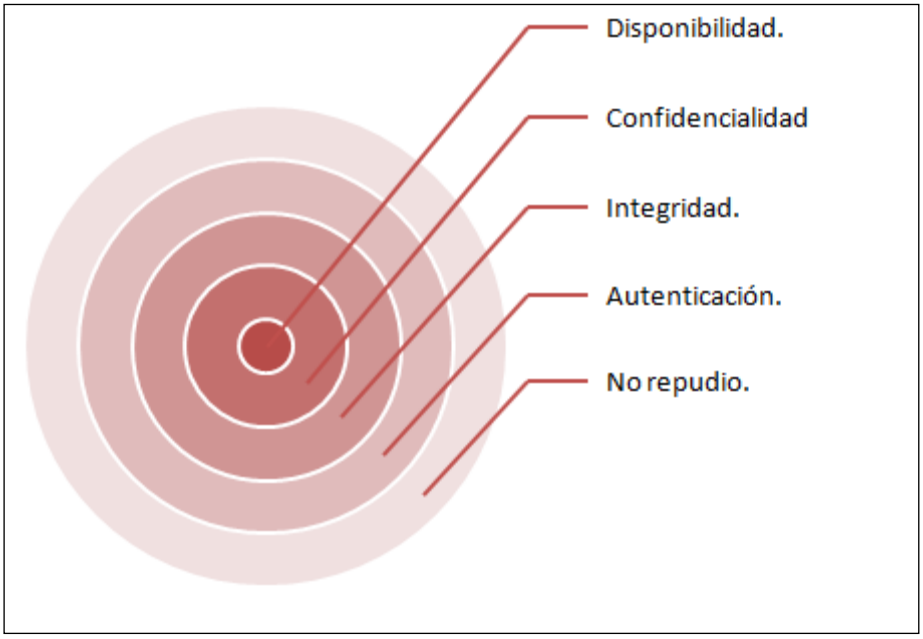


Figura 2.1.1 Relación de los servicios de seguridad

Fuente: Costas, J. (2010)

2.1.2.1 Confidencialidad.

Se trata de la cualidad que debe tener la información para que ésta sea accedida únicamente por las personas o sistemas que tienen autorización para hacerlo. [10]

2.1.2.2 Integridad.

Se trata de la cualidad que debe tener la información para garantizar que ésta no ha sido borrada, copiada o alterada, no sólo en su trayecto, sino también desde su origen. [11]

2.1.2.3 Disponibilidad.

Se trata de la capacidad de un servicio, de los datos o sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando éstos lo requieran. También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo,

bien sea por ataques dolosos, mala operación accidental o situaciones fortuitas o de fuerza mayor[1]. [10]

2.1.2.4 Autenticación.

La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice.

Aplicando a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. La autenticación en los sistemas informáticos habitualmente se realiza mediante un usuario y una contraseña (password)[2]. [10]

2.1.2.5 No repudio.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero, de este modo, existirán dos posibilidades [10]:

- **No repudio en origen:** el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

- **No repudio en destino:** El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente

[1] Por caso fortuito entendemos la situación no prevista, aleatoria y en la que no existió voluntad de alguien en su creación. También se está relacionado con el concepto de fuerza mayor y en todo caso debe diferenciarse de otros términos como, por ejemplo, negligencia, donde se ha descuidado la actuación debida. http://www.derecho.com/c/Caso+fortuito.

[2] En la lengua inglesa se tienen dos denominaciones distintivas para las contraseñas: password (palabra de acceso) y pass code (código de acceso).

lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

2.1.3 Elementos Vulnerables.

Los elementos de información son todos los componentes que contienen, mantienen o guardan información también son llamados Activos o Recursos. [12]

2.1.3.1 Hardware

Firtman (2005,p.20) encontró lo siguiente:

El hardware se encuentra formado por todos los elementos físicos de un sistema informático, como CPU, terminales, cableado, medios de almacenamiento (Cintas, CD\DVD - ROM, etc.) o tarjetas de red.

2.1.3.2 Software

El software es el conjunto de programas lógicos que hacen funcionar el hardware, tanto en sistemas operativos como aplicaciones. "Ibíd."

2.1.3.3 Datos.

Los información son el conjunto de datos que manejan el software y hardware (registros, entradas en base de datos, paquetes que viajan por los cables de red). Vale aclarar que no es lo mismo dato que información. Un dato no tiene coherencia por sí solo, sino que la tiene por medio de un entorno o contexto. Si bien el dato es esencial, el juicio sobre lo que se debe hacer con el mismo se realiza por medio de un programa o persona. "Ibíd."

A diferencia de los datos, la información sí tiene significado. Es más, los datos se convierten en información cuando su creador les añade significado.

2.1.3.4 Elementos fungibles.

Son elementos que se gastan o desgastan con el uso continuo (papel de impresión, tóner, cintas magnéticas) insumos en general y todo lo que de alguna

manera está conectado a una máquina. Algunos administradores de seguridad no consideran estos elementos para protegerlos, y están equivocados.

Una buena administración se basa en controlar los recursos de la empresa, ya que los mismos no son infinitos ni el dinero con el que se cuenta es ilimitado, y menos para usarlo como gasto y no como inversión. Para lograr eficiencia y calidad se tiene que tomar conciencia y crear una política para el correcto uso de las herramientas con las que cuenta la empresa. "Ibíd."

2.1.4 Amenazas

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales. [13]

2.1.4.1 Formas de la amenaza. [17]

Firtman (2005,p.21 -24) encontró lo siguiente: Las cuatro categorías generales de amenazas son las siguientes:

2.1.4.1.1 Interrupción (Ataque contra la disponibilidad).

Cuando los datos o la información de un sistema se ven corruptos, ya sea porque los mismos se han perdido, se han bloqueado o simplemente porque no están disponibles para su uso. Este tipo de amenaza en la mayoría de las ocasiones no tiene mucha lógica por parte del atacante, salvo que se vea encerrado o perseguido.

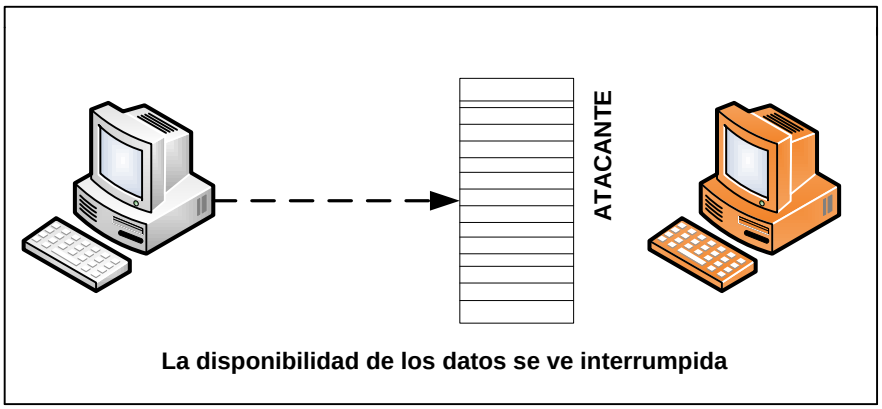


Figura 2.1.2 Como se paraliza el flujo de datos.

Fuente: Firtman, S. (2005)

2.1.4.1.2 Intercepción (Ataque contra la confidencialidad).

Esta amenaza logra que un usuario no autorizado pueda acceder a un recurso y, por ende, la confidencialidad se vea divulgada. Hay muchos tipos de intercepción, por ejemplo, cuando se intercepta la cabecera de los paquetes y logramos identificar usuarios tanto del lado del remitente como del receptor; eso es llamado interceptación de identidad, en cambio, el sniffear (ver legítimamente la información que pasa por un medio) se llama sencillamente interceptación de datos. "Ibíd."

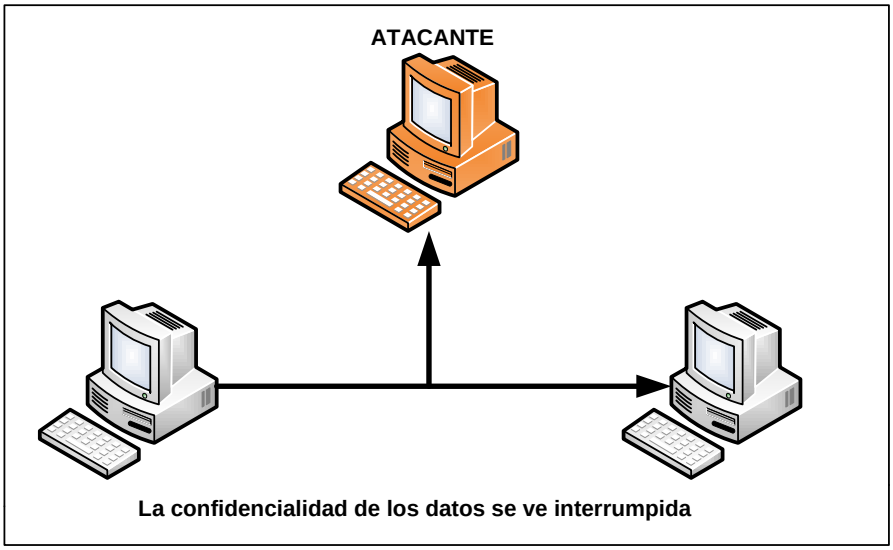


Figura 2.1.3 Desvío de los datos.

Fuente: Firtman, S. (2005)

2.1.4.1.3 Modificación (Ataque contra la integridad).

Un atacante, que puede contar o no con autorización para ingresar al sistema, manipula los datos de tal manera que la integridad se ve afectada por su accionar. Cambiar datos de archivos, modificar paquetes, alterar un programa o aplicación son sólo algunos ejemplos de este tipo de ataque que, sin ninguna duda, es el que reviste mayor grado de peligrosidad. "Ibíd."

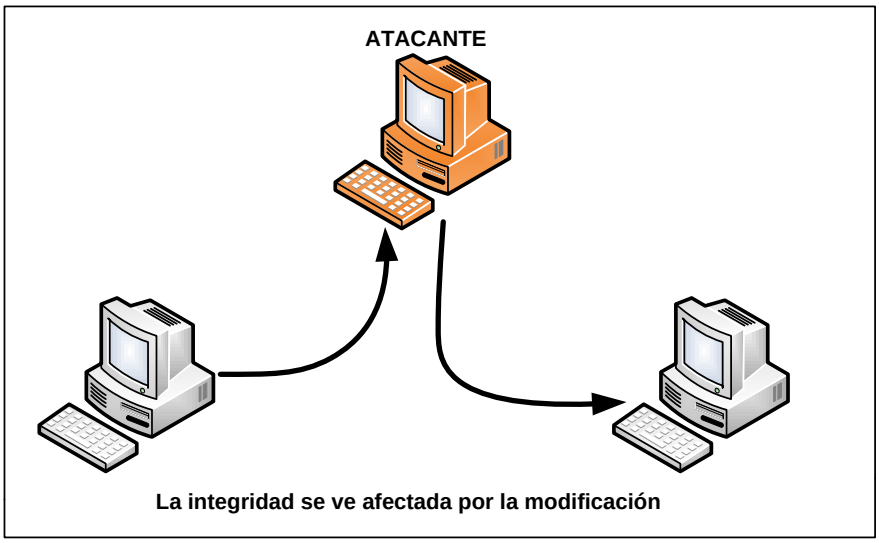


Figura 2.1.4 Esquema de flujo de datos inventado.

Fuente: Firtman, S. (2005)

2.1.4.1.4 Fabricación (Ataque contra la autenticidad).

El ataque contra la autenticidad tiene lugar cuando un usuario malicioso consigue colocar un objeto en el sistema atacado.

Este tipo de ataque puede llevarse a cabo con el objeto de hacer creer que ese archivo/paquete es el correcto o bien con la finalidad de agregar datos y obtener, de esta manera, un provecho propio. "Ibíd."

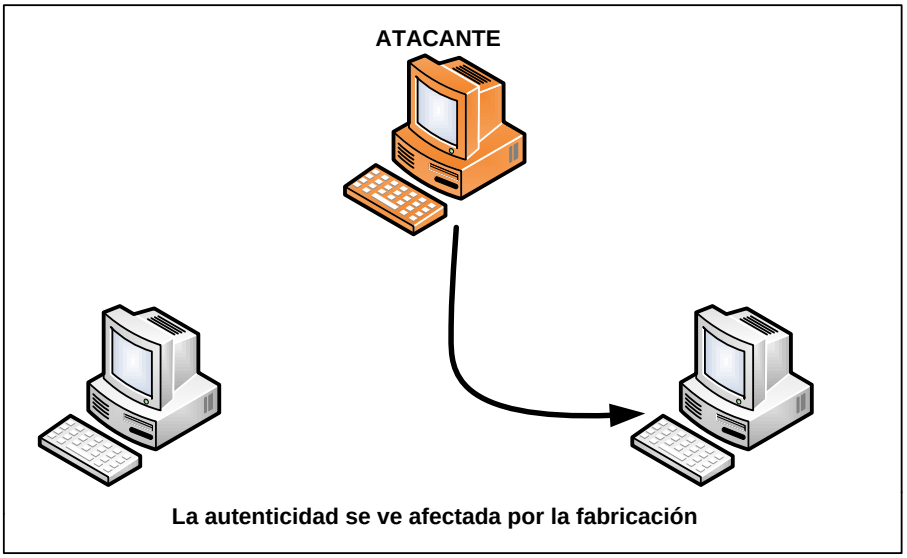


Figura 2.1.5 El momento de cambio de datos.

Fuente: Firtman, S. (2005)

2.1.4.2 Tipos de Amenaza.

Los ataques anteriormente descritos, se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

2.1.4.2.1 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.

2.1.4.2.2 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.

2.1.4.3 Origen de las Amenazas. [10]

Costas, J. (2010, pag.32,33), encontró lo siguiente:

A esta altura de los tiempos y con las sociedades que evolucionan, suena raro decir que estamos cuidándonos de nosotros mismos y, más aún sabiendo que esos elementos que protegemos son, en su mayoría, cosas creadas por nosotros mismos. El factor más importante que incita a las personas a cometer actos en contra de los cuatro pilares (integridad, disponibilidad, confidencialidad y autenticidad) es, sin ninguna duda, el poder. Este poder reside en los datos y en la información, y son compartidos por el mundo.

2.1.4.3.1 Humanas.

La mayoría de ataques a nuestros sistemas van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando algunos de los riesgos lógicos, especialmente agujeros de software. "Ibíd."

A continuación se describen los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para los sistemas; generalmente se dividen en dos grandes grupos: los atacantes pasivos aquellos que fisgonean por el sistema pero no lo modifican o destruyen, y los activos aquellos que dañan el objetivo atacado, o lo modifican en su favor.

- **Personal.** Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce los sistemas y sus debilidades), lo normal es que más que ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad. "Ibíd."

- **Ex-empleados.** Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente, pueden insertar software malicioso o simplemente

conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la empresa), conseguir el privilegio necesario, y dañarlo de la forma que deseen, incluso chantajeando a sus ex compañeros o ex jefes. "Ibíd."

- **Curiosos.** Los curiosos son los atacantes más habituales de sistemas. En la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema. "Ibíd."

- **Hacker.** Es un término general que se ha utilizado históricamente para describir a un experto en programación.

  Los hackers han evolucionado de ser grupos clandestinos a ser comunidades con identidad bien definida. De acuerdo a los objetivos que un hacker tiene, y para identificar las ideas con las que comulgan, se clasifican principalmente en: hackers de sombrero negro, de sombrero gris, de sombrero blanco, script kiddie y Phreaker. [14]

  - **Hackers de sombrero negro:** Se le llama hacker de sombrero negro a aquel que penetra la seguridad de sistemas para obtener una ganancia personal o simplemente por malicia. La clasificación proviene de la identificación de villanos en las películas antiguas del vejo oeste, que usaban típicamente sombreros negros. [14]
  - **Hackers de sombrero blanco:** Se le llama hacker de sombrero blanco a aquel que penetra la seguridad de sistemas para encontrar puntos vulnerables. La clasificación proviene de la identificación de héroes en las películas antiguas del viejo oeste, que usaban típicamente sombreros blancos. [14]

- **Hackers de sombrero gris:** Se le llama hacker de sombrero gris a aquel que es una combinación de sombrero blanco con sombrero negro, dicho en otras palabras: que tiene ética ambigua. Pudiera tratarse de individuos que buscan vulnerabilidades en sistemas y redes, con el fin de luego ofrecer sus servicios para repararlas bajo contrato. [14]
- **Script kiddies:** Se les denomina script kiddies a los hackers que usan programas escritos por otros para lograr acceder a redes de computadoras, y que tienen muy poco conocimiento sobre lo que está pasando internamente. [14]
- **Phreaker.** El Phreaker es el hacker de los sistemas telefónicos, telefonía móvil, tecnologías inalámbricas y la voz sobre IP (VoIP). Un phreaker es una persona que investiga los sistemas telefónicos, mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas.[15]

- **Cracker.** Es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa. Cracker viene del inglés "crack" (romper) y justamente es lo que ellos hacen. Saben más o menos lo mismo que los hackers pero no comparten la ética. Por consiguiente, no les importa romper una arquitectura o sistema una vez dentro, ni tampoco borrar, modificar o falsificar algo; es por eso que la teoría habla de que: los hackers son buenos y los crackers son malos. [10]

- **Intrusos remunerados.** Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una persona generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía) o simplemente para dañar la imagen de la entidad afectada.

2.1.4.3.2 Amenazas Lógicas.

Costas, J. (2010,pag. 34-37), encontró lo siguiente:

Constituyen todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros).

- **Software incorrecto.** A los errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits.
- **Herramientas de seguridad.** Cualquier herramienta de seguridad representa un arma de doble filo; de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.
- **Puertas traseras.** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar atajos en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando.
- **Bombas lógicas.** Estas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

2.1.4.3.3 Amenazas físicas.

Algunas de las amenazas físicas que pueden afectar a la seguridad y por tanto al funcionamiento de los sistemas son, "Ibíd.":

- Robos, sabotajes, destrucción de sistemas.
- Cortes, subidas y bajadas bruscas de suministro eléctrico.
- Condiciones atmosféricas adversas. Humedad relativa excesiva o temperaturas extremas que afecten al comportamiento normal de los componentes informáticos. "Ibíd."
- Catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales, simplemente por su ubicación geográfica. Un

subgrupo de las catástrofes es el denominado de riesgos poco probables. Como ejemplos de catástrofes tenemos terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podemos pensar). "Ibíd."

2.1.5 Vulnerabilidades. [16]

Alulema, D. (2008,pag. 9-12), encontró lo siguiente:

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

2.1.5.1 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. "Ibíd."

2.1.5.2 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. "Ibíd."

2.1.5.3 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. "Ibíd."

2.1.6 Mecanismos.

Un mecanismo de seguridad es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático. "Ibíd."

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

2.1.6.1 Mecanismos de prevención.

Son aquellos cuya finalidad consiste en prevenir la ocurrencia de un ataque informático. Básicamente se concentran en el monitoreo de la información y de los bienes, registro de las actividades que se realizan en la organización y control de todos los activos y de quienes acceden a ellos. "Ibíd."

- **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). "Ibíd."

- **Mecanismos de control de acceso**

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

- **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. "Ibíd."

- **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. "Ibíd."

2.1.6.2 Mecanismos de detección.

Son aquellos que tienen como objetivo detectar todo aquello que pueda ser una amenaza para los bienes. Ejemplos de éstos son las personas y equipos de monitoreo, quienes pueden detectar cualquier intruso u anomalía en la organización. "Ibíd."

2.1.6.3 Mecanismos de respuesta.

Estos se encargan de reparar los errores cometidos o daños causados una vez que se ha cometido un ataque, o en otras palabras, modifican el estado del sistema de modo que vuelva a su estado original y adecuado. "Ibíd."

- **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. "Ibíd."

2.1.7 Modelos de Seguridad.

Un modelo de seguridad es un diseño formal que promueve consistentes y efectivos mecanismos para la definición e implementación de controles. Los componentes deben estar dirigidos a identificar los niveles de riesgo presentes y las acciones que se deben implementar para reducirlos. "Ibíd."

2.1.7.1 Seguridad por Oscuridad.

La seguridad por oscuridad es un controvertido principio de ingeniería de la seguridad, que intenta utilizar el secreto (de diseño, de implementación, etc.) para garantizar la seguridad. Este principio se puede plasmar en distintos aspectos como por ejemplo "Ibíd.":

- Mantener el secreto del código fuente del software.
- Mantener el secreto de algoritmos y protocolos utilizados.
- Adopción de políticas de no revelación pública de la información sobre vulnerabilidades.

Un sistema que se apoya en la seguridad por ocultación puede tener vulnerabilidades teóricas o prácticas, pero sus propietarios o diseñadores creen que sus puntos débiles, debido al secreto que se mantiene sobre los entresijos del sistema, son muy difíciles de encontrar, y por tanto los atacantes tienen muy pocas probabilidades de descubrirlos. "Ibíd."

2.1.7.2 Perímetro de defensa.

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

- **A nivel de red.** Busca proteger al sistema informático de los ataques de hackers, intrusiones o robo de información en conexiones remotas. "Ibíd."

- **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. "Ibíd."

2.1.7.3 Defensa en profundidad.

Estrategia de seguridad usando distintas técnicas para limitar los daños en el caso de intrusión, es el modelo más robusto y consiste en la protección y monitoreo de cada sistema aisladamente, dotándoles de la capacidad de defenderse por sí mismos. [18]

La defensa en profundidad tiene una doble finalidad:

1) Reforzar la protección del sistema de información mediante un enfoque cualitativo que permita verificar la finalización y la calidad del dispositivo.
2) Brindar un medio de comunicación que permita a los responsables de la toma de decisiones y a los usuarios tomar conciencia de la gravedad de los incidentes de seguridad.

La defensa en profundidad consiste en la implementación de una serie de prácticas que permiten asegurar los sistemas y redes de una organización en diversas capas y su principio se basa en que cada capa al estar asegurada utilizando buenas prácticas, ayudará a mitigar los ataques y reducir el impulso del ataque conforme este avance en cada una de las capas.

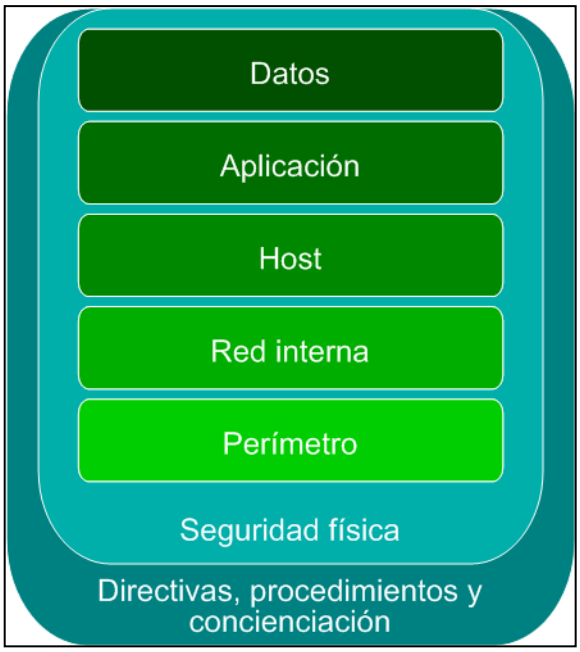


Figura 2.1.6 Capas del modelo de seguridad en profundidad.

Fuente: Technet (2014).

Las capas de dicho modelo consisten en:

1. Directivas, procedimientos y concienciación: Consiste en todas las normas o políticas de seguridad, la concienciación hacia los usuarios en materia de seguridad, que permitan entablar la base para las siguientes capas.
2. Seguridad Física: En esta capa se busca implementar todas aquellas medidas de seguridad que permitan resguardar los activos físicos de la organización.
3. Seguridad Perimetral: Consiste en la implementación de todas aquellas medidas que permitan asegurar la red de la organización.
4. Seguridad de la Red Interna: En esta capa se pueden implementar sistemas de detección de intrusiones, sistemas de prevención de intrusiones, entre otras medidas que permitan mitigar los ataques provenientes desde internet.
5. Seguridad en el Host: Esta capa busca asegurar los servidores y estaciones de trabajo de la organización, realizado el proceso de hardening.

6. Seguridad en las aplicaciones: En este nivel del modelo, se realizan prácticas para garantizar que las aplicaciones sean seguras, como realización de auditorías a las aplicaciones constantemente.
7. Seguridad en los datos: Este que es el ultimo nivel, consiste en las medidas que permitan manejar los datos de manera segura.

Las capas Datos, Aplicación y Host se pueden combinar en dos estrategias defensivas para proteger los clientes y servidores de la organización. Aunque estas defensas comparten determinadas estrategias, las diferencias al implementarlas en el cliente y en el servidor son suficientes para hacer necesario un único enfoque defensivo en cada una de ellas.

Las capas Red interna y Red perimetral también se pueden combinar en una estrategia de defensas de red común, ya que las tecnologías implicadas son las mismas para ambas. Sin embargo, los detalles de la implementación diferirán en cada capa, según la posición de los dispositivos y las tecnologías de la infraestructura de la organización. [47]

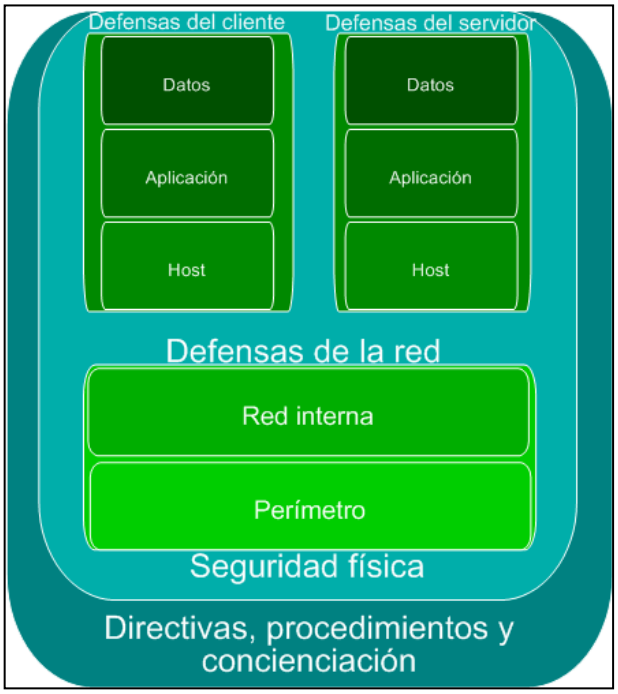


Figura 2.1.7 Vista de una defensa en profundidad específica

Fuente: Technet (2014)

2.2 POLÍTICAS DE SEGURIDAD. [19]

Gómez, A. (2006, pág. 25-72) encontró que:

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. "Ibíd."

2.2.1 Políticas y procedimientos.

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. "Ibíd."

2.2.1.1 Procedimiento de seguridad.

Un procedimiento de seguridad es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los procedimientos de seguridad permiten aplicar e implantar las Políticas que han sido aprobadas por la organización. "Ibíd."

Los procedimientos de seguridad se descomponen en tareas y operaciones concretas, las cuales, a su vez, pueden generar una serie de registros y evidencias que facilitan el seguimiento, control y supervisión del funcionamiento de un sistema de gestión de la información. "Ibíd."

Los procedimientos de seguridad permiten implementar las políticas de seguridad definidas, describiendo cuáles son las actividades que se tienen que realizar en el sistema, en qué momento o lugar, quiénes serían los responsables de su ejecución y cuáles serían los controles aplicables para supervisar su correcta ejecución. "Ibíd."

2.2.1.2 Políticas de seguridad.

Podemos definir una Política de Seguridad como una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

Las políticas definen qué se debe proteger en el sistema, mientras que los procedimientos de seguridad describen el cómo se debe conseguir dicha protección. "Ibíd."

2.2.2 Objetivo de las políticas de seguridad.

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. "Ibíd."

2.2.2.1 Administración de riesgos.

La administración de riesgos es el proceso iterativo basado en el conocimiento, valoración, tratamiento y monitoreo de los riesgos y sus impactos en el negocio. Es casi imposible asegurar completamente el patrimonio informático de una organización, ya que los riesgos se pueden minimizar, pero nunca eliminarlos completamente. "Ibíd."

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

2.2.2.2 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. "Ibíd."

2.2.2.3 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. "Ibíd."

2.2.2.4 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. "Ibíd."

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. "Ibíd."

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

2.2.2.5 Proteger a la organización de la responsabilidad.

La existencia de políticas y procedimientos son esenciales 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. "Ibíd."

2.2.2.6 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. "Ibíd."

2.2.3 Desarrollo de las políticas de seguridad.

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. "Ibíd."

A continuación se presentan de forma esquemática las principales características y requisitos que deberían cumplir las políticas de seguridad:

- Las políticas de seguridad deberían poder ser implementadas a través de determinados procedimientos administrativos y la publicación de unas guías de uso aceptable del sistema por parte del personal, así como mediante la instalación, configuración y mantenimiento de determinados dispositivos y herramientas hardware y software que implanten servicios de seguridad. "Ibíd."
- Deben definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización. "Ibíd."
- Deben cumplir con las exigencias del entorno legal (Protección de datos personales, protección de la propiedad intelectual, código penal). "Ibíd."

- Se tienen que revisar de forma periódica para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal. En este sentido, se debería contemplar un procedimiento para garantizar la revisión y actualización periódica de las políticas de seguridad. "Ibíd."
- Aplicación del principio de defensa en profundidad: definición e implantación de varios niveles o capas de seguridad. Así, si un nivel falla, los restantes todavía podrían preservar la seguridad de los recursos del sistema. De acuerdo con este principio es necesario considerar una adecuada selección de medidas de prevención, de detección y de corrección. "Ibíd."
- Asignación de los mínimos privilegios: los servicios, aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tareas. La política por defecto debe ser aquella en la que todo lo que no se encuentre expresamente permitido en el sistema estará prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberían ser eliminados de los sistemas informáticos. "Ibíd."
- Configuración robusta ante fallos: los sistemas deberían ser diseñados e implementados para que, en caso de fallo, se situaran en un estado seguro y cerrado, en lugar de uno abierto y expuesto a accesos no autorizados.
- Las políticas de seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros (clientes, administración pública, etc.), sino que deberían estar adaptadas a las necesidades reales de cada organización. "Ibíd."

Por otra parte, es necesario tener en consideración una serie de dificultades a la hora de definir las políticas de seguridad.

Así, en primer lugar conviene destacar que la información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad, situación que no se produce con los equipos informáticos, la documentación o las aplicaciones informáticas. "Ibíd."

Además, con la proliferación de las redes de ordenadores, la información de las empresas ha pasado de concentrarse en los grandes sistemas (sistemas

centralizados) a distribuirse por los ordenadores y servidores ubicados en los distintos departamentos y grupos de trabajo. Por este motivo, en la actualidad muchas organizaciones no conocen con precisión toda la información que hay en los puestos de trabajo (generalmente, ordenadores personales de la propia organización), ni los riesgos que tienden a sufrir (ataques u otro tipo de desastres), ni cómo la propia organización utiliza esta información. "Ibíd."

2.2.3.1 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. "Ibíd."

Debemos tener en cuenta dos aspectos contradictorios en las redes y sistemas informáticos: por un lado, su principal razón de ser es facilitar la comunicación y el acceso a la información y, por otro, asegurar que sólo acceden a ella los usuarios debidamente autorizados. Esta contradicción está presente continuamente, ya que las medidas adoptadas para mejorar la seguridad (autenticación, control de acceso, monitorización del uso, encriptación, herramientas de detección de ataques, antivirus, etc.) dificultan el uso de las redes y sistemas, al ralentizar los accesos e imponer ciertas restricciones, por lo que es necesario mantener un compromiso entre la usabilidad y rendimiento de los sistemas informáticos, por una parte, y su seguridad, por otra. "Ibíd."

La adopción de ciertas medidas burocráticas (registro de entradas y salidas, inventario de soportes informáticos, etc.) o de determinados controles y

procedimientos de seguridad se traducen generalmente en una mayor incomodidad para los usuarios, por lo que resultará fundamental explicar la importancia de la correcta aplicación de estas medidas para mejorar la seguridad en el trabajo cotidiano con los recursos de la organización. "Ibíd."

2.2.4 Definición e Implantación de las políticas de seguridad.

2.2.4.1 Definición de las políticas de seguridad.

Los siguientes elementos pueden ser considerados a la hora de definir las políticas de seguridad en una organización "Ibíd.":

- Alcance: recursos, instalaciones y procesos de la organización sobre los que se aplican.
- Objetivos perseguidos y prioridades de seguridad.
- Compromiso de la Dirección de la organización.
- Clasificación de la información e identificación de los activos a proteger.
- Análisis y gestión de riesgos.
- Elementos y agentes involucrados en la implantación de las medidas de seguridad.
- Asignación de responsabilidades en los distintos niveles organizativos.
- Definición clara y precisa de los comportamientos exigidos y de los que están prohibidos por parte del personal.
- Identificación de las medidas, normas y procedimientos de seguridad a implantar.
- Gestión de las relaciones con terceros (clientes, proveedores, partners).
- Gestión de incidentes.
- Planes de contingencia y de continuidad del negocio.
- Cumplimiento de la legislación vigente.
- Definición de las posibles violaciones y de las consecuencias derivadas del incumplimiento de las políticas de seguridad.

Asimismo, se debe señalar cuáles son los distintos colectivos que deberían estar implicados en la definición de las políticas de seguridad dentro de una organización "Ibíd.":

- Directivos y responsables de los distintos departamentos y áreas funcionales de la organización.
- Personal del Departamento de informática y de Comunicaciones.
- Miembros del equipo de respuesta a incidentes de seguridad informática, en caso de que este exista.
- Representantes de los usuarios que pueden verse afectados por las medidas adoptadas.
- Consultores externos expertos en seguridad informática.

También sería aconsejable una revisión de las medidas y directrices definidas en las políticas de seguridad por parte de los asesores legales de la organización. "Ibíd."

Por otra parte, de cara a facilitar su difusión en el seno de la organización, resultará fundamental poner en conocimiento de todos los empleados que se puedan ver afectados por las políticas de seguridad cuales son los planes, normas y procedimientos adoptados por la organización. El establecimiento claro y preciso de cuáles son las actuaciones exigidas, las recomendadas y las totalmente prohibidas dentro del sistema informático o en el acceso a los distintos recursos e información de la organización, citando ejemplos concretos que faciliten su comprensión por parte de todos los empleados, contribuirán a la difusión e implantación de estas medidas. "Ibíd."

El acceso a la documentación clara y detallada sobre todas las medidas y directrices de seguridad, así como los planes de formación y sensibilización inicial de los nuevos empleados que se incorporan a la organización son otros dos aspectos de vital importancia. La documentación debería incluir contenidos sencillos y asequibles para personal no técnico, incorporando un glosario con la terminología técnica empleada en los distintos apartados. En todo momento, los autores deberían ponerse en el lugar del lector a la hora de preparar los materiales para dar a conocer las políticas de seguridad. "Ibíd."

En cada documento se podría incluir la siguiente información:

- Título y codificación.

- Fecha de publicación.
- Fecha de entrada en vigor.
- Fecha prevista de revisión o renovación.
- Ámbito de aplicación (a toda la organización o sólo a un determinado departamento o unidad de negocio).
- Descripción detallada (redactada en términos claros y fácilmente comprensibles por todos los empleados) de los objetivos de seguridad.
- Persona responsable de la revisión y aprobación.
- Documento (o documentos) al que reemplaza o modifica.
- Otros documentos relacionados.

En los procedimientos de seguridad será necesario especificar además otra información adicional "Ibíd.":

- Descripción detallada de las actividades que se deben ejecutar.
- Personas o departamentos responsables de su ejecución.
- Momento y/o lugar en que deben realizarse.
- Controles para verificar su correcta ejecución.

2.2.4.2 Implantación de las políticas de seguridad.

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.

La implantación de un adecuado sistema de gestión documental facilitará el registro, clasificación y localización de toda la documentación que se haya generado, además de constituir un aspecto fundamental si la organización desea

conseguir la certificación del Sistema de Gestión de Seguridad de la Información. "Ibíd."

Las políticas de seguridad constituyen una herramienta para poder hacer frente a futuros problemas, fallos de sistemas, imprevistos o posibles ataques informáticos. Sin embargo, se puede incurrir en una falsa sensación de seguridad si las políticas de seguridad no se han implantado correctamente en toda la organización. "Ibíd."

En consecuencia, la organización debería tratar de evitar que las políticas de seguridad se conviertan en un libro más en las estanterías de los despachos. En este sentido, para conseguir una implantación real y eficaz de las medidas y directrices definidas será necesario contar con el compromiso e implicación real de los directivos de la organización, aspecto fundamental para poder disponer de los recursos necesarios y para que su actuación sirva de guía y referencia para el resto de los empleados. "Ibíd."

Se podrían adoptar una serie de medidas para recordar la importancia de la seguridad a los distintos empleados de la organización en el día a día. Por otra parte, la organización también debe contemplar una serie de actuaciones para verificar el adecuado nivel de cumplimiento e implantación de las directrices y procedimientos de seguridad: auditorías y revisiones periódicas, simulacros de fallos y ataques informáticos, inspección manual de los procedimientos y tareas realizadas día a día por el personal, utilizar herramientas para detectar contraseñas poco robustas o instalación de software no autorizado en los equipos de la organización; cuestionarios y entrevistas al personal para determinar su nivel de sensibilización y conocimiento de las políticas. "Ibíd."

Otra medida que contribuye a una adecuada implantación sería la actualización y revisión de las políticas de seguridad cuando sea necesario, manteniendo plenamente vigentes las directrices y medidas establecidas. "Ibíd."

2.2.5 Elementos de las políticas de seguridad.

2.2.5.1 Seguridad frente al personal.

La política de seguridad del sistema informático frente al personal de la organización requiere contemplar los siguientes aspectos "Ibíd.":

2.2.5.1.1 Alta de empleados.

El requerimiento de alta de nuevos empleados requiere prestar atención a aspectos como el adecuado chequeo de referencias y la incorporación de determinadas cláusulas de confidencialidad en los contratos, sobre toda si la persona en cuestión va a tener acceso a datos sensibles y/o va a manejar aplicaciones críticas dentro del sistema informático. "Ibíd."

Es necesario definir claramente el procedimiento seguido para la creación de nuevas cuentas de usuarios dentro del sistema, así como para la posterior asignación de permisos en función de las atribuciones y áreas de responsabilidad de cada empleado.

Por último, no se debería descuidar una adecuada formación de estos nuevos empleados, trasladando claramente cuáles son sus obligaciones y responsabilidades en relación con la seguridad de los datos y las aplicaciones del sistema informático de la organización.

2.2.5.1.2 Baja de empleados.

El procedimiento de actuación ante una baja de un empleado también debería quedar claramente definido, de tal modo que los responsables del sistema informático puedan proceder a la cancelación o bloqueo inmediato de las cuentas de usuario y a la revocación de los permisos y privilegios que tenían concedidos. "Ibíd."

Este procedimiento debe contemplar la devolución de los equipos, tarjetas de acceso y otros dispositivos en poder de los empleados que causan baja en la organización.

2.2.5.1.3 Funciones, obligaciones y derechos de los usuarios.

La organización debe definir con claridad cuáles son los distintos niveles de acceso a los servicios y recursos de su sistema informático. "Ibíd."

De este modo, en función de las distintas atribuciones de los usuarios y del personal de la organización, se tendrá que establecer quién está autorizado para realizar una serie de actividades y operaciones dentro del sistema informático; a qué datos, aplicaciones y servicios puede acceder cada usuario; desde qué equipos o instalaciones podrá acceder al sistema y en qué intervalo temporal (día de la semana y horario). "Ibíd."

Recurso	Tipo de acceso o de utilización	Usuario o grupo de usuarios al que se concede	Lugares o equipos desde los que se permite el acceso	Período de validez del acceso (días y horarios)	Responsable que autoriza el acceso	Fecha de la autorización

Tabla 2.2.1 Usuarios o grupos de usuarios con acceso a los recursos del sistema informático.

Fuente: Gómez, A. (2006).

En relación con este aspecto de la seguridad, la organización debe prestar especial atención a la creación de cuentas de usuarios y la asignación de permisos de acceso para personal ajeno a ésta, que pueda estar desempeñando con carácter excepcional determinados trabajos o actividades que requieran de su acceso a algunos recursos del sistema informático de la organización. "Ibíd."

Es necesario establecer qué datos y documentos podrá poseer o gestionar cada empleado. La organización también debe contemplar la privacidad de los usuarios que tienen acceso a estos recursos y servicios del sistema informático, estableciendo en qué condiciones sus ficheros, mensajes de correo u otros documentos podrían ser intervenidos por la organización. "Ibíd."

Todas estas medidas deberían completarse con la preparación de una serie de manuales de normas y procedimientos, que incluyesen las medidas de carácter administrativo y organizativo adoptadas para garantizar la adecuada utilización de los recursos informáticos por parte del personal de la organización. "Ibíd."

2.2.5.1.4 Formación y sensibilización de los usuarios

La organización deberá informar puntualmente a sus empleados con acceso al sistema de información de cuáles son sus obligaciones en materia de seguridad. Asimismo, debería llevar a cabo acciones de formación de formación de forma periódica para mejorar los conocimientos informáticos y en materia de seguridad de estos empleados. "Ibíd."

Las personas que se incorporen a la organización tendrán que ser informadas y entrenadas de forma adecuada, sobre todo en las áreas de trabajo con acceso a datos sensibles y aplicaciones importantes para el funcionamiento de la organización. "Ibíd."

2.2.5.2 Adquisición de productos

La política de seguridad relacionada con la adquisición de productos tecnológicos necesarios para el desarrollo y el mantenimiento del sistema informático de la organización debe contemplar toda una serie de actividades ligadas al proceso de la compra "Ibíd.":

- Evaluación de productos de acuerdo con las necesidades y requisitos del sistema informático de la organización: características técnicas, características específicas de seguridad, relación coste beneficio del producto, documentación facilitada por el fabricante, referencia de su instalación en empresas del mismo sector, etc.
- Evaluación de proveedores y del nivel de servicio que ofrecen: garantías, mantenimiento, asistencia postventa.
- Análisis comparativo de ofertas.
- Definición de los términos y condiciones de la compra, que deberían estar reflejados en un contrato previamente establecido por la organización.

- Instalación y configuración de los productos.
- Formación y soporte a usuarios y a personal técnico.
- Tareas de soporte y mantenimiento postventa.
- Actualización de los productos con nuevas versiones y parches de seguridad.

Todas estas actividades deberían ser incluidas en una guía de compras y evaluación de productos TIC, para garantizar que éstos satisfacen las características de seguridad definidas por la organización. "Ibíd."

2.2.5.3 Relación con proveedores

La política de seguridad relacionada con la subcontratación de determinados trabajos y actividades a proveedores externos requiere contemplar aspectos como la negociación de los mismos niveles de servicio y calidad, en especial con aquellos proveedores relacionados con la informática, las comunicaciones o el tratamiento de los datos. "Ibíd."

Se debería exigir el cumplimiento de ciertas medidas de seguridad que puedan afectar al sistema informático de la organización. Este aspecto resulta de especial importancia en los tratamientos de datos personales.

En la política de relación con proveedores se deberían estipular las cláusulas y exigencias habituales en la firma de contratos con los proveedores, a fin de delimitar las responsabilidades y los requisitos del servicio contratado. "Ibíd."

2.2.5.4 Seguridad física de las instalaciones

Los inmuebles donde se ubiquen los ordenadores que contienen los datos más sensibles de la organización deben ser objeto de una especial protección, de modo que se pueda garantizar la confidencialidad, integridad y disponibilidad de los datos y aplicaciones más críticas. Estos inmuebles deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad que pudieran producirse como consecuencia de incidencias fortuitas o intencionadas. "Ibíd."

Las medidas relacionadas con la seguridad física deberían contemplar, en primer lugar, las características de construcción de los edificios o instalaciones donde se vayan a ubicar los recursos informáticos y del sistema de información, analizando los siguientes aspectos "Ibíd.":

- Protección contra daño por fuego, inundación, explosiones, accesos no autorizados.
- Selección de los elementos de construcción internos más adecuados: puertas, paredes, suelos y techos falsos, canalizaciones eléctricas y de comunicaciones. Estos elementos deberían cumplir con el máximo nivel de protección exigido por la normativa de construcción. Para evitar el polvo y la electricidad estática se debería aplicar un revestimiento especial en las paredes, el techo y el suelo de las salas donde se vayan a ubicar los servidores y equipos con los datos y aplicaciones más importantes.
- Definición de distintas áreas o zonas de seguridad dentro del edificio:
    - Áreas públicas: pueden acceder sin restricciones personas ajenas a la organización.
    - Áreas internas: reservadas a los empleados.
    - Áreas de acceso restringido: áreas críticas a las que sólo pueden acceder un grupo reducido de empleados con el nivel de autorización requerido.
- Disponibilidad de zonas destinadas a la carga, descarga y almacenamiento de suministros.
- Implantación de sistemas de vigilancia basados en cámaras en circuito cerrado de televisión y en alarmas y detectores de movimiento.
- Control de condiciones ambientales en las instalaciones, mediante un sistema independiente de ventilación, calefacción, aire acondicionado y humidificación/deshumidificación que, a ser posible, debería funcionar de forma ininterrumpida, 24 horas al día durante los 365 días del año. El objetivo perseguido es tratar de mantener estables la temperatura y la humedad de la sala donde se ubiquen los servidores y equipos informáticos más importantes para la organización, dentro de los límites recomendados por los fabricantes.

En lo referente al control de acceso físico la política de seguridad debería definir cómo se va a llevar a cabo la identificación del personal propio y del personal ajeno, estableciendo asimismo los procedimientos de acceso a las áreas críticas y se debe contemplar la existencia de un registro de entradas y salidas del personal, sobre todo en las áreas de acceso restringido, a fin de poder monitorizar las actividades y horarios del personal. "Ibíd."

Si las instalaciones de la organización no pudiesen garantizar un adecuado nivel de protección de los activos en lo que se refiere a la seguridad física del edificio, control de accesos, cableado, alarmas y demás, la solución podría pasar por la ubicación de estos recursos en el data center de un operador de servicios de telecomunicaciones, bajo la modalidad de housing o de hosting, firmando un contrato con unas determinadas garantías de nivel de servicio (SLA). "Ibíd."

2.2.5.5 Sistemas de protección eléctrica

Las directrices de seguridad relacionadas con la protección eléctrica de los equipos informáticos deberían definir los siguientes aspectos "Ibíd.":

- Adecuada conexión de los equipos a la toma de tierra.
- Revisión de la instalación eléctrica específica para el sistema informático, siendo recomendable disponer de tomas protegidas y estabilizadas, asiladas del resto de la instalación eléctrica de la organización.
- Eliminación de la electricidad estática en las salas donde se ubiquen los equipos más importantes, para ello sería recomendable emplear un revestimiento especial en las paredes, techo, suelo del local para evitar el polvo y la electricidad estática.
- Filtrado de ruidos e interferencias electromagnéticas, que puedan afectar el normal funcionamiento de los equipos.
- Utilización de sistemas de alimentación ininterrumpida, estos permiten proteger a los equipos informáticos frente a picos o caídas de tensión, así como de los cambios en la frecuencia del fluido eléctrico. De esta modo, se consigue una mayor estabilización del suministro y se dispone de una alimentación auxiliar para afrontar posibles cortes en este suministro (aunque sólo por tiempo limitado, debido al uso de baterías).

2.2.5.6 Vigilancia de la red y de los elementos de conectividad

Los dispositivos de red (switches de acceso, routers o puntos de acceso inalámbricos) podrían facilitar el acceso a la red a usuarios no autorizados si no se encuentran protegidos de forma adecuada. "Ibíd."

Las políticas de seguridad deberían contemplar las medidas previstas para reforzar la seguridad de estos equipos y de toda la infraestructura de red. "Ibíd."

2.2.5.7 Protección en el acceso y configuración de los servidores

Los servidores, debido a su importancia para el correcto funcionamiento de muchas aplicaciones y servicios de la red y a que suelen incorporar información sensible, tendrían que estar sometidos a mayores medidas de seguridad en comparación con los equipos de los usuarios. "Ibíd."

Estas medidas, que deberían estar definidas en las políticas de seguridad, podrían contemplar aspectos como los citados a continuación "Ibíd.":

- Utilización de una contraseña a nivel de BIOS para proteger el acceso a este elemento que registra la configuración básica del servidor.
- Utilización de contraseñas de encendido del equipo.
- Inicio de sesión con tarjetas inteligentes y/o técnicas biométricas.
- Ubicación de los servidores en salas con acceso restringido y otras medidas de seguridad físicas.
- Separación de los servicios críticos: se debería procurar que los servicios más importantes para la organización dispongan de una o varias máquinas en exclusiva.
- Configuración más robusta y segura de los servidores:
    - Desactivación de los servicios y las cuentas de usuarios que no se vayan a utilizar. Desinstalación de las aplicaciones que no sean estrictamente necesarias.
    - Documentar y mantener actualizada la relación de servicios y aplicaciones que se hayan instalado en cada servidor.
    - Cambiar la configuración por defecto del fabricante: permisos de las cuentas, contraseñas, etc.

- Instalación de los últimos parches de seguridad y actualizaciones publicados por el fabricante. No obstante, convendría comprobar su correcto funcionamiento en un ambiente de pruebas antes de realizarlo en producción.
- Ejecución de los servicios con los mínimos privilegios necesarios.
- Enlazar sólo los protocolos y servicios necesarios a las tarjetas de red.
- Activar los registros de actividad de los servidores (logs).
- Disponer de una copia de seguridad completa del sistema operativo de cada servidor tras una configuración correcta y suficientemente robusta.
- Instalación de una herramienta que permita comprobar la integridad de los ficheros del sistema.
- Modificar los mensajes de inicio de sesión para evitar que se pueda mostrar información sobre la configuración y recursos del sistema a un posible atacante.

2.2.5.8 Protección de los equipos y estaciones de trabajo

Los equipos de los usuarios y estaciones de trabajo también deben estar sometidos a las directrices establecidas en las políticas de seguridad de la organización. "Ibíd."

En estos equipos sólo se deben utilizar las herramientas corporativas, quedando totalmente prohibida la instalación de otras aplicaciones software en los ordenadores de la empresa por parte de los usuarios. En cualquier caso, el usuario del equipo debería solicitar la aprobación del Departamento de Informática antes de proceder a instalar un nuevo programa en su equipo.

Los usuarios deben tener especial cuidado con su equipo de trabajo, impidiendo que éste pueda ser utilizado por personal que no se encuentre debidamente autorizado. Los usuarios no podrán cambiar las configuraciones de sus equipos ni deberían intentar solucionar los problemas de funcionamiento e incidencias de seguridad por su propia cuenta, debiendo notificarlas en todo caso al Departamento de Informática. "Ibíd."

La organización podría implantar determinadas soluciones para facilitar el control de la conexión de dispositivos USB (como los pendrive) en los equipos de los usuarios, así como el control del acceso a puertos de comunicaciones como los puertos serie, paralelo.

También se podría limitar el uso de disqueteras y unidades lectoras/grabadoras de CDs y DVDs, para evitar que se pudiera grabar información sensible o se pudieran introducir determinados contenidos dañinos en el equipo. "Ibíd."

2.2.5.9 Control de los equipos que pueden salir de la organización

Las políticas de seguridad también deberían prestar atención al control de los equipos que pueden salir de la organización, como los ordenadores portátiles, como norma general, los equipos y medios informáticos de la organización no podrán ser sacados fuera de sus instalaciones por los empleados sin la correspondiente autorización. Para ello, se establecerán medidas, procedimientos y controles de seguridad para los equipos que deban usarse fuera de los locales de la empresa, de forma que estén sujetos a una protección equivalente a la de los equipos internos. "Ibíd."

Los usuarios de estos equipos deben ser conscientes de sus obligaciones y responsabilidades en relación con la seguridad de los datos y las aplicaciones instaladas. Estos equipos portátiles deberían ser transportados en bolsas especialmente acondicionadas (con protección frente a caídas y golpes), estando provistos de los medios de protección contra accesos no autorizados: aplicación de contraseñas de acceso, encriptación de los datos del disco duro y otras unidades de almacenamiento, utilización de técnicas de seguridad biométrica o de tarjetas criptográficas, protección contra virus y programas dañinos, etc. "Ibíd."

2.2.5.10 Copias de seguridad

Para garantizar la plena seguridad de los datos y de los ficheros de una organización no sólo es necesario contemplar la protección de la confidencialidad, sino que también se hace imprescindible salvaguardar su integridad y disponibilidad. Para garantizar estos dos aspectos fundamentales de la seguridad

es necesario que existan unos procedimientos de realización de copias de seguridad y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos y los ficheros dañados o eliminados. "Ibíd."

Por copia o respaldo de seguridad (backup) se entiende una copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

La Política de Copia de Seguridad debería establecer la planificación de las copias que se deberían realizar en función del volumen y tipo de información generada por el sistema informático, especificando el tipo de copias (completa, incremental o diferencial) y el ciclo de esta operación (diario, semanal).

Las copias de seguridad de los datos y ficheros de los servidores deberían ser realizadas y supervisadas por personal debidamente autorizado. No obstante, si existen datos o ficheros ubicados en equipos de usuarios sin conexión a la red, podría ser el propio usuario el responsable de realizar las copias de seguridad en los soportes correspondientes. "Ibíd."

Será preciso establecer cómo se van a inventariar y etiquetar las cintas y otros soportes utilizados para las copias de seguridad, registrando las copias de seguridad realizadas, así como las posibles restauraciones de datos que se tengan que llevar a cabo. "Ibíd."

Registro de Copias de Seguridad			
Tipo de Copia	☐ Completa ☐ Incremental ☐ Diferencial		
Tipo de Soporte	☐ Cinta DAT ☐ Disquette ☐ Disco Duro ☐ CD-ROM ☐ Pen - Drive (USB) ☐ Otro:		
Etiqueta	**Fecha de la copia**	**Fecha de los datos**	**Contenido de la copia**
. . .	. . .	. . .	. . .
Lugar de almacenamiento			

Responsable del almacenamiento	
	Fecha y firma

Tabla 2.2.2 Registro de copias de seguridad.

Fuente: Gómez, A. (2006).

Las cintas y soportes utilizados deberían ser almacenados en lugares seguros, preferiblemente en locales diferentes de donde reside la información primaria. Será necesario contemplar, además, la implantación de medidas de protección frente a posibles robos y a daños provocados por incendios o inundaciones, siendo por ello muy aconsejable que estos soportes se depositen, convenientemente etiquetados, dentro de cajas fuertes ignífugas y especialmente acondicionadas para proteger a los soportes informáticos (discos, cintas) de altas temperaturas o radiaciones. "Ibíd."

También será preciso establecer qué sistemas o técnicas se van a emplear (algoritmos criptográficos, por ejemplo) para garantizar la privacidad de los datos que se guarden en las citas y otros soportes. Por otra parte, la organización podría mantener un registro de las copias de seguridad realizadas en el sistema informático, a fin de disponer de la trazabilidad de este importante procedimiento.

La organización debería establecer cómo y cuándo se realizarán comprobaciones de forma periódica para verificar el estado de los soportes y el correcto funcionamiento del proceso de generación de copias de seguridad. "Ibíd."

La pérdida o destrucción, parcial o total, de los datos de un fichero debería anotarse en un registro de incidencias. Las restauraciones de datos deberían llevarse a cabo con la correspondiente autorización de un responsable del sistema informático, siendo anotadas en el propio registro de incidencias o en un registro específico habilitado a tal fin por la organización. "Ibíd."

Registro de Copias de Seguridad	
Fecha y hora de la operación	
Ficheros restaurados	

Tipo de Soporte utilizado	☐ Cinta DAT ☐ Pen - Drive (USB) ☐ Disquette ☐ Otro: ☐ Disco Duro ☐ CD-ROM
Identificación soporte utilizado	
Incidencia que ha motivado la operación	
Consecuencias de la incidencia	
Lugar donde se ha realizado la operación	
Equipo utilizado	
Lugar de almacenamiento	
Operación realizada por (fecha y firma)	**Operación autorizada por (fecha y firma)**

Tabla 2.2.3 Registro de restauración de copias de seguridad.

Fuente: Gómez, A. (2006).

2.2.5.11 Control de la seguridad de impresoras y otros dispositivos periféricos

Las impresoras y otros dispositivos periféricos también pueden manejar información sensible de la organización, por lo que su seguridad debería ser contemplada a la hora de definir e implantar las Políticas de Seguridad. "Ibíd."

En lo que se refiere a la protección física de las impresoras y otros periféricos, éstas no deberían estar situadas en áreas públicas. Además, a la hora de controlar las salidas impresas, la organización debería insistir en la necesidad de que sea el propio usuario del sistema informático que envía un documento a la impresora el que asuma su responsabilidad para evitar que dicho documento pueda caer en manos de personas no autorizadas. "Ibíd."

Por otra parte, la definición e implantación de las medidas de protección lógica permitirán limitar el acceso de los usuarios a cada impresora o periférico compartido a través de la red de la organización. "Ibíd."

2.2.5.12 Gestión de cuentas de usuarios

La gestión de cuentas de usuarios constituye un elemento fundamental dentro de las políticas de seguridad de la organización, ya que de ella dependerá

el correcto funcionamiento de otras medidas y directrices de seguridad como el control de acceso lógico a los recursos o el registro de la actividad de los usuarios. "Ibíd."

Por este motivo, la organización debería incluir en sus políticas de seguridad las directrices relativas al proceso de solicitud, creación, configuración, seguimiento y cancelación de cuentas de usuarios. Asimismo, se debería definir una norma homogénea de identificación de usuarios para toda la organización. "Ibíd."

Dentro de la documentación de este proceso, será necesario definir qué personas pueden ejercer la potestad de autorizar la creación de cuentas de usuario, así como qué usuario o usuarios tendrán privilegios administrativos y constituyen, por lo tanto, una autoridad dentro del sistema. "Ibíd."

En relación con estas cuentas de usuario con privilegios administrativos, se tendrá que especificar hasta qué punto y en que determinadas condiciones este usuario o usuarios podrán hacer uso de los privilegios administrativos para acceder a carpetas o ficheros de otros usuarios, monitorizar el uso de la red y de los equipos, instalar o desinstalar aplicaciones, cambiar la configuración de los equipos, etc. contando para ello con la autorización de la Dirección de la organización. "Ibíd."

Es recomendable que cada usuario con privilegios administrativos emplee otra cuenta con menos privilegios para su trabajo cotidiano, recurriendo a la cuenta de administrador sólo para las tareas que así lo requieran. La organización debería mantener un registro actualizado de los usuarios que ostentan privilegios administrativos en el sistema, indicando en qué momento se conceden estos privilegios, por qué razón y finalidad y durante cuánto tiempo. "Ibíd."

Los responsables de la seguridad deberían proceder a la cancelación o cambio de contraseñas de las cuentas incluidas por defecto en el sistema informático, así como a la desactivación de todas las cuentas de usuario genéricas (como las de los usuarios anónimos). "Ibíd."

Las políticas de seguridad deberían establecer revisiones periódicas sobre la administración de las cuentas, los grupos asignados y los permisos de acceso establecidos, contemplando actividades como las enumeradas a continuación "Ibíd.":

- Revalidación anual de usuarios y grupos dentro del sistema.
- Asignación de permisos y privilegios teniendo en cuenta las necesidades operativas de cada usuario en función de su puesto de trabajo.
- Modificaciones de permisos derivadas de cambios en la asignación de funciones de un empleado, procediendo al registro de dichas modificaciones.
- Detección de actividades no autorizadas, como podrían ser las conexiones a horas extrañas o desde equipos que no se habían contemplado inicialmente.
- Detección y bloqueo de cuentas inactivas, entendiendo como tales aquellas que no hayan sido utilizadas en los últimos meses.

La organización debe prever cómo actuar en el caso de las bajas en el sistema por desvinculaciones del personal, procediendo a la revocación de permisos y cancelación inmediata de las cuentas de usuario afectadas. No obstante, en ocasiones será necesario mantener el identificador de la cuenta en los registros de actividad del sistema, si bien en estos casos los administradores deberían bloquear la cuenta para que no pueda volver a ser utilizada. "Ibíd."

También se debería definir dentro de las políticas de seguridad cuáles son las directrices fijadas por la organización en relación con la eliminación de los datos y ficheros de ámbito personal de aquellos usuarios que hayan causado baja en el sistema, previa grabación de éstos en un CD u otro soporte para que puedan ser entregados a los interesados. "Ibíd."

2.2.5.13 Identificación y autenticación de usuarios

La organización debe disponer de una relación actualizada de usuarios que tienen acceso autorizado a los recursos de un sistema informático, estableciendo determinados procedimientos de identificación y autenticación para dicho acceso. "Ibíd."

La identificación y autenticación de usuarios constituye uno de los elementos del modelo de seguridad conocido como (AAA) Autenticación, Autorización y Contabilidad (Registro). Este modelo o paradigma de seguridad se utiliza para poder identificar a los usuarios y controlar su acceso a los distintos recursos de un sistema informático, registrando además cómo se utilizan dichos recursos. "Ibíd."

Este modelo se basa en tres elementos fundamentales "Ibíd.":

- **Identificación y autenticación de los usuarios:** La identificación es el proceso por el cual el usuario presenta una determinada identidad para acceder a un sistema, mientras que la autenticación permite validar la identidad del usuario.
- **Control de acceso a los recursos** del sistema informático (equipos, aplicaciones, servicios y datos), mediante la autorización en función de los permisos y privilegios de los usuarios.
- **Registro del uso de los recursos** del sistema por parte de los usuarios y de las aplicaciones, utilizando para ello los logs (registros de actividad) del sistema.

Todos estos elementos deberían estar claramente definidos en las políticas de seguridad de la organización. "Ibíd."

En lo que se refiere al proceso de identificación, los elementos utilizados para identificar a un usuario pueden basarse en:

- Lo que se sabe: contraseñas, PINS.
- Lo que se posee (token): tarjeta de crédito, tarjeta inteligente, teléfono móvil, llave USB.
- Lo que se es: características biométricas del individuo.
- Lo que se sabe hacer: firma manuscrita.
- Donde se encuentra el usuario: conexión desde un determinado equipo u ordenador con dirección IP previamente asignada, en un acceso a través de redes físicas protegidas y controladas (que no permitan que los usuarios puedan manipular las direcciones de los equipos).

El mecanismo que se ha venido utilizando en la práctica con mayor frecuencia para identificar a los usuarios se basa en nombres de usuario (login) y las contraseñas (password). "Ibíd."

De este modo, a cada usuario se le asigna un identificador o nombre de usuario, que tiene asociada una determinada contraseña que permite verificar dicha identidad en el proceso de autenticación. En este caso, la seguridad del proceso de autenticación depende totalmente de la confidencialidad de la contraseña.

Por este motivo, toda contraseña debería cumplir con unos mínimos requisitos para garantizar su seguridad, los cuales deberían estar definidos en la política de gestión de contraseñas del sistema informático de la organización "Ibíd.":

- Tamaño mínimo de la contraseña: número mínimo de caracteres que la puedan componer (hoy en día se recomienda un tamaño mínimo de 8 caracteres).
- Caducidad de la contraseña: período de validez para su uso en el sistema antes de que tenga que ser sustituida por otra.
- Registro del historial de contraseñas previamente seleccionadas por un usuario para impedir que puedan volver a ser utilizadas.
- Control de la adecuada composición de una contraseña, a fin de conseguir que ésta difícil de adivinar. Para ello, la contraseña debería estar formada por una combinación de todo tipo de caracteres alfanuméricos (por lo menos una letra y un número, así como algún signo de puntuación), evitando la repetición de secuencias de caracteres. Además no debería estar relacionada con el propio nombre de usuario, nombres de familiares o mascotas, fechas de cumpleaños u otras fechas señaladas, matrícula del coche, domicilio, nombre de la empresa, etc. También es necesario comprobar la robustez de la contraseña frente a ataques de diccionario, basados en listas de nombres o palabras comunes.
- Bloqueo de las cuentas de usuario tras varios intentos fallidos de autenticación.

- Ocultar el último nombre de usuario en el acceso desde un equipo informático conectado al sistema.

La autenticación de usuarios basada en contraseñas es un mecanismo ampliamente extendido, soportado por prácticamente todos los sistemas operativos del mercado. Sin embargo, debemos tener en cuenta que su seguridad depende de una elección segura de la contraseña y de su correcta conservación por parte del usuario, siendo el factor humano uno de los principales puntos débiles de la seguridad informática. Por este motivo, los usuarios deberían asumir su responsabilidad en este proceso, aplicando unas mínimas normas de seguridad que deberían ser definidas en la Política de Gestión de Contraseñas del sistema "Ibíd.":

- Al iniciar una sesión por primera vez en el sistema, se debería obligar al usuario a cambiar la contraseña previamente asignada a su cuenta.
- La contraseña no debería ser anotada en un papel o agenda, ni guardada en un archivo o documento sin encriptar.
- La contraseña sólo debería ser conocida por el propio usuario.
- La contraseña nunca debería ser revelada a terceros, el propietario debería cambiar dicha contraseña lo antes posible, una vez haya terminado la situación de emergencia que justificaba su revelación.
- Ante la menor sospecha de que la contraseña pudiera haber sido comprometida, ésta debería ser cambiada de forma inmediata por el usuario.
- El usuario no debería empelar la misma contraseña o una muy similar en el acceso a distintos sistemas.

En definitiva, la sensibilización de los usuarios es un aspecto fundamental para garantizar una adecuada gestión de las contraseñas.

2.2.5.14 Autorización y control de acceso (Seguridad Lógica)

La organización debe establecer determinados mecanismos para evitar que un usuario, equipo, servicio o aplicación informática pueda acceder a datos o recursos con derechos distintos de los autorizados. "Ibíd."

Mediante el control de acceso a los distintos recursos del sistema es posible implementar las medidas definidas por la organización, teniendo en cuenta las restricciones de acceso a las aplicaciones, a los datos guardados en el sistema informático, a los servicios ofrecidos (tanto internos como externos) y a otros recursos de tipo lógico del sistema. "Ibíd."

La implantación de control de acceso en un sistema informático depende fundamentalmente a la gestión de cuentas de usuarios y de la gestión de permisos y privilegios. Para facilitar el control de acceso a los datos y aplicaciones se pueden definir distintos grupos de usuarios dentro del sistema. Estas reglas de control de acceso se pueden aplicar también a equipos, redes, servicios y aplicaciones informáticas. "Ibíd."

El modelo de seguridad aplicado en el control de acceso se basa en la definición y gestión de determinados objetos lógicos (dispositivos lógicos, ficheros, servicios) y sujetos (usuarios y grupos, equipos, procesos, roles) a los que se conceden derechos y privilegios para realizar determinadas operaciones sobre los objetos. Estos derechos y privilegios se pueden verificar mediante el proceso de autorización de acceso. "Ibíd."

Podemos distinguir dos tipos de control de acceso:

- Control de acceso obligatorio (MAC, Mandatory Access Control): Los permisos de acceso son definidos por el sistema operativo.
- Control de acceso y direccional (DAC, Discrecionary Access Control): Los permisos de acceso los controla y configura el propietario de cada objeto.

La política de control de acceso permite definir una serie de restricciones de acceso no sólo ya en función de la identidad del sujeto (usuario o proceso), sino también en función del horario y/o de la ubicación física del sujeto. Asimismo, en los sistemas gráficos se pueden establecer determinadas limitaciones en la interfaz de usuario de las aplicaciones, indicando qué menús, campos de información, botones u otros elementos gráficos pueden visualizar cada usuario. Por lo tanto, se puede aplicar la gestión de la seguridad lógica tanto a nivel de sistema operativo como a nivel de las aplicaciones y servicios de red. "Ibíd."

El principio de seguridad básico que se debería tener en cuenta es que "todo lo que no está expresamente permitido en el sistema debería estar prohibido", asignando por defecto los mínimos privilegios y permisos necesarios a cada usuario del sistema, revisando de forma periódica los permisos de acceso a los recursos y registrando los cambios realizados en estos permisos de acceso. "Ibíd."

También es necesario restringir los derechos y privilegios administrativos de los usuarios. Sólo los administradores del sistema informático podrán conceder, altera o anular el acceso autorizado sobre datos y recursos, conforme a los criterios establecidos por la Dirección de la organización. "Ibíd."

Por otra parte, es recomendable controlar los intentos de acceso fraudulento a los datos, ficheros y aplicaciones del sistema informático y, cuando sea técnicamente posible, se debería guardar en un registro la fecha, la hora, código y clave errónea que se ha introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos. "Ibíd."

2.2.5.15 Monitorización de servidores y dispositivos de la red

La monitorización del estado y del rendimiento de los servidores y dispositivos de red constituyen una medida fundamental que debería estar prevista por las políticas de seguridad, con el objetivo de facilitar la detección de usos no autorizados, situaciones anómalas o intentos de ataque contra estos recursos. "Ibíd."

Para ello, es necesario activar y configurar de forma adecuada en estos equipos los registros de actividad (logs), para que puedan facilitar información e indicadores sobre aspectos como los siguientes "Ibíd.":

- Sesiones iniciadas por los usuarios en los servidores.
- Procesos ejecutados en cada equipo informático.
- Conexiones externas.
- Acceso y utilización de los recursos del sistema.

- Intentos de violación de la política de seguridad: autenticación fallida de usuarios, intentos de acceso no autorizados a determinados recursos (Carpetas, ficheros, impresoras) por parte de algunos usuarios.
- Detección de ataques sistemáticos y de intentos de intrusión.

El propio sistema operativo de los sistemas y servidores podría ser configurado para registrar distintos eventos de seguridad que faciliten la detección de intrusiones y de intentos de violación de acceso a los recursos: intentos de acceso repetitivos a recursos protegidos, utilización del sistema fuera de horario por un usuario autorizado. "Ibíd."

La organización tendría que especificar qué alarmas, alertas e informes van a ser generados a partir de los registros de actividad de los servidores y dispositivos de red, definiendo qué personas y departamentos podrán tener acceso a éstos. En los casos más urgentes se podrían enviar mensajes de correo, mensajes a teléfonos móviles. También será necesario definir el procedimiento para evaluar los informes de violación de acceso a los recursos del sistema informático de la organización. "Ibíd."

2.2.5.16 Protección de datos y documentos sensibles

La política de seguridad relacionada con la protección de datos debe contemplar en primer lugar la clasificación de los documentos y los datos de la organización atendiendo a su nivel de confidencialidad. "Ibíd."

Una posible clasificación de los documentos y los datos que se podría adoptar en una empresa sería la que se presenta a continuación:

- **Información sin clasificar o desclasificada:** podría ser conocida por personas ajenas a la empresa.
- **Información de uso interno:** conocida y utilizada sólo por empleados de la organización, así como por algún colaborador externo autorizado. No obstante, no conviene que ésta sea divulgada a terceros.
- **Información confidencial:** sólo puede ser conocida y utilizada por un determinado grupo de empleados. Su divulgación podría ocasionar daños significativos para la organización.

- **Información secreta o reservada:** sólo puede ser conocida y utilizada por un grupo muy reducido de empleados. Su divulgación podría ocasionar graves daños para la organización.

La organización tendría que mantener una base de datos actualizada con la relación de los documentos más sensibles, registrando la fecha de creación, la utilización prevista, la fecha de destrucción, el cambio de clasificación del documento, etc. Esta base de datos podría servir de soporte al ciclo de vida de cada documento, reflejando su creación, utilización, modificación y, finalmente, su destrucción. "Ibíd."

La política de seguridad también debería especificar qué medidas de protección se tendrían que adoptar en la manipulación de los documentos más sensibles: operaciones de almacenamiento, transmisión, transporte, tratamiento informático, impresión o destrucción. Así por ejemplo, para el almacenamiento de documentos impresos o soportes con material sensible se deberían utilizar cajas de seguridad. "Ibíd."

También sería recomendable incluir cláusulas de confidencialidad en los contratos de los empleados con acceso a los documentos y datos más sensibles de la organización. Del mismo modo, la revelación de información o documentos sensibles a terceros debería contemplar la exigencia de firmar acuerdos o de incluir en los contratos Cláusulas de Confidencialidad y de No Divulgación. "Ibíd."

2.2.5.17 Seguridad en las conexiones remotas

En la política de seguridad relativa a las conexiones remotas deberían estar incluidas las medidas necesarias para garantizar la seguridad en las conexiones con las delegaciones y otras dependencias de la organización, así como la seguridad en los equipos clientes remotos que deseen acceder a los servicios informáticos centrales de la organización. "Ibíd."

Así, por una parte, se deberían utilizar protocolos para el encapsulamiento de datos e la implantación de Redes Privadas Virtuales (VPN). Por otra parte, en lo que se refiere a la seguridad de los clientes remotos, hay que tener en cuenta que los equipos de los usuarios remotos son más vulnerables que los internos, ya

que pueden estar más expuestos a la introducción de virus y otros códigos dañinos, así como a la revelación de información sensible (por ejemplo, si el equipo cae en manos de usuarios maliciosos). Por todo ello, conviene adoptar medidas de seguridad adicionales, entre las que podríamos citar "Ibíd.":

- Aislamiento de los equipos remotos: se deben limitar los permisos de acceso de estos equipos y registrar toda actividad sospechosa.
- Registro de las sesiones abiertas por usuarios remotos, estableciendo temporizadores para detectar y cerrar las sesiones inactivas.
- Utilización de herramientas para controlar los equipos remotos y poder conectarse a éstos para realizar tareas administrativas o, incluso, para proceder a su bloqueo.

La política de seguridad debería definir también cuál es el procedimiento a seguir para facilitar el acceso remoto a un usuario, considerando los siguientes aspectos "Ibíd.":

- Cumplimiento del documento de solicitud de la conexión remota:
    - Justificación de la conexión remota: descripción de la finalidad o de las tareas que se van a realizar a través de esta conexión remota.
    - Recursos requeridos en la conexión.
    - Mecanismos de autenticación y de control de acceso a los recursos.
    - Horario y días en los que se termine la conexión.
    - Período de validez de la conexión.
    - Persona responsable que autoriza la conexión.

- Configuración del equipo remoto:
    - Software instalado.
    - Configuración de seguridad del equipo.

- Documentación que se debería entregar al usuario remoto:
    - Procedimientos de seguridad básicos.
    - Personas de contacto dentro de la organización para poder notificar y tratar de resolver cualquier incidencia.
    - Confirmación de aceptación de las condiciones de uso de la conexión remota.

Por otra parte, la transmisión de datos y documentos a través de una conexión remota, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello, merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales. "Ibíd."

Si se realiza la entrada o salida de datos sensibles mediante sistemas de transferencia de ficheros a través de una conexión remota, únicamente un usuario autorizado podrá realizar esas operaciones. "Ibíd."

2.2.5.18 Detección y respuesta ante incidentes de seguridad

La organización debería definir un procedimiento de notificación y gestión de incidencias, de tal modo que se puedan realizar una serie de actividades previamente especificadas para controlar y limitar el impacto del incidente. Además, en las políticas de seguridad se podrían establecer qué herramientas se van a utilizar para facilitar la detección y rápida respuesta ante incidentes, como podría ser el caso de los Sistemas de Detección de Intrusiones (IDS). "Ibíd."

Entre las posibles medidas a implantar, una de las más aconsejables es la creación de una base de datos para registrar cada incidencia, indicando el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quien se le comunica y los efectos que se hubieran derivado de la misma. "Ibíd."

En el siguiente cuadro se detallan todos los datos que se podrían registrar de cada una de las incidencias que afecten a la seguridad del sistema de información y/o ficheros con datos de carácter personal:

Registro de Incidencias	
☐ **Número de registro de la incidencia**	
☐ **Fecha y hora de la incidencia**	

☐ **Fecha de notificación**	
☐ **Persona que realiza la notificación**	
☐ **Persona a quien se comunica la incidencia**	
☐ **Tipo de incidencia**	
☐ **Tipo de incidencia**	
☐ **Descripción detallada de la incidencia**	
☐ **Efectos y posibles consecuencias**	
☐ **Acciones adoptadas para subsanar las consecuencias**	
☐ **Persona que comunica**	☐ **Tipo de incidencia**

Tabla 2.2.4 Registro de una incidencia.

Fuente: Gómez, A. (2006).

Este registro de incidencias constituye una herramienta imprescindible para la prevención de posibles ataques que puedan comprometer la seguridad de los recursos del sistema informático, así como para la persecución de los responsables de los mismos. "Ibíd."

En esta base de datos de incidencias también se podrán registrar las distintas actualizaciones y parches instalados en el sistema operativo, bases de datos y aplicaciones informáticas de la empresa. "Ibíd."

En este contexto, se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, por lo que no se refiere únicamente a cuestiones informáticas (mal funcionamiento de los equipos o las aplicaciones, por ejemplo), sino que también se deberían tener en cuenta otras cuestiones de tipo humano u organizativo (como las pérdidas de contraseñas). "Ibíd."

En las políticas de seguridad se podría establecer que el conocimiento y la no notificación o registro de una incidencia por parte de un usuario podría ser considerado como una violación de las políticas de seguridad de la organización por parte de este usuario. "Ibíd."

2.2.6 Formato de la política de seguridad.

2.2.6.1 Declaración de política

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

2.2.6.2 Propósito

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

2.2.6.3 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. "Ibíd."

2.2.6.4 Acatamiento

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

Las posibles violaciones de las políticas de seguridad pueden tener lugar por desconocimiento o falta de la adecuada formación, por negligencia, por un fallo accidental o bien por una actuación malintencionada de un determinado usuario del sistema. Como consecuencia de estas violaciones de las directrices y medidas de seguridad, la organización deberá determinar cuál es el nivel de responsabilidad del usuario y de la gravedad de su actuación, adoptando las correspondientes medidas disciplinarias que correspondan en cada caso. "Ibíd."

2.2.6.5 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. "Ibíd."

Las medidas disciplinarias tendrían que haber sido previamente aprobadas y publicitadas por la Dirección de Talento Humano, contando con la participación de los propios representantes de los trabajadores. Estas medidas disciplinarias deberían ser consecuentes con el resto de las políticas de la empresa, respetando además los derechos fundamentales de los trabajadores y la legislación laboral vigente. "Ibíd."

2.2.6.6 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. "Ibíd."

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. "Ibíd."

2.2.6.7 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. "Ibíd."

2.2.6.8 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. "Ibíd."

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. "Ibíd."

Por otra parte, la organización debería tener identificado al personal clave para garantizar el adecuado nivel de cumplimiento de las normas y procedimientos de seguridad. En estos casos, se podría solicitar la firma de una carta o documento por pate de estos empleados en el que se comprometan a cumplir con las directrices y principios establecidos en las políticas de seguridad de la organización. También se podrían contemplar las obligaciones y responsabilidades mediante una serie cláusulas anexas al contrato laboral de cada uno de estos empleados. Esta medida podría extenderse, si se considera necesario, a todo el personal de la organización. "Ibíd."

2.3 TÉCNICAS DE ATAQUE.

2.3.1 Ataque.

Un ataque es el método por el cual un individuo, mediante un sistema informático intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador personal, red privada, etc.).

2.3.2 Software Malicioso [10]

Costas, J. (2010,pag. 124, 130, 134) encontró lo siguiente:

Actualmente, gracias a las comunicaciones y al creciente uso de las TIC, los sistemas de información se han convertido en objetivo de todo tipo de ataques y son sin duda el principal foco de amenazas. Por esta razón es fundamental identificar qué recursos y elementos necesitan protección así como conocer los mecanismos o herramientas que podemos emplear para procurar su protección.

Con el nombre de software malicioso o malware agrupamos a los virus, gusanos, troyanos y en general todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto. "Ibíd."

Para referirse a todos ellos también se suelen emplear las palabras: código malicioso, software malicioso, software mal intencionado, programas maliciosos o, la más usual, malware, que procede de las siglas malicious software. "Ibíd."

Los programas maliciosos afectan a cualquier dispositivo que tenga un sistema operativo que pueda entender el fichero malicioso, es decir:

- Ordenadores personales.
- Servidores.
- Teléfonos móviles.
- PDA
- Videoconsolas.`

2.3.2.1 Virus.

Su nombre es una analogía a los virus reales ya que afectan otros archivos, es decir, sólo pueden existir en un equipo dentro de otro fichero. Los ficheros infectados generalmente son ejecutables: .exe, .src. o en versiones antiguas .com, .bat; pero también pueden infectar otros archivos, por ejemplo, un virus de Macro infectará programas que utilicen macros, como los productos Office. "Ibíd."

Los virus se ejecutan cuando se ejecuta el fichero infectado, aunque algunos de ellos además están preparados para activarse sólo cuando se cumple una determinada condición, por ejemplo que sea una fecha concreta. Cuando están en ejecución, suelen infectar otros ficheros con las mismas características que el fichero anfitrión original. Si el fichero que se infecta se encuentra dentro de un dispositivo extraíble o una unidad de red, cada vez que un nuevo usuario acceda al fichero infectado, su equipo también se verá comprometido. "Ibíd."

2.3.2.2 Gusanos. [20]

Alveniz, (2011), encontró lo siguiente:

Son programas cuya característica principal es realizar el máximo número de copias posible de sí mismos para facilitar su propagación. A diferencia de los virus no infectan otros ficheros. Los gusanos se suelen propagar por los siguientes métodos:

- Correo electrónico.
- Redes de compartición de ficheros (P2P).
- Explotando alguna vulnerabilidad.
- Mensajería instantánea.

- Canales de chat.

Generalmente, los gusanos utilizan la ingeniería social para incitar al usuario receptor a que abra o utilice determinado fichero que contiene la copia del gusano. De este modo, si el gusano se propaga mediante redes P2P, las copias del gusano suelen tener un nombre sugerente de, por ejemplo, alguna película de actualidad; para los gusanos que se propagan por correo, el asunto y el adjunto del correo suelen ser llamativos para incitar al usuario a que ejecute la copia del gusano.

Eliminar un gusano de un ordenador suele ser más fácil que eliminar un virus. Al no infectar ficheros la limpieza del código malicioso es más sencilla, no es necesario quitar sólo algunas partes del mismo, basta con eliminar el archivo en cuestión.

2.3.2.3 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. [16]

2.3.2.4 Puertas traseras.

Un back door o puerta trasera es un método para eludir los procedimientos normales de autenticación a la hora de conectarse a una computadora. Una vez que el sistema ha sido comprometido (por uno de los anteriores métodos o de alguna otra forma) una puerta trasera puede ser instalada para permitir un acceso remoto más fácil en el futuro. Las puertas traseras también pueden ser instaladas previamente al software malicioso para permitir la entrada de atacantes. Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, intentando permanecer ocultos ante una posible inspección. Para

instalar puertas traseras los crakers pueden usar troyanos, gusanos u otros métodos. [21]

2.3.2.5 Bombas lógicas.

Una bomba lógica es una parte de código insertada intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones pre programadas, en ese momento se ejecuta una acción maliciosa. Por ejemplo, un programador puede ocultar una pieza de código que comience a borrar archivos cuando sea despedido de la compañía (en un disparador de base de datos (trigger) que se dispare al cambiar la condición de trabajador activo del programador). [22]

Ejemplos de acciones que puede realizar una bomba lógica

- Borrar información del disco duro
- Mostrar un mensaje
- Reproducir una canción
- Enviar un correo electrónico
- Apagar el monitor

2.3.2.6 Escáner de puertos. [16]

Alulema, D. (2008,pág. 20-24) encontró lo siguiente:

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. "Ibíd."

2.3.2.7 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. "Ibíd."

- **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. "Ibíd."

- **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. "Ibíd."

- **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. "Ibíd."

- **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). "Ibíd."

- **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. "Ibíd."

- **Redirección.** Es otro método de ataque DNS, consiste en comprometer links de una página web con links falsos, aparentemente estos enlaces son legítimos, pero redireccionan 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. "Ibíd."

2.3.2.8 Ataque de repetición.

Un ataque por repetición se produce cuando un atacante copia una secuencia de mensajes entre dos partes y reproduce la secuencia a una o más partes. A menos que se mitigue, el equipo objeto del ataque procesa la secuencia como mensajes legítimos, produciendo una gama de malas consecuencias, como pedidos redundantes de un elemento. "Ibíd."

2.3.2.9 Password cracking.

Es un proceso informático que consiste en descifrar 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. "Ibíd."

2.3.2.10 Ingeniería Social.

La ingeniería social hace referencia a una serie de técnicas utilizadas para engañar a los usuarios internos a fin de que realicen acciones específicas o revelen información confidencial. "Ibíd."

A través de estas técnicas, el atacante se aprovecha de usuarios legítimos desprevenidos para obtener acceso a los recursos internos y a información privada, como números de cuentas bancarias o contraseñas. "Ibíd."

Los atacantes de ingeniería social aprovechan el hecho de que a los usuarios generalmente se los considera uno de los enlaces más débiles en lo que se refiere a la seguridad. Los ingenieros sociales pueden ser internos o externos a la organización; sin embargo, por lo general no conocen a sus víctimas cara a cara. "Ibíd."

2.3.2.11 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. "Ibíd."

Esto se hace mediante aplicaciones que actúan sobre todos los sistemas que componen el tráfico de una red, así como la interactuación con otros usuarios y ordenadores. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis (contraseñas, mensajes de correo electrónico, datos bancarios, etc.). Por ello, cada vez es más importante enviar encriptada la información. "Ibíd."

2.3.2.12 Modificación de sitios Web (Defacing).

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. "Ibíd."

2.3.2.13 War Dialing.

Es un método de escaneo automático de números telefónicos empleando un módem para encontrar computadoras conectadas a estos. Este escaneo se realiza empleando programas llamados war dialers. "Ibíd."

Hoy en día está en desuso debido a las interconexiones ofrecidas por los proveedores de acceso a Internet. "Ibíd."

2.3.2.14 Negación del servicio.

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

- **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). "Ibíd."

  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. "Ibíd."

- **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. "Ibíd."

- **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. "Ibíd."

- **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. "Ibíd."

2.3.2.15 Criptoanálisis.

El objetivo del criptoanálisis es encontrar debilidades en los sistemas criptográficos que permitan elaborar ataques (ataques criptoanalíticos) que rompan su seguridad sin el conocimiento de información secreta.

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. "Ibíd."

2.3.2.16 Fuerza bruta.

Se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Los ataques por fuerza bruta suelen utilizarse para superar sistemas criptográficos como los protegidos con contraseñas. Los cyber delincuentes utilizan programas informáticos para probar una gran cantidad de contraseñas y descifrar el mensaje o acceder al sistema. Para evitar ataques por fuerza bruta, es importante utilizar contraseñas lo más seguras posible. [23]

2.4 PROTECCIONES.

2.4.1 Encriptación

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. [16]

2.4.1.1 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. [16]

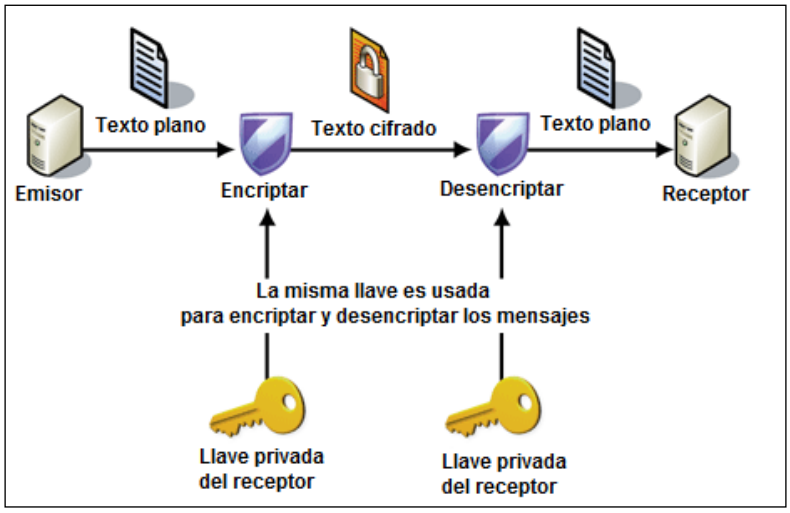


Figura 2.4.1 Encriptación de clave privada.

Fuente: Blogspot (2012).

Dentro de los algoritmos de encriptación simétrica podemos encontrar los siguientes: [28]

- **DES** (Digital Encryption Standard): Creado en 1975 con ayuda de la NSA (National Security Agency), en 1982 se convirtió en un estándar. Su arquitectura está basada en un sistema monoalfabético, donde un algoritmo de cifrado aplica sucesivas permutaciones y sustituciones al texto en claro. En un primer momento la información de 64 bits se somete a una permutación inicial, y a continuación se somete a una permutación con entrada de 8 bits, y otra de sustitución de entrada de 5 bits, todo ello constituido a través de un proceso con 16 etapas de cifrado. [28]

  El algoritmo DES usa una clave simétrica de 64bits, los 56 primeros bits son empleados para el cifrado, y los 8 bits restantes se usan para comprobación de errores durante el proceso. La clave efectiva es de 56 bits, por tanto, tenemos 2^{47} combinaciones posibles, por lo que la fuerza bruta se hace casi imposible.

- **3DES** (Three DES o Triple DES): Antes de ser quebrado DES, ya se trabajaba en un nuevo algoritmo basado en el anterior. Este funciona aplicando tres veces el proceso con tres llaves diferentes de 56 bits. La importancia de esto es que si alguien puede descifrar una llave, es casi

imposible poder descifrar las tres y utilizarlas en el orden adecuado. Hoy en día es uno de los algoritmos simétricos más seguros. [28]

3DES aumenta de forma significativa la seguridad del sistema de DES, pero requiere más recursos del ordenador.

- **IDEA** (International Data Encryption Algorithm): Más conocido como un componente de PGP (encriptación de mails), trabaja con llaves de 128 bits. Realiza procesos de shift y copiado y pegado de los 128 bits, dejando un total de 52 sub llaves de 16 bits cada una. Es un algoritmo más rápido que DES, pero al ser nuevo, aun no es aceptado como un estándar, aunque no se le han encontrado debilidades aún. [28]

- **AES** (Advanced Encryption Standard): Éste fue el ganador del primer concurso de algoritmos de encriptación realizado por la NIST (National Institute of Standards and Technology) en 1997. Después de 3 años de estudio y habiendo descartado a 14 candidatos, este algoritmo, también conocido como Rijndael por Vincent Rijmen y Joan Daemen, fue elegido como ganador. Aun no es un estándar, pero es de amplia aceptación a nivel mundial. Junto a 3DES es de los más seguros. [28]

Cualquiera de estos algoritmos utiliza los siguientes dos elementos. Ninguno de los dos debe pasarse por alto ni subestimar su importancia.

- **IV** (Vector de inicialización): Ésta cadena se utiliza para empezar cada proceso de encriptación. Un error común es utilizar la misma cadena de inicialización en todas las encriptaciones. En ese caso, el resultado de las encriptaciones es similar, pudiendo ahorrarle mucho trabajo a un hacker en el desciframiento de los datos. Tiene 16 bytes de largo.

- **Key** (llave): Esta es la principal información para encriptar y desencriptar en los algoritmos simétricos. Toda la seguridad del sistema depende de donde este esta llave, como esté compuesta y quien tiene acceso. El largo de las llaves depende del algoritmo.

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.	Requiere compartir información secreta.
Seguridad relativa.	Administración compleja.
Ampliamente difundido.	No autenticación.
	No controla el No repudio.

Tabla 2.4.1 Ventajas y desventajas de la Encriptación Simétrica.

Fuente: Blogspot (2012).

2.4.1.2 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. [28]

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.

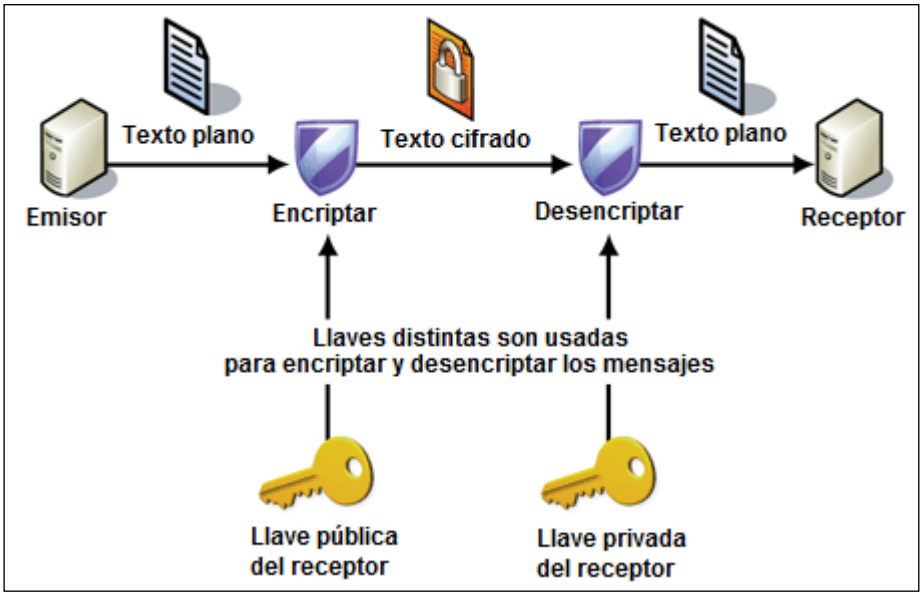


Figura 2.4.2 Encriptación de clave pública.

Fuente: Blogspot (2012).

Los algoritmos de encriptación asimétrica más conocidos son:

- **RSA** (Rivest, Shamir, Adleman): Creado en 1978, hoy es el algoritmo de mayor uso en encriptación asimétrica. Tiene dificultades en encriptar grandes volúmenes de información, por lo que es usado por lo general en conjunto con algoritmos simétricos. [28]

- **Diffie-Hellman** (& Merkle): No es precisamente un algoritmo de encriptación sino un algoritmo para generar llaves públicas y privadas en ambientes inseguros.

- **ECC** (Elliptical Curve Cryptography): Es un algoritmo que se utiliza poco, pero tiene importancia cuando es necesario encriptar grandes volúmenes de información.

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

Tabla 2.4.2 Ventajas y desventajas de la Encriptación Asimétrica.

Fuente: Blogspot (2012).

2.4.1.3 Localización de los dispositivos de cifrado [16]

Alulema, D. (2008, pág. 35-37), encontró lo siguiente:

Existen dos alternativas para la ubicación del cifrado:

- **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 dónde 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. "Ibíd."

- **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. "Ibíd."

Una variante es el cifrado mixto (enlace-enlace, extremo-extremo), donde las cabeceras van cifradas enlace a enlace y los datos extremo a extremo.

Pero con esto, a un intruso se le oculta las direcciones y los contenidos, pero no el volumen de información intercambiado. Para ocultar dicha información, se integra tráfico de relleno, para ocultar el volumen de información real. "Ibíd."

2.4.1.4 Relleno de tráfico

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. "Ibíd."

2.4.1.5 Integridad de mensajes.

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

- **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. "Ibíd."

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. "Ibíd."

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 2.4.3 Algoritmos Hashing.

Fuente: Alulema, D. (2008)

2.4.1.6 Autenticación.

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. "Ibíd."

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

- **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. "Ibíd."

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. "Ibíd."

2.4.1.7 Ventajas y desventajas.

En muchas ocasiones se implementan sistemas cifrados híbridos, en los que se usa la llave pública del receptor para encriptar una clave simétrica que se usará en el proceso de comunicación encriptada. De esta forma se aprovechan las ventajas de ambos sistemas, usando el sistema asimétrico para el envío de la clave sensible y el simétrico, con mayor velocidad de proceso, para el envío masivo de datos.

El algoritmo RSA es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas híbridos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

El algoritmo AES es el algoritmo de encriptación de más amplia difusión y más común en uso de los sistemas simétricos.

2.4.2 Secure Sockets Layer (SSL).

SSL en español capa de conexión segura y su sucesor Transport Layer Security (TLS; en español seguridad de la capa de transporte) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet. [24]

Se utiliza la encriptación asimétrica para preparar la sesión SSL y la encriptación simétrica para transmitir datos de forma segura sobre una red insegura. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar. [24]

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Puede proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP). [24]

2.4.2.1 HTTPS

Uno de los usos más importantes de SSL es junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos. 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. [24]

El proceso consiste en preparar una sesión SSL: [16]

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.

La tecnología SSL en las transacciones de comercio electrónico, los procesos de trabajo online y los servicios por Internet sirve para: [25]

- Para proteger transacciones realizadas con tarjetas de banco.
- Para ofrecer protección online a los accesos al sistema, la información confidencial transmitida a través de formularios web o determinadas áreas protegidas de páginas web.
- Para proteger el correo web y las aplicaciones como el acceso web a Outlook o los servidores Exchange y Office Communications.
- Para proteger los procesos de trabajo y la virtualización de aplicaciones como plataformas Citrix Delivery o las plataformas de cloud computing.
- Para proteger la conexión entre un cliente de correo como Microsoft Outlook y un servidor de correo como Microsoft Exchange.
- Para proteger la transferencia de archivos sobre HTTPS y servicios de FTP, como podrían ser las actualizaciones de nuevas páginas por parte de un propietario de una página web o la transmisión de archivos pesados.
- Para proteger los accesos a redes y cualquier otro tráfico de red con VPN de SSL como podrían ser los servidores de acceso VPN o las aplicaciones como Citrix Access Gateway.

2.4.3 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. [16]

- **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. [16]

- **PEM** (Privacy-Enhamsed Mail). 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. [16]

- **S/MIME** (Secure 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. [16]

2.4.4 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. [16]

Hay varios motivos para dividir una LAN en segmentos:

- Aislar los problemas de red: Segmentos aislados también aumentan la estabilidad de la red, ya que los fallos dentro de un segmento no afecta al resto de la red. [26]

- Reducción de la congestión: Cada vez que un equipo de una LAN quiere comunicar, los paquetes se envían a través de la red donde más de un ordenador envía paquetes a la vez. En una LAN segmentada, existen paquetes dentro de un primer segmento antes de ser transmitida en el resto de la red. Una LAN segmentada generalmente tienen una velocidad más alta, porque no pierde tiempo al procesar el tráfico innecesario. [26]

- Mayor seguridad: Los administradores de red pueden configurar segmentos de tal manera que transmiten y reciben paquetes sólo dentro de su subred o segmento. Este filtrado de los paquetes entrantes y salientes en una red LAN asegura que los paquetes no autorizados no se envían dentro o fuera del segmento. [26]

- Redes de Extensión: Una LAN puede alcanzar su límite físico y no puede soportar hosts adicionales con el hardware existente. Un segmento de red por lo tanto se puede añadir como una extensión de la red, mientras que esta físicamente distinto del resto de la red. [26]

- Asignación de ancho de banda: Las aplicaciones que requieren un ancho de banda dedicado se pueden implementar en segmentos separados sin necesidad de utilizar el resto del ancho de banda de LAN. Los segmentos también pueden dividirse de acuerdo con su uso de los recursos de ancho de banda en el que los recursos con gran ancho de banda pueden tener los segmentos dedicados sin competir con el resto de los clientes de la LAN. [26]

2.4.5 Sistemas Honeypot. [27]

Katz, M. (2013,pág. 237-240) encontró lo siguiente:

El término honeypot (tarro de miel) se refiere a un equipo que posee un bajo nivel de seguridad de manera intencional, con el fin de tentar y atraer potenciales atacantes, y de esa manera intentar identificarlos y analizar sus técnicas de ataque.

Son una herramienta de seguridad muy importante que nos permite proteger nuestra red y equipos de manera simple y económica. En resumen, su implementación se centraliza en la instalación de un equipo en la red pública o en la red DMZ. Es preciso instalarle aplicaciones y servicios, pero sin realizarle configuraciones de seguridad. Además, se le debe asignar una conexión directa hacia la red pública con total visibilidad desde fuera de nuestro perímetro. "Ibíd."

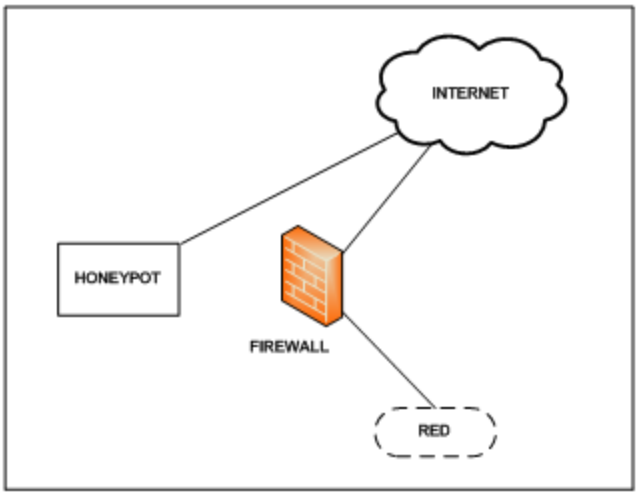


Figura 2.4.3 Honeypot en la red pública.

Fuente: Katz, M. (2013).

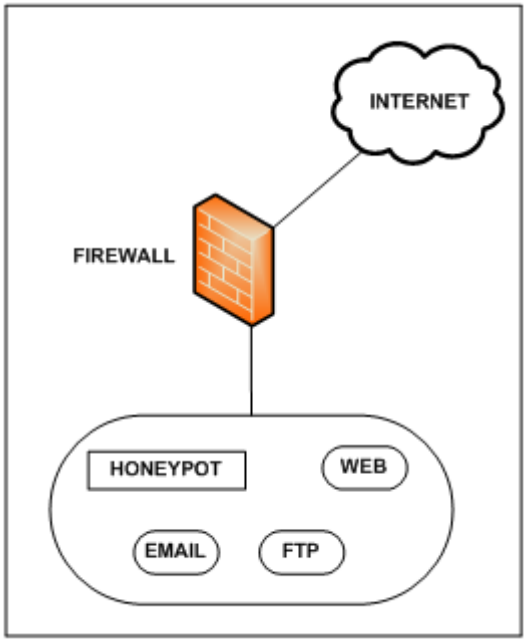


Figura 2.4.4 Honeypot en la red DMZ.

Fuente: Katz, M. (2013).

Los atacantes poseen herramientas automatizadas de análisis y búsqueda de equipos vulnerables. Una honeypot aparecerá rápidamente en esa búsqueda, y el atacante procederá luego a intentar una intrusión en dicho equipo. Como el equipo en cuestión es extremadamente vulnerable, el atacante probablemente podrá obtener acceso y comenzará a buscar información utilizando métodos propios y personales. "Ibíd."

En ese momento, la honeypot comenzará a almacenar información de toda la actividad del atacante, que luego estará a disponibilidad del administrador para

revisar los comportamientos del atacante, y sobre la base de ello analizar el nivel de seguridad de sus verdaderos equipos ante las técnicas de intrusión que se ejecutaron sobre la honeypot. Paralelamente, el uso de una honeypot logrará desviar la atención del atacante de los equipos reales e importantes de nuestra red. "Ibíd."

Existen dos tipos de honeypots, según su nivel de interacción:

1. Honeypots de baja interacción: simplemente simulan sistemas operativos y servicios, sin proveer una interacción real. Son fácilmente detectables por el atacante, pero requieren menores recursos y su implementación es extremadamente simple. "Ibíd."

2. Honeypots de alta interacción: son equipos reales con sistemas operativos y servicios reales ejecutándose. Son más difíciles de detectar por el atacante, pero requieren de un servidor dedicado ejecutando servicios reales, que deberán configurarse con información falsa para simular ser un equipo real. "Ibíd."

Sin embargo, una honeypot mal configurada se puede tornar en un arma de doble filo, ya que un atacante podría ingresar a nuestra red a través del acceso que obtuvo en la honeypot. Como medida de seguridad, las honeypots no deberán tener información real ni conexiones privadas con el resto de la red. Deberá ser un equipo aislado del resto de la red al que solo se podrá acceder físicamente para administrarlo, y el cien por ciento de la información que almacene deberá ser falso. Para grupos grandes de honeypots dentro de una red, se utiliza el término honeynet. "Ibíd."

CAPÍTULO 3

ANÁLISIS DE TECNOLOGÍAS DE SEGURIDAD PERIMETRAL

3.1 SEGURIDAD PERIMETRAL

La seguridad perimetral basa su filosofía en la protección de todo el sistema informático de una empresa desde fuera, es decir, establecer una coraza que proteja todos los elementos sensibles frente amenazas diversas como virus, gusanos, troyanos, ataques de denegación de servicio, robo o destrucción de datos, hackeo de páginas web corporativas, etcétera. [42]

Toda esta tipología de amenazas posibles ha fomentado una división de la protección perimetral en dos vertientes:

- **A nivel de red:** en el que podemos encontrar los riesgos que representan los ataques de hackers, las intrusiones o el robo de información en las conexiones remotas.

- **A nivel de contenidos:** en donde se engloban las amenazas que constituyen los virus, gusanos, troyanos, spyware, phishing y demás clases de malware, el spam o correo basura y los contenidos web no apropiados para las compañías.

Esta clara división unida al modo de evolución de las amenazas en los últimos años ha propiciado que el mercado de seguridad perimetral se centrase en la creación de dispositivos dedicados a uno u otro fin. [42]

3.2 FIREWALL

Katz, M. (2013, pág. 219- 225), encontró lo siguiente:

El firewall (cortafuegos) es un componente de red cuya función principal es la de bloquear los accesos hacia la red y desde ella, según un conjunto de reglas y criterios personalizables. En toda red existe lo que se denomina el perímetro, que consiste en una línea imaginaria que bordea cada red. Esta línea imaginaria se corresponde con las segmentaciones físicas y lógicas que se establecen utilizando dispositivos de ruteo.

La función del firewall es regular la información que transita entre el perímetro de nuestra red y las redes públicas conectadas a nuestra red. La tarea del firewall es revisar cada bit que intenta ingresar o egresar de nuestra red, aplicarle una lógica de comparación (obtenida de la configuración de políticas de seguridad en el mismo firewall), y según los resultados permitir o denegar el paso de dicha información hacia la red destino. "Ibíd."

Sobre la base de este comportamiento, existen dos premisas principales:

1. **Restrictiva:** todo lo que no esté explícitamente permitido, será restringido.

2. **Permisiva:** todo lo que no esté explícitamente restringido, será permitido.

El firewall basará su proceso de decisión en la premisa que haya sido seleccionada en su política de configuración, y continuará realizando las comparaciones necesarias para determinar si permite el tránsito de la información o lo bloquea.

3.2.1 Características de diseño y configuración.

Principios de diseño:

El Firewall es colocado entre la red local y la Internet (red no confiable).

- **Objetivos:**

  - Establecer un enlace controlado.
  - Proteger la red local de ataques basados en la Internet.
  - Proveer un único punto de choque.

- **Metas de Diseño:**

  - Todo el tráfico interno debe pasar a través del firewall para ir hacia el exterior.
  - El firewall determina si el trafico externo (tráfico que entra a la red considerado desde el exterior) accede a los servicios internos de la organización.
  - Sólo el tráfico autorizado (definido por política de seguridad local) se le permitirá pasar.
  - El firewall por sí mismo es inmune a penetraciones (usando un sistema confiable con un sistema operativo seguro).

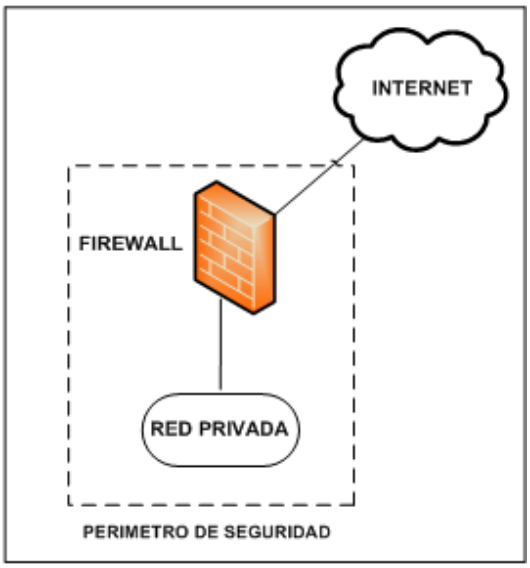


Figura 3.2.1 Perímetro de Seguridad.

Fuente: Katz, M. (2013).

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

- Políticas de seguridad de la organización.

- Nivel de monitoreo, redundancia y control.
- Aspecto económico.

3.2.2 Componentes

Un firewall puede estar representado por un equipo de hardware dedicado, o puede tratarse de un software que se ejecuta sobre un sistema operativo. En definitiva, a modo arquitectónico se trata de un equipo que intermedie las comunicaciones de la red (o redes) que desea proteger. "Ibíd."

3.2.2.1 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: [16]

- 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. [16]

- **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.

3.2.2.2 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. [16]

- **Proxy a nivel de aplicación.**

Son aplicaciones software (servicios proxy) para bloquear o reenviar conexiones a servicios como 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. [16]

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). [16]

3.2.2.3 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: [16]

- 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 router desconocidos.

Existen herramientas que permiten realizar el monitoreo de la actividad en la red, a continuación se mencionan los principales:

- **Wireshark:** Es un analizador de protocolos basado en software libre y se ejecuta sobre la mayoría de sistemas operativos Unix así como en Microsoft Windows, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca. Permite ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo[3]. También incluye una versión basada en texto llamada tshark. [58]

  Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. [58]

- **Ntop (Network Top):** Es una herramienta que permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y para ayudarnos a detectar malas configuraciones de algún equipo, (facilitando la tarea ya que, justo al nombre del equipo, aparece sale un banderín amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de servicio. Posee un microservidor web

[3] En informática, el modo promiscuo es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella. Este modo está muy relacionado con los sniffers que se basan en este modo para realizar su tarea. http://es.wikipedia.org/wiki/Modo_promiscuo

desde el que cualquier usuario con acceso puede ver las estadísticas del monitorizaje. [58]

El software está desarrollado para platarfomas Unix y Windows. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico. Los protocolos que es capaz de monitorizar son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11. [58]

- **Nmap:** Es un programa de código abierto que sirve para efectuar rastreo de puertos, se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática. Ha llegado a ser uno de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general. Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking. [58]

  Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crackers pueden usarlo para descubrir objetivos potenciales. [58]

  Nmap es a menudo confundido con herramientas para verificación de vulnerabilidades como Nessus. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas. [58]

- **Nagios**: Es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas. [58]

  Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante correo electrónico, mensajes SMS cuando estos parámetros exceden de los márgenes definidos por el administrador de red. Nagios está licenciado bajo la GNU General Public License Versión 2 publicada por la Free Software Fundation. [58]

Las herramientas antes mencionadas permiten a los administradores de red contar con un sistema aliado, que lo mantiene informado de la actividad de la red, por lo tanto se recomienda la utilización de herramientas especializadas que permitan realizar esta labor. La elección de la herramienta dependerá de las características de nuestra red y de los recursos a ser monitoreados.

3.2.3 Arquitecturas

3.2.3.1 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. [16]

3.2.3.2 Bastión Host

El firewall está ubicado en la red privada, y tanto las conexiones entrantes como salientes están configuradas para ser automáticamente redirigidas hacia este equipo, que las filtrará según su propio conjunto de reglas. Este equipo funcionará de intermediario entre las redes privadas y públicas, aunque no exista una segmentación lógica o física entre ellas (salvo por el router del perímetro). Esta función es conocida como proxy. Es importante destacar que, aunque el bastión host se encuentre en la red privada, tendrá visibilidad directa y total desde la red pública, pasando a ser una indefectible víctima de ataque. [27]

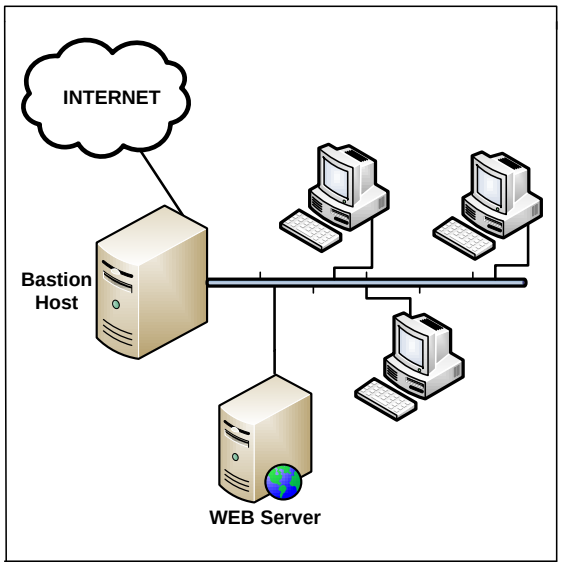


Figura 3.2.2 Bastion Host.

Fuente: Katz, M. (2013).

3.2.3.3 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 pública. El análisis y filtrado de información se realiza en el momento en el que los bits atraviesan el equipo. Esta técnica es la más usada debido a su efectividad. En esta situación, es imposible circunvalar el control, ya que el firewall se encuentra físicamente intermediando ambas redes. [27]

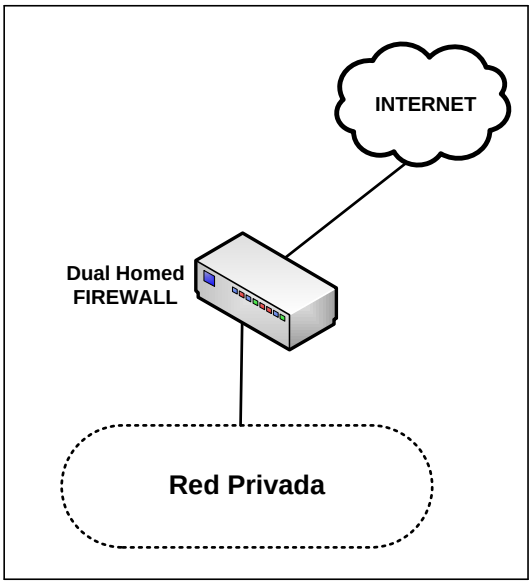


Figura 3.2.3 Dual Homed firewall

Fuente: Katz, M. (2013).

3.2.3.4 Screened Host

Consiste en combinar un router (filtrado de paquetes) con un host bastión (ejecuta los proxies de las aplicación). [27]

3.2.3.5 DMZ (Demilitarized Zone)

Utilizando las iniciales DMZ se identifica a una subred semipública dentro de nuestra red general. También se la puede encontrar nombrada como red de perímetro, ya que ahí es donde justamente se encuentra ubicada. Esta disposición estructural está diseñada para proveer una capa adicional de protección a nuestra red general, ya que es aquí donde se deberán posicionar los servidores que suministren servicio hacia las redes públicas. De esta forma, la red privada permanecerá resguardada, ya que no se necesitará permitir el acceso a ella desde otras redes. [27]

El firewall que regule esta subred deberá tener una política restrictiva, pero con reglas no muy específicas. Así podrá permitir el tránsito desde dichos servidores y hacia ellos.

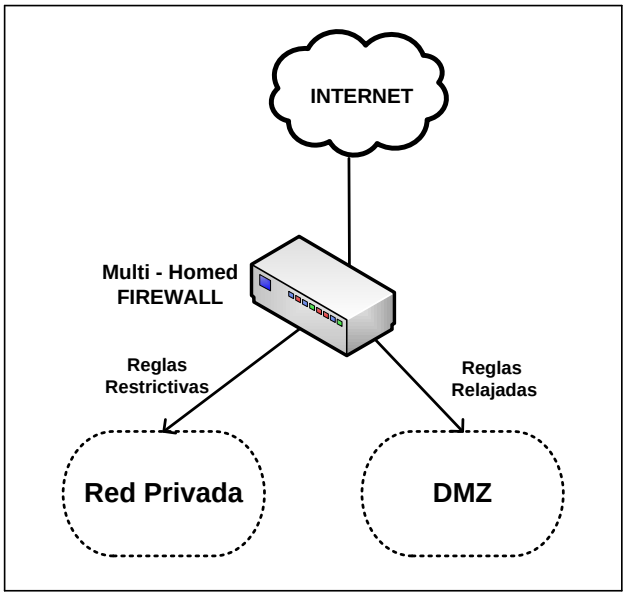


Figura 3.2.4 Estructura de DMZ con multi-homed firewall

Fuente: Katz, M. (2013).

Una forma alternativa de implementar una red DMZ es utilizando dos dual-homed firewalls:

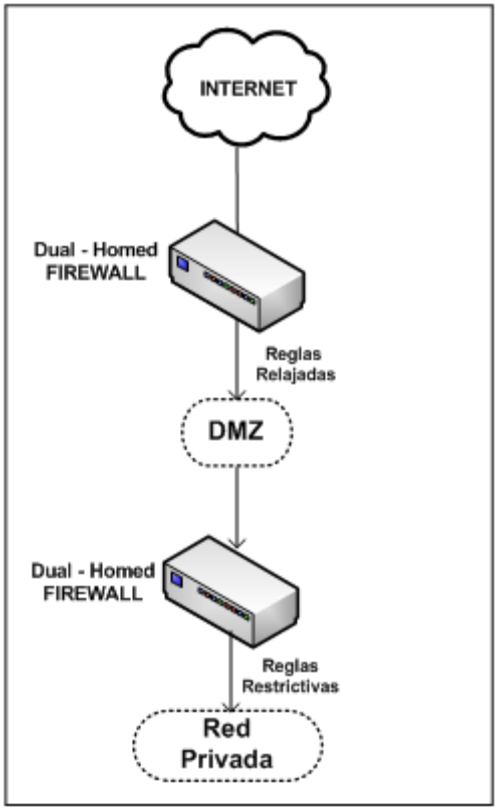


Figura 3.2.5 Estructura de DMZ con dos dual-homed firewalls

Fuente: Katz, M. (2013).

Este método es el más seguro de todos al requerir que la información atraviese dos barreras hasta llegar a la red privada.

Para obtener el mejor rendimiento en una red DMZ sin desmerecer la seguridad, los firewalls que intermedien en las comunicaciones, al igual que los servidores (tanto en la red semipública como en la red privada) deberán estar configurados correctamente según roles y ubicación en la red. [27]

3.2.4 Ventajas y desventajas.

Básicamente la función de un firewall es proteger la red de accesos no deseados por intrusos que pueden robar datos confidenciales, causar perdida de información valiosa o incluso denegar servicios en nuestra red.

Existen firewall basados en hardware especializado y firewall por software. Los firewall de hardware dedicado son una solución excelente en el caso de querer proteger una red empresarial ya que el dispositivo protegerá a la totalidad de equipos de la red y además su configuración y administración será en un solo equipo. Los firewall por software se acostumbran a usar por usuarios domésticos o en redes pequeñas.

Los firewall basados en código abierto como Linux, FreeBSD, OpenBSD, estos tienen características de red y de seguridad incorporadas, por lo que son las plataformas naturales para la construcción de productos de seguridad. La mayoría de los firewalls comerciales se basan en uno de ellos. A continuación se nombran varias opciones:

- **ClearOS:** Esta distribución basada en Red Hat/CentOS, es una solución integral y ofrece:
    - Firewall.
    - Sistema de detección de intrusos SNORT.
    - Red Privada Virtual (PPPT,IPSec,OpenVpn).
    - Proxy con filtrado de contenidos. (Squid, DansGuardian).
    - servicios e-mail (Webmail, Postfix, SMTP, POP3/s, IMAP/s).
    - Base de Datos y Web Server.

- Servidor de archivos y servicios de impresión (Samba and CUPS).
- Flexshares (almacenamiento unificado multiprotocolo que emplea CIFS, HTTP/S, FTP/S, and SMTP)
- MultiWAN (Diseño Internet tolerante a fallos).
- Informes de estadísticas de Sistema y servicios (MRTG y otros).

- **h3Devil Linux:** Es una distribución GNU/Linux para ser usada como Router/Firewall, que corre y se ejecuta desde un Live-CD. No usa interfaz gráfica, incluye servicios DNS, Web, FTP, SMTP, herramientas como Mysql, Wget, Lynx y utilidades de seguridad como OpenVPN y Shorewall. Está basada en Linux From Scratch(Linux desde el principio) un sistema de construcción de distribuciones Linux que permite al usuario crear sus propias versiones personalizadas.

- **Endian Firewall:** Es una distribución GNU/Linux de código abierto especializada en Routing/Firewalling, desarrollada por italian Endian Srl y la comunidad Endian. Está basada originalmente en IpCop otra distribución que a su vez fue un fork de SmoothWall.

- **Openwrt:** Es una distribución de GNU/Linux que se encuentra en routers y dispositivos embebidos. Comprende un conjunto de cerca de 2000 paquetes de software que se instalan y desinstalan bajo el sistema de administración de paquetes opkg. OpenWrt pude ser configurado usando la interface de línea de comandos de BusyBox ash, o la interfaz web LuCI. Operwrt puede correr en routers CPE, puertas de enlace residenciales, smartphones, computadores de bolsillo o PDA’s y laptops pequeñas como OLPC, pero también es posible que corra en computadores x86.

Queda claro que es altamente recomendable la utilización de un firewall, la arquitectura (basado en hardware o software) a ser implementada dependerá de los requerimientos de nuestra red, presupuesto y de las funcionalidades como gestión, flexibilidad, soporte, emisión de informes y documentación deberán ser tomados en cuenta al momento de seleccionar la mejor solución.

A continuación se describen las principales ventajas y desventajas que ofrecen los dispositivos firewall:

- **Ventajas:**
    - **Refuerza políticas.**

Muchos de los servicios que la gente quiere de Internet son inherentemente inseguros. El firewall permite pasar a través de él solo servicios aprobados y solo aquellos que se hayan configurado. Un firewall puede reforzar las políticas de seguridad añadiendo políticas más complejas. Por ejemplo bloqueando una transferencia de ficheros desde una parte de nuestra red y controlando qué usuarios tienen acceso. [29]

    - **Registra la actividad**

Como todo el tráfico pasa a través del firewall, este provee un buen lugar para recoger una colección de información sobre los usos de los sistemas y redes. Puede recopilar qué ocurre entre la zona protegida y la red externa. [29]

    - **Limita la exposición**

Este es uno de los usos más relevantes de los firewalls. A veces un firewall se usa para mantener una sección de la red separada de otra, haciendo esto se mantienen los problemas que puedan impactar en una sección separada del resto. En estos casos, una parte de la red puede ser más segura que otra, en otros casos una sección puede ser más sensible que otra. Cualquiera que sea la razón de la existencia de un firewall este limita el daño que puede hacer una red a otra. [29]

- **Desventajas:**
    - **Qué no pueden hacer**

Los firewalls ofrecen una excelente protección, pero no son la solución única y completa para la seguridad. Ciertos procesos están fuera del control del firewall. Y se necesita otros métodos para protegerse de estos sucesos incorporando otras herramientas. [29]

- **Dentro de la red**

Un firewall puede prohibir a un usuario enviar información confidencial fuera de la red a través de la conexión a internet pero el mismo usuario puede copiar los datos en un disco, imprimirlos y llevárselos fuera del edificio. Si el atacante esta dentro de la red el firewall no puede hacer nada. Dentro los usuarios pueden robar datos, dañar hardware y software, modificar programas sin siquiera pasar a través del firewall. Es necesario protegerse con medidas internas de seguridad. [29]

- **Conexiones que no van a través de él**

Un firewall puede controlar el tráfico que pasa a través de él pero no puede hacer nada con el tráfico que no pasa a través de él. Por ejemplo, si hay otra conexión (dial in) para conectarse a los sistemas detrás del firewall, este no tiene ninguna forma de proteger a los intrusos que usen modem. [29]

- **Virus**

Los firewalls no pueden mantener a los virus alejados de la red interna. Muchos firewalls escanean todo el tráfico entrante para determinar si este está permitido, pero el escaneo de los datos son la mayoría de veces solo las direcciones y puertos origen y destino, no para los detalles de los datos. Incluso los firewalls más sofisticados no son muy prácticos contra los viruses. Simplemente hay muchas maneras para esconder un virus entre otros datos. Determinar que existe un virus dado un paquete que pasa a través del firewall es muy difícil. La forma más práctica de defenderse de los virus es mantener un software de protección basado en los ordenadores, y educando de los posibles peligros a los usuarios y de cómo protegerse de ellos. [29]

3.3 SOFTWARE ANTIVIRUS

Un antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar códigos maliciosos. Aunque se sigue utilizando la palabra antivirus, estos programas han evolucionado y son capaces de detectar y eliminar, no sólo virus, sino también otros tipos de códigos maliciosos como gusanos, troyanos, etc. [10]

Un antivirus tiene tres principales funciones y componentes:

- **Vacuna:** Es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real. [35]

- **Detector:** Que es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o path. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura. [35]

- **Eliminador:** Es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas. [35]

3.3.1 Cómo funciona el antivirus

Los antivirus funcionan escaneando continuamente el equipo en busca de alguno de los virus que hay en la base de datos, por lo que es importante tenerlo siempre actualizado. [36]

- **Detección de virus:** El programa antivirus analiza todos los archivos que el sistema operativo crea, abre o cierra. De esta manera, se puede detectar un virus inmediatamente después de recibirlo. Aunque usted no lo vea su programa antivirus está siempre trabajando en segundo plano haciendo un seguimiento de procesos para interceptar los posibles virus. [36]

- **Reconocer el virus:** Esta aplicación utiliza una lista de definiciones de virus. Una definición de virus, o firma, es una descripción de un virus. Debido a que cada día se añaden nuevos virus, hay nuevas definiciones de virus a diario. Estas definiciones son programadas por los técnicos que trabajan en las compañías antivirus. [36]

- **Actualización:** El programa antivirus entra en contacto a través de Internet de forma regular con la compañía de antivirus para ver si hay nuevas

definiciones de virus. Si es así, estas se agregan a la lista de definiciones de virus. La mayoría de programas antivirus tienen una función que los actualiza de forma automática. Es importante que esta función está activada. De lo contrario, el programa antivirus no reconoce los virus más recientes. Casi todos los días hay nuevas actualizaciones disponibles. [36]

- **Comportamiento sospechoso:** Dado que, por lógica, siempre hay más virus que definiciones de virus, puede ocurrir que un programa antivirus no detecte un determinado virus. Por otra parte, hay virus que son difíciles de detectar, ya que están constantemente cambiando de forma (mutando). Por lo tanto, además de utilizar un software anti virus también es bueno conocer métodos adicionales para detectar la presencia de virus. [36]

- **Escanear:** La mayoría de los programas antivirus realizan de forma automática el trabajo de detección constante, utilizando la lista de definiciones de virus y observando el método de comportamientos sospechosos de aplicaciones. También es posible para el usuario escanear periódicamente el disco duro, o ciertas carpetas, para comprobar la existencia de virus, este método se denomina barrido y se utiliza para detectar virus, que se cuelan a través del antivirus o en momentos en los que el antivirus haya tenido que ser desconectado. Para realizar este escaneo deberá hacerlo de forma manual y se recomienda que hacerlo con cierta regularidad. La mayoría de programas antivirus permiten planificar está acción, para que no tenga que estar pendiente de ello. [36]

- **Qué sucede con el virus:** Supongamos que el programa antivirus ha detectado un virus, en un correo electrónico entrante o en el disco, en la mayoría de los casos, el programa antivirus eliminará automáticamente el archivo de virus. Si no es posible, entonces el virus será puesto en cuarentena[4]. Esto significa que existe una determinada carpeta en el disco duro donde se colocan los archivos que se están comportando de forma sospechosa. Usted puede decidir si desea eliminar el archivo o no. [36]

[4] La cuarentena es una zona segura del software donde los archivos son cifrados y almacenados para que no puedan transferir el virus a otros archivos.

Existen dos formas diferentes de utilizar un antivirus condicionando por dónde esté instalado, en el escritorio de forma local o en un servidor externo para acceder en línea.

3.3.2 Antivirus de Escritorio

Los antivirus de escritorio se suelen utilizar en modo residente para proteger al ordenador en todo momento de cualquier posible infección, ya sea al navegar por internet, recibir algún correo infectado o introducir en el equipo algún dispositivo extraíble que esté infectado. No necesitan que el ordenador esté conectado a internet para poder funcionar, pero sí que es necesario actualizarlos frecuentemente para que sean capaces de detectar las últimas amenazas de virus. Es recomendable tener sólo un antivirus de escritorio en el ordenador, ya que tener varios antivirus puede ocasionar problemas de incompatibilidad entre ellos. [10]

Característica	McAfee	Norton (Symantec)	ESET NOD32	Panda Security
Antivirus	SI	SI	SI	SI
Antispyware	SI	SI	SI	SI
Link Scanner	NO	NO	NO	SI
Antirootkit	SI	SI	SI	SI
Web Shield	NO	SI	SI	SI
ID Protection	SI	SI	NO	SI
Firewall	SI	SI	SI	SI
Antispam	NO	NO	NO	SI
Consumo de recursos	Medio	Alto	Bajo	Bajo

Figura 3.3.1 Antivirus de escritorio

Fuente: Costas, J. (2010).

- **Antivirus en Línea**

Los antivirus en línea son útiles para analizar el ordenador con un segundo antivirus cuando sospechamos que el equipo puede estar infectado. Si bien son

muy útiles para realizar un scaneo del ordenador y, de este modo, comprobar que no está infectado, no sirven para prevenir infecciones, esto sólo lo hacen los antivirus de escritorio. Estos antivirus no se instalan en el PC como un programa convencional, sino que se accede mediante un navegador web. El tiempo de scaneo varía en función de la velocidad de la conexión, la carga momentánea de los servidores o el volumen de datos que se analicen. La mayoría de estos servicios descargan un subprograma, por lo que la primera vez que se accede tardan unos minutos en arrancar. [10]

Los antivirus en línea son útiles para realizar un segundo análisis, cuando se sospecha que el ordenador puede estar infectado, pero el antivirus de escritorio no detecta nada extraño.

- **Antispyware**

Los spyware, programas espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de internet, generalmente a alguna empresa de publicidad. Todas estas acciones se hacen de forma oculta al usuario o bien se enmascaran tras confusas autorizaciones al instalar terceros programas, por lo que rara vez el usuario es consciente de ello. [10]

No todas las herramientas anti espías que se puede descargar de manera gratuita a través de internet son confiables, algunas de ellas pueden contener código malicioso, publicidad engañosa, no ofrecer la protección prometida e incluso dar como resultado falsos positivos.

- **Anti espías de Escritorio**

Los anti espías de escritorio son aquellos que requieren de instalación en el PC. Se suelen utilizar en modo residente, analizan cualquier fichero al que accede el PC en tiempo real, como complemento a los antivirus para proteger al ordenador en todo momento de cualquier posible infección de código espía. No requieren de conexión a internet para poder funcionar, pero sí necesitan estar actualizados para que sean capaces de detectar las amenazas más recientes. [10]

- **Anti espías en línea**

Los anti espías en línea son accesibles a través de un navegador web y no necesitan de la instalación de una aplicación completa en nuestro equipo para su funcionamiento. Necesitan por tanto de una conexión a internet para acceder a ellas, y, al estar disponibles directamente en línea se accede a la versión más actualizada de la herramienta. [10]

3.3.3 Ventajas y Desventajas

A la hora de escoger un antivirus hay que fijarse en las características de detección, rendimiento y funciones adicionales como copias de seguridad, almacenamiento en la nube, protección del navegador, cifrado o protección parental que ofrecen los fabricantes.

Un creciente número de suites de seguridad ahora disponen de herramientas especiales para ayudar a proteger las redes sociales, mismas que son objetivo de grupos que quieren hacerse con información personal. Mantenerlo al día es generalmente una buena idea, dado que nuevas amenazas aparecen constantemente.

Existen programas antivirus gratuitos para uso personal o para uso no comercial. En la mayoría de los casos estos antivirus gratuitos son versiones menos confiables que las versiones comerciales que pueden ser compradas. Los fabricantes de antivirus esperan que sus clientes hagan la prueba con la versión gratuita para la posterior compra de la versión comercial, que es lo que suele ocurrir en la mayoría de los casos. La gran ventaja del antivirus gratuito es precisamente esa, que sea gratis.

Es recomendable invertir y adquirir una solución antivirus efectiva y confiable a un fabricante especializado antes que confiar en los antivirus gratuitos, existe el riesgo de perder datos importantes y sufrir el desperfecto de nuestro computador, lo cual generará un gasto mucho mayor que el que genera adquirir anualmente el soporte, licenciamiento y actualización de la solución adquirida.

A continuación se describen las ventajas y desventajas que ofrecen los sistemas antivirus:

- **Ventajas**

  - **Protección contra código malicioso:** La mayor y más obvia ventaja de instalar un software antivirus es que evitará que entren virus, troyanos, malware y software espía. Los virus se clasifican por severidad desde inofensivos a totales atrocidades en el sistema. Un virus no sólo puede destruir todos los valiosos datos del computador, también puede hacer que sea completamente inútil infectando y destruyendo los procesos vitales para el rendimiento de la computadora. [37]

  - **Protección de la información personal:** Los hackers y los virus van de la mano. Un buen programa antivirus te protegerá mientras navegas por Internet, evitando que los hackers consigan información personal como tarjetas de crédito y acceso a cuentas bancarias. La función de cortafuegos incluida en la mayoría del software antivirus bloqueará cualquier conexión entrante no autorizada, evitando que los hackers pongan sus garras en tu vida y computadora. [37]

  - **Proteger la inversión:** Algunos programas antivirus son costosos, hay buenas opciones para quienes quieren algo relativamente barato o incluso gratis. Aunque elijas un programa por el que tengas que pagar, el coste del programa y de la suscripción a su servicio seguramente alargará la vida de tu computadora, lo que significa que tendrás que comprar computadoras nuevas con menos frecuencia que quienes no usan un software antivirus. [37]

  - El sistema tradicional de antivirus nos ofrece una serie de características muy importantes al momento de gestionar todo lo relacionado con los archivos infectados como la posibilidad de realizar copias de seguridad de los mismos en las llamadas Cuarentenas o la posibilidad de excluir del escaneo determinadas carpetas, posibilidades que no ofrecen los sistemas antivirus en línea. [37]

- **Desventajas**

  - Hay muchos programas antivirus gratuitos disponibles que protegerán tu sistema pero no garantizarán que todas las amenazas sean detectadas y eliminadas. La protección no es 100% garantizada al navegar por internet. [38]

  - Un programa antivirus puede requerir demasiados recursos (procesador, memoria RAM) para su óptimo funcionamiento al realizar un análisis exhaustivo. [38]

  - Obviamente, para que el sistema funcione, debemos tener conexión constante a Internet, elemento del cual puede prescindir un Antivirus Tradicional. [38]

  - Los antivirus en línea como cualquier otro servicio alojado en la nube, expondrá nuestros datos en mayor medida a los cyber delincuentes que si utilizamos un Antivirus Tradicional. [38]

  - Otro punto negativo que ofrecen los Antivirus en línea es una cuestión relacionada con la disponibilidad del servicio, tanto de los propios servidores de la empresa prestadora del servicio como de los servicios de nuestro ISP. [38]

3.4 SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS

3.4.1 Sistemas de Detección de Intrusos (IDS)

Los IDS son equipos que proveen un nivel de seguridad mayor a nuestra red, complementando al firewall y trabajando en conjunto con él. Su función principal es la detectar intrusiones a su área de cobertura, mediante el análisis exhaustivo de cada paquete de información que ingresa en ella. Al detectar una intrusión, el IDS podría realizar cualquier tipo de tarea pre configurada por el administrador, ya sea de rechazar futuros paquetes de igual origen o contenido, arrojar alertas de sistema, enviar un correo electrónico o sms al administrador, reconfigurar el firewall a un modo más preventivo, etc. [27]

Cada ataque posee su propio patrón de comportamiento. El IDS detecta este patrón a mitad del camino y neutraliza el remanente del ataque rechazando las conexiones que le correspondan. El IDS utiliza una técnica llamada sniffing (olfateo) mediante la cual el equipo es capaz de recopilar toda la información que circule dentro de su área de cobertura, ingresarla en su sistema de y analizarla, comparándola con su conjunto de reglas y políticas preestablecidas. El IDS puede utilizar la información encontrada en las siete capas del modelo OSI para hacer su análisis. Según sus niveles de tolerancia, esperará más o menos al sospechar de un supuesto ataque, antes de tomar una acción correctiva. [27]

- **Problemática con los IDS**

Existen dos problemáticas importantes que afectan a todo IDS:

1) **Falso negativo:** El IDS pasa por alto un ataque o intento de intrusión, tomándolo como una comunicación legítima y sin realizar ninguna acción correctiva al respecto. De esta forma, el atacante puede satisfactoriamente realizar su intrusión sin ser detectado ni detenido. [27]

2) **Falso positivo:** El IDS identifica un supuesto ataque y realiza las acciones correctivas correspondientes, basándose en un análisis incorrecto sobre una comunicación en realidad legítima. Esto puede tornarse un problema serio si el IDS tiene configurado acciones correctivas que sean restrictivas en relación al acceso a la red. Por ejemplo, si un IDS está configurado para cerrar el puerto 80 del firewall de perímetro al encontrarse con un supuesto ataque. En este caso, un falso positivo deshabilitaría el acceso público a los sitios web que la organización maneje, por culpa de una mala configuración del IDS. [27]

El nivel de tolerancia y rigurosidad que se le configure al IDS determinará la cantidad de falsos negativos y falsos positivos que ocurran. Cada IDS deberá ser configurado acorde a los parámetros y límites aceptables de cada organización.

- **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 [16]:

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

- **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 [16]:

- Sistemas expertos.
- Transición de estados.
- Comparación y emparejamiento de patrones.
- Detección basada en modelos.

3.4.1.1 Sistemas de detección de intrusos para red (NIDS).

Los NIDS (IDS de red) son equipos IDS que trabajan sobre los paquetes que circulan en el segmento de red al que están conectados, analizando todo el tránsito en él. Al igual que un firewall, puede estar representado por un equipo de hardware dedicado o puede tratarse de un software ejecutándose sobre un sistema operativo. [27]

Estos sistemas disponen de una o varias interfaces de red conectadas a determinados puntos estratégicos de la red. Monitorizan el tráfico que pasa por dichos puntos en busca de tráfico malicioso. Aunque estos sistemas en principio

son dispositivos absolutamente pasivos, con frecuencia se colocan los NIDS en cortafuegos y enrutadores, de manera que el propio sistema puede forzar el cierre de conexiones y modificar reglas de filtrado de una manera más directa. Mediante uno solo de estos sistemas se puede monitorizar el tráfico tanto interno como externo de una red para muchas máquinas. Los NIDS no suelen controlar toda la red sino determinados puntos estratégicos. La mayoría de las redes hoy en día son conmutadas, así que colocar los sensores de red suele implicar utilizar conmutadores especiales con un puerto "monitor" que reproduce todo el tráfico recibido en cualquiera de los puertos. [39]

Los NIDS tienen dos componentes:

- **Un sensor:** situado en un segmento de la red, la monitoriza en busca de tráfico sospechoso.
- **Una Consola:** recibe las alarmas del sensor o sensores y dependiendo de la configuración reacciona a las alarmas recibidas.

Este tipo de sistemas son bastante rápidos de instalar y mantener, y no dependen del sistema operativo instalado en las máquinas cubiertas. Suelen ser invisibles para los atacantes, por lo que los registros de sucesos que almacenan son poco vulnerables a la eliminación o alteración maliciosa, y suponen un recurso valioso para el almacenamiento de pruebas. [39]

Diferentes ubicaciones de los NIDS nos proporcionarán diferentes perspectivas de la seguridad de la red. Colocados fuera del cortafuegos permiten evaluar los ataques que se intentan producir aunque no alcancen a los servidores internos, mientras que si se colocan en el interior del cortafuegos nos permiten evaluar si este está bien configurado. [39]

3.4.1.2 Sistemas de detección de intrusos para hosts (HIDS).

Los HIDS (IDS de equipo) son un aplicativo de software que trabaja sobre el sistema operativo de un equipo, proveyéndolo de una protección adicional a ese equipo en particular. Al combinarse con un firewall por software, el equipo en cuestión tendrá lo que se llama protección en capas. [27]

Así como los NIDS se instalan en determinados puntos de la infraestructura de red, los HIDS se instalan en las máquinas que componen la red: tanto servidores como estaciones de trabajo. Un sensor, instalado directamente como un módulo sobre una máquina, dispone de información de mayor nivel semántico que los NIDS: llamadas al sistema, eventos complejos dentro de aplicaciones de alto nivel, etc. Un sistema basado únicamente en red tendría que ser mucho más complejo para entender la gran diversidad de protocolos que existen, y los que se implementan por encima de éstos. Por otra parte, la tendencia actual al uso de conexiones encriptadas, de indiscutible interés para mejorar la seguridad de los sistemas, hace que un sistema que solo escuche la red disponga de muy poca información para distinguir el tráfico malicioso del aceptable. [39]

3.4.2 Sistema de Prevención de Intrusiones (IPS)

Los IPS son equipos que trabajan de la misma forma que los IDS, pero con la diferencia de permitir el análisis de la información en tiempo real. Estos equipos poseen una puerta de entrada y una de salida. Al momento de recibir información por un extremo de conexión, se la analiza inmediatamente en búsqueda de potenciales ataques o intrusiones. Si la información es aprobada, el paquete es transmitido a través del otro extremo de conexión. En caso de sospechar de un ataque, el IPS podría reaccionar de manera preventiva, logrando que ni siquiera un paquete malicioso sea incorporado en la red o el equipo bajo su protección. [27]

Es importante resaltar que al implementar un IPS, todas las conexiones, tanto entrantes como salientes, que se realicen en el área de cobertura del IPS serán analizadas constantemente. Esto puede ocasionar graves problemas de rendimiento en la red y los equipos protegidos, por lo que es recomendable analizar el entorno donde se implementará el IPS. [27]

- **Características de un IPS**

  - Capacidad de reacción automática ante incidentes.
  - Aplicación de nuevos filtros conforme detecta ataques en progreso.
  - Mínima vigilancia.

- Disminución de falsas alarmas de ataques a la red.
- Bloqueo automático frente a ataques efectuados en tiempo real.
- Protección de sistemas no parchados.
- Optimización en el rendimiento del tráfico de la red.

3.4.2.1 IPS basados en host (HIPS)

Esta aplicación de prevención de intrusiones reside en la dirección IP específica de un solo equipo, permite prevenir posibles ataques en los nodos débiles de una red es decir los host. [40]

3.4.2.2 IPS basada en red (PIN)

Esta aplicación IPS es en hardware y cualquier acción tomada para prevenir una intrusión en una red específica de host (s) se hace de una máquina con otra dirección IP en la red. Son desarrollados específicamente para la plataformas hardware / software que analizan, detectan e informan sobre eventos relacionados con la seguridad. PIN están diseñados para inspeccionar el tráfico y la configuración de la política de seguridad, sobre la cual pueden verificar el tráfico malicioso. [40]

3.4.3 Ventajas y Desventajas.

Se ha visto que la diferencia entre los IDS y los IPS radica en la forma cómo reaccionan ante las intrusiones, los primeros se limitan a detectar y notificar de la intrusión mientras que los segundos toman acciones de algún tipo frente a tales eventos.

Debido a esto, se tiene que el uso de los IDS implica un corto lapso de tiempo para enterarse, analizar y determinar la acción correctiva a adoptar frente a la intrusión, para finalmente reaccionar manualmente al ataque. Por esta razón, el fuerte de los IDS es ayudar a la reconstrucción del ataque para su posterior análisis. Sin embargo es deseable detener el ataque de manera oportuna es así que los IPS son la solución adecuada, siempre y cuando estén debidamente configurados y puestos a punto con el fin de maximizar su nivel de precisión.

Existen distribuciones open source que permiten implementar los sistemas IDS/IPS, al estar basados en software libre se hacen propicios en entornos donde no se cuente con recursos económicos para adquirir otro tipo de soluciones comerciales. A continuación se describe las principales soluciones open source:

- **Snort:** Es un potente IDS/IPS basado en código abierto que se ha convertido en un estándar en el campo de la seguridad de sistemas informáticos. Es una herramienta que utiliza una filosofía muy similar a IPtables, ya que utiliza reglas sobre los paquetes que viajan en una red, sin embargo, dependiendo del modo de ejecución va un poco más allá, permitiendo tomar decisiones sobre la información intercambiada y la detección de posibles ataques sobre peticiones que aunque aparentemente son legitimas, pueden encajar en algún patrón de ataque. [55]

- **Smooth-Sec:** Es un sistema de detección de intrusiones IDS / IPS cuyo motor está basado en Suricata y con una interface web Snorby. Está montado sobre Linux UBUNTU 10.04 LTS. Se trada de un sistema completamente configurado y listo para usarse. Creado por Phillip Bailey. [55]

- **Suricata:** Se trata de motor IDS/IPS de The Open Information Security Foundation. Es Open Source y tiene unas características especiales que hacen de Suricata un motor muy interesante. Además es totalmente compatible con las reglas Snort y Emerging Threads. [55]

  Se destacan las siguientes características de Suricata:

  Multi-Threaded Processing. Una de la características más importantes de Suricata que permite la ejecución de varios procesos / subprocesos de forma simultánea. Podemos entonces asignar el número de subprocesos por CPU/Cores y qué subprocesos. De esta forma es capaz, entre otras cosas, de procesar una gran cantidad de paquetes de forma simultánea aumentando así el rendimiento. [55]

Automatic Protocol Detection. A parte de los protocolos IP, TCP, UDP e ICMP, Suricata tiene palabras claves para otros protocolos como FTP, HTTP, TLS, SMB. De esa forma podemos escribir reglas independientemente del puerto que un protocolo use, ya sea por defecto o no ya que éste es automáticamente detectado.

- **Snorby:** Snorby es un front-end web, para la gestión de alertas IDS/IPS basado en sensores. En el caso de Smooth-Sec basado en motor Suricata. Su interface gráfica es muy sencilla con una visión amplia e intuitiva de la visualización de las alertas. [55]

Se recomienda la utilización de los sistemas IDS/IPS, la arquitectura (basado en hardware o software) a ser implementada dependerá de los requerimientos de nuestra red, presupuesto y de las funcionalidades como gestión, flexibilidad, soporte, garantía deberán ser tomados en cuenta al momento de seleccionar la mejor solución.

A continuación se describen las ventajas y desventajas que ofrecen los sistemas IDS e IPS:

- **Ventajas**

  - **NIDS:**
    - Detectan accesos no deseados a la red.
    - No necesitan instalar software adicional en los servidores en producción.
    - Fácil instalación y actualización por que se ejecutan en un sistema dedicado.

  - **HIDS:**
    - Permiten asociar usuarios y eventos.
    - Pueden analizar tráfico cifrado.
    - Pueden proveer información acerca de un ataque en una máquina durante el mismo ataque.

- **IPS:**
  - Protección preventiva antes de que ocurra el ataque.
  - Defensa completa (Vulnerabilidades del sistema operativo, puertos, tráfico de IP, códigos maliciosos e intrusos).
  - Maximiza la seguridad y aumenta la eficiencia en la prevención de intrusiones o ataques a la red de una empresa.
  - Fácil instalación, configuración y administración.
  - Es escalable y permite la actualización de dispositivos a medida que crece la empresa.
  - No requiere tanta dedicación como un IDS tradicional; esto en consecuencia requeriría menos inversión en recursos para administrar y operar estos sistemas (en comparación con un IDS).

- **Desventajas:**

- **NIDS:**
  - Examinan el tráfico de la red en el segmento en el cual se conecta, pero no puede detectar un ataque en diferentes segmentos de la red. La solución más sencilla es colocar diversos sensores.
  - Pueden generar tráfico en la red.
  - Ataques con sesiones encriptadas son difíciles de detectar.

- **HIDS:**
  - La información provista deja de ser confiable tan pronto como un ataque ha sido exitoso.
  - Cuando la máquina cae también lo hace el IDS.
  - No son capaces de detectar mapeos de red.
  - Pueden dejar de ser efectivos durante un ataque DOS.
  - Requieren recursos locales para operar.

- **IPS:**
  - Como ocurre con cualquier tipo de dispositivo de seguridad que inspecciona paquetes, su uso puede generar potenciales inconvenientes en términos de rendimiento, latencia y disponibilidad. Después de todo, se trata de dispositivos que abren cada paquete y

realizan sobre él una inspección profunda a través de todos los niveles hasta alcanzar el de aplicación (Nivel 7) antes de tomar la decisión de si dejarlo pasar o no. [41]

3.5 RED PRIVADA VIRTUAL (VPN)

Muchas organizaciones operan de manera distribuida, teniendo diferentes sucursales en diversas partes del mundo. Hasta hace un tiempo, la única forma de interconectar dichas sucursales era mediante líneas dedicadas o enlaces punto a punto. Estos enlaces son extremadamente costosos, por lo que muchas organizaciones desistían de su uso. [27]

Las redes privadas virtuales (VPN) representan una infraestructura de red privada, establecida de modo virtual a través de comunicaciones públicas (Internet), de manera tal que las organizaciones puedan interconectar sus sucursales en forma segura y económica. Al implementar una red VPN, una organización podrá contar virtualmente con una única red privada con total visibilidad e interoperabilidad, sin importar donde se ubiquen geográficamente los equipos que la conformen, mediante el uso de encriptación, autenticación y encapsulamiento (tunneling), con el fin de asegurar la integridad y privacidad de los datos. [27]

3.5.1 Componentes de las VPN

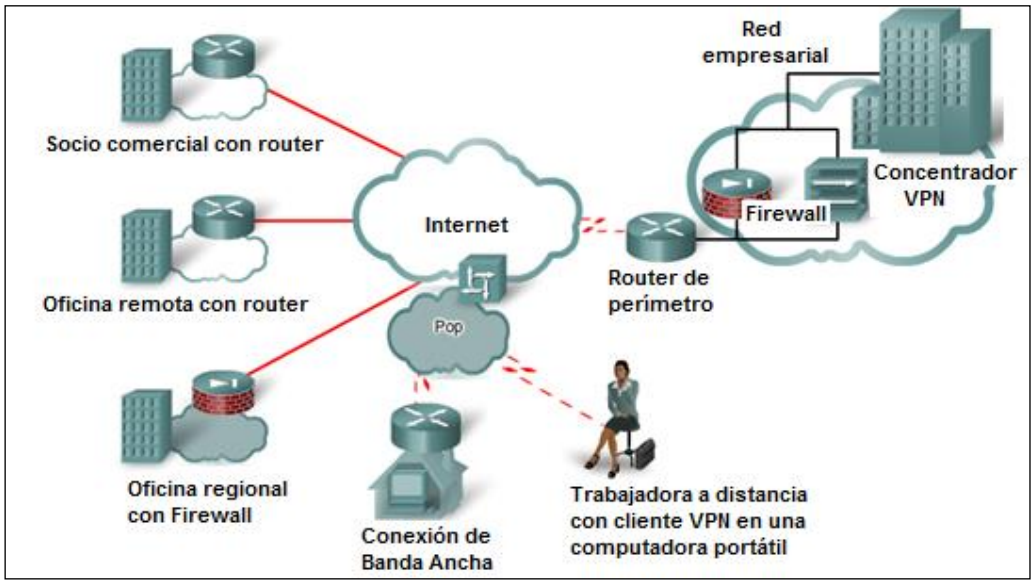


Figura 3.5.1 Componentes de una VPN.

Fuente: Ramírez, O. (2013).

La figura muestra una topología de VPN típica. Los componentes necesarios para establecer esta VPN incluyen lo siguiente:

- Una red existente con servidores y estaciones de trabajo.
- Una conexión a Internet.
- Gateways VPN, como routers, firewalls, concentradores VPN y ASA, que actúan como extremos para establecer, administrar y controlar las conexiones VPN.
- Software adecuado para crear y administrar túneles VPN.

Existen varias razones para la implantación de VPN's:

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

3.5.2 Tipos de VPN

Existen dos formas de implementar una conexión de red VPN:

3.5.2.1 VPN de acceso remoto

Este modelo consiste en que los usuarios se conectan desde un sitio remoto y se utiliza internet como un vínculo de acceso, cada usuario tendrá sus propias credenciales de acceso y deberá gestionar sus propias conexiones. Es útil para proveer acceso remoto a la red a un subgrupo específico de usuarios. [27]

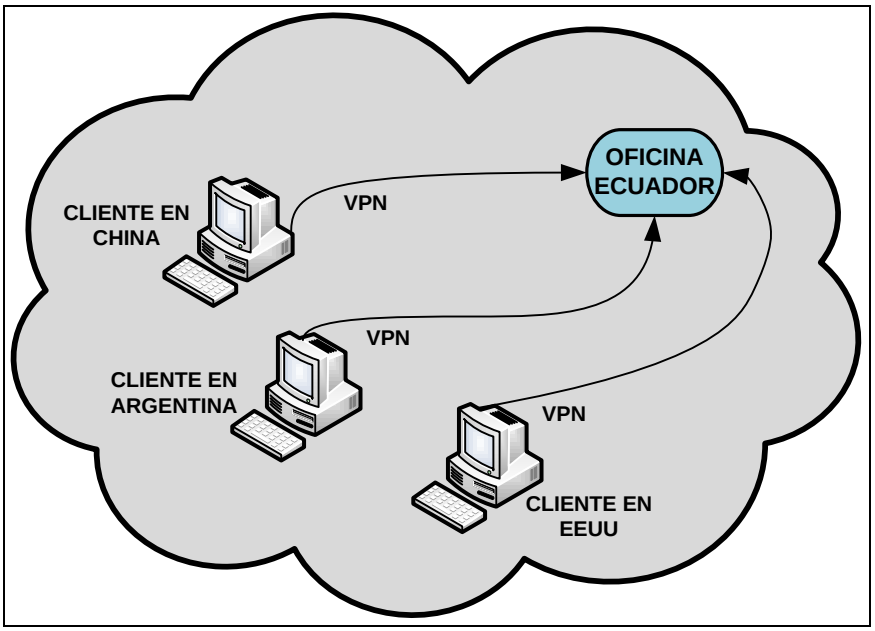


Figura 3.5.2 VPN de acceso remoto

Fuente: Katz, M. (2013).

3.5.2.2 VPN Punto a Punto

Este modelo consiste en que dos redes independientes pueden estar comunicadas al cien por ciento a través de un único túnel. Está técnica incorpora el uso de terminadores VPN en cada extremo del túnel. Estos equipos poseen dos (o más) dispositivos de red, uno de ellos estará conectado a la red pública y el otro a la red privada. Son estos equipos los que generarán la negociación de conexión, las asignaciones de seguridad necesarias y establecerán las comunicaciones, suministrando los servicios de VPN a todos los equipos que estén conectados a la red privada. [27]

Es útil para interconectar sucursales separadas geográficamente de manera transparente, ya que los usuarios de cada red privada no tendrán que gestionar sus propias conexiones. Con el simple hecho de estar conectados a sus redes privadas, tendrán acceso transparente a los recursos en el otro extremo del túnel, al igual que a los recursos locales de su propia red. El proceso es tan transparente que el usuario no se enterará siquiera de cuáles recursos pertenecen a cada red. [27]

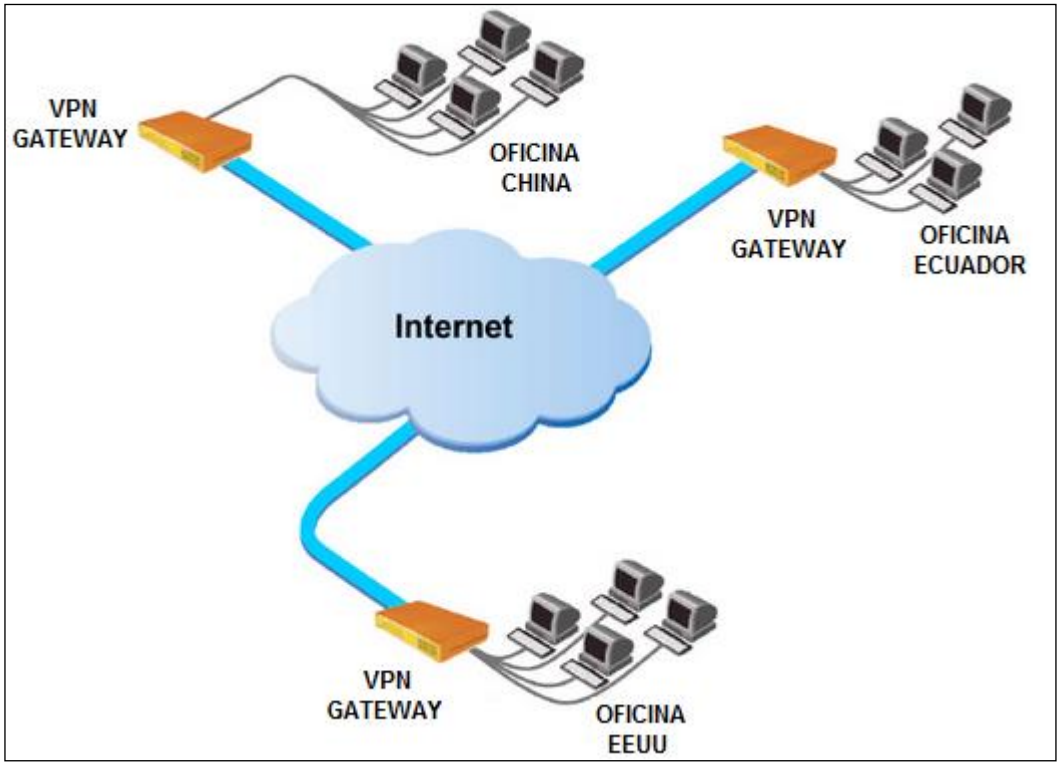


Figura 3.5.3 VPN Punto a Punto

Fuente: Checkpoint (2012).

3.5.3 Seguridad

Una VPN sin seguridad deja de ser privada, la cual es uno de los principales objetivos de las mismas. La seguridad en las VPN se describe con los siguientes aspectos:

3.5.3.1 Privacidad (Confidencialidad)

Los datos transmitidos sólo deberán estar disponibles para el receptor autorizado.

- **Modo Encriptación.** Consiste en cifrar la porción de datos del paquete usando encriptación simétrica o asimétrica, la cabecera del paquete no es modificada. [16]
- **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. [16]

3.5.3.2 Confiabilidad (Integridad)

La información transmitida no deberá cambiar entre el receptor y el transmisor. Para asegurar la integridad de los datos las soluciones VPN utilizan los algoritmos hash.

3.5.3.3 Disponibilidad

La información transferida deberá estar disponible cuando sea necesaria.

3.5.3.4 Autenticación

Las soluciones VPN soportan varios esquemas de autenticación de usuarios como [16]:

- User / Password.
- Autenticación vía token.
- Smartcards.
- Certificados X.509.

3.5.3.5 Autorización

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

3.5.3.6 Control de acceso

Las soluciones VPN proveen un control de acceso por razones de seguridad y auditoría basado en [16]:

- User ID.
- Host ID.
- IP address.
- Subnetwork address.

3.5.3.7 Auditoría

Las soluciones VPN definen un registro de actividad del usuario.

3.5.3.8 Facilidad de Administración

Los sistemas 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.

3.5.4 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 VPN 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 [16]:

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

3.5.5 Protocolos de Tunelización

Varios protocolos de red se han hecho populares como consecuencia de la evolución de VPN:

3.5.5.1 PPTP (Point to Point Tunneling Protocol)

Su uso es simple, liviano y rápido, pero a la vez presenta un bajo nivel de seguridad. Su aceptación se hizo masiva gracias a su adopción por parte de grandes empresas como Microsoft y 3Com. Más allá de ello, no deja de ser un protocolo débil y anticuado. Sin embargo, se convirtió rápidamente en un estándar de facto en cualquier red VPN de baja envergadura por su simple y rápida

implementación. Paralelamente, no todos los dispositivos y sistemas operativos (incluso actuales) soportan otros protocolos más que PPTP. [27]

3.5.5.2 L2TP (Layer 2 Tunneling Protocol)

Fue creado a partir de la unión entre PPTP y un protocolo privativo de CISCO llamado L2F (Layer 2 Forwarding Protocol). Trabaja en capa 2 (al igual que PPTP), pero ofrece mayores servicios de seguridad que su antecesor. No brinda encriptación por sus propios medios, por lo que la opción popular para poder proveer dichos servicios es mediante la combinación L2TP/IPSec. [27]

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.
- A pesar de que la información contenida en los paquetes PiPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

3.5.5.3 IPSec (Internet Protocol Security)

IPSec es un protocolo de capa 3 específicamente diseñado para el protocolo IP, que brinda herramientas de seguridad a través de la autenticación de orígenes y la encriptación de las comunicaciones que se realicen mediante su uso. La principal particularidad que presenta este protocolo es el hecho de operar en una

capa muy baja del modelo OSI, lo cual le permite ofrecer interoperabilidad con casi todos los protocolos de capas superiores. Este beneficio se debe a que al operar en una capa tan baja, los protocolos de altas capas no tienen necesidad de enterarse de que la red en donde transitan opera bajo IPSec, por ende no deben prepararse para trabajar con él. [27]

Los servicios de seguridad proveídos por IPSec son:

- **Autenticación y autenticidad de origen:** cada extremo de una comunicación IPSec deberá pasar inevitablemente por un proceso de autenticación, que validará su identidad ante el agente de control. Asimismo, cada paquete enviado en la comunicación será verificado para corroborar que realmente haya sido enviado desde la entidad que reclama haberlo efectuado.
- **Confidencialidad:** Las comunicaciones que se realicen con este protocolo pasarán por un proceso de encriptación fuerte que lo protegerá de divulgaciones.
- **Integridad:** Todo mensaje transmitido a través de IPSec pasará por verificaciones en destino para corroborar si fue recibido íntegramente o si hubo corrupción de datos.
- **Anti-replay:** Cada paquete cuenta con una identificación propia que será utilizada únicamente para dicho paquete y luego será descartada. Esta técnica inhabilita el llamado replay attack, que consta de la captura y repetición de mensajes específicos por un agente malicioso con fines de obtener réplicas de las respuestas de dicho mensaje desde destino.

3.5.6 Ventajas y desventajas.

Existen en el mercado soluciones VPN basadas en hardware o través de software. Las VPN basadas en hardware utilizan básicamente equipos dedicados, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios, por lo general tienen alto costo y poseen sistemas operativos propios y a veces también protocolos propietarios.

En cuanto a las soluciones VPN basadas en software libre, OpenVPN es una solución libre para la implementación de Redes Privadas Virtuales basadas en SSL, esta liberado bajo la Licencia Pública General GPL versión 2, incluye características que permiten configuraciones simples para túneles Punto a Punto, Acceso Remoto, VPN sitio a sitio, además incluye funcionalidades de nivel empresarial para proveer balanceo de cargas, failover y controles de acceso refinados. Iniciando con la premisa fundamental de que la complejidad es enemiga de la seguridad, OpenVPN ofrece una alternativa ligera y económica a otras tecnologías VPN.[5]

El Internet Protocol Security (IPSec) es generalmente más conveniente para conexiones estáticas o de largo plazo, por ejemplo, para atar una sucursal a la matriz. Las razones radican en el hecho de que la mayoría de las VPN IPSec requieren la instalación de software de cliente (agente) en el dispositivo final por lo tanto todos los dispositivos de los usuarios necesitan contar con dicho agente.

La principal desventaja de PPTP cuando se compara con L2TP/IPSec es la fuerza del cifrado, además, L2TP ofrece protección contra modificación de los datos durante el transcurso desde el origen al destino, autentificación de origen y protección contra reproducción, mientras que PPTP no puede ofrecer ninguna de estas prestaciones.

Por lo tanto, si la prioridad es la seguridad definitivamente se debe usar L2TP/IPSec pero si se requiere una solución rápida, fácil de usar y que funcione en la mayoría de dispositivos PPTP es la opción recomendada.

Por la antes expuesto se recomienda la utilización de redes privadas virtuales, la arquitectura (basado en hardware o software) a ser implementada dependerá de los requerimientos de nuestra red y presupuesto.

A continuación se describen las ventajas y desventajas que ofrecen las redes privadas virtuales:

[5] http://es.wikipedia.org/wiki/OpenVPN

- **Ventajas:**

  - **Reducción de costos de implementación**

Las organizaciones pueden usar transporte de Internet de terceros y económico para conectar oficinas y usuarios remotos al sitio corporativo principal. Esto elimina los enlaces WAN exclusivos y caros, y los bancos de módems. Mediante el uso de banda ancha, las VPN reducen los costos de conectividad mientras aumenta el ancho de banda de las conexiones remotas. [30]

  - **Reducción de costos operativos**

La organización puede reducir los costos totales de la operación si sus dispositivos de red VPN son manejados por el ISP. La razón para esta afirmación es que la organización no necesitará contratar personal altamente entrenado y calificado para el mantenimiento de la VPN si ella misma la maneja. [30]

  - **Seguridad en las transacciones**

Debido al uso tecnologías de túnel y las medidas de seguridad tales como cifrados, autenticación y autorización para garantizar la seguridad, confiabilidad e integridad de los datos transmitidos. Como resultado una VPN ofrece un alto grado de seguridad en las transacciones. [30]

  - **Escalabilidad**

Las VPN usan la infraestructura de Internet dentro de los ISP y las empresas de telecomunicaciones, y es más fácil para las organizaciones agregar usuarios nuevos. Las organizaciones, grandes y pequeñas, pueden agregar grandes cantidades de capacidad sin incorporar una infraestructura significativa. [30]

- **Desventajas:**

  - El desempeño de las redes virtuales privadas es altamente dependiente del desempeño de la Internet, es necesario tener una buena conexión, ya que una mala conexión podría ocasionar problemas de desconexión y lentitud.

- No todos los equipos de red son compatibles entre sí al utilizar las tecnologías VPN.
- Una brecha en la seguridad del equipo remoto puede poner en riesgo los recursos de la red a la cual se establece la conectividad. [30]

3.6 GESTIÓN UNIFICADA DE AMENAZAS (UTM).

Se denomina UTM o Gestión Unificada de Amenazas a los cortafuegos o firewall de red que engloban las diferentes funcionalidades de seguridad. Un dispositivo UTM se puede considerar la evolución de los firewalls de hardware, dado que analiza y procesa todo el tráfico de red en tiempo real.

Una de las últimas tendencias que van ganando campo entre los expertos informáticos es la protección en capas de una red, por lo que la utilización de UTM es la manera más eficaz de hacerlo. Hay que tomar en cuenta que existen en el mercado muchas marcas que ofrecen al usuario diversas funciones que integran servicios según las necesidades de cada organización, por lo que solo mediante una gestión de planificación, se podría dotar a la red de una excelente protección. [42]

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. [16]

Las principales funciones de seguridad de un sistema UTM son:

- **Firewall:** Un firewall sigue siendo un sólido elemento de seguridad y el origen del firewall de los dispositivos UTM ilustra su apropiado modelo de despliegue. Dondequiera que se entienda suficientemente bien una red, desarrollar un firewall es probablemente el lugar idóneo para aplicar otras características de seguridad. Además, los proveedores de firewalls no se han quedado quietos. [59]

- **Antivirus:** La definición original de UTM incluía antivirus en los gateways, lo que típicamente significaba escaneo SMTP y HTTP. Algunos productos

extendían sus protecciones a protocolos par a par, a protocolos de transferencia de archivos o a clientes de chat. No hay algo que se pueda considerar una característica antivirus pura en recientes productos UTM; por el contrario, están representadas características anti-spyware, anti-spam y anti-software malicioso. Las últimas tecnologías usan escaneo conductual para implementar chequeos en archivos que se transfieren y, así, identificar posibles amenazas sin cimentarse en una base estática de huellas dactilares. Desde luego, tanto si una detección es conductual o basada en firma sigue siendo todavía un ejemplo de una política de permiso por default. [59]

- **Capacidades de infraestructura de redes:** Dada la filosofía que hay detrás de UTM y la tendencia ya común hacia la integración de otros tipos de redes, como las VPN, los dispositivos UTM pueden incluir características como NAT, calidad de servicio o VPN. La funcionalidad VPN en los productos UTM incluso sitio-a-sitio, así como SSL u otras tecnologías VPN cliente-servidor, permiten a los empleados remotos acceder a los recursos internos. [59]

- **Prevención de filtraciones de datos (DLP):** Cierto número de productos disponen ahora de mecanismos simples de filtrado de datos, como un filtrado de contraseñas de e-mail o bloqueo de archivos adjuntos. [59]

- **Bloqueo y filtrado de contenido Web:** Acceso a sitios Web que contengan software y/o contenido malicioso tales como sitios de pornografía, juegos en línea, redes sociales, sitios para compras, subastas en línea, descarga de programas, almacenamiento en línea, sitios de farándula, apuestas en línea, videos en línea, etc. [59]

- **Bloqueo de archivos específicos:** Torrentes, ejecutables, archivos de script como JAR, VBS, JS, archivos multimedia, archivos comprimidos, entre otros. [59]

- **Protección de Malware y Spyware:** Disminuye en un alto porcentaje el riesgo de infección y propagación de archivos de contenido malicioso que

provengan en su mayoría tanto de la red externa, como también de la interna. [59]

- **Protección frente al correo no deseado:** Regula mediante la aplicación de reglas, la recepción y envío de correo masivo y mensajes de contenido restringido como sexo, comercio, racismo etc. y correos que no estén relacionados con las actividades de la empresa. [59]

- **Control de ancho de banda y tráfico de la red:** Regula la carga y descarga de archivos que sobrepasen el límite permitido por las políticas de control definidas en la empresa, la tasa de transferencia por equipo al acceder a la Web, mediante la implementación de políticas de control del ancho de banda demandad a por sitio, contenido y protocolo. [59]

- **Creación de redes DMZ:** Define la segmentación de redes a proteger permitiendo la configuración de zonas seguras y zonas menos seguras. [59]

- **Enrutamiento:** Posee características de enrutador de red para enlazar las redes y aplicar las políticas que estén definidas en su configuración. [59]

3.6.1 Modos de operación.

Se trata de cortafuegos a nivel de capa de aplicación que pueden trabajar de dos modos:

- **Modo proxy:** Hacen uso de proxies para procesar y redirigir todo el tráfico interno. [43]

- **Modo Transparente:** no redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones de hardware. [43]

El UTM a veces es referido también como firewalls multi-funcionales. Gartner, por ejemplo, usa este nombre para la categoría UTM. También, los términos descriptos son referidos muchas veces en Ingles como:

- Stateful Packet Inspection (SPI): Inspección de estado de los paquetes.
- Deep Packet Inspection (DPI): Inspección profunda de los paquetes.

La inspección profunda incluye tres componentes principales:

- **Anti Virus en Red:** El sistema reconoce la transferencia de archivos con un protocolo (web, correo, mensajeria instantanea, etc.) y escaneo los archvos en busqueda de viruses, troyanos y otros tipos de elementos nocivos en el mismo. [44]

- **Deteccion y Prevecion de Intrusos:** El sistema aquí analiza la parte de la data del paquete por ataques conocidos a vulnerabilidades. Incluso, puede reconocer cuando agentes nocivos instalados en las PCs de usuarios se comunican con centro de controles en el Internet. [44]

- **Anti Spyware:** Anti spyware es parecido a cómo opera el IPS. Solo cambia en los componentes que busca como, por ejemplo, código nocivo escrito en JavaScript o Active X que lee el navegador web del usuario. [44]

3.6.2 Ventajas y desventajas.

Las soluciones UTM simplifican la configuración, resolución de problemas y la completa gestión de amenazas al tiempo que reducen los costos de gestión en vista de que no será necesario administrar varias soluciones de diferentes proveedores.

Una alternativa a las soluciones propietarias son las soluciones Open Source, para el caso de UTM existe Endian Firewall para la gestión unificada de amenazas (UTM) que protege la red y mejora la conectividad, además de ofrecer diversos servicios de soporte integrales y altamente calificados, indispensables para toda solución de seguridad. Sobre la base de Red Hat Enterprise Linux, Endian Firewall e incluye funciones de seguridad tales como el paquete dinámico de Firewall, VPN, anti-virus, anti-spam, protección de la web y filtración de correo electrónico, ayudándole a reducir tiempo y gastos administrativos. Endian ha sido

diseñado para cubrir las necesidades de todo tipo de negocio, pequeño o grande, en la búsqueda por una protección óptima para su sistema de red. [56]

Sus principales características son:

- Administración unificada de amenazas para proteger su red y optimizar el flujo de información.
- Funciona con cualquier tipo de Hardware y lo convierte en un dispositivo multifuncional de seguridad.
- Fácil configuración y manejo de funciones avanzadas de seguridad.
- Protección de correo electrónico y de internet con diversos niveles de filtro.
- Siempre actualizado con lo último en anti-spam, anti-spyware, anti-virus y servicios de filtración de contenidos.
- Administración y servicio centralizado a través de la red Endian.
- Recuperación de datos instantánea, minimizando caídas y fallas en el sistema.

A continuación se describen las ventajas y desventajas que ofrecen los sistemas de gestión unificada de amenazas:

- **Ventajas**

  - UTM es un término que se refiere a un firewall de red con múltiples funciones añadidas, trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo. [44]
  - Reduce la complejidad al manejar un sólo sistema de seguridad. [44]
  - Simplicidad, mantenimiento e instalación de una única solución. [44]
  - Menor requerimientos técnicos de aprendizaje, un sólo producto que aprender. [44]

- **Desventajas**

    - Se crea un punto único de fallo y un cuello de botella, es decir si falla este sistema la organización queda desprotegida totalmente. A menos que se maneje un sistema de alta disponibilidad.
    - Punto único de compromiso en caso de existir vulnerabilidades en el sistema.
    - Genera un gran impacto en la latencia y ancho de banda de la red cuando el sistema no se encuentra bien configurado.

No hay duda de que la reducción en costos, complejidad y la mejora en la eficacia que resulta de tener una amplia gama de capacidades de seguridad en un único dispositivo son ventajosas. Sin embargo, se debe tener en cuenta que los resultados pueden variar, después de todo, no todas la tecnologías UTM son iguales. Las diferencias varían considerablemente entre un producto y otro, diferencias como la integración funcional con el resto de la arquitectura de la empresa, la capacidad de gestión de todos los servicios de seguridad, y la idoneidad del hardware sobre el que se implementa la plataforma.

3.7 SEGURIDAD FÍSICA DE RED.

Alulema, D. (2008, pág. 48-51), encontró lo siguiente:

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. "Ibíd."

3.7.1 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. "Ibíd."

3.7.1.1 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. "Ibíd."

- **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. "Ibíd."

- **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. "Ibíd."

3.7.1.2 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. "Ibíd."

- **Terremotos:** Para saber qué 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). "Ibíd."

- **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. "Ibíd."

- **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. "Ibíd."

3.7.1.3 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. "Ibíd."

  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. "Ibíd."

- **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.). "Ibíd."

- **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. "Ibíd."

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

3.7.2 Modelos de autenticación

Autenticación: Consiste en un sistema para certificar que el usuario es quien dice ser; lo más común es utilizar una combinación de identificador de usuario único y contraseña, aunque existen otros. [31]

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías:

- Sistemas basados en algo conocido. Ejemplo, un password (Unix) o passphrase (PGP). [31]
- Sistemas basados en algo poseído. Ejemplo, una tarjeta de identidad, una tarjeta inteligente (smartcard), dispositivo USB tipo epass token, smartcard o dongle criptográfico. [31]
- Sistemas basados en una característica física del usuario o un acto involuntario del mismo: Ejemplo, verificación de voz, de escritura, de huellas, de patrones oculares. [31]

3.7.2.1 Contraseñas.

Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. Aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso. [32]

- **Posibilidad de que algún atacante pueda adivinar o inventar la contraseña**

La posibilidad de que algún atacante pueda proporcionar una contraseña que adivinó es un factor clave al determinar la seguridad de un sistema. Algunos sistemas imponen un límite de tiempo después de que sucede un pequeño número de intentos fallidos de proporcionar la clave. Al no tener otras vulnerabilidades, estos sistemas pueden estar relativamente seguros con simples contraseñas, mientras estas no sean fácilmente deducibles, al no asignar datos

fácilmente conocidos como nombres de familiares o de mascotas, el número de matrícula del automóvil o contraseñas sencillas como "administrador" o "1234". [32]

Otros sistemas almacenan o transmiten una pista a modo de sugerencia de recordatorio de la contraseña, de manera que la propia pista puede ser fundamental para el acceso de algún atacante. Cuando esto ocurre, (y suele ser común), el atacante intentará suministrar contraseñas frecuentemente en una alta proporción, quizás utilizando listas extensamente conocidas de contraseñas comunes. También están sujetas a un alto grado de vulnerabilidad aquellas contraseñas que se usan para generar claves criptográficas, por ejemplo, cifrado de discos, o seguridad wifi, por lo tanto son necesarias contraseñas más inaccesibles en estos casos. [32]

- **Formas de almacenar contraseñas**

Algunos sistemas almacenan contraseñas como archivos de texto. Si algún atacante gana acceso al archivo que contienen las contraseñas, entonces todas éstas se encontrarán comprometidas. Si algunos usuarios emplean la misma contraseña para diferentes cuentas, éstas estarán comprometidas de igual manera. Los mejores sistemas almacenan las contraseñas en una forma de protección criptográfica, así, el acceso a la contraseña será más difícil para algún espía que haya ganado el acceso interno al sistema, aunque la validación todavía sigue siendo posible. [32]

- **Procedimientos para cambiar las contraseñas**

Usualmente, un sistema debe proveer una manera de cambiar una contraseña, ya sea porque el usuario sospeche que la contraseña actual ha (o ha sido) descubierto, o como medida de precaución. Si la nueva contraseña es introducida en el sistema de una manera no cifrada, la seguridad puede haberse perdido incluso antes de que la nueva contraseña haya sido instalada en la base de datos. Si la nueva contraseña fue revelada a un empleado de confianza, se gana poco. Algunos web sites incluyen la opción de recordar la contraseña de un usuario de una manera no cifrada al mandárselo por email. [32]

Los Sistemas de Administración de Identidad, se utilizan cada vez más para automatizar la emisión de reemplazos para contraseñas perdidas. La identidad del usuario se verifica al realizar algunas preguntas y compararlas con las que se tienen almacenadas. Preguntas típicas incluyen las siguientes: ¿Dónde naciste?, ¿Cuál es tu película favorita?, ¿Cuál es el nombre de tu mascota?. En muchos casos las respuestas a estas preguntas pueden ser adivinadas, determinadas con un poco de investigación, u obtenidas a través de estafa con ingeniería social. [32]

- **Probabilidad que una contraseña pueda ser descubierta**

Una contraseña débil sería una que fuese muy corta o que fuese la predeterminada, o una que pudiera adivinarse rápidamente al buscar una serie de palabras que es posible encontrar en diccionarios, nombres propios, palabras basadas en variaciones del nombre del usuario. Una contraseña fuerte debe ser suficientemente larga, al azar, o producirse sólo por el usuario que la eligió, de modo tal que el adivinarla requiera un largo tiempo. Ese tiempo demasiado largo variará de acuerdo al atacante, sus recursos, la facilidad con la que la contraseña se pueda descubrir, y la importancia de ésta para el atacante. Por lo tanto, una contraseña de un estudiante quizás no valga la pena para invertir más de algunos segundos en la computadora, mientras que la contraseña para acceder al control de una transferencia de dinero del sistema de un banco puede valer varias semanas de trabajo en una computadora. [32]

Fuerte y débil tienen significado solamente con respecto a tentativas de descubrir la contraseña de un usuario, ya sea por una persona que conoce al usuario, o una computadora que trate de usar millones de combinaciones. En este contexto, los términos pueden tener una precisión considerable. Pero hay que notar que una contraseña fuerte en este sentido puede ser robada, truqueada o extraída del usuario ya sea mediante la extracción del historial de un teclado, grabada mediante aparatos de comunicación o copiada de notas dejadas por olvido. [32]

3.7.3 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. [16]

Las tarjetas inteligentes son una plataforma segura adaptada especialmente para proporcionar una mayor seguridad y privacidad a aplicaciones que se ejecutan en entornos de computación de propósito general como los PCs, ya que son capaces de proporcionar funcionalidades de almacenamiento seguro para información sensible como puede ser [33]:

- Claves privadas
- Números de cuentas
- Contraseñas
- Información médica

Al mismo tiempo la tarjeta inteligente proporciona la capacidad de realizar distintos procesos con la información que contiene, de forma aislada, sin exponerla al entorno operativo del PC.

Una tarjeta inteligente (smart card) o tarjeta con circuito integrado (TCI), es cualquier tarjeta generalmente del tamaño de una tarjeta de crédito que contiene un circuito integrado con microprocesador que permite ejecutar programas y almacenar datos, e incorporan ciertos mecanismos de seguridad. La energía necesaria para su funcionamiento proviene de un lector de tarjetas inteligentes. [33]

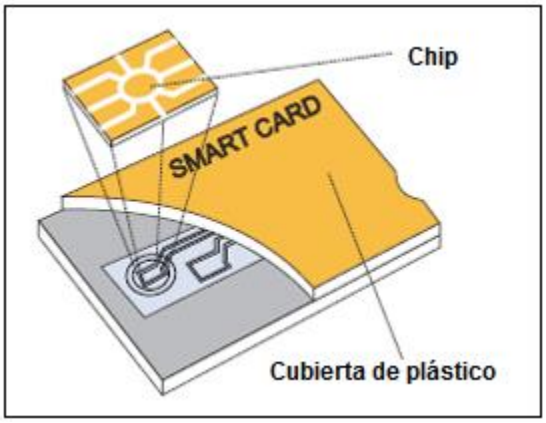


Figura 3.7.1 Tarjeta Inteligente

Fuente: SCS Smart Card (2013)

Las tarjetas inteligentes soportan autenticación y autorización, el poseedor de la tarjeta se autentica por medio del PIN, y puede ser autorizado a acceder sólo a un rango de datos particular de la tarjeta, o a realizar unas operaciones particulares con la tarjeta.

Las tarjetas inteligentes se pueden clasificar según:

- **Capacidad del chip**:

- **Memoria:** tarjetas que únicamente son un contenedor de ficheros pero que no albergan aplicaciones ejecutables. [33]

- **Microprocesadas:** tarjetas con una estructura análoga a la de un ordenador (procesador, memoria volátil, memoria no volátil). Albergan ficheros y aplicaciones y suelen usarse para identificación y pago con monederos electrónicos. [33]

- **Criptográficas:** tarjetas microprocesadas avanzadas en las que hay módulos hardware para la ejecución de algoritmos de cifrado y firma digitales. En estas tarjetas se puede almacenar de forma segura un certificado digital (y su clave privada) y firmar documentos o autenticarse con la tarjeta sin que el certificado salga de la tarjeta ya que es el procesador de la propia tarjeta el que realiza la firma. [33]

- **Estructura del sistema operativo:**

- **Tarjetas de memoria:** Tarjetas que disponen de un sistema operativo limitado con una serie de comandos básicos de lectura y escritura de las distintas secciones de memoria y pueden tener capacidades de seguridad para proteger el acceso a determinadas zonas de memoria. [33]

- **Basadas en sistemas de ficheros, aplicaciones y comandos:** estas tarjetas disponen del equivalente a un sistema de ficheros compatible con el estándar ISO/IEC 7816 parte 4 y un sistema operativo con una o más aplicaciones que exponen una serie de comandos. [33]

- **Java Cards:** una Java Card es una tarjeta capaz de ejecutar aplicaciones Java (hay que tener en cuenta el espacio de memoria a la hora de programarlas). En este tipo de tarjetas el sistema operativo es una pequeña máquina virtual Java (JVM) y en ellas se pueden cargar dinámicamente aplicaciones desarrolladas específicamente para este entorno. [33]

- **Tamaño según la ISO 7816** [33]**:**

  - **ID 000:** tarjetas SIM para módulos GSM.
  - **ID 00:** tamaño poco utilizado.
  - **ID 1:** tamaño equivalente a una tarjeta de crédito.

- **Interfaz:**

  - **Tarjeta inteligente de contacto:** disponen de unos contactos metálicos visibles y debidamente estandarizados. Deben ser insertadas en una ranura de un lector para poder operar con ellas. [33]

  - **Tarjeta inteligente sin contacto:** tarjeta inteligente sin contacto mediante etiquetas RFID en el cual el chip se comunica con el lector de tarjetas mediante inducción. [33]

- **Tarjeta inteligente híbrida:** tarjeta inteligente sin contacto que incluye otro chip de contacto.

El uso de tarjetas inteligentes es, hoy en día, muy común en: la banca, seguros médicos, monedero (prepago), telefonía móvil, y muchos otros como las oficinas inteligentes, controles de acceso, etc. [33]

3.7.4 Biometría

Cualidad que el individuo es, constituye 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 [16]:

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

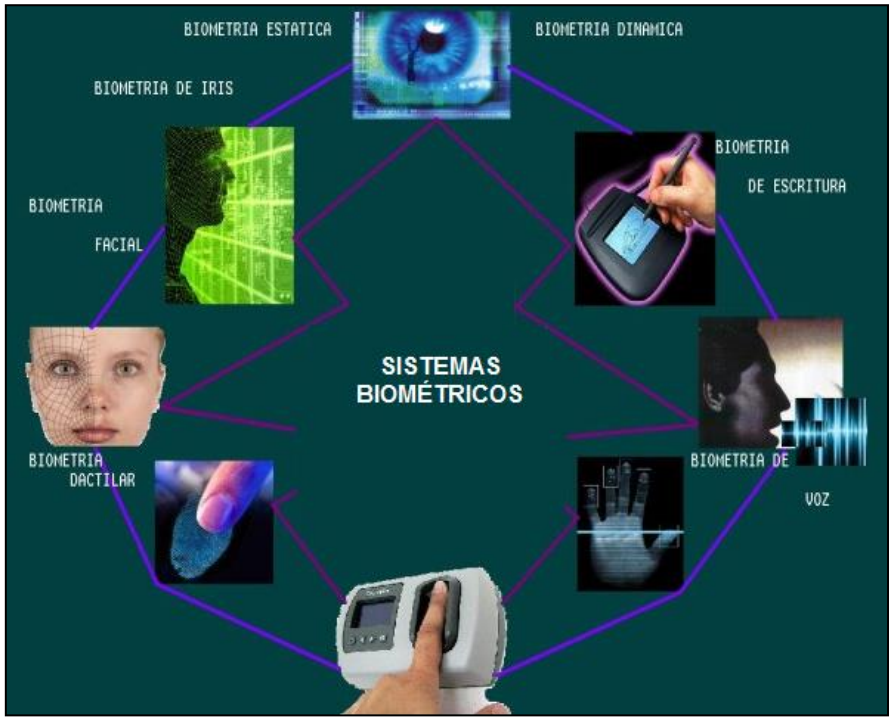


Figura 3.7.2 Sistemas Biométricos.

Fuente: Neo-Sistem (2013)

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. [16]

	Ojo - Iris	Ojo Retina	Huellas Dactilares	Geometría de la Mano	Escritura Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación	Si	Si	Si	No	Si	NO
Autenticación	Si	Si	Si	SI	Si	SI
Estándar	----	----	ANSI/NIST, FBI	----	----	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas	Artritis, reumatismo	Firmas fáciles o cambiantes	Ruido, resfriados

Tabla 3.7.1 Comparación de métodos biométricos.

Fuente: Neo-Sistem (2013)

3.7.5 Comparación entre la biometría y técnicas de identificación tradicionales.

A continuación se realiza una comparación de las técnicas de identificación tradicionales (usuario-contraseña, tarjeta magnética) con los sistemas basados en biometría, destacando los beneficios que resultan del uso de biometría junto con aspectos en los que las técnicas tradicionales siguen siendo superiores.

- **Necesidad de secreto:** Las contraseñas han de ocultarse y las tarjetas no deben estar al alcance de terceros, mientras que la biometría no requiere de estas medidas de protección que son exclusivamente dependientes del usuario. [34]

- **Posibilidad de robo:** Las tarjetas y contraseñas pueden ser robadas. Sin embargo, robar un rasgo biométrico es extremadamente complejo. [34]

- **Posibilidad de pérdida:** Las contraseñas son fácilmente olvidables y las tarjetas se pueden perder. Los rasgos biométricos permanecen invariables

salvo en contadas excepciones y siempre están con el sujeto a quien identifican. [34]

- **Registro inicial y posibilidad de regeneración:** La facilidad con la que se puede enviar una contraseña o tarjeta nueva contrasta con la complejidad que supone el registro en un sistema biométrico, ya que requiere de la presencia física del individuo en esta fase. Hay que añadir que los rasgos biométricos son por definición limitados, mientras que la generación de contraseñas tiene la ventaja de ser ilimitada. [34]

- **Proceso de comparación:** La comparación de dos contraseñas es un proceso sencillo. Sin embargo, comparar dos rasgos biométricos requiere de mayor capacidad computacional. [34]

- **Comodidad del usuario:** El usuario ha de memorizar una o múltiples contraseñas y, en el caso de que use una tarjeta, ha de llevarse siempre consigo. Utilizando tecnología biométrica no se necesita realizar estos esfuerzos. [34]

- **Vulnerabilidad ante el espionaje:** Una discreta vigilancia de nuestra actividad podría servir para obtener nuestra contraseña o robar nuestra tarjeta. Ese método no es válido ante los sistemas biométricos. [34]

- **Vulnerabilidad a un ataque por fuerza bruta:** Las contraseñas tienen una longitud de varios caracteres. Por su parte, una muestra biométrica digitalizada emplea cientos de bytes, lo que complica mucho los ataques por fuerza bruta. [34]

- **Medidas de prevención:** Los ataques contra sistemas protegidos por contraseña o tarjeta se producen desde hace años, y las medidas de prevención contra ellos ya se encuentran maduras. Por el contrario, los ataques a los sistemas biométricos son un área en la que estas medidas de prevención se están generando en estos momentos. [34]

- **Autenticación de usuarios reales:** La autenticación de usuarios mediante contraseña o tarjeta y su efectividad, dependen absolutamente de la voluntad del usuario a la hora de hacerlas personales e intransferibles. La

biometría está altamente relacionada con el propio usuario pues no puede ser prestada ni compartida. [34]

- **Coste de implantación:** En el momento de la implantación, el hecho de instaurar un sistema de contraseñas tiene un coste bajo, mientras que en el caso de un sistema basado en muestras biométricas es más costoso. [34]

- **Coste de mantenimiento:** El coste de mantenimiento de un sistema biométrico una vez está implantado con éxito es menor al de un sistema de contraseña o tarjeta ya que no conlleva gastos de gestión asociados a la pérdida u olvido de credenciales. [34]

Podemos resumir que los sistemas basados en biometría son más seguros que los sistemas tradicionales, son más cómodos ya que el elemento de identificación es una parte de nosotros y no un elemento externo. Económicamente también presentan ventajas ya que no supone coste de mantenimiento y al no haber ningún dispositivo externo de identificación no hay que preocuparse por licenciamiento cada cierto tiempo, desperfectos, robo o pérdida.

Sin duda, las tecnologías biométricas pueden ser una alternativa o un complemento de las técnicas de identificación y autenticación ya existentes.

3.7.6 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. "Ibíd."

- **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. "Ibíd."

- **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 sí; se puede realizar backups cifrados y controlar más el acceso al lugar donde se guardan. "Ibíd."

Es importante garantizar la seguridad física de los recursos tecnológicos utilizados en el centro de información, en especial el centro de datos, por lo tanto se debe considerar:

- El buen estado de las conexiones eléctricas. incluir una conexión a tierra para dirigir la energía perdida a la tierra y reducir el riesgo de descargas eléctricas en caso de fallas.
- Un equipo de aire acondicionado que permita mantener en una temperatura óptima los recursos tecnológicos ante el calentamiento natural producido por el permanente trabajo de sus dispositivos electrónicos.
- La implementación de un sistema contra incendios que permita combatir el fuego en su inicio.
- El tratamiento adecuado del problema acústico y de las vibraciones generadas por impresoras, sistema de aire acondicionado o cualquier equipo sujeto a grandes vibraciones.
- Un control de acceso del personal que debe permitir identificar claramente quién ingresa y quién sale.
- El uso de sistemas de seguridad como monitores, cámaras y sistemas de circuito cerrado, principalmente en los puntos de entrada y salida.
- El montaje del piso falso que permite transportar la electricidad estática a través de todo el sistema evitando que las descargas provoquen daños progresivos en los equipos de cómputo. También permite una mejor distribución del cableado, canaletas, aire

acondicionado y, en general, de todo tipo de cables e instalaciones que no deben estar expuestos al tráfico del personal.

- Racks adecuados que permitan una buena organización, distribución y acceso a los diferentes recursos tecnológicos.

CAPÍTULO 4

DESCRIPCIÓN DE LA SITUACIÓN ACTUAL DE LA RED DE ANT

4.1 INFRAESTRUCTURA DE RED

El crecimiento de la red de ANT ha sido progresivo de acuerdo a las necesidades operacionales que rodean a esta institución. Actualmente ANT se presenta a nivel nacional con sus Direcciones Provinciales (24) y sus Oficinas de Atención al Usuario (65) las mismas que se encuentran interconectadas. A continuación se detalla su ubicación geográfica:

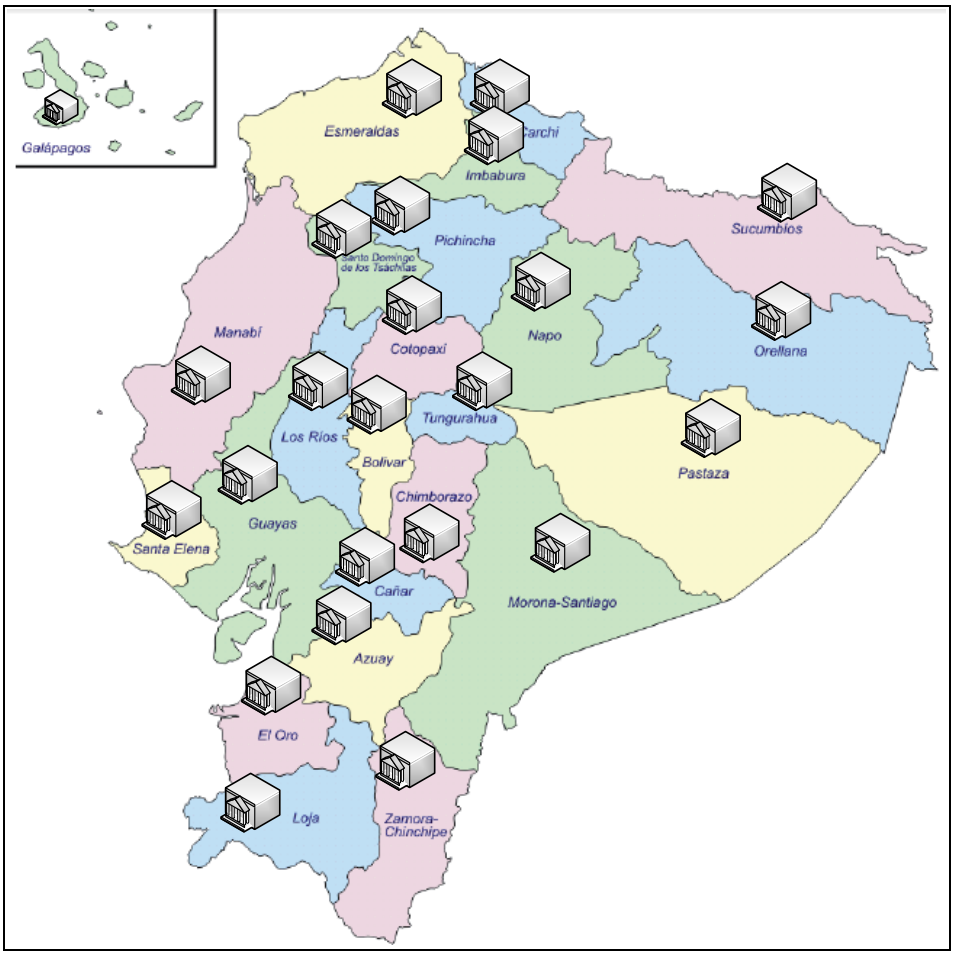


Figura 4.1.1 Presencia de ANT en el territorio ecuatoriano

Fuente: Chicaiza, D. (2014)

4.1.1 Estado actual de la red LAN/WAN

Todos los recursos humanos de la Agencia Nacional de Tránsito se encuentran ubicados en el edificio matriz localizado en la avenida Antonio José de Sucre (Av. Occidental) y Carlos V; los servidores y equipos de comunicación principales están instalados en el centro de cómputo de la Corporación Nacional de Comunicaciones CNT EP. En la modalidad de alojamiento (Housing), ambos en la ciudad de San Francisco de Quito.

4.1.1.1 Edificio Matriz

El proveedor de servicios de comunicación (internet y datos) es la Corporación Nacional de Telecomunicaciones CNT EP.

- **Centro de Datos**

El edificio matriz dispone de un cuarto de distribución principal con espacio para 6 racks de 42 UR, 2 cuartos de distribución (planta baja norte y planta alta sur) con 2 racks de 42 UR cada uno.

El centro de datos fue construido para albergar únicamente equipos de comunicación, por lo tanto el dimensionamiento se realizó para que cumpla los requisitos de un centro de datos básico no tiene redundancia, está expuesto a interrupciones tanto planeadas y no planeadas por lo tanto si falla uno de sus componentes puede afectar el funcionamiento de los servicios y de la tecnología que integra el centro de datos. Este tipo de centro de dato brinda una disponibilidad del 99.671% (Tier I[7]) y cuenta con los siguientes sistemas:

- Sistema de control de accesos biométrico (por huella digital).
- Sistema de aire de precisión redundante.
- Sistema de extinción de incendios.
- Sistema de video seguridad.
- Piso falso.

[7] Tier nos indica el nivel de fiabilidad de un centro de datos asociados a cuatro niveles de disponibilidad definidos. A mayor número en el Tier, mayor disponibilidad, y por lo tanto mayores costes asociados en su construcción y más tiempo para su implementación.

- Sistema UPS redundante (UPS principal 50 KVA para abastecer a todo el edificio; UPS redundante 8KVA exclusivo para los racks).
- 5 Racks de 42 UR (1 rack para proveedores, 2 racks para servidores, 2 racks para equipamiento activo de red) todos cerrados con llave.
- Espacio para ubicar 1 rack de 42 UR.

Figura 4.1.2 Sistemas de control de acceso y aire de precisión

Fuente: Chicaiza, D. (2014)

Figura 4.1.3 Centro de datos matriz ANT

Fuente: Chicaiza, D. (2014)

Figura 4.1.4 Sistema de energía ininterrumpida

Fuente: Chicaiza, D. (2014)

La empresa cuenta también con una planta generadora de energía eléctrica, que entra a funcionar en caso de cortes de energía prolongados, ésta abastece al edificio matriz por alrededor de 45 minutos.

- **Sistema de Cableado Estructurado**

Se consideró un diseño jerárquico de red (capa de núcleo, distribución y acceso), su topología es tipo estrella por sus características de fácil administración, bajo costo de implementación y mantenimiento.

El sistema de cableado estructurado está implementado de acuerdo a los estándares y recomendaciones ANSI/EIA/TIA descritas a continuación:

- ANSI/TIA/EIA-568-B (Cómo instalar el Cableado): Cableado de Telecomunicaciones en Edificios Comerciales. El estándar especifica:
  - Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina, para distintas tecnologías de cables (cobre y fibra).
  - Topología y distancias recomendadas.
  - Parámetros de desempeño de los medios de comunicación (cables de cobre, fibra).

- ANSI/TIA/EIA-569-A (Cómo enrutar el cableado): Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales. Esta norma indica los siguientes elementos para espacios y recorridos de telecomunicaciones en construcciones:

    - Recorridos Horizontales.
    - Armarios de Telecomunicaciones.
    - Recorridos para Backbones.
    - Sala de Equipos.
    - Estación de Trabajo.
    - Sala de Entrada de Servicios.

A continuación se describen los componentes del sistema de cableado estructurado:

Cableado Horizontal, es decir, el cableado que va desde el armario de telecomunicaciones a las tomas de usuario, cumple con:

- Par trenzado con blindaje (STP).
- Categoría 6A marca Furukawa.
- 2 salidas (datos, voz) por área de trabajo.
- Etiquetas en los patch panel y salidas de área de trabajo.
- No tiene puentes, derivaciones y empalmes a lo largo de todo el trayecto del cableado.
- No supera la máxima longitud permitida (100m = 90 m + 3 m usuario + 7 m patch pannel).

Cableado vertical, es decir, la interconexión entre los armarios de telecomunicaciones, cuarto de equipos y entrada de servicios.

- Utiliza un cableado por Fibra óptica Multimodo a 10 GB entre cuartos de comunicación y 1 GB entre dispositivos de comunicación dentro de los racks.

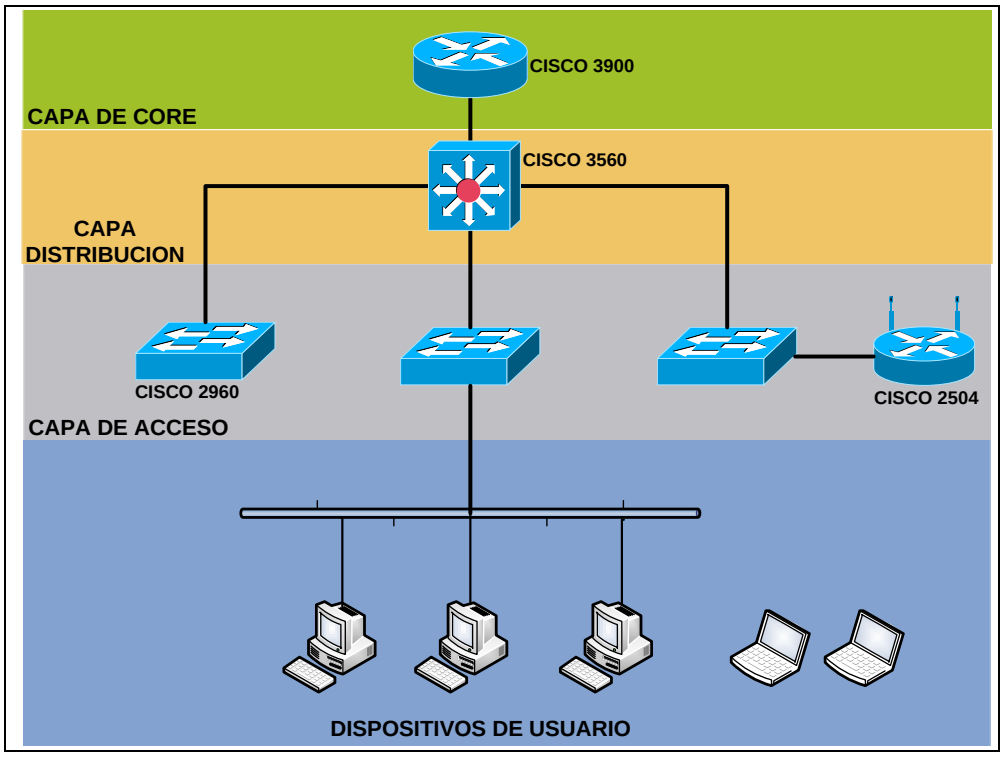


Figura 4.1.5 Arquitectura de RED

Fuente: Chicaiza, D. (2014)

- **Dispositivos de comunicación**

Los equipos de red (switches: core, distribución y acceso), solución inalámbrica (controlador y puntos de acceso), telefonía IP (central telefónica y teléfonos) son marca Cisco. Todos los equipos son de la línea corporativa, administrables por medio del protocolo SNMP.

El switch core es un dispositivo Cisco C3560E-12D de 12 puertos para conexión de fibra óptica a 10 Gb, actualmente están activados 7 puertos. Se cuenta con un total de 18 equipos Cisco C2960S distribuidos de la siguiente manera:

- Cuarto distribución principal: 6 dispositivos.
- Cuarto distribución planta baja norte: 5 dispositivos.
- Cuarto de distribución planta alta sur: 7 dispositivos.

Todos los dispositivos son PoE+. Actualmente se cuenta con 20 VLAN activas, mismas que permiten segmentar la red, la distribución de las VLAN son:

VLAN	Name	Status
1	default	active
10	VLAN_ADMN_EQUIPOS	active
11	VLAN_WIRELESS	active
12	VLAN_TEL_IP	active
13	VLAN_DATOS_CNT	active
14	VLAN_INTERNET_PUBLICO_ASTARO	active
15	Centro_Monitoreo	active
16	VLAN_SEGURIDADES	active
17	TEST_WLAN	active
18	TEST_TOIP	active
19	VLAN_DIGITALIZACION	active
20	VLAN_ANT_CORPAIRE	active
21	ANT_DINACOM	active
22	ANT_CTE	active
23	CNT_GPRS	active
24	RED_INTERMINISTERIAL	active
25	ANT_GADS_CNT	active
26	VLAN_INTERNET_TRAN_SEGURO	active
27	VLAN_DINARDAP	active
28	WESTERN_UNION	active
29	ANT_GADS_TELCO	active

Figura 4.1.6 VLAN activas Matriz ANT

Fuente: Chicaiza, D. (2014)

Existen 11 puntos de acceso inalámbrico Cisco AIR-LAP-1262N-A-K9 (802.11n) gestionados desde un controlador especializado Cisco AIR-CT2504-25-K9 (que soporta hasta 25 APs).

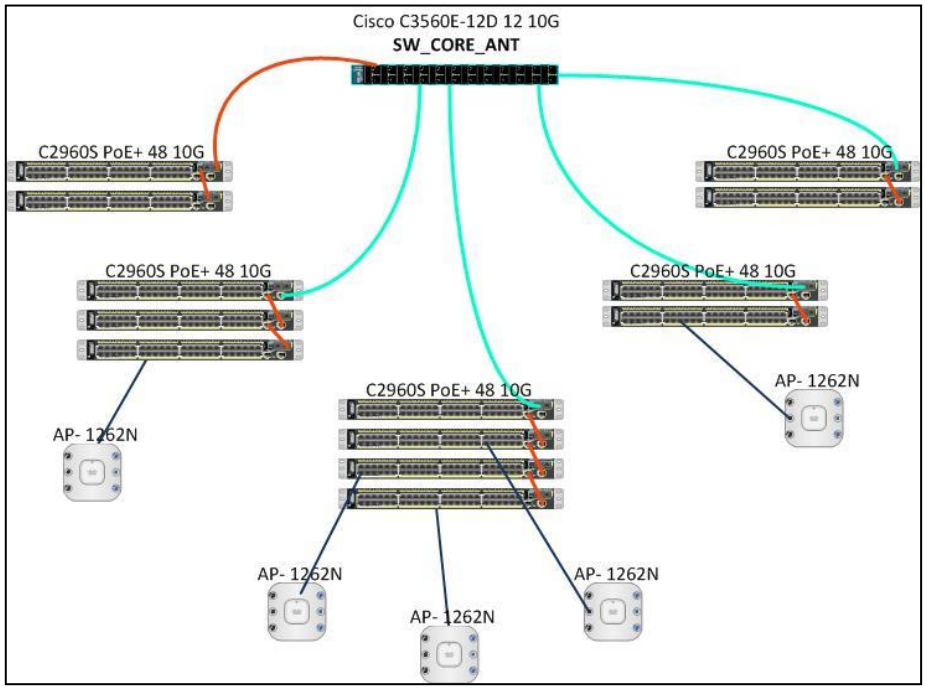


Figura 4.1.7 Diseño LAN - Edificio matriz

Fuente: Chicaiza, D. (2014)

Existen 3 redes WLAN para brindar movilidad a los funcionarios que requieren el acceso a la red en todas las áreas del edificio matriz dando prioridad a las áreas de:

- Sala de reuniones de la Dirección Ejecutiva (Planta Baja).
- Sala de prensa (Planta Baja).
- Sala de capacitaciones (Planta Alta).

La capacidad de las WLAN es de 300 Mbps y manejan el esquema de seguridad WPA2-PSK con SSID oculto.

Profile Name	WLAN SSID	Admin Status	Security Policies
DIRECTORES	DIRECTORES_AP	Disabled	[WPA2][Auth(PSK)]
Funcionarios	wANT_AP	Enabled	[WPA2][Auth(PSK)]
VISITAS_AP	VISITAS_AP	Enabled	[WPA2][Auth(PSK)]

Figura 4.1.8 Perfiles WLAN creados

Fuente: Chicaiza, D. (2014)

La seguridad de los equipos de comunicaciones está basada en la aplicación de buenas prácticas que proporciona el proceso de fortalecimiento (hardening[8]), a continuación se describe la seguridad de los equipos de comunicación:

1. Seguridad física para todos los equipos, estos se encuentran instalados en cuartos con racks cerrados con llave.

2. VLAN de administración dedicada.

3. Administración remota, la conexión se realiza de forma cifrada a través del protocolo SSH. Adicionalmente se restringe el acceso a través de una lista de acceso para los equipos de los administradores de red.

4. Autenticación por usuario-contraseña y banner de acceso.

[8] El Hardening o fortalecimiento es el proceso de configuración de seguridad de sistemas, para reducir la mayor cantidad de riesgos y minimizar la cantidad de vulnerabilidades sobre dichos sistemas. Mientras que las configuraciones de seguridad predeterminadas para muchos productos han mejorado mucho a lo largo de los años, algunas de las opciones y configuraciones favorecer el uso pero dejan al descubierto vulnerabilidades que pueden ser utilizadas para comprometer un sistema (usabilidad vs seguridad).

Figura 4.1.9 Pantalla de acceso a los equipos de comunicación.

Fuente: Chicaiza, D. (2014)

5. Acceso al CLI del sistema operativo por medio de contraseña de Enable.

6. Se utiliza contraseñas cifradas (service password-encriyption).

7. Cierre de sesiones automático a los 60 segundos.

8. Administración y monitoreo de equipos por protocolo SNMP versión 2. Se tiene configurada la comunidad de ANT en modo de solo lectura y se restringe la recepción de las peticiones únicamente hacia la IP del servidor PRTG a través de una lista de acceso.

9. Monitoreo de los equipos a través del software PRTG. Se tiene implementados sensores para verificar el rendimiento (CPU, memoria), tiempo de respuesta, disponibilidad, estado del equipo (temperatura, ventiladores, voltajes) y el tráfico por las interfaces.

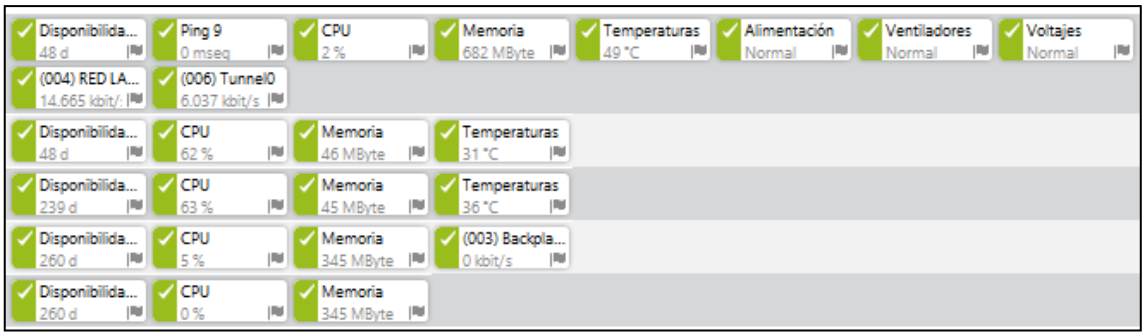


Figura 4.1.10 Monitoreo de equipos de Comunicación.

Fuente: Chicaiza, D. (2014)

10. Todos los servicios que no son requeridos se encuentran deshabilitados.

11. Se realiza un backup de la configuración semanalmente y/o después de realizar un cambio en la configuración.

- **Dispositivo de Seguridad y acceso a internet**

La seguridad informática se sustenta en un equipo de protección de borde (Astaro Security Gateway) adquirido para abastecer las necesidades de la matriz en el año 2011. Este dispositivo se encuentra instalado en el cuarto de distribución principal y realiza las siguientes funciones:

- Firewall, IPS, IDS, filtrado web, antispam, filtrado de aplicaciones.
- Conversión de direcciones de red (NAT).
- Suministrar internet a varias agencias.

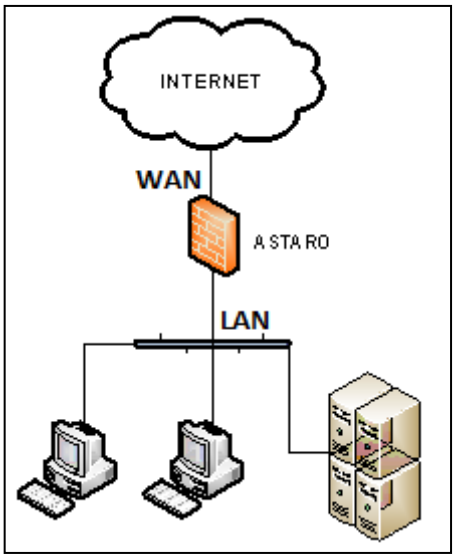


Figura 4.1.11 Acceso a Internet matriz ANT

Fuente: Chicaiza, D. (2014)

El dispositivo Astaro Security Gateway ha presentado problemas durante los 3 años de operación por lo que actualmente no satisface los requerimientos de ANT, a continuación se describen los principales inconvenientes:

- Daño del dispositivo (avería del disco duro) lo que causo que todos los módulos que integran este dispositivo estén fuera de servicio por 24 horas, hasta realizar el trámite de garantía.
- Problemas con el módulo de Autenticación vía Directorio Activo, lo que causa la desconexión del servicio de internet de todo el personal.

- Continua recepción de correo electrónico no deseado (spam) esta es una grave vulnerabilidad de seguridad.
- Problemas con el módulo de filtrado web y de aplicaciones, varias veces los usuarios han podido hacer omisión de las políticas de acceso a internet haciendo uso de proxy alternos.
- Problemas de compatibilidad con la publicación a internet (NAT) de servicios y aplicativos de ANT para acceder vía citrix.
- Problemas con el acceso vía VPN al integrar los usuarios del directorio activo que cuentan con dichos permisos. Adicionalmente no se puede mantener conexión con terceros vía VPN ya que no permite crear portales personalizados para cada empresa.

4.1.1.2 Oficinas de Atención al Usuario

Actualmente existen 65 oficinas de atención al usuario distribuidas a nivel nacional, cada una de ellas cuenta con los servicios de datos (1 Mbps) e internet (1 Mbps) por fibra óptica (1:1).

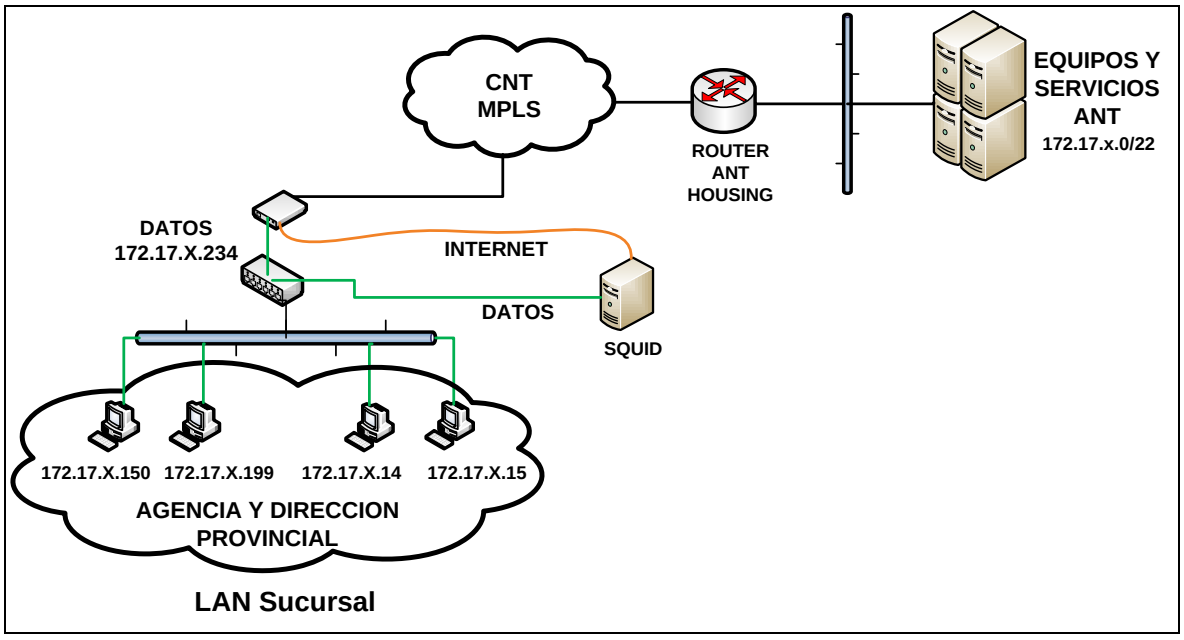


Figura 4.1.12 Esquema LAN de una sucursal

Fuente: Chicaiza, D. (2014)

Las redes de área local de las oficinas remotas están construidas con switches de distintas marcas y modelos, en su mayoría de línea doméstica y pequeñas oficinas, no configurables para ser administrados por medio del

protocolo SNMP. Son equipos descontinuados, desactualizados y sin contrato de mantenimiento, el sistema de cableado estructurado varía entre Categoría 5, 6 y 6A. Existe asignación de rangos de direccionamiento IP clase C para cada oficina de atención al usuario.

Figura 4.1.13 Sistema de Cableado Estructurado Oficinas de Atención al Usuario
Fuente: Chicaiza, D. (2014)

4.1.1.3 Centro de Datos CNT EP.

La Agencia Nacional de Tránsito tiene instalados 3 racks en el centro de datos de CNT, la finalidad es aprovechar las características del centro de cómputo de CNT diseñado para cumplimientos de acuerdo al estándar internacional TIA-942, que plantea que para aumentar la redundancia y los niveles de confiabilidad, los puntos únicos de falla deben ser eliminados tanto el centro de cómputo como

en la infraestructura que lo soporte. Su nivel de cumplimiento es TIER III es decir una disponibilidad del 99.982% por lo tanto cuenta con:

- Sistema de control de accesos por huella digital y tarjeta inteligente.
- Sistema de aire de precisión redundante.
- Sistema de extinción de incendios.
- Sistema UPS redundante.
- Sistema de Video Vigilancia.
- Espacio para ubicar 4 rack de 42 UR.
- Piso falso, techo falso.
- Centro de monitoreo 24/7.

El edificio cuenta con guardias de seguridad ubicados en la entrada principal. El ingreso al centro de datos se realiza por correo electrónico al Director del Centro de Datos, es necesario describir las actividades a realizar, personal que accede (nombres y número de cédula), horario de ingreso y salida.

Figura 4.1.14 Sistema de extinción de incendios

Fuente: Chicaiza, D. (2014)

Figura 4.1.15 Racks de ANT en centro de datos de CNT

Fuente: Chicaiza, D. (2014)

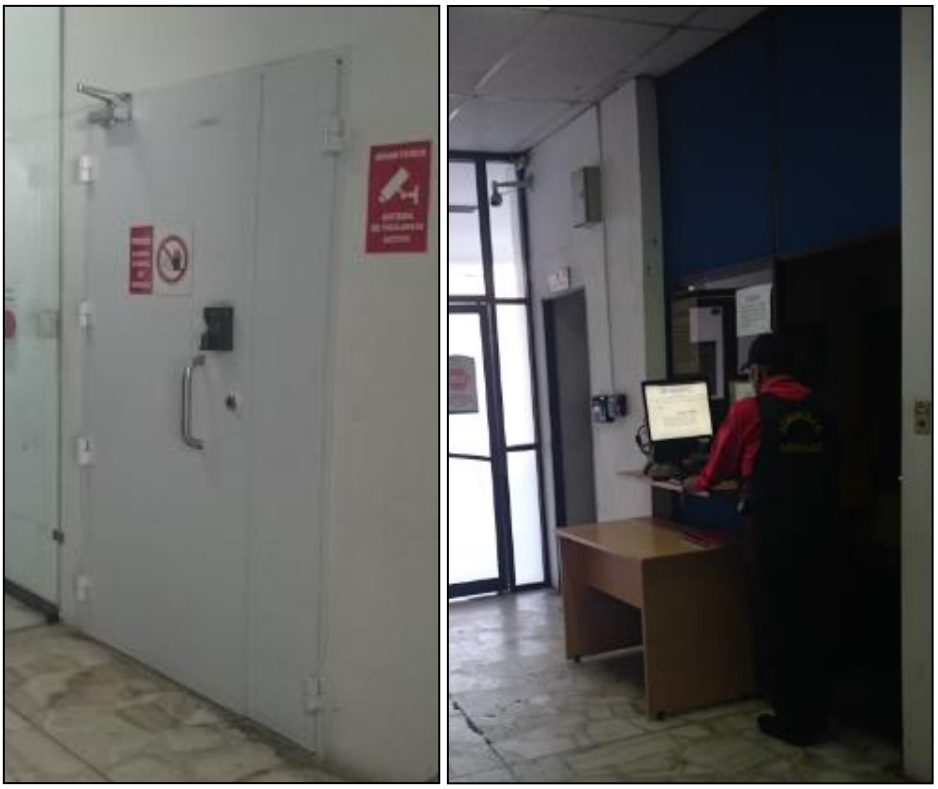


Figura 4.1.16 Sistemas de control de acceso al Centro de Datos

Fuente: Chicaiza, D. (2014)

Figura 4.1.17 Sistema de aire acondicionado de precisión

Fuente: Chicaiza, D. (2014)

La red LAN cuenta con 3 equipos Cisco C2960S interconectados por medio de enlaces de fibra óptica a 1 Gb. Se mantiene el mismo esquema de seguridad que en la matriz de ANT para estos dispositivos.

Existen enlaces punto a punto con instituciones públicas y financieras como: Comisión de Tránsito del Ecuador (10 Mbps), Dirección Nacional de Tránsito (5 Mbps), Red Interministerial (10 Mbps datos y 20 Mbps internet), Servicio de Rentas Internas (1 Mbps), Banco del Pacífico (1 Mbps), entre otros. Estos enlaces cuentan con enlace principal a cargo de ANT y enlace backup a cargo de la institución que mantiene el convenio con ANT.

Actualmente la conexión de estos servicios se concentra en el centro de datos de la matriz de ANT, se analiza el requerimiento de acceso y se enruta para que estas instituciones alcancen la red de servidores en el centro de datos de CNT (Housing). Se realiza el control de acceso a la red de servidores por medio de una lista de acceso en la cual se registran las direcciones IP de las instituciones que mantienen conectividad hacia ANT.

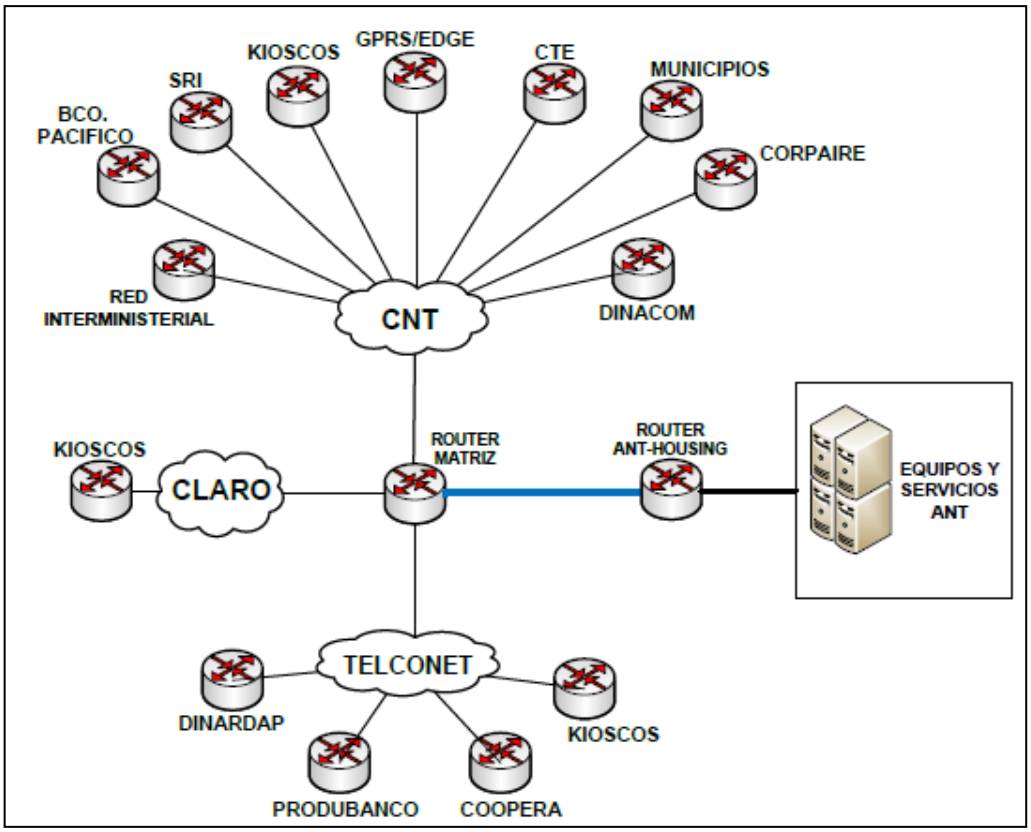


Figura 4.1.18 Esquema de conexión de Terceros hacia ANT

Fuente: Chicaiza, D. (2014)

4.1.2 Recursos informáticos.

4.1.2.1 Computadores

Dentro del fortalecimiento informático que realiza la Agencia Nacional de Tránsito y por el incremento de personal que ha ingresado a laborar a la institución además de equipos que han cumplido su tiempo de vida útil, el año 2013 se inicio un proceso de adquisición por medio de catálogo electrónico de los computadores que forman parte de la red de ANT (450 PC Matriz y 600 PC Oficinas de Atención al Usuario) que se encuentran distribuidos a nivel nacional en las diferentes sucursales.

A fin de mantener las estaciones de trabajo seguras y disminuir las potenciales vulnerabilidades se han realizado las siguientes tareas:

- Se maneja el principio de privilegios mínimos, es decir se limita los derechos administrativos y se concede a los empleados sólo los privilegios de lectura a las funciones del sistema.

- Configuración adecuada de cuentas de usuario, la autenticación se realiza por medio de ID y contraseña otorgados por el Directorio Activo.
- Evitar que los usuarios puedan realizar cambios (instalar ó desinstalar software) en los sistemas operativos y ajustes de configuración de las máquinas a través del uso de directivas de grupo.
- Activación y/o configuración adecuada de servicios de actualizaciones automáticas de Windows para mantener todos los equipos cliente con las actualizaciones de seguridad y los Service Pack más recientes.
- Renombramiento y posterior deshabilitación de cuentas estándar del sistema, como administrador e invitado.
- Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema.
- Configuración de acceso remoto estableciendo un canal cifrado de comunicaciones (SSH).
- Instalación, configuración y mantención del software antivirus y su firewall, estos nos permiten realizar un control de dispositivos, control de aplicaciones y acceso web.

Figura 4.1.19 Control de dispositivos con Kaspersky Endpoint Security

Fuente: Chicaiza, D. (2014)

A continuación se detallan las principales características de los ejemplares existentes en la red:

- **Equipos de escritorio**

DESCRIPCIÓN	CARACTERÍSTICAS
Marca	**Dell**[9]
Modelo	Optiplex 9020
Chasis	Minitower
Main board	Intel
Procesador	Tercera generación Intel Core i7
Velocidad del procesador	3.4 GHz
Velocidad de BUS Frontal	5 GT/s
Memoria cache	8MB
Memoria RAM	4GB
Slots de memoria	Cuatro ranuras DIMM
Tipo de memoria	DDR3
Expandible	>=32GB de RAM
Tarjeta de Video	Tarjeta Integrada Intel® HD Graphics 4000
Disco Duro Interno	500GB
Velocidad rotacional disco duro	7200RPM
Interfaz	SATA
Interfaces	4 puertos USB 3.0 externos (2 frontales, 2 posteriores); 6 puertos USB 2.0 externos (2 frontales, 4 posteriores) y 2 puertos USB 2.0 internos; 1 RJ-45; 1 Serial; 1 VGA; 2 DisplayPort;
Número de núcleos	4 núcleos
Soporte para 64 bits	SI
Teclado	Español Latinoamérica USB
Mouse Óptico	Tipo USB
Unidad Óptica	DVD+/-RW
Interfaz	SATA
Audio	SI
Tarjeta de Red	Integrado 10/100/1000
Ranuras de expansión	1 full height PCIe x16 1 full height PCIe x16 (wired x 4)
Voltaje	110V – 220V
Fuente de Poder	275 W
Sistema Operativo	Windows 8 Pro, 64-bit Español.
MONITOR	19", TIPO FLAT PANEL
Mantenimiento	Preventivo y/o correctivo durante el tiempo que dure la garantía. Mínimo dos mantenimientos al año.

Tabla 4.1.1 Especificaciones técnicas de los equipos de escritorio

Fuente: Chicaiza, D. (2014)

[9] DELL es una compañía multinacional estadounidense establecida en Round Rock (Texas) que desarrolla, fabrica, vende y da soporte a computadoras personales, servidores, switches de red, programas informáticos, periféricos y otros productos relacionados con la tecnología.

- **Equipos portátiles**

DESCRIPCIÓN	CARACTERÍSTICAS
Marca	Toshiba
Formato	Portátil liviana
Procesador	Tercera generación Intel Core i7
Velocidad del procesador	2.0 GHz
Memoria RAM	8 GB, DDR3-1600MHz SDRAM (un solo modulo instalado)
Slots de memoria	2 SLOTS
Tipo	DDR3
Expandible	Hasta 16GB
Tarjeta de Video	Tarjeta integrada: Intel HD Graphics 4000
Disco Duro Interno	500GB
Velocidad rotacional	7200rpm, SERIAL ATA
Puertos	1 RJ-45, USB 3.0 (2); 1 USB/eSATA combo, 1 VGA, 1 HDMI
Número de núcleos	2 núcleos
Soporte para 32, 64 bits	SI
Teclado	Integrado español
Unidad Óptica	DVD+/-RW
Audio	Integrado
Tarjeta de Red	Integrado 10/100/1000 Gigabit Ethernet
Wireless	Incluida 802.11 b,g,n
Pantalla	17 pulgadas
Ranuras	Memory card reader
Cargador de batería	65W A/C
Batería	6 celdas
Sistema Operativo	Windows 8 Pro, 32 o 64-bit Español.
Mantenimiento	Preventivo y/o correctivo durante el tiempo que dure la garantía. Mínimo dos mantenimientos al año.

Tabla 4.1.2 Especificaciones técnicas de los equipos portátiles

Fuente: Chicaiza, D. (2014)

4.1.2.2 Servidores

En el año 2010 se adquirió un chasis IBM BladeCenter H[10] poblado con 9 hojas o cuchillas de 14 posibles. En 3 cuchillas (host) se ha procedido a virtualizar 14 servidores. Los servidores ejecutan diversas versiones de sistemas operativos como: MS Windows 2003, MS Windows 2008, CentOS, AIX, y otros, sobre VMware vSphere. En estos ambientes se ejecutan varias aplicaciones empresariales de apoyo como: Sistema de emisión de licencias y matrículas

[10] http://www-03.ibm.com/systems/ec/bladecenter/hardware/chassis/bladeh/

(SITCON), servicios Web inter-institucionales, mail, DNS, Directorio Activo, base de datos, entre otras.

Las capacidades de equipos para contingencia por daños en servidores son mínimas, así como por recuperación en caso de desastres. Más aún si se presenta una concurrencia por daños en varios equipos.

En un muestreo pudimos tabular cuantos servidores ejecutan alguna versión de MS Windows Server. Las diferencias entre versiones del mismo producto se dan por la aplicación de parches que libera mensualmente el fabricante Microsoft. Como se puede apreciar se tiene 4 versiones de Windows 2003 Server y 4 de Windows 2008 Server.

Sistema Operativo – Versión	Equipos
Win 2003 Server	2
Win 2003 Server Standard SP1	1
Win 2003 Server R2 Standard SP1	1
Win 2003 Server R2 Standard SP2	5
Win 2008 Server R2 Standard (x64) SP1	1
Win 2008 Server Enterprise SP2	1
Win 2008 Server R2 Enterprise (x64)	3
Win 2008 Server R2 Enterprise (x64) SP1	8
TOTAL	**22**

Tabla 4.1.3 Servidores Windows

Fuente: Chicaiza, D. (2014)

Figura 4.1.20 Rack IBM #01 Almacenamiento

Fuente: Chicaiza, D. (2014)

La figura 4.1.20 proporciona una visión general de los elementos del sistema de almacenamiento IBM System Storage DS3400 (equipo central DS3400 y expansiones EXP3000 y EXP3512). A continuación un resumen las capacidades instaladas:

Ubicación (U)	Equipo	Distribución discos	Capacidad
33-32	EXP3512	8 * SAS FRU 1 TB	8,0 TB
31-30	EXP3512	8 * SAS FRU 450 GB	3,6 TB
29-28	DS3400	8 * SAS FRU 300 GB + 4 * SAS FRU 450 GB	4,2 TB
26-27	EXP3000	8 * SAS FRU 300 GB + 4 * SAS FRU 450 GB	4,2 TB
25-24	EXP3000	6 * SAS FRU 300 GB + 4 * SAS FRU 450 GB	3,6 TB
21-20	DS3524	16* SAS FRU 146 GB	1,7 TB
		Total general[11]	25,4 TB

Tabla 4.1.4 Resumen de Almacenamiento

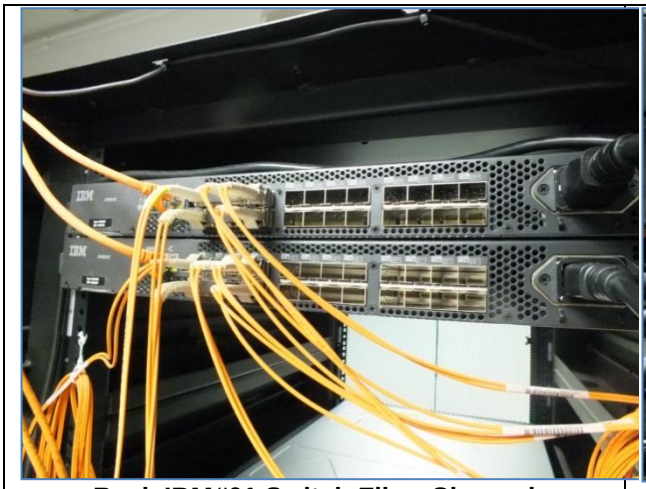
Fuente: Chicaiza, D. (2014)

[11] La capacidad disponible es menor, depende del nivel de arreglo (RAID) y de las áreas de control utilizadas por el programa gestor de almacenamiento.

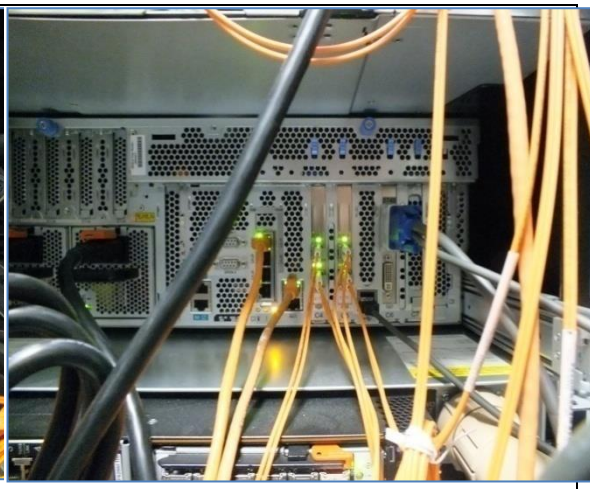
Figura 4.1.21 Rack IBM#01 Blade Center H

Fuente: Chicaiza, D. (2014)

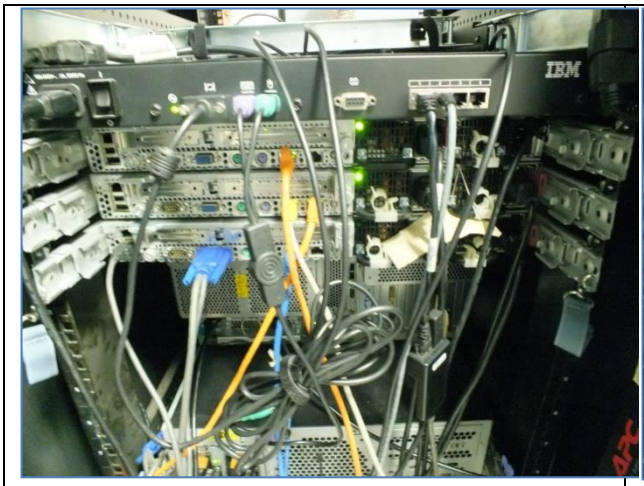
La figura 4.1.21 presenta al chasis para consolidación de equipos IBM BladeCenter H, de 14-cuchillas. ANT utiliza las cuchillas modelos: HS22 (x86) y PS700 (x64). En la parte superior del chasis se encuentra el servidor IBM Power 740. El equipo ha tenido inconvenientes que provocaron cortes de servicios informáticos, ya que es un equipo único y corazón de la plataforma tecnológica de la ANT.



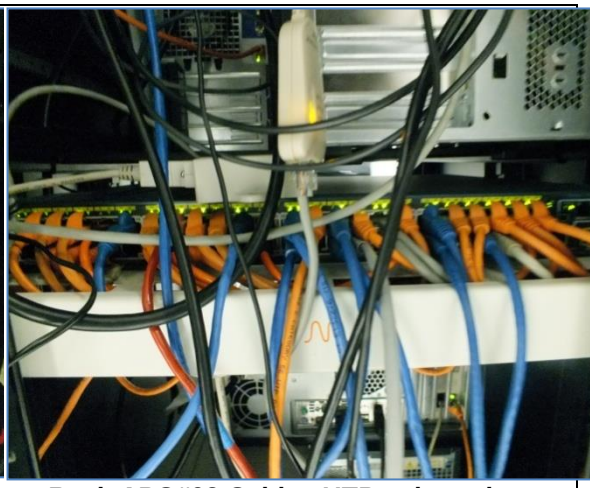
Rack IBM#01 Switch Fiber Channel



Rack IBM#01 Cables de fibra óptica



Rack IBM#02 Cables UTP y de poder



Rack APC#03 Cables UTP y de poder

Figura 4.1.22 Sistema de cableado Rack IBM

Fuente: Chicaiza, D. (2014)

La figura 4.1.22 presenta cables de fibra óptica hacia el Switch FC, cables UTP hacia switch de red y cables de poder. Se puede observar que los cables no están identificados y etiquetados como lo indica la norma para data center TIA-942, que enseña que todo cable debe estar identificado en ambos extremos y que la documentación técnica indique que dispositivo está conectado en cada puerto de conexión origen y destino (conmutadores, ruteadores, almacenamiento, y otros) y en la toma de pared.

A fin de mantener los servidores seguros y disminuir las potenciales vulnerabilidades se han realizado las siguientes tareas que recomienda el proceso de endurecimiento para servidores:

- Los servidores cuentan con seguridad física, están instalados en los racks cerrados en el centro de cómputo de CNT.
- Habilitación de password de BIOS.
- Deshabilitación del arranque para unidades externas como disquetes, Unidades Ópticas de Cd o DvD, USB, etc.
- Definir un número máximo de usuarios conectados a los servidores, para ANT se restringió a 3 usuarios.
- Configuración adecuada de cuentas de usuario, la autenticación se realiza por medio de ID y contraseña establecidos por el personal administrador de Servidores.

- Activación y/o configuración adecuada de servicios de actualizaciones automáticas de Windows para mantener todos los equipos cliente con las actualizaciones de seguridad y los Service Pack más recientes.
- Renombramiento y posterior deshabilitación de cuentas estándar del sistema, como root.
- No permitir acceso remoto al usuario Root.
- Configuración de acceso remoto estableciendo un canal cifrado de comunicaciones (SSH).
- Instalación, configuración y mantención de programa de seguridad antivirus.

4.2 SERVICIOS, PROTOCOLOS Y APLICACIONES.

4.2.1 Servicios de red.

La red de ANT ofrece servicios a nivel LAN y WAN mediante el establecimiento físico (enlaces) y lógico (protocolos de red) de la red.

A continuación se presentan los principales servicios:

- De archivo: Este permite a los usuarios leer, escribir, controlar el acceso y mantenimiento de datos en un repositorio configurado para cada departamento. Las principales ventajas son:
    - Transferencia de archivos.
    - Almacenamiento y migración de datos de archivo.
    - Sincronización de actualizaciones de archivos.
    - Almacenamiento de archivos.
- De impresión: Controlan y administran el acceso a impresoras y equipo multifunciones. Los servicios de impresión aceptan solicitudes de trabajos de impresión, interpretan los formatos de trabajos de impresión y configuración de impresoras, administran las colas de impresión e interactúan con impresoras de red. Los servicios de impresión de red nos ayudan para:
    - Reducir el número de impresoras que la organización necesita.

- Colocar las impresoras donde se considere más conveniente.
- Las colas de trabajos de impresión reducen el tiempo que la computadora espera para enviar el trabajo de impresión.
- Compartir impresoras especializadas eficientemente.

- De aplicativos.
- De base de datos.
- De internet a nivel LAN y WAN, inyectado a ciertas dependencias logrado mediante la provisión centralizada de este servicio a través del dispositivo Astaro Security Gateway que actúa como un servidor Proxy y ejecuta NAT.

4.2.2 Protocolos de red.

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

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	SNMP usa el ASN.1 para representar sus objetos gestionables
Nivel de Sesión	NETBIOS	Recursos básicos de red
	ONC	Establecer sesiones remotas
	RPC	Establecer sesiones remotas
	DCE / RPC	Establecer sesiones remotas
Nivel de Transporte	TCP	Transmisión de cadenas de datos
	UDP	Transmisión de unidades de datos
Nivel De Red	IP	Asignar dirección de Red IP
	IPX	Asignar dirección de Red IPX
Nivel de Enlace	Ethernet	Redes LAN
	MPLS	Red WAN (Backbone)
	Wi-Fi	Redes W-LAN

Nivel Físico	Cable de Fibra Óptica	Redes LAN / WAN
	Cable de par trenzado	Redes LAN
	Inalámbricas	Redes LAN

Tabla 4.2.1 Protocolos y Tecnologías que utiliza la Red de ANT

Fuente: Chicaiza, D. (2014)

4.3 ACCESO.

4.3.1 Accesos a Internet.

Para el acceso a Internet se cuenta con un canal dedicado (clear channel) con capacidad de 10240/10240 Kbps contratado con el ISP CNT, este canal se enlaza al puerto externo del dispositivo Astaro Security Gateway y brinda el servicio de Internet a la matriz de ANT y a ciertas agencias pequeñas (menos de 5 usuarios).

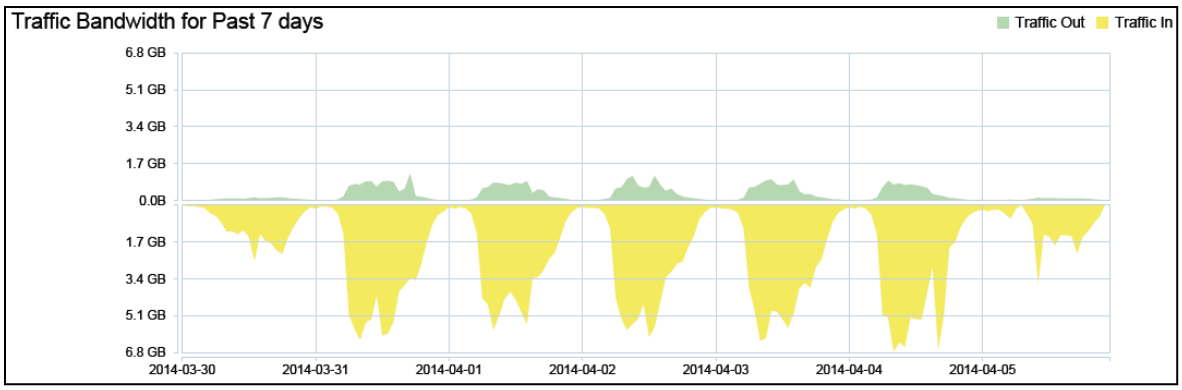


Figura 4.3.1 Tráfico de internet

Fuente: Chicaiza, D. (2014)

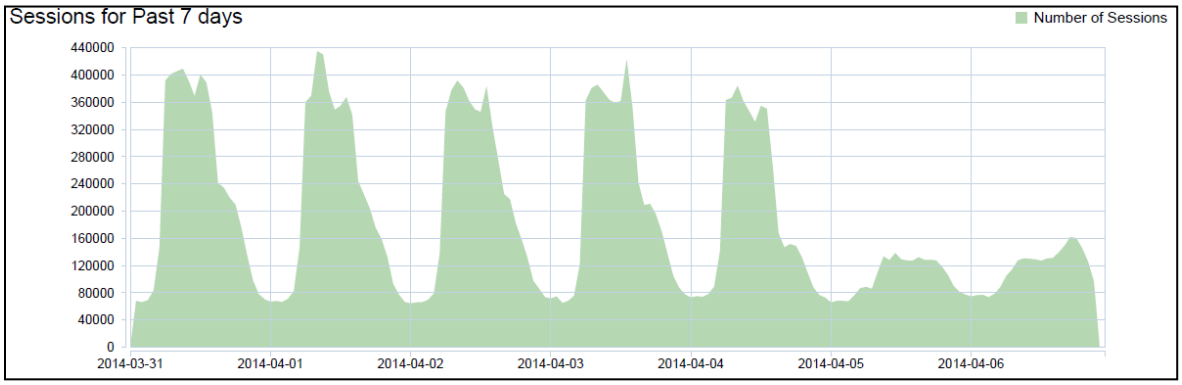


Figura 4.3.2 Número de sesiones (7 días)

Fuente: Chicaiza, D. (2014)

De acuerdo a las figuras 4.3.1 y 4.3.2, la capacidad actual del canal (10 Mbps) es adecuada, ya que no hay saturaciones en el enlace; también muestra el

comportamiento en el uso del Internet, viendo que el número de sesiones se mantienen constantes durante los 5 días laborables. Adicionalmente se muestra a continuación en detalle el uso del ancho de banda por protocolo.

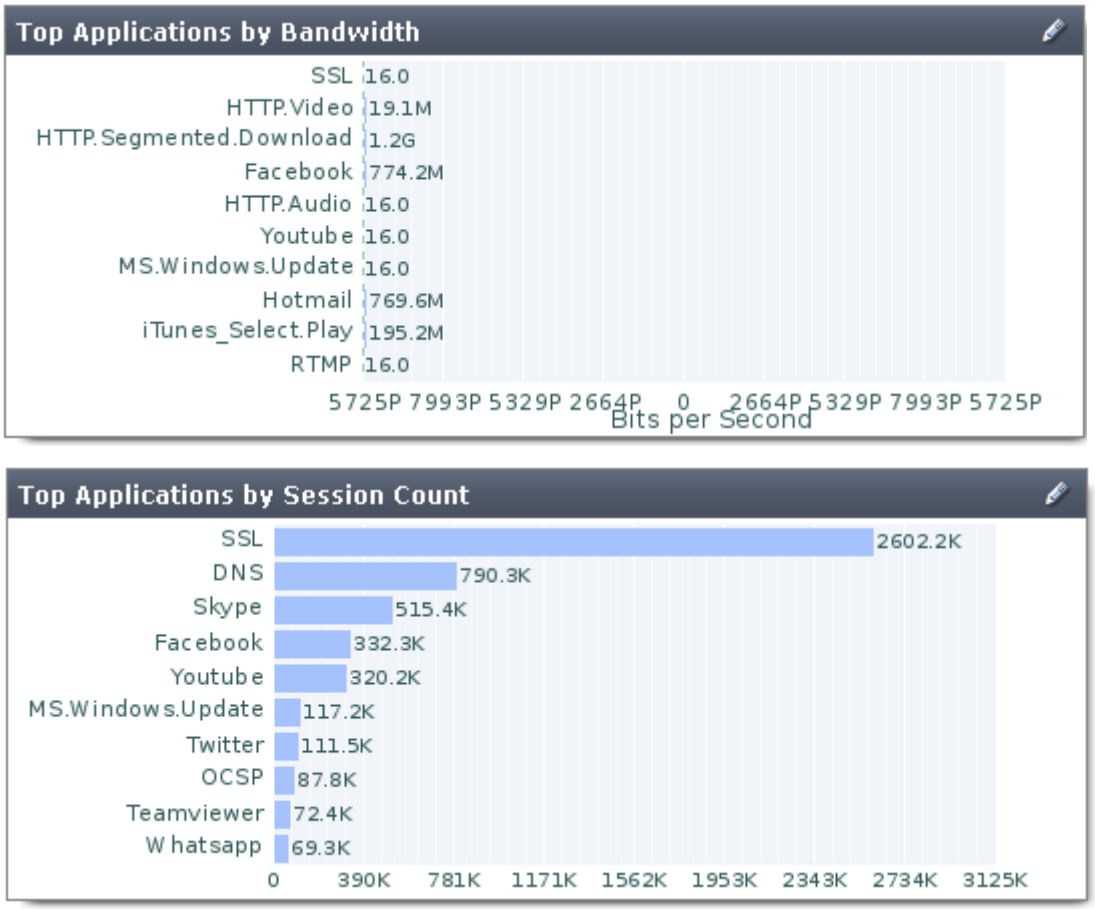


Figura 4.3.3 Top 10 de aplicaciones que consumen Ancho de Banda

Fuente: Chicaiza, D. (2014)

4.3.2 Acceso de sucursales.

El acceso de las sucursales hacia la red Matriz se establece mediante un enlace de datos con capacidad de 1 Mbps y su última milla es por fibra óptica; el acceso desde la matriz hacia la red de servidores (centro de datos CNT) se establece mediante un enlace redundante de 40 Mbps (Principal) y 20 Mbps (Backup).

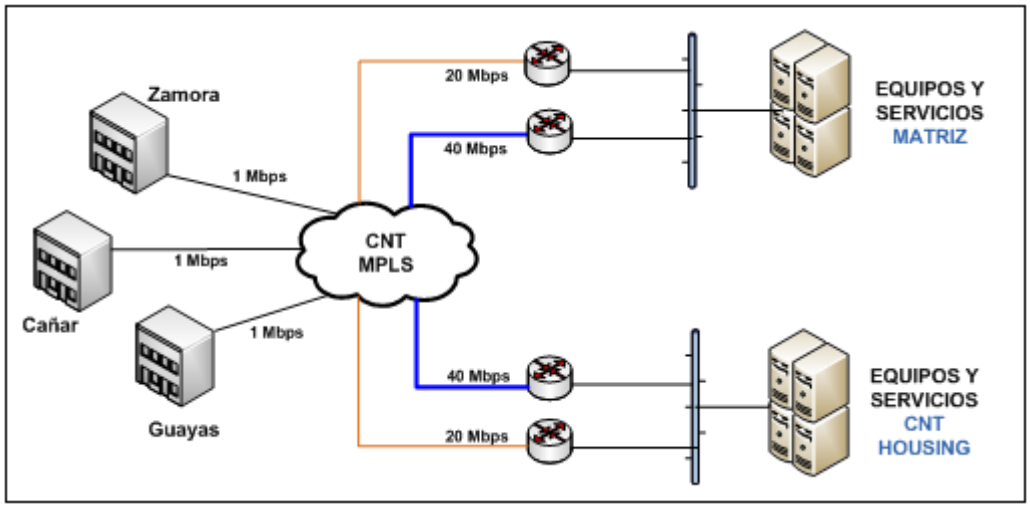
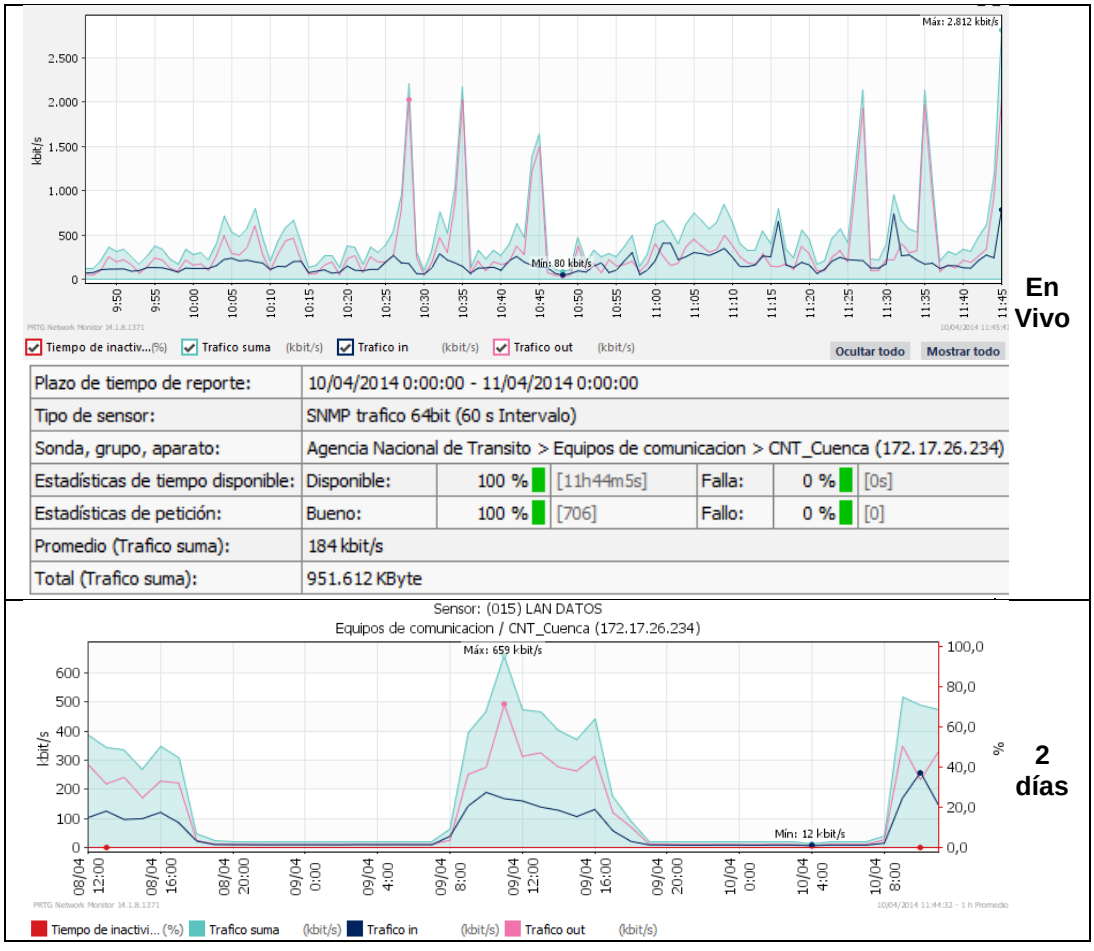


Figura 4.3.4 Acceso a sucursales

Fuente: Chicaiza, D. (2014)

A continuación se presenta el análisis de tráfico que generan las agencias con mayor afluencia de usuarios.

- **Agencia Cuenca (2Mbps)**



En Vivo

Plazo de tiempo de reporte:	10/04/2014 0:00:00 - 11/04/2014 0:00:00					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Cuenca (172.17.26.234)					
Estadísticas de tiempo disponible:	Disponible:	100 %	[11h44m5s]	Falla:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[706]	Fallo:	0 %	[0]
Promedio (Trafico suma):	184 kbit/s					
Total (Trafico suma):	951.612 KByte					

2 días

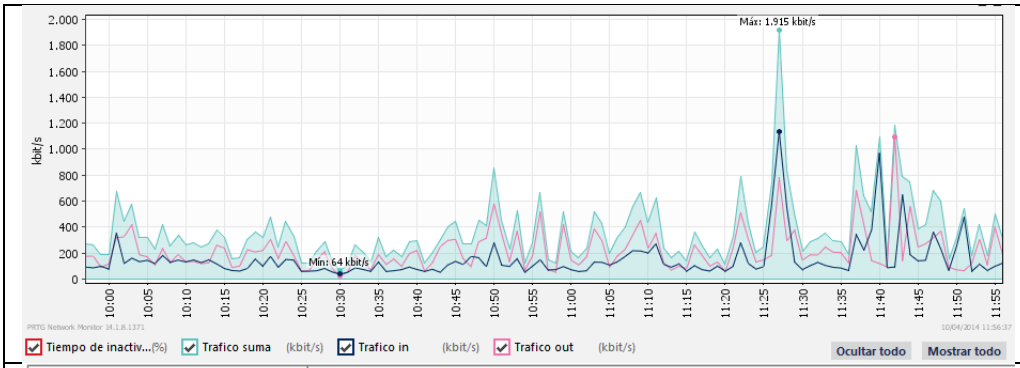
Plazo de tiempo de reporte:	08/04/2014 11:49:00 - 10/04/2014 11:49:00					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Cuenca (172.17.26.234)					
Estadísticas de tiempo disponible:	Disponible:	100 %	[1d23h53m5s]	Falla:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[2875]	Fallo:	0 %	[0]
Promedio (Trafico suma):	164 kbit/s					
Total (Trafico suma):	3.394.000 KByte					

Figura 4.3.5 Enlace Agencia Cuenca - Azuay

Fuente: Chicaiza, D. (2014)

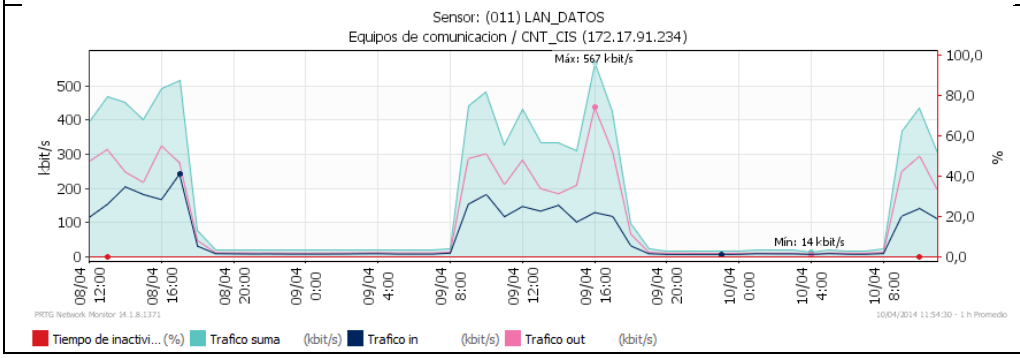
La figura 4.3.5 presenta las estadísticas del servicio de datos de la agencia Cuenca a partir del software PRTG para lo cual se verificó el tráfico en vivo y de 2 días. Para interpretar correctamente la gráfica se deben sumar los tráficos salientes y entrantes, es decir, el tráfico Suma (Kbit/s). Fácilmente el consumo alcanza un pico de 2.2 Mb/s, con lo que se verifica que existe saturación del canal a ciertas horas del día. De acuerdo a la información del personal de TI las actualizaciones del software Antivirus se realizaba desde el servidor central (Matriz) debido a una mala configuración del servidor esclavo.

- **Agencia Samborondón (2 Mbps)**



Plazo de tiempo de reporte:	09/04/2014 11:57:00 - 10/04/2014 11:57:00					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_CIS (172.17.91.234)					
Estadísticas de tiempo disponible:	Disponible:	100 %	[23h53m6s]	Falla:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[1435]	Fallo:	0 %	[0]
Promedio (Trafico suma):	151 kbit/s					
Total (Trafico suma):	1.519.870 KByte					

En Vivo



2 días

Plazo de tiempo de reporte:	08/04/2014 11:54:00 - 10/04/2014 11:54:00					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_CIS (172.17.91.234)					
Estadísticas de tiempo disponible:	Disponible:	100 %	[1d23h53m6s]	Falla:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[2875]	Fallo:	0 %	[0]
Promedio (Trafico suma):	167 kbit/s					
Total (Trafico suma):	3.452.459 KByte					

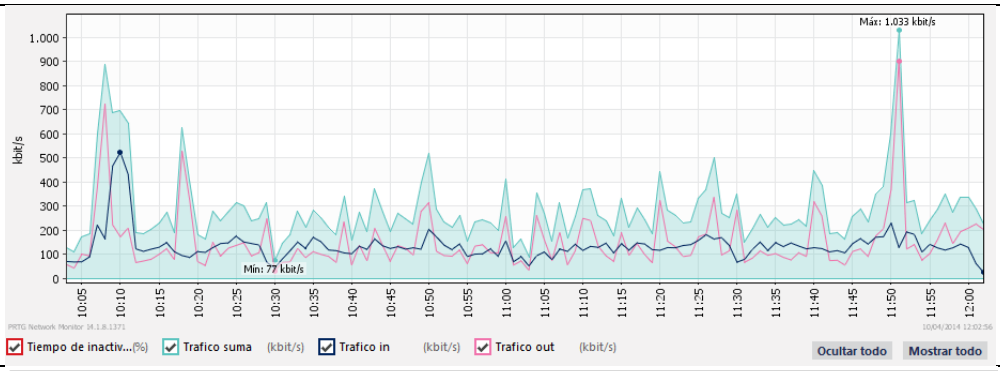
Figura 4.3.6 Enlace Samborondón - Guayas

Fuente: Chicaiza, D. (2014)

En la figura 4.3.6 podemos observar los picos al inicio del día y después de la hora aproximada de almuerzo, la capacidad utilizada llega a ser 1915 (Kbit/s).Se consultó al personal de TI de la provincia y nos supieron indicar que debido a la implementación del nuevo sistema de tránsito dicha agencia fue escogida para realizar el plan piloto para verificar dicho sistema.

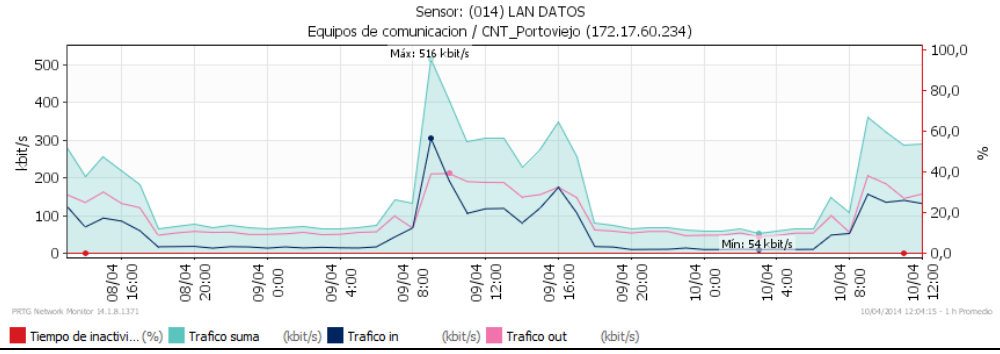
- **Agencia Portoviejo (1 Mbps)**

En Vivo



Plazo de tiempo de reporte:	09/04/2014 12:03:00 - 10/04/2014 12:03:00					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Portoviejo (172.17.60.234)					
Estadísticas de tiempo disponible:	Disponible:	100 %	[23h55m0s]	Falla:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[1437]	Fallo:	0 %	[0]
Promedio (Trafico suma):	156 kbit/s					
Total (Trafico suma):	1.642.355 KByte					

2 días



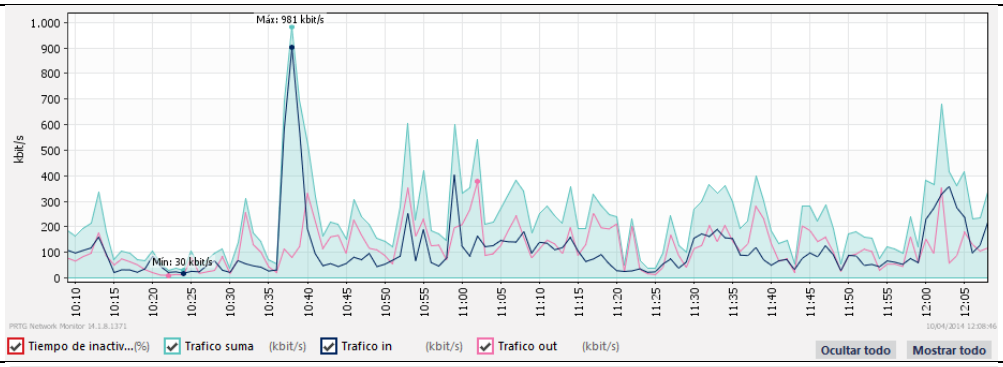
Plazo de tiempo de reporte:	08/04/2014 12:04:00 - 10/04/2014 12:04:00						
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)						
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Portoviejo (172.17.60.234)						
Estadísticas de tiempo disponible:	Disponible:	100 %	[1d23h55m0s]	Falla:	0 %	[0s]	
Estadísticas de petición:	Bueno:	100 %	[2877]	Fallo:	0 %	[0]	
Promedio (Trafico suma):	158 kbit/s						
Total (Trafico suma):	3.331.309 KByte						

Figura 4.3.7 enlace Portoviejo - Manabí

Fuente: Chicaiza, D. (2014)

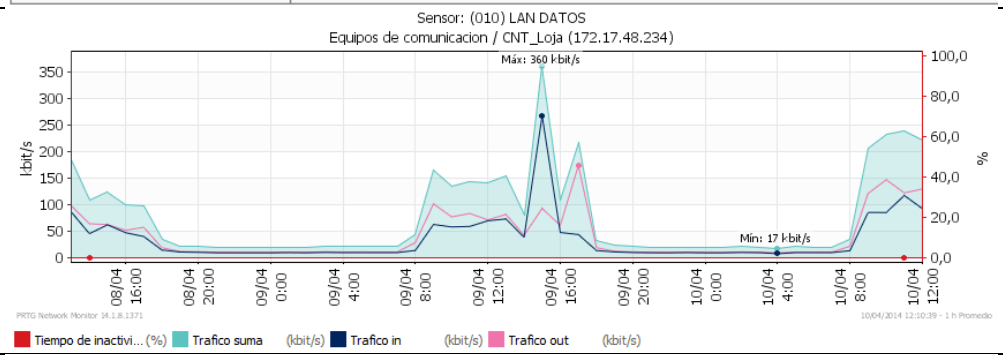
En la figura 4.3.7 podemos observar que el tráfico promedio es 500 Kbit/s. Se verifica que la capacidad contratada es suficiente para el buen desempeño de los sistemas contratados.

- **Agencia Loja (1 Mbps)**



Plazo de tiempo de reporte:	09/04/2014 12:09:00 - 10/04/2014 12:09:00						
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)						
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Loja (172.17.48.234)						
Estadísticas de tiempo disponible:	Disponible:	100 %	[23h54m7s]	Falla:	0 %	[0s]	
Estadísticas de petición:	Bueno:	100 %	[1436]	Fallo:	0 %	[0]	
Promedio (Trafico suma):	89 kbit/s						
Total (Trafico suma):	930.740 KByte						

En Vivo



Plazo de tiempo de reporte:	08/04/2014 12:10:00 - 10/04/2014 12:10:00						
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)						
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Loja (172.17.48.234)						
Estadísticas de tiempo disponible:	Disponible:	100 %	[1d23h54m7s]	Falla:	0 %	[0s]	
Estadísticas de petición:	Bueno:	100 %	[2876]	Fallo:	0 %	[0]	
Promedio (Trafico suma):	77 kbit/s						
Total (Trafico suma):	1.610.719 KByte						

2 días

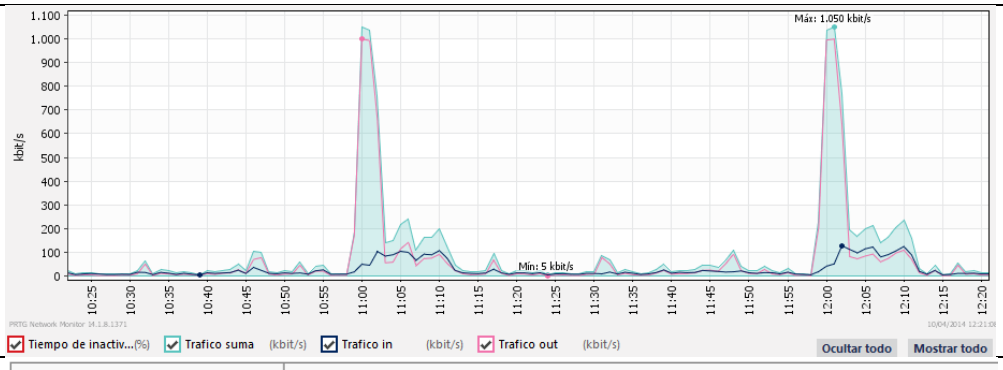
Figura 4.3.8 enlace Loja - Loja

Fuente: Chicaiza, D. (2014)

En la figura 4.3.8 podemos observar que el tráfico promedio es 600 Kbit/s. Existiendo picos durante la mañana en donde la capacidad llega al tope del valor contratado. De acuerdo a información de personal de TI de la provincia en la mañana hasta aproximadamente las 11:00 de la mañana el personal tiene como política despachar toda la documentación pendiente a través del Sistema de Gestión Documental (Quipux) al cual se accede a través del servicio de datos del anillo interministerial al cual se encuentra conectado ANT (Matriz).

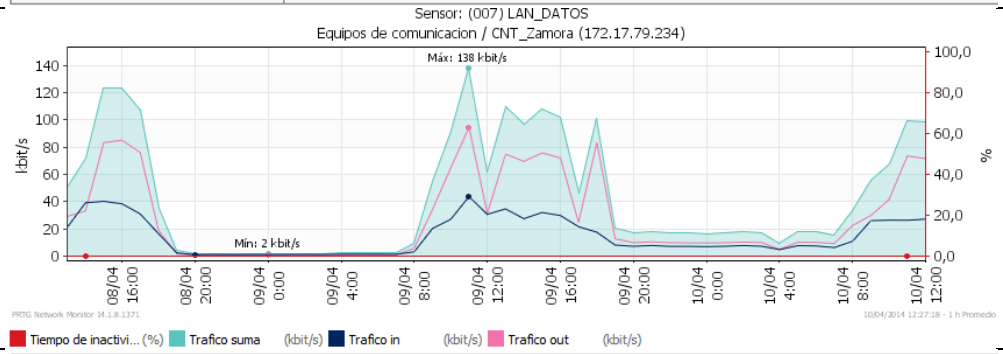
- **Agencia Zamora (1 Mbps)**

En Vivo



Plazo de tiempo de reporte:	09/04/2014 12:24:00 - 10/04/2014 12:24:00					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Zamora (172.17.79.234)					
Estadísticas de tiempo disponible:	Disponible:	100 %	[23h50m5s]	Falla:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[1432]	Fallo:	0 %	[0]
Promedio (Trafico suma):	46 kbit/s					
Total (Trafico suma):	471.247 KByte					

2 días



Plazo de tiempo de reporte:	08/04/2014 12:27:00 - 10/04/2014 12:27:00					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Agencia Nacional de Transito > Equipos de comunicacion > CNT_Zamora (172.17.79.234)					
Estadísticas de tiempo disponible:	Disponible:	100 %	[1d23h50m5s]	Falla:	0 %	[0s]
Estadísticas de petición:	Bueno:	100 %	[2872]	Fallo:	0 %	[0]
Promedio (Trafico suma):	42 kbit/s					
Total (Trafico suma):	883.677 KByte					

Figura 4.3.9 Enlace Zamora - Zamora

Fuente: Chicaiza, D. (2014)

En la figura 4.3.9 podemos observar que el tráfico promedio es 300 Kbit/s. con lo cual se verifica que la capacidad contratada es suficiente para el normal funcionamiento de los servicios. Cabe indicar que esta es una dependencia de tamaño mediano.

4.4 ADMINISTRACIÓN DE LA RED

4.4.1 Administración y monitoreo de equipos

ANT cuenta con la herramienta PRTG Network Monitor[12] (versión 14.1.8.1371) con un licenciamiento para 1000 sensores. Las principales ventajas que brinda el software de monitoreo son:

- Gestionar sobre una plataforma unificada el monitoreo de servidores (físicos y virtuales), servicios y equipos de comunicación de toda la red (Matriz y Dependencias) a través del protocolo SNMP.
- Mejorar el tiempo de respuesta en casos de problemas fortuitos.
- Obtener un sistema de alarmas (por correo) para prevenciones tempranas frente a problemas de hardware o software en los diferentes entornos de infraestructura tecnológica.
- Brindar un servicio de calidad enfocado en los conceptos de eficiencia y eficacia a los funcionarios de la ANT.

[12] http://www.es.paessler.com/prtg

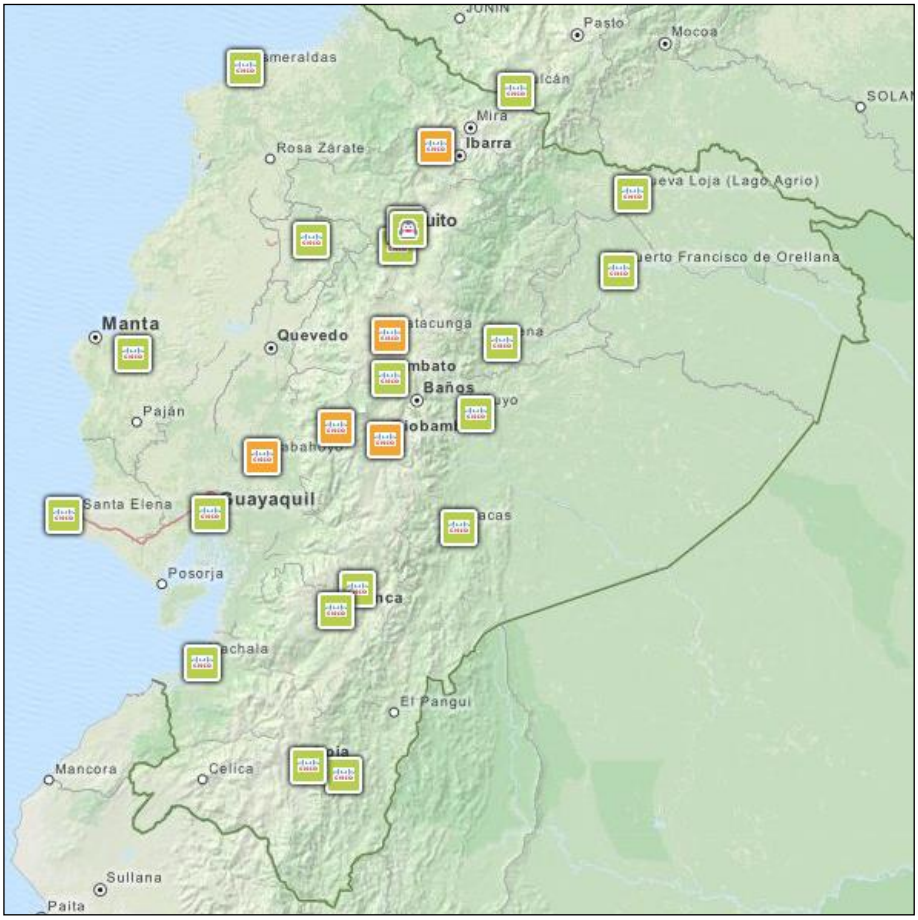


Figura 4.4.1 Mapa de Monitoreo - PRTG Network Monitor

Fuente: Chicaiza, D. (2014)

4.4.2 Gestión de Software y Hardware

ANT cuenta con software de administración de sistemas de TI llamado Kaseya[13], este permite automatizar todas las tareas rutinarias de mantenimiento, tanto generales como específicas de la empresa, controladas centralmente, minimizando el tiempo de las tareas al máximo sacando la máxima productividad.

Actualmente la herramienta está siendo utilizada para:

- **Actualización de parches de seguridad**: Permite mantener actualizados todos los PC de la empresa contra cualquier agujero de seguridad.
- **Instalación de aplicaciones**: Permite instalar software de la empresa de forma remota.
- **Control remoto.**

[13] http://www.kaseya.com/

- **Copias de Seguridad - Backup**
- **Auditoría:** Inventario completo de hardware y software.
- **Control de incidencias (Help Desk, Tickets):** El usuario puede notificar al administrador un problema vía email.
- **Elaboración de Informes**: Permite obtener informes completos del estado de la red.

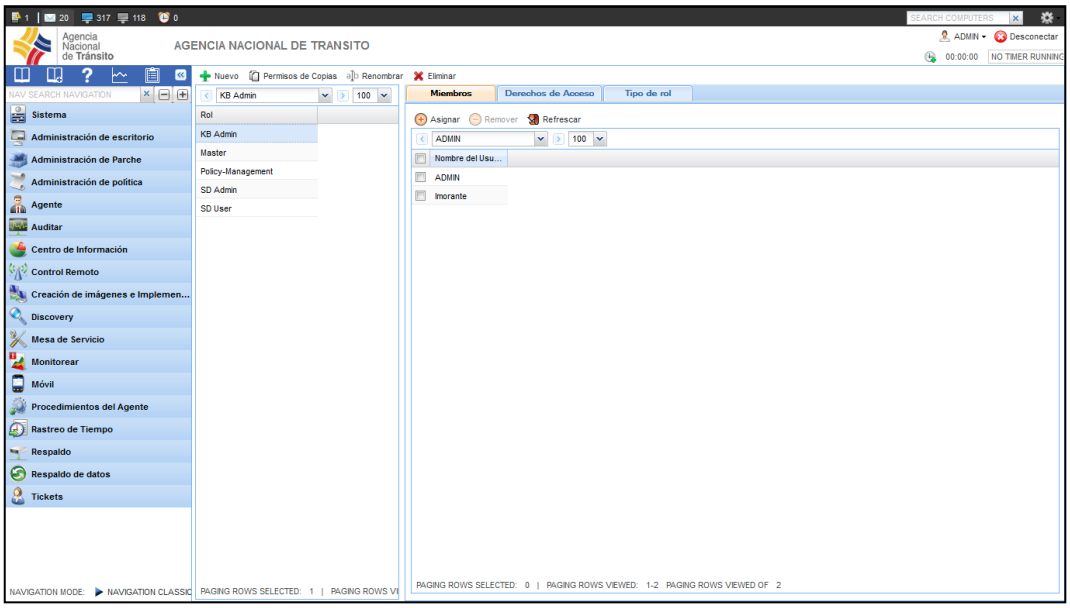


Figura 4.4.2 Pantalla de administración de Kaseya

Fuente: Chicaiza, D. (2014)

4.4.3 Gestión de usuarios

La creación y administración de usuarios de red está a cargo del personal de Infraestructura. Existe un formulario para creación, modificación y eliminación de usuarios, se maneja dos modelos de creación de cuentas y perfiles de usuario.

- **Cuenta de red:**
  - Basado en la sucursal de usuario.
  - Basado en el cargo del usuario.
- **Perfil:**
  - Usuario Administrador de dominio (Personal de TI).
  - Usuario de dominio (Personal Administrativo).

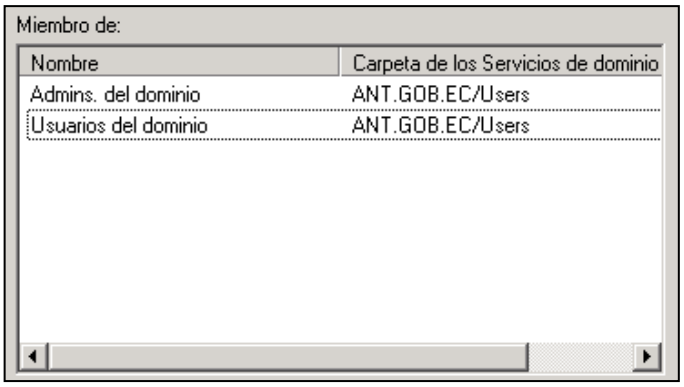


Figura 4.4.3 Perfil de usuarios en el Directorio Activo de ANT

Fuente: Chicaiza, D. (2014)

4.4.4 Gestión de virus

La Agencia Nacional de Tránsito actualmente cuenta con 1.000 licencias de la solución Kaspersky Antivirus Business Space Security que en la actualidad es equivalente a la solución Kaspersky KES Business Select. El sistema de protección cuenta con licencia por tres años al igual que el servicio de soporte técnico y mantenimiento, estos caducarán en el año 2017.

Las principales funcionalidades del sistema antivirus son:

- **Protección Endpoint:**
  - Antimalware de endpoint superior.
  - Protección asistida en la nube.

- **Controles Endpoint:**
  - Control de aplicaciones.
  - Control de dispositivos.
  - Control web.
  - Lista blanca dinámica

- **Características de seguridad móvil.**
  - Tecnologías antimalware
  - Soporte para los dispositivos propiedad del empleado
  - Herramientas antirrobo remotas.
  - Control de aplicaciones para dispositivos móviles

Figura 4.4.4 Kaspersky Endpoint Security 10

Fuente: Chicaiza, D. (2014)

La solución mencionada está implementada de la siguiente manera:

La consola Maestra se encuentra instalada en la matriz de ANT en la ciudad de Quito, la cual gestiona treinta y siete (37) repositorios de actualización de firmas en servidores de las Agencias a nivel nacional.

1. El repositorio maestro periódicamente descarga el motor y los archivos de actualización desde el sitio de origen Kaspersky.

2. El repositorio principal replica los paquetes a los repositorios distribuidos de la red.

3. Los sistemas administrados en la red descargan las actualizaciones desde un repositorio esclavo de agencias. Si los sistemas administrados no pueden acceder a los repositorios distribuidos o el repositorio principal, ellos recuperan las actualizaciones desde el sitio de origen Kaspersky.

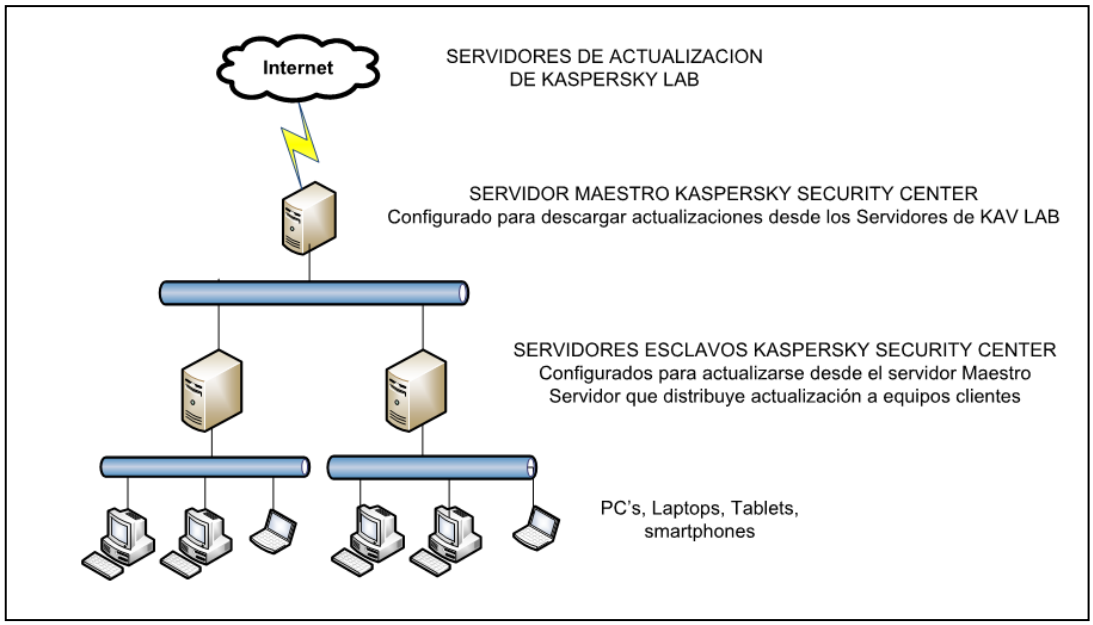


Figura 4.4.5 Diagrama de implementación Kaspersky

Fuente: Chicaiza, D. (2014)

4.4.5 Gestión de almacenamiento

El espacio de almacenamiento se encuentra de la siguiente forma:

- Centralizada: Edificio matriz almacena en el servidor de archivos denominado SRVDF02.
- 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 la capacidad de almacenamiento tanto para sistema operativo como para datos de usuario es suficiente en la actualidad.

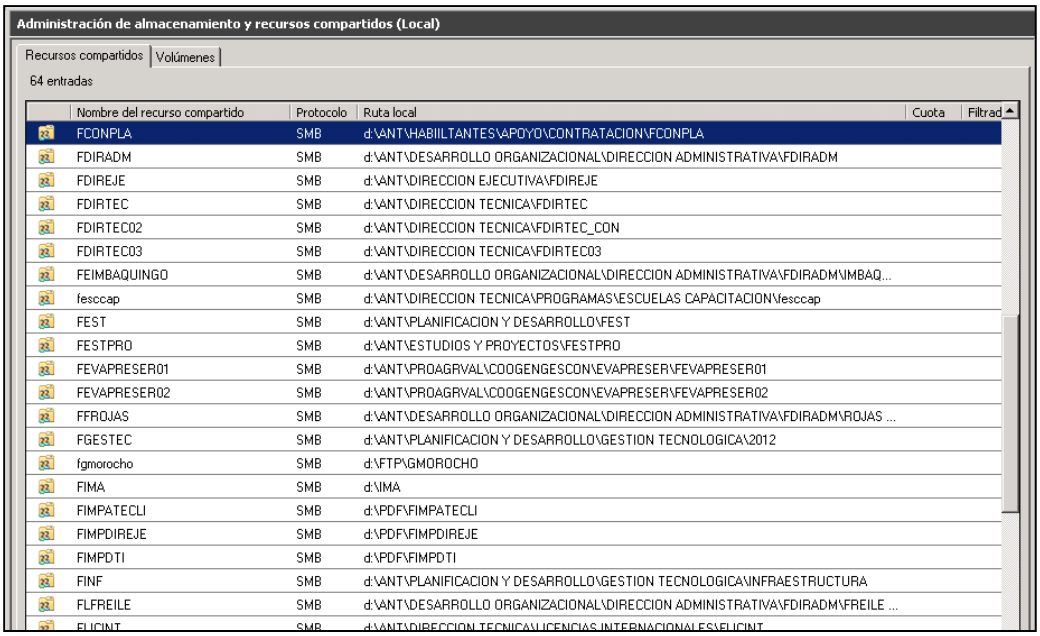


Figura 4.4.6 Recursos de Almacenamiento y recursos compartidos matriz de ANT

Fuente: Chicaiza, D. (2014)

4.5 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES EN LA RED.

4.5.1 Vulnerabilidades y Amenazas

Para el diagnóstico de la seguridad en la presente red, se utilizo las herramientas de software: GFI LAN Guard 2014 Versión: 11.2 Build: 20130809 en su versión trial, NESSUS Versión: 5.2.6 Web UI: 2.3.2 en su versión de evaluación y el software Kaspersky Antivirus Endpoint Security 10.

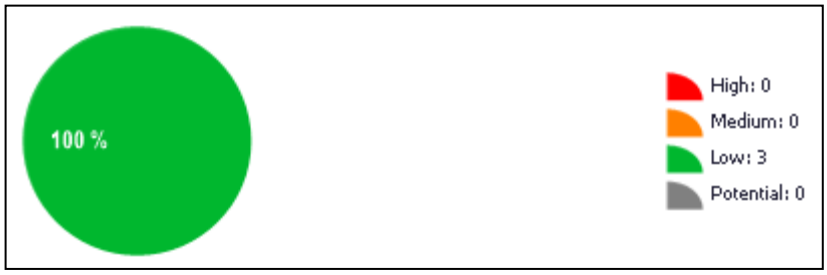
4.5.1.1 Análisis con GFI LAN Guard

GFI LAN Guard es una solución que permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad de la red y permite obtener la siguiente información:

- Exploración de puertos del sistema.
- Vulnerabilidades encontradas en el sistema.

A continuación se presentan las vulnerabilidades encontradas mediante el software GFI en los principales equipos de la red de ANT:

- **Servidor Sistema de Tránsito (SITCOM)**



Vulnerability level:

The average vulnerability level for this scanning session is: **Low**

Results statistics:

Audit operations processed:	2478 audit operations processed
Other vulnerabilities:	3 (0 Critical/High)
Open ports:	8

Services (3)
- Service running: SSH
  - Description: If this computer is not administered via secure shell, the SSH service is most likely unnecessary.
- Service running: FTP
  - Description: 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: CUPS
  - Description: If this is not a CUPS print server, the CUPS server service is most likely unnecessary.

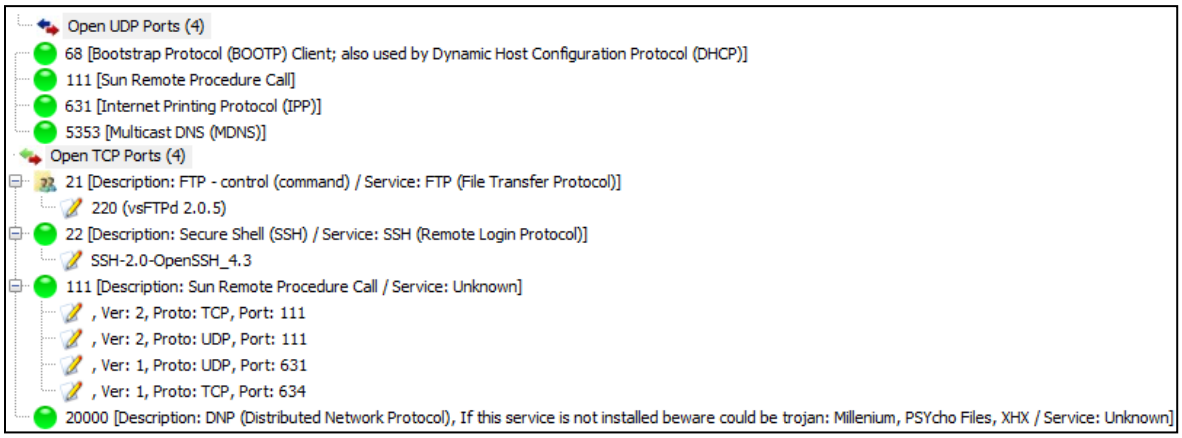
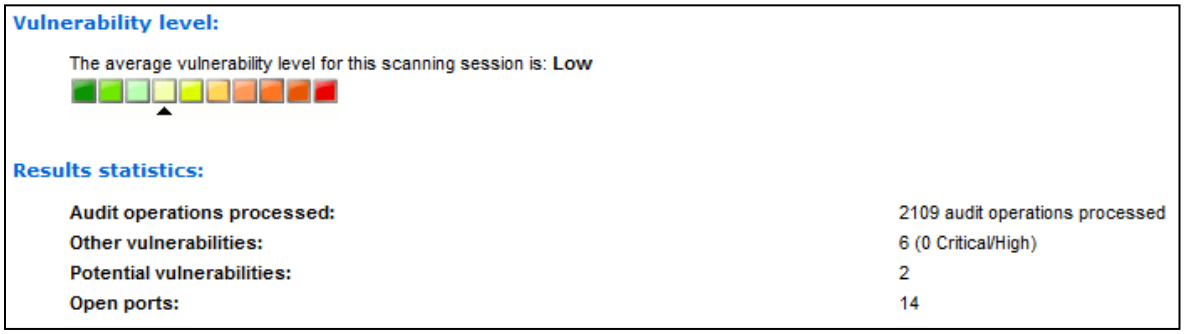
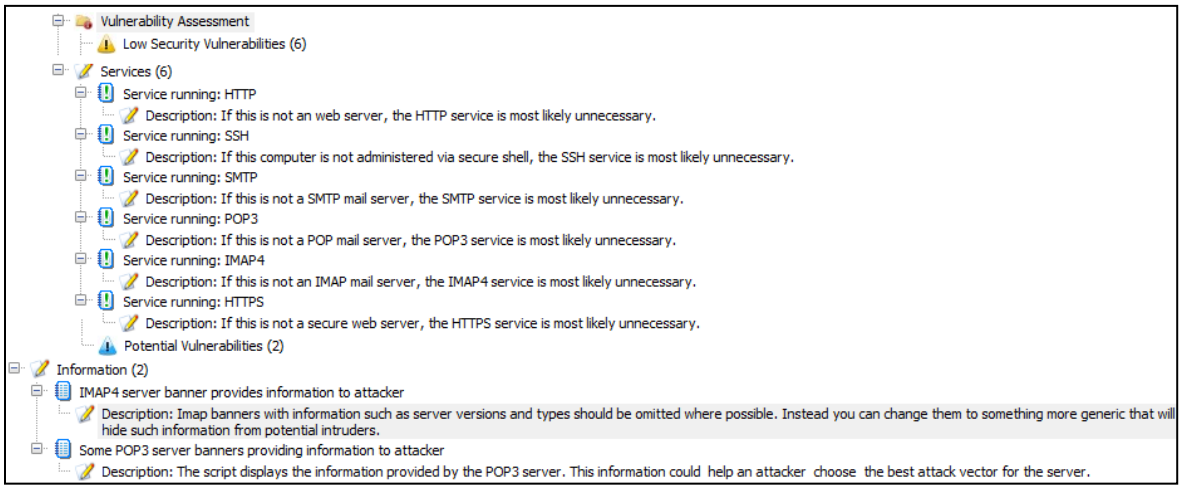


Figura 4.5.1 Vulnerabilidades y Puertos Abiertos Servidor de Tránsito

Fuente: Chicaiza, D. (2014)

- **Servidor Mail**





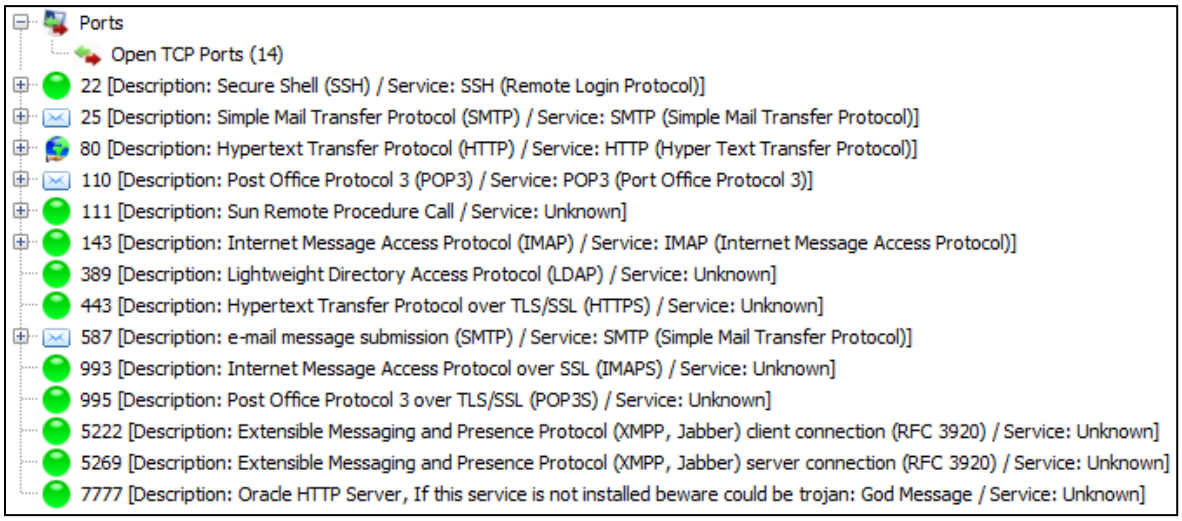
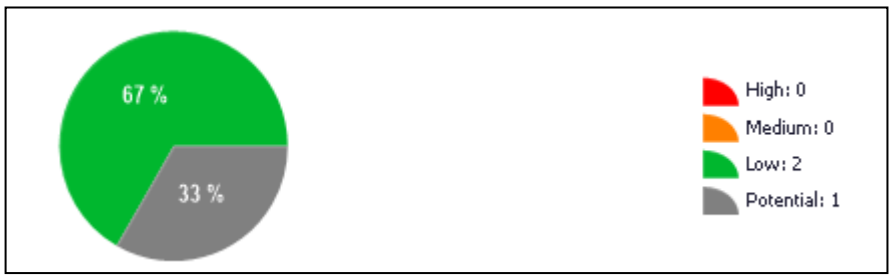
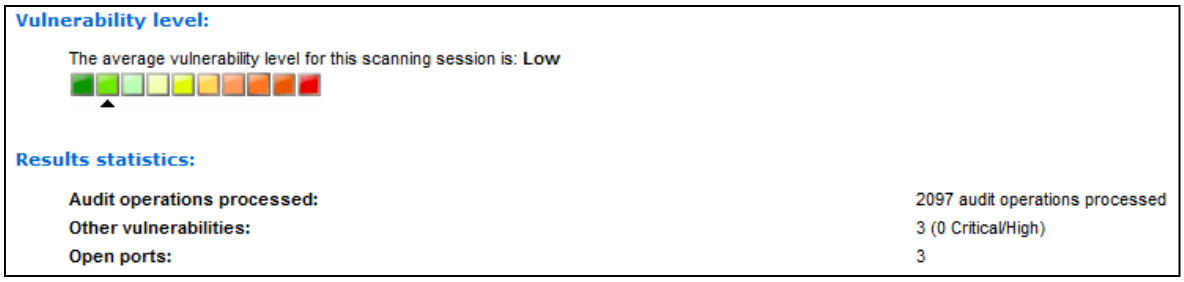


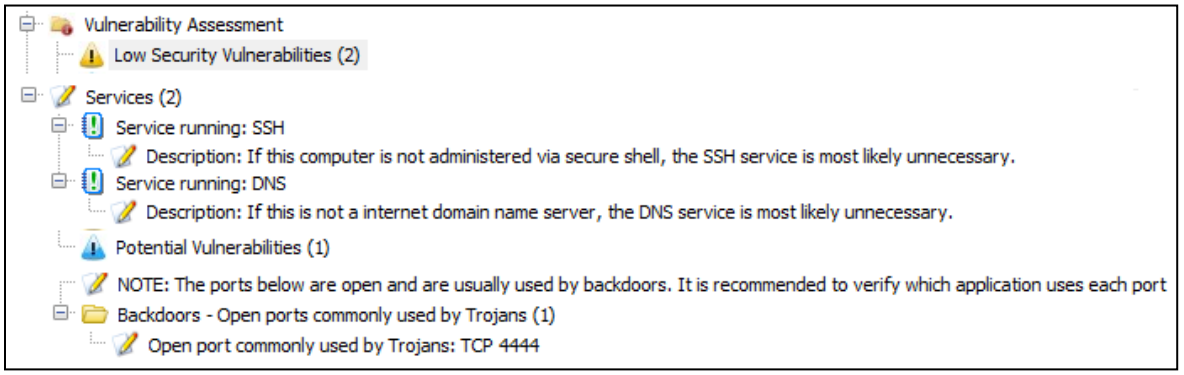
Figura 4.5.2 Vulnerabilidades y Puertos Abiertos Servidor de Correo

Fuente: Chicaiza, D. (2014)

- **Dispositivo Astaro Security Gateway**







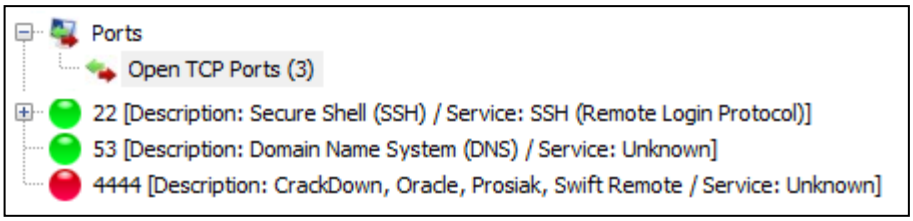
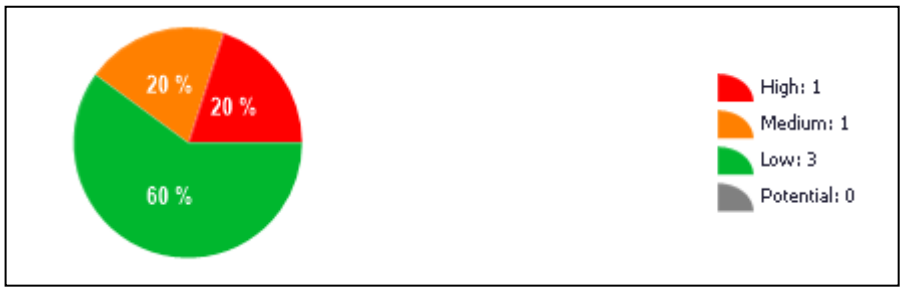


Figura 4.5.3 Vulnerabilidades y Puertos Abiertos Dispositivo Astaro

Fuente: Chicaiza, D. (2014)

- **Servidor de archivos**



Vulnerability level:

The average vulnerability level for this scanning session is: **High**

Results statistics:

Audit operations processed:	5452 audit operations processed
Other vulnerabilities:	5 (1 Critical/High)
Installed applications:	6 (0 unauthorized)
Open ports:	9
Open shares:	64

Vulnerability Assessment
- High Security Vulnerabilities (1)
- Miscellaneous (1)
  - AutoRun is enabled
    - Description: Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a security risk in the case where a CD or removable disk containing malware that automatically installs itself once the disc is inserted.

      It is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives.
- Medium Security Vulnerabilities (1)
- Software (1)
  - OVAL:12566: Microsoft Windows Human Interface Device (HID) driver is prone to security bypass vulnerability.
    - Description: Microsoft Windows does not properly warn the user before enabling additional Human Interface Device (HID) functionality over USB, which allows user-assisted attackers to execute arbitrary programs via crafted USB data, as demonstrated by keyboard and mouse data sent by malware on a smartphone that the user connected to the computer.
- Low Security Vulnerabilities (3)
- Miscellaneous (1)
  - AutoRun is enabled
    - Description: Microsoft Windows supports automatic execution in CD/DVD drives and other removable media. This poses a security risk in the case where a CD or removable disk containing malware that automatically installs itself once the disc is inserted.

      It is recommended to disable AutoRun both for CD/DVD drives and also for other removable drives.

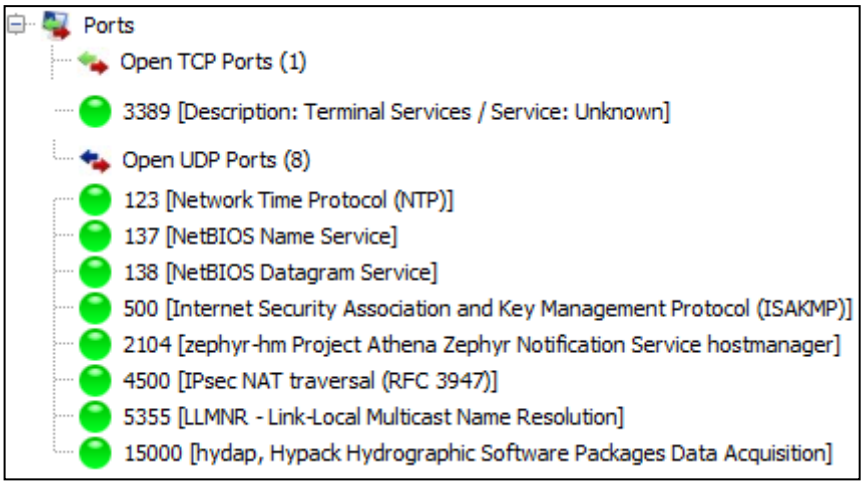


Figura 4.5.4 Vulnerabilidades y Puertos Abiertos Servidor de de Archivos

Fuente: Chicaiza, D. (2014)

- **Dominio (40 Equipos analizados)**

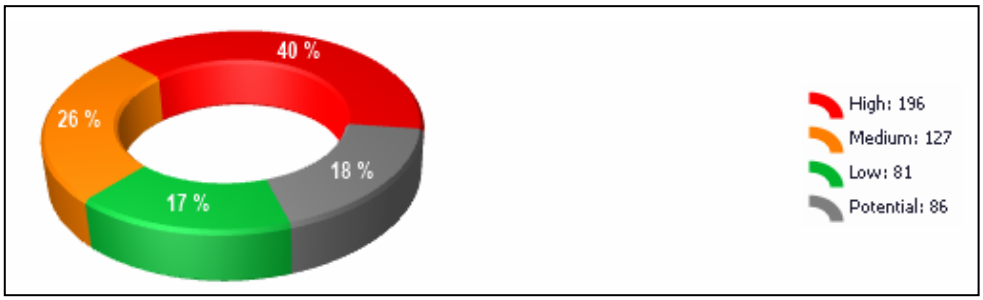


Figura 4.5.5 Vulnerabilidades y Puertos Abiertos Matriz ANT

Fuente: Chicaiza, D. (2014)

4.5.1.1.1 Resumen de Puertos TCP Y UDP abiertos

- **Puertos TCP Abiertos (39)**

Puerto	Proceso	No. de PC	Puerto	Proceso	No. de PC
TCP 22		2	TCP 636		1
TCP 25		1	TCP 993		1
TCP 53		2	TCP 995		1

TCP 80		1	TCP 1198		1
TCP 88		1	TCP 2002		1
TCP 110		1	TCP 3268		1
TCP 111		1	TCP 3269		1
TCP 135		13	TCP 3306		3
TCP 135	svchost.exe	1	TCP 3389		3
TCP 139		17	TCP 3389	svchost.exe	1
TCP 143		1	TCP 4444		1
TCP 389		2	TCP 5222		1
TCP 443		1	TCP 5269		1
TCP 445		17	TCP 5405		2
TCP 445	System	1	TCP 5800		1
TCP 464		1	TCP 5800		2
TCP 554		1	TCP 5900		3
TCP 587		1	TCP 7777		1
TCP 593		1	TCP 13000		1
TCP 623	LMS.exe	1			

Tabla 4.5.1 Puertos TCP abiertos

Fuente: Chicaiza, D. (2014)

- **Puertos UDP Abiertos (271)**

Puerto	No. de PC	Puerto	No. de PC	Puerto	No. de PC	Puerto	No. de PC
UDP 1	1	UDP 383	1	UDP 631	1	UDP 1169	1
UDP 35	1	UDP 384	1	UDP 636	1	UDP 1182	1
UDP 56	1	UDP 387	1	UDP 639	1	UDP 1194	1
UDP 88	1	UDP 389	1	UDP 646	1	UDP 1198	1
UDP 113	1	UDP 401	1	UDP 657	1	UDP 1200	1
UDP 118	1	UDP 427	1	UDP 666	1	UDP 1201	1
UDP 123	3	UDP 444	1	UDP 698	1	UDP 1223	1
UDP 123	1	UDP 445	1	UDP 749	1	UDP 1241	1
UDP 135	1	UDP 464	1	UDP 750	1	UDP 1270	1
UDP 137	3	UDP 500	3	UDP 751	1	UDP 1293	1
UDP 137	1	UDP 500	1	UDP 752	1	UDP 1387	1
UDP 138	4	UDP 512	1	UDP 753	1	UDP 1417	1
UDP 152	1	UDP 513	1	UDP 754	1	UDP 1418	1
UDP 153	1	UDP 514	1	UDP 760	1	UDP 1419	1
UDP 156	1	UDP 517	1	UDP 953	1	UDP 1420	1
UDP 161	1	UDP 518	1	UDP 989	1	UDP 1433	1
UDP 162	1	UDP 520	1	UDP 990	1	UDP 1434	1
UDP 177	1	UDP 524	1	UDP 991	1	UDP 1512	1
UDP 194	1	UDP 525	1	UDP 992	1	UDP 1524	1

UDP 201	1	UDP 530	1	UDP 1028	1	UDP 1547	1
UDP 209	1	UDP 533	1	UDP 1031	1	UDP 1581	1
UDP 213	1	UDP 542	1	UDP 1032	1	UDP 1677	1
UDP 217	1	UDP 546	1	UDP 1058	1	UDP 1701	1
UDP 218	1	UDP 547	1	UDP 1059	2	UDP 1723	1
UDP 220	2	UDP 550	1	UDP 1085	1	UDP 1755	1
UDP 259	1	UDP 554	1	UDP 1098	1	UDP 1761	1
UDP 264	1	UDP 560	1	UDP 1099	1	UDP 1762	1
UDP 318	1	UDP 561	1	UDP 1111	1	UDP 1763	1
UDP 366	1	UDP 563	1	UDP 1116	1	UDP 1764	1
UDP 369	1	UDP 593	1	UDP 1140	1	UDP 1765	1
UDP 371	1	UDP 623	2	UDP 1167	1	UDP 1766	1

Tabla 4.5.2 Puertos UDP abiertos

Fuente: Chicaiza, D. (2014)

4.5.1.1.2 Resumen de vulnerabilidades encontradas

- **Vulnerabilidades de Seguridad Alta**

Nombre de la Vulnerabilidad	Producto
AutoRun is enabled	
OVAL:10983: Adobe Flash Player and AIR Unspecified Multiple Memory Corruption Vulnerabilities	Adobe Flash Player,Adobe AIR
OVAL:12219: Untrusted search path vulnerability in Microsoft Office PowerPoint 2007	Microsoft Office PowerPoint 2007
OVAL:12689: Fax Cover Page Use After Free Vulnerability	
OVAL: 13830: The browser engine in Mozilla Firefox before 8.0 and Thunderbird before 8.0 does not properly handle links from SVG mpath elements to non-SVG elements, which allows remote attackers to cause a denial of service (memory corruption and...	Mozilla Thunderbird,Mozilla Firefox
OVAL:17031: Use-after-free vulnerability in the nsFrameList::FirstChild function in Mozilla Firefox before 21.0, Firefox ESR 17.x before 17.0.6, Thunderbird before 17.0.6, and Thunderbird ESR 17.x before 17.0.6 allows remote attackers to execute...	Mozilla Firefox,Mozilla Thunderbird
OVAL: 17039: The debugger in the developer-tools subsystem in Mozilla Firefox before 15.0, when remote debugging is disabled, does not properly restrict access to the remote-debugging service, which allows remote attackers to execute arbitrary code...	Mozilla Firefox
OVAL:6758: Adobe Flash Player Memory Corruption Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:6762: Adobe Flash Player Invalid Pointer Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:6765: Adobe Flash Player Use-After-Free Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:6766: Adobe Flash Player Integer Overflow Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:6781: Adobe Flash Player Memory Corruption Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:7501: Adobe Flash Player Multiple Vulnerabilities that could lead to code execution	Adobe Flash Player,Adobe AIR
OVAL:7508: Adobe Flash Player Memory Exhaustion Vulnerability	Adobe Flash Player,Adobe AIR

OVAL:7528: Adobe Flash Player Invalid Pointer Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:7577: Adobe Flash Player Buffer Overflow Vulnerability	Adobe Flash Player,Adobe AIR

Tabla 4.5.3 Vulnerabilidades de Seguridad Alta

Fuente: Chicaiza, D. (2014)

- **Vulnerabilidades de Seguridad Media**

Nombre de la Vulnerabilidad	Producto
OVAL:11532: Adobe Flash Player and AIR Unspecified Click-jacking Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:12355: Microsoft Internet Explorer PDF Printing Information Disclosure	Microsoft Internet Explorer 6,Microsoft Internet Explorer 7,Microsoft Internet Explorer 8
OVAL: 12566: Microsoft Windows Human Interface Device (HID) driver is prone to security bypass vulnerability.	
OVAL:12638: Microsoft Internet Explorer cross-site scripting (XSS) vulnerability	Microsoft Internet Explorer 8
OVAL:12693: Information disclosure vulnerability in Internet Explorer 8 on Windows 7	
OVAL: 20932: Mozilla Firefox before 26.0 and SeaMonkey before 2.23 do not properly consider the sandbox attribute of an IFRAME element during processing of a contained OBJECT element, which allows remote attackers to bypass intended sandbox...	Mozilla Firefox,Mozilla Seamonkey
OVAL: 20982: Mozilla Firefox before 26.0 does not properly remove the Application Installation doorhanger, which makes it easier for remote attackers to spoof a Web App installation site by controlling the timing of page navigation.	Mozilla Firefox
OVAL: 21024: Mozilla Firefox before 26.0, Firefox ESR 24.x before 24.2, Thunderbird before 24.2, and SeaMonkey before 2.23 do not recognize a user's removal of trust from an EV X.509 certificate, which makes it easier for man-in-the-middle attackers...	Mozilla Firefox,Mozilla Thunderbird,Mozilla Seamonkey
OVAL: 21047: Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 26.0 and SeaMonkey before 2.23 makes it easier for remote attackers to inject arbitrary web script or HTML by leveraging a Same Origin Policy violation triggered by lack...	Mozilla Firefox,Mozilla Seamonkey
OVAL: 21091: Multiple integer overflows in the binary-search implementation in SpiderMonkey in Mozilla Firefox before 26.0 and SeaMonkey before 2.23 might allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly...	Mozilla Firefox,Mozilla Seamonkey
OVAL:7187: Adobe Flash Player SWF Version Null Pointer Dereference Denial of Service Vulnerability	Adobe Flash Player,Adobe AIR
OVAL:8393: Adobe Flash Player and AIR Denial of Service Vulnerability	Adobe Flash Player,Adobe AIR

Tabla 4.5.4 Vulnerabilidades de Seguridad Media

Fuente: Chicaiza, D. (2014)

- **Vulnerabilidades de Seguridad Baja**

Nombre de la Vulnerabilidad	Producto
AutoShareServer	Windows
AutoShareWKS	Windows
Cached Logon Credentials	Windows NT

IM installed: Skype	Skype
OVAL:16935: The nsLocation::CheckURL function in Mozilla Firefox before 15.0, Firefox ESR 10.x before 10.0.7, Thunderbird before 15.0, Thunderbird ESR 10.x before 10.0.7, and SeaMonkey before 2.12 does not properly follow the security model of the...	Mozilla Firefox
Service running: DNS	
Service running: HTTP	
Service running: HTTPS	
Service running: MySQL	
Service running: SMTP	
Service running: SSH	
Shutdown without logon	
Windows AutoUpdate is enabled but requires user interaction to install patches	Windows

Tabla 4.5.5 Vulnerabilidades de Seguridad Baja

Fuente: Chicaiza, D. (2014)

- **Potenciales Vulnerabilidades**

Nombre de la Vulnerabilidad	Producto
A modem is installed on this computer	6
IMAP4 server banner provides information to attacker	1
List of modems installed	6
Some POP3 server banners providing information to attacker	1
USB devices installed over time	16
User HomeGroupUser$ never logged on	2
User Invitado never logged on	3
VNC server listening on port 5901	1
Open port commonly used by Trojans: UDP 1	1
Open port commonly used by Trojans: TCP 623 - LMS.exe	1
Open port commonly used by Trojans: UDP 1116	1
Open port commonly used by Trojans: UDP 1772	1
Open port commonly used by Trojans: TCP 2002	1
Open port commonly used by Trojans: UDP 2140	1
Open port commonly used by Trojans: UDP 2222	1
Open port commonly used by Trojans: UDP 2339	1
Open port commonly used by Trojans: UDP 2989	1
Open port commonly used by Trojans: UDP 3150	1
Open port commonly used by Trojans: UDP 3215	1
Open port commonly used by Trojans: UDP 3996	1
Open port commonly used by Trojans: TCP 4444	1
Open port commonly used by Trojans: UDP 5555	2
Open port commonly used by Trojans: UDP 6666	1
Open port commonly used by Trojans: UDP 6667	1

Open port commonly used by Trojans: UDP 6766	1
Open port commonly used by Trojans: UDP 6767	1
Open port commonly used by Trojans: UDP 6838	1
Open port commonly used by Trojans: UDP 7424	1
Open port commonly used by Trojans: UDP 8012	1
Open port commonly used by Trojans: UDP 9325	1
Open port commonly used by Trojans: UDP 10067	1
Open port commonly used by Trojans: UDP 10666	1
Open port commonly used by Trojans: UDP 11225	1
Open port commonly used by Trojans: UDP 12321	1
Open port commonly used by Trojans: UDP 12623	1
Open port commonly used by Trojans: UDP 15486	1
Open port commonly used by Trojans: UDP 18753	1

Tabla 4.5.6 Potenciales Vulnerabilidades

Fuente: Chicaiza, D. (2014)

4.5.1.2 Análisis con Nessus (Tenable Network Security®)

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un daemon, nessusd, que realiza el escaneo en el sistema objetivo, ynessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron. [46]

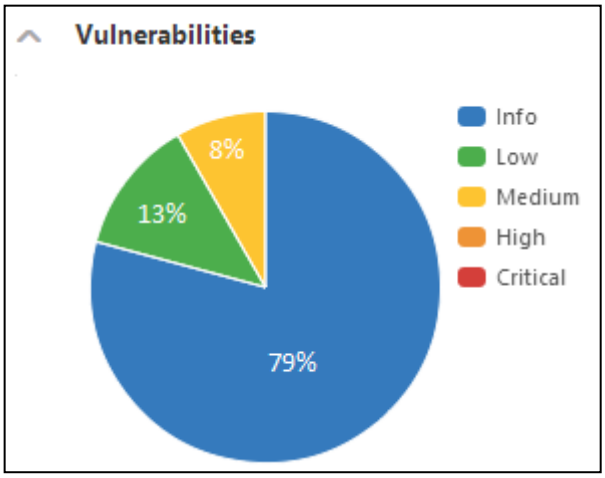
En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploitspara atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes. [45]

Nessus provee la siguiente información:

- Falta de parches de seguridad y configuraciones vulnerables encontradas en el sistema.
- Exploración de puertos del sistema.

A continuación se presentan las vulnerabilidades encontradas mediante el software Nessus en los principales equipos de la red de ANT:

- **Servidor Sistema de Tránsito (SITCOM)**



Summary

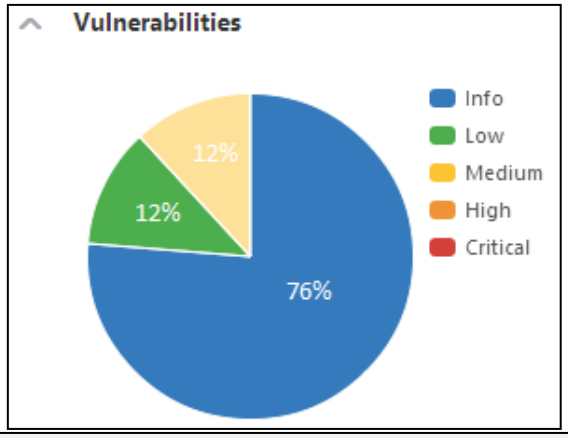
Critical	High	Medium	Low	Info	Total
0	0	2	3	19	24

Severity	Plugin Id	Name
Medium (5.0)	10079	Anonymous FTP Enabled
Medium (5.0)	12218	mDNS Detection (Remote Network)
Low (2.6)	34324	FTP Supports Clear Text Authentication
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10092	FTP Server Detection
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10223	RPC portmapper Service Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11111	RPC Services Enumeration
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported

Figura 4.5.6 Vulnerabilidades Servidor de Tránsito ANT

Fuente: Chicaiza, D. (2014)

- **Servidor de Correo**



Summary

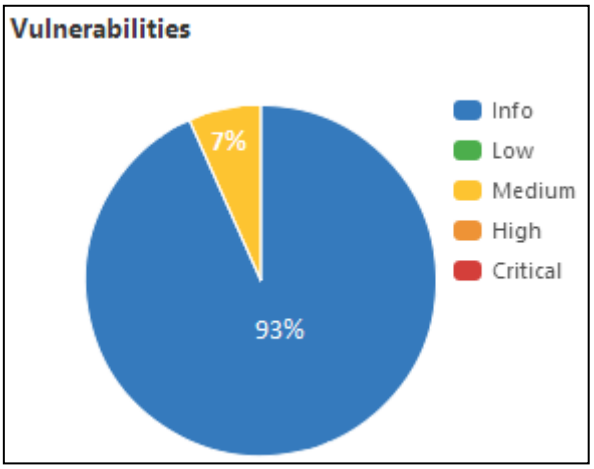
Critical	High	Medium	Low	Info	Total
0	0	7	7	45	59

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12218	mDNS Detection (Remote Network)
Medium (5.0)	20007	SSL Version 2 (v2) Protocol Detection
Medium (5.0)	72585	Zimbra Collaboration Server skin Parameter Traversal Local File Inclusion
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	15855	POP3 Cleartext Logins Permitted
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported
Low (2.6)	54582	SMTP Service Cleartext Login Permitted
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10185	POP Server Detection
Info	10223	RPC portmapper Service Detection
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10302	Web Server robots.txt Information Disclosure
Info	10863	SSL Certificate Information

Figura 4.5.7 Vulnerabilidades Servidor de Correo

Fuente: Chicaiza, D. (2014)

- **Dispositivo Astaro**



Summary

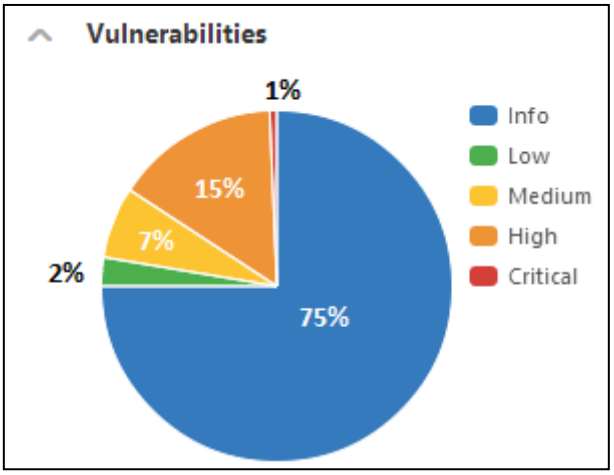
Critical	High	Medium	Low	Info	Total
0	0	1	0	14	15

Severity	Plugin Id	Name
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21745	Authentication Failure - Local Checks Not Run
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

Figura 4.5.8 Vulnerabilidades Dispositivo Astaro Security Gateway

Fuente: Chicaiza, D. (2014)

- **Servidor de Dominio**



Critical	High	Medium	Low	Info	Total
1	23	10	4	208	246

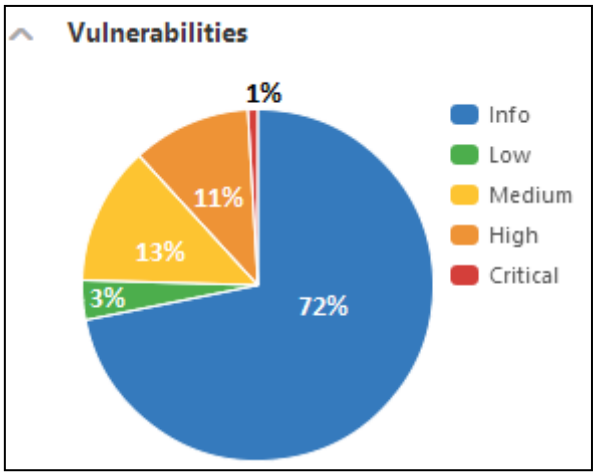
Details

Severity	Plugin Id	Name
Critical (10.0)	20284	Kaspersky Anti-Virus Detection
High (9.3)	40362	Mozilla Foundation Unsupported Application Detection
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
High (9.3)	60043	Firefox < 14.0 Multiple Vulnerabilities
High (9.3)	61715	Firefox < 15.0 Multiple Vulnerabilities
High (9.3)	62580	Firefox < 16.0 Multiple Vulnerabilities
High (9.3)	62589	Firefox < 16.0.1 Multiple Vulnerabilities
High (9.3)	62998	Firefox < 17.0 Multiple Vulnerabilities
High (9.3)	63551	Firefox < 18.0 Multiple Vulnerabilities
High (9.3)	64723	Firefox < 19.0 Multiple Vulnerabilities
High (9.3)	65131	Firefox < 19.0.2 nsHTMLEditor Use-After-Free
High (9.3)	65806	Firefox < 20 Multiple Vulnerabilities
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA)
Medium (4.3)	62744	Firefox < 16.0.2 Multiple Vulnerabilities
Medium (4.0)	73992	MS KB2960358: Update for Disabling RC4 in .NET TLS
Low (3.6)	70395	MS KB2532445: AppLocker Rules Bypass
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration

Figura 4.5.9 Vulnerabilidades Servidor de Dominio

Fuente: Chicaiza, D. (2014)

- **Servidor de Archivos**



Summary

Critical	High	Medium	Low	Info	Total
1	12	14	4	79	110

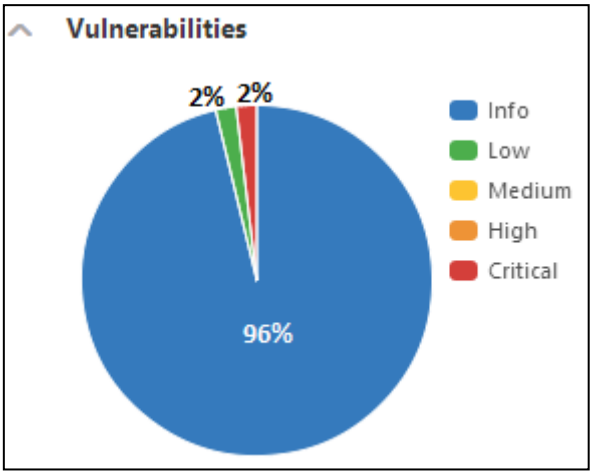
Severity	Plugin Id	Name
Critical (10.0)	20284	Kaspersky Anti-Virus Detection
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
High (9.3)	72430	MS14-007: Vulnerability in Direct2D Could Allow Remote Code Execution (2912390)
High (9.3)	72432	MS14-009: Vulnerabilities in .NET Framework Could Allow Privilege Escalation (2916607)
High (9.3)	72433	MS14-010: Cumulative Security Update for Internet Explorer (2909921)
High (9.3)	72434	MS14-011: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (2928390)
High (9.3)	72930	MS14-012: Cumulative Security Update for Internet Explorer (2925418)
High (9.3)	73415	MS14-018: Cumulative Security Update for Internet Explorer (2950467)
High (9.3)	73805	MS14-021: Security Update for Internet Explorer (2965111)
High (9.3)	73985	MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732)
High (9.3)	73988	MS14-029: Security Update for Internet Explorer (2962482)

Medium (4.3)	73990	MS KB2871997: Update to Improve Credentials Protection and Management
Medium (4.0)	69334	MS KB2862973: Update for Deprecation of MD5 Hashing Algorithm for Microsoft Root Certificate Program
Medium (4.0)	73992	MS KB2960358: Update for Disabling RC4 in .NET TLS
Low (3.6)	70395	MS KB2532445: AppLocker Rules Bypass
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10396	Microsoft Windows SMB Shares Access
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration

Figura 4.5.10 Vulnerabilidades Servidor de Archivos

Fuente: Chicaiza, D. (2014)

- **Servidor DHCP**



Summary

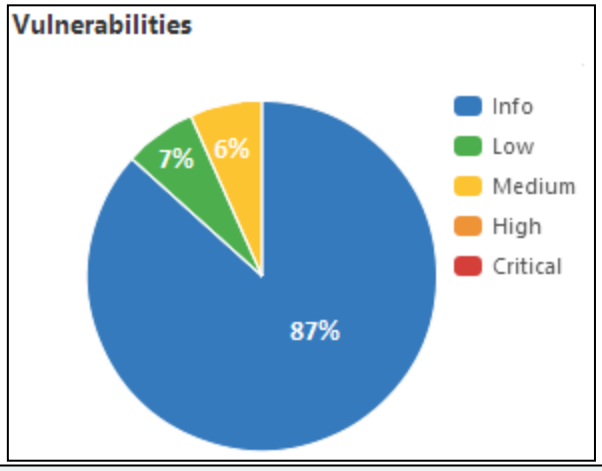
Critical	High	Medium	Low	Info	Total
1	0	0	1	51	53

Severity	Plugin Id	Name
Critical (10.0)	20284	Kaspersky Anti-Virus Detection
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10396	Microsoft Windows SMB Shares Access
Info	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
Info	10399	SMB Use Domain SID to Enumerate Users
Info	10400	Microsoft Windows SMB Registry Remotely Accessible
Info	10456	Microsoft Windows SMB Service Enumeration
Info	10736	DCE Services Enumeration

Figura 4.5.11 Vulnerabilidades Servidor DHCP

Fuente: Chicaiza, D. (2014)

- **Router Core**



Summary					
Critical	High	Medium	Low	Info	Total
0	0	1	1	13	15

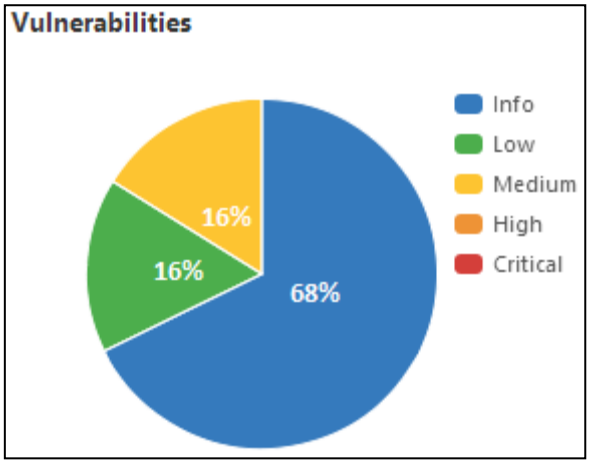
Details

Severity	Plugin Id	Name
Medium (4.0)	10882	SSH Protocol Version 1 Session Key Retrieval
Low (3.2)	50686	IP Forwarding Enabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	10919	Open Port Re-check
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21642	Session Initiation Protocol Detection
Info	22964	Service Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

Figura 4.5.12 Vulnerabilidades Router Core

Fuente: Chicaiza, D. (2014)

- **Switch Core**



Summary

Critical	High	Medium	Low	Info	Total
0	0	5	5	21	31

Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.0)	10882	SSH Protocol Version 1 Session Key Retrieval
Medium (4.0)	35291	SSL Certificate Signed using Weak Hashing Algorithm
Low (3.2)	50686	IP Forwarding Enabled
Low (2.6)	42263	Unencrypted Telnet Server
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11936	OS Identification

Figura 4.5.13 Vulnerabilidades Switch Core

Fuente: Chicaiza, D. (2014)

4.5.1.3 Análisis con Kaspersky Antivirus

Kaspersky Antivirus provee la siguiente información:

- Vulnerabilidades encontradas en el sistema.
- Informe de virus detectados en los dispositivos.

A continuación se presentan las vulnerabilidades y virus encontrados en la red de ANT:

Figura 4.5.14 Informe de Vulnerabilidades Kaspersky Antivirus

Fuente: Chicaiza, D. (2014)

4.5.1.3.1 Resumen de Vulnerabilidades

- **Vulnerabilidades Nivel Crítico**

Crítico	SA53846	Sun Microsystems	Sun Java JRE 1.6.x /
Crítico	SA53846	Sun Microsystems	Sun Java JRE 1.6.x /
Crítico	SA53846	Sun Microsystems	Sun Java JRE 1.6.x /
Crítico	SA53846	Sun Microsystems	Sun Java JRE 1.6.x /
Crítico	SA53846	Sun Microsystems	Sun Java JRE 1.6.x / 6.x
Crítico	SA53846	Sun Microsystems	Sun Java JRE 1.6.x / 6.x
Crítico	SA53846	Sun Microsystems	Sun Java JRE 1.6.x / 6.x
Crítico	SA53953	Mozilla Foundation	Mozilla Firefox
Crítico	SA53953	Mozilla Foundation	Mozilla Firefox
Crítico	SA53953	Mozilla Foundation	Mozilla Firefox
Crítico	SA53953	Mozilla Foundation	Mozilla Firefox 21.x
Crítico	SA53953	Mozilla Foundation	Mozilla Thunderbird 3.1.x
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox 20.x
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox 4.x
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox 8.x
Crítico	SA53970	Mozilla Foundation	Mozilla Firefox 9.x
Crítico	SA54060	Microsoft	Windows 7
Crítico	SA54060	Microsoft	Windows 7
Crítico	SA54060	Microsoft	Windows 7
Crítico	SA54060	Microsoft	Windows 7
Crítico	SA54060	Microsoft	Windows 7
Crítico	SA54060	Microsoft	Windows 8
Crítico	SA54060	Microsoft	Windows 8

Figura 4.5.15 Vulnerabilidades Nivel Crítico - Kaspersky Antivirus

Fuente: Chicaiza, D. (2014)

- ## Vulnerabilidades Nivel Alto

Alta	SA11165	Microsoft	Windows XP
Alta	SA11165	Microsoft	Windows XP
Alta	SA13482	Microsoft	Windows XP
Alta	SA13482	Microsoft	Windows XP
Alta	SA13482	Microsoft	Windows XP
Alta	SA14190	Microsoft	Windows XP
Alta	SA14190	Microsoft	Windows XP
Alta	SA14190	Microsoft	Windows XP
Alta	SA14193	Microsoft	Windows XP
Alta	SA14193	Microsoft	Windows XP
Alta	SA14193	Microsoft	Windows XP
Alta	SA14896	Microsoft	Windows XP
Alta	SA14896	Microsoft	Windows XP
Alta	SA14896	Microsoft	Windows XP
Alta	SA15368	Microsoft	Windows XP
Alta	SA15368	Microsoft	Windows XP
Alta	SA15606	Microsoft	Windows XP
Alta	SA15606	Microsoft	Windows XP
Alta	SA15683	Microsoft	Windows XP
Alta	SA15683	Microsoft	Windows XP
Alta	SA15683	Microsoft	Windows XP

Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 10.x
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 10.x
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 10.x
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 11.0 (x86 es-ES)
Máx.	SA48932	Mozilla Foundation	Mozilla Firefox 11.0 (x86 es-ES)
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 11.0 (x86 es-ES)
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 11.x
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 11.x
Alta	SA48932	Mozilla Foundation	Mozilla Firefox 11.x

Figura 4.5.16 Vulnerabilidades Nivel Alta - Kaspersky Antivirus

Fuente: Chicaiza, D. (2014)

4.5.1.3.2 Informe de Virus

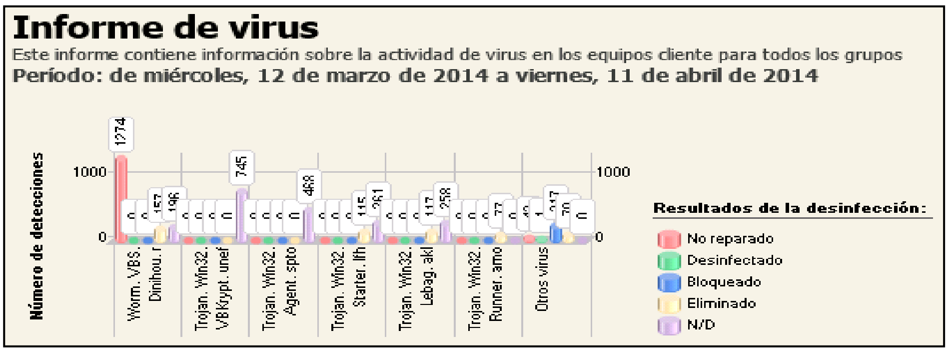


Figura 4.5.17 Resumen de virus red ANT

Fuente: Chicaiza, D. (2014)

- **Análisis de virus Matriz ANT**

Equipos administrados : Red 172.17.04.x - SVR MATRIZ

Objetos diferentes: 23 **Archivos diferentes: 98**

Objeto detectado	Tipo de objeto	Número de detecciones	Archivos diferentes
Backdoor.PHP.PhpShell.dg	Troyano	3	1
EICAR-Test-File	virus	1	1
HEUR:Virus.Acad.Generic	virus	2	2
Net-Worm.Win32.Kido.kz	virus	2	1
PDM:RiskWare.Unsupported.Windows.a	Desconocido	1	1
Trojan.Acad.Dwgun.e	Troyano	1	1
Trojan.Win32.AutoRun.bun	Troyano	1	1
Trojan.Win32.Neurevt.afz	Troyano	2	2
Trojan.Win32.Pasta.keh	Troyano	12	6
Trojan.Win32.Pasta.qzk	Troyano	4	2
Trojan.Win32.Staser.tgg	Troyano	3	3
Trojan.Win32.VBKrypt.uilk	Troyano	1	1
Trojan-Dropper.Win32.Agent.jkcd	Troyano	1	1
Trojan-Dropper.Win32.Injector.jfdz	Troyano	1	1
Trojan-Dropper.Win32.VB.bway	Troyano	1	1
Virus.Acad.Bursted.a	virus	9	9
Virus.Win32.Induc.b	virus	1	1
Virus.Win32.Virut.ce	virus	1	1
Worm.VBS.Dinihou.r	virus	23	23
Worm.Win32.AutoRun.hxw	virus	36	36
Worm.Win32.Debris.a	virus	1	1
Worm.Win32.Debris.b	virus	1	1
Worm.Win32.WBNA.bul	virus	6	1

Figura 4.5.18 Informe de Virus Servidor Matriz ANT

Fuente: Chicaiza, D. (2014)

- **Análisis de virus Oficina de Atención al Usuario Cuenca**

Equipos administrados : Red 172.17.26.x - SRV CUENCA

Objetos diferentes: 5 **Archivos diferentes: 7**

Objeto detectado	Tipo de objeto	Número de detecciones	Archivos diferentes
Backdoor.Win32.Ruskill.vca	Troyano	2	2
Trojan.WinLNK.Runner.ea	Troyano	2	1
Trojan-Downloader.Win32.Dofoil.rpk	Troyano	1	1
Worm.Win32.AutoRun.gcln	virus	1	1
Worm.Win32.Debris.abv	virus	2	2

Figura 4.5.19 Informe de Virus Servidor Cuenca

Fuente: Chicaiza, D. (2014)

- **Análisis de virus Oficina de Atención al Usuario Tulcán**

Equipos administrados : Red 172.17.37.x - SVR TULCAN			
Objetos diferentes: 4		Archivos diferentes: 17	
Objeto detectado	**Tipo de objeto**	**Número de detecciones**	**Archivos diferentes**
Email-Worm.Win32.Runouce.r	virus	2	2
Trojan.WinLNK.Runner.ea	Troyano	13	13
Worm.VBS.Dinihou.o	virus	1	1
Worm.Win32.Debris.abl	virus	1	1

Figura 4.5.20 Informe de Virus Servidor Tulcán

Fuente: Chicaiza, D. (2014)

- **Análisis de virus Oficina de Atención al Usuario Sto. Domingo**

Equipos administrados : Red 172.17.70.x - SVR STO DOMINGO			
Objetos diferentes: 4		Archivos diferentes: 38	
Objeto detectado	**Tipo de objeto**	**Número de detecciones**	**Archivos diferentes**
Backdoor.PHP.Agent.vd	Troyano	1	1
Trojan-Downloader.Win32.Agent.elds	Troyano	2	1
Worm.VBS.Dinihou.b	virus	2	1
Worm.VBS.Dinihou.r	virus	37	35

Figura 4.5.21 Informe de Virus Servidor Santo Domingo

Fuente: Chicaiza, D. (2014)

4.5.1.4 Diagnóstico de la Red

Luego de realizadas las pruebas de diagnóstico a los principales dispositivos, se descubren diferentes deficiencias que dan como resultado potenciales amenazas para la seguridad; es así que entre las potenciales amenazas al sistema se encuentran:

- Puertos TCP / UDP abiertos (backdoors) usados por troyanos.
- Servicios levantados innecesariamente.
- 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 Email Relay and Spam.
- Acceso a los servidores 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, en el caso del Directorio Activo.
- Equipos de escritorio fuera del dominio.
- Estaciones de trabajo y servidores con la base de firmas del antivirus desactualizadas.
- Servidores y equipos de escritorio que tienen el software antivirus deshabilitado, por ende no se realiza el proceso de análisis automático.
- Estaciones de escritorio infectado con software malicioso (virus).
- Software de navegación web con versiones desactualizadas (Firefox, Internet Explorer) lo cual causa que sean vulnerables.

Se encontró que los servidores de DNS, DHCP y Active Directory son únicos. Si por algún motivo se pierde el servicio del servidor DNS la red dejaría de funcionar para la resolución de nombres desde la dirección IP y viceversa. Algo parecido podría suceder si el servidor de control de directorio activo falla.

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 suscitan en los servidores, estas revisiones se realizan solamente cuando se presentan problemas graves.

A continuación se presenta los detalles de algunos troyanos que pueden aprovechas las brechas de seguridad[14]:

- **Troyano backdoor:** Este tipo de troyano habilita un canal de acceso no convencional en el sistema permitiendo que otros malware y/o personas malintencionadas ingresen sin inconvenientes al mismo.

- **Troyano drooper:** Se caracteriza por ejecutar otros códigos maliciosos al momento de su ejecución.

[14] http://www.infospyware.eu/tipos-de-troyanos/

- **Troyano keylogger:** En este caso, el troyano se encarga de monitorear y registrar todo lo que se teclea. Está netamente orientado al robo de información confidencial. Algunos de ellos tienen la capacidad de realizar capturas de pantallas.

- **Troyano bancario:** Se refiere a aquellos que ayudan en la ejecución de ataques de phishing. En muchos casos modifican el contenido del archivo hosts de los sistemas Windows.

- **Troyano downloader:** Estos códigos maliciosos se encargan de descargar otros códigos maliciosos mientras se encuentran activos.

- **Troyano Bot:** La función principal de este tipo de troyanos es convertir una computadora en zombi. Cada una de estas computadoras zombis formará parte de redes botnets.

CAPÍTULO 5

METODOLOGÍA

5.1 DISEÑO DEL SISTEMA DE SEGURIDAD

5.1.1 Selección del Modelo de Seguridad

La carencia de control frente al acceso a Internet y la falta de protección de la información almacenada en los servidores representan los mayores inconvenientes de la red de ANT, problemas que se dan debido a la ausencia de políticas de seguridad y la carencia de tecnología que permitan ejercer un control efectivo; esta situación provoca el uso inadecuado de Internet y debido a la cantidad de información que maneja esta institución y la necesidad de su distribución y disponibilidad hacia las diferentes sucursales, resulta poco práctica la manera como se realiza en la actualidad.

Por lo tanto, es preocupante la situación que enfrentaría esta red ante un desastre que involucre el daño de los principales dispositivos que constituyen el núcleo de la red y la pérdida de información por la modificación no autorizada, intencional o no por parte de usuarios de dicha información.

Se ha considerado para la propuesta de diseño el modelo de seguridad en profundidad (defensa en profundidad) ya que consiste en la implementación de una serie de prácticas que permiten asegurar los sistemas y redes de una organización en diversas capas y su principio se basa en que cada capa al estar asegurada utilizando buenas prácticas, ayudará a mitigar los ataques y reducir el

impulso del ataque conforme este avance en cada una de las capas como se apreció en el literal 2.1.7.1 Modelos de Seguridad (página 49).

- **Asignación de funciones**

El organigrama vigente de la Dirección de Tecnologías de la Información y Comunicaciones de acuerdo al Registro Oficial del 17 de agosto de 2012 es:

Figura 5.1.1 Presencia en el territorio ecuatoriano

Fuente: Chicaiza, D. (2014)

Existe una propuesta de reorganización para ampliar el nivel de detalle y responsabilidad de las 4 áreas funcionales de acuerdo al siguiente organigrama:

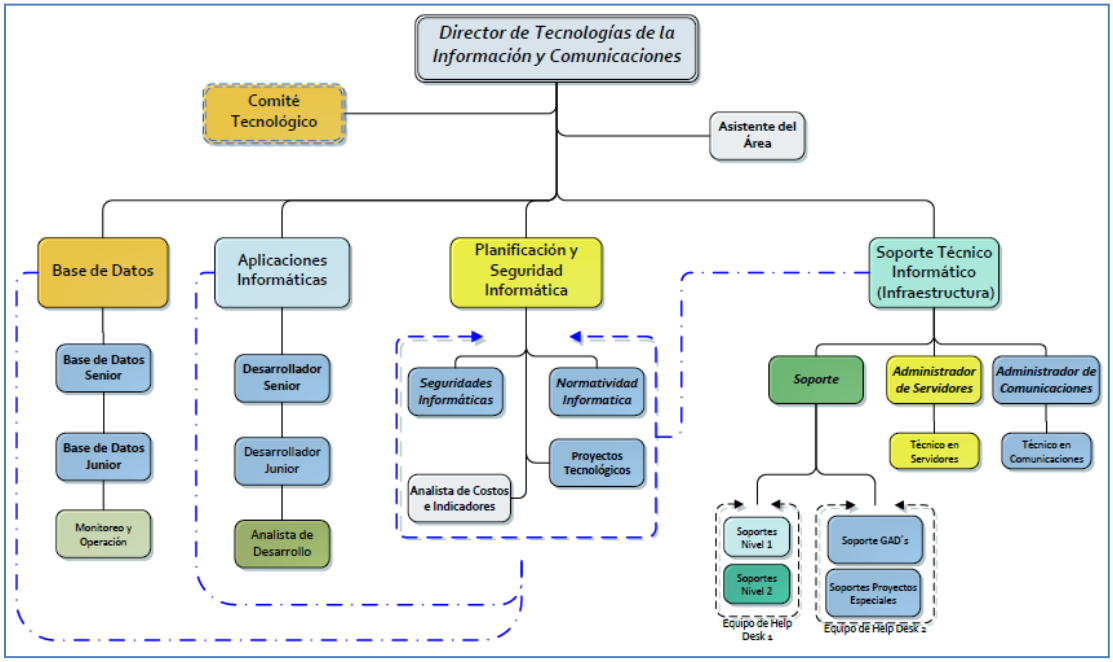


Figura 5.1.2 Estructura Dirección de Tecnologías de la Información

Fuente: Chicaiza, D. (2014)

Es importante que se desarrollen las funciones de seguridad informática para agruparlas en el cargo de Oficial de Seguridad Informática (en inglés CSO).

Entre sus funciones deben estar:

- Definir políticas y facilitar la creación de procedimientos de seguridad.
- Revisar su cumplimiento.
- Realizar análisis de riesgo de seguridad de información (para cada aplicación o nuevo servicio).
- Ser un facilitador del proceso de clasificación de la información.
- Diseñar y actualizar la arquitectura de seguridad.
- Velar por el cumplimiento de las políticas.
- Ayudar en el proceso del plan de continuidad del negocio.

5.1.2 Selección de Tecnología

De acuerdo al análisis de los principales dispositivos de red de la Agencia Nacional de Tránsito (Capítulo 4) se pudo apreciar que existen deficiencias que dan como resultado potenciales amenazas para la seguridad, es así que se ha considerado que la Agencia Nacional de Tránsito necesita incorporar en su red un sistema de seguridad integral que permita realizar una completa gestión de amenazas.

Las redes actuales rebasan las fronteras tradicionales, evolucionan de forma constante y generan nuevos vectores de ataque: dispositivos móviles, aplicaciones para móviles y de Internet, hipervisores, redes sociales, navegadores web y equipos domésticos. Las soluciones que solo actúan en un momento concreto no pueden responder a la infinidad de tecnologías y estrategias que emplean los sujetos malintencionados. [57]

A fin de evitar el aumento en las probabilidades de que se comprometa información de los clientes, propiedad intelectual y otros datos confidenciales debido a la implementación de un conjunto de tecnologías dispares que no se concibieron para funcionar conjuntamente se descarta la implementación de un sistema heterogéneo compuesto por diferentes plataformas tecnológicas y/o basadas en software libre, cada una de ellas enfocada en una parte concreta del problema global como se apreció en el Capítulo 3 (Análisis de Tecnologías de Seguridad Perimetral), este tipo de solución de seguridad perimetral puede resultar costosa y de enorme complejidad de gestión, administración y

mantenimiento. Además el rendimiento de estas soluciones parciales no está dirigido al análisis del tráfico en tiempo real.

Tomando en cuenta las ventajas que ofrecen los sistemas de Gestión Unificada de Amenazas (Capítulo 3 página 158) y considerando que su principal característica es la integración de diferentes módulos de seguridad (capítulo 3 página 153) que garantizan la adecuada protección de la red sin degradar su rendimiento ya que cuentan con hardware y software optimizado para realizar una la completa gestión de amenazas al tiempo que reducen los costos de gestión en vista de que no será necesario administrar varias soluciones parciales de diferentes proveedores, es así que la institución necesita una solución de gestión multi-amenaza que proporcione:

- Cobertura funcional, es decir que combine una amplia gama de medidas, incluidas las que son de prevención (IPS) complementadas a su vez con las que son reactivas, como pueden ser los antivirus.
- Cobertura lógica, es decir que proporcione protección contra amenazas a todos los elementos de la infraestructura del cliente (redes, sistemas, servicios, aplicaciones y datos).
- Cobertura física, no sólo aplicable en los límites/accesos a Internet, sino en lugares a lo largo de la organización.

Es así que se considera la tecnología UTM para el diseño del sistema de seguridad perimetral de la Agencia Nacional de Tránsito.

La implementación de tecnología UTM permitirá contribuir con la disminución del consumo de energía eléctrica, minimizar las emisiones de CO2 y reducir el impacto generado por los excedentes de basura electrónica derivados de la adquisición de otros productos de seguridad no consolidados una vez que hayan cumplido su tiempo de vida útil, esto permitirá cumplir con estándares mínimos de protección ambiental, tecnologías verdes o amigables con el medio ambiente.

5.1.3 Requerimientos del Sistema

A continuación se describen los dispositivos que permitirán cubrir los requerimientos de seguridad y especificaciones técnicas requeridos por la Agencia Nacional de Tránsito:

ITEM	DESCRIPCIÓN	CANTIDAD
1	EQUIPOS DE SEGURIDAD INFORMÁTICA	2
2	EQUIPO DE ANALISIS Y ALMACENAMIENTO DE LOGS	1
3	EQUIPOS DE PROTECCIÓN DE CORREO ELECTRÓNICO	2

Tabla 5.1.1 Cantidad de equipos de Seguridad Perimetral, protección de Correo Electrónico, análisis y almacenamiento de Logs.

Fuente: Chicaiza, D. (2014)

El sistema de seguridad que requiere la Agencia Nacional de Tránsito debe presentar las siguientes características:

- Tecnología UTM línea alta.
- Un dispositivo 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.
- Una plataforma dedicada de seguridad integral de correo electrónico ofreciendo las características de protección (Antispam, antivirus, Antiphising), así como la gestión de cuarentenas y la administración centralizada mediante acceso Web al interfaz de gestión.
- Un sistema analizador y de reporte de red en tiempo real (incluyendo datos de tráfico, eventos, virus, ataque, filtrado de contenidos y filtrado de correo electrónico).

- **Presupuesto**

El presupuesto estimado para el proyecto es de $ 463.000,00 (cuatrocientos sesenta y tres mil con 00/100 dólares americanos) más impuestos.

Descripción	Cantidad	Precio Unitario	Precio Total
DETALLE DE EQUIPOS			
Equipo de Seguridad Informática	2	131.833,45	263.666,90
Equipo de Análisis y Almacenamiento de Logs	1	42.699,00	42.699,00
Equipo de Protección de Correo Electrónico	2	36.731,75	73.463,50
DETALLE DE SERVICIOS			
Servicio de Instalación de Equipos de Seguridad	1	19.500,00	19.500,00
Servicio de Soporte y Mantenimiento	3	12.900,00	38.700,00
Servicio de Capacitación de la Solución	1	24.970,60	24.970,60
		SUBTOTAL	**463.000,00**
		IVA	55.560,00
		TOTAL	**518.560,00**

Tabla 5.1.2 Presupuesto Referencial dispositivo UTM

Fuente: Chicaiza, D. (2014)

5.1.4 Selección de la Marca

Elegir la marca adecuada ayudará de forma significativa la gestión de seguridad de redes. Gartner proporciona cada año a través de su representación gráfica (cuadrante mágico) la situación del mercado de un producto tecnológico en un momento determinado.

Figura 5.1.3 Cuadrante Mágico de Gestión de Amenazas Unificadas

Fuente: Gartner (2013)

A continuación se realiza la comparación de las características de seguridad independientes de los dispositivos UTM de las principales marcas:

Función	SOPHOS UTM	SONICWALL NSA	WATCH GUARD XTM	FORTINET Fortigate	Check Point UTM-1
SEGURIDAD BASICA					
Cortafuegos	X	X	X	X	X
Motores Antivirus Simultáneos e independientes	2	1	1	1	1
Protección integrada de estaciones	X	Limitado	Limitado	X	Limitado
TECNOLOGÍAS DE PROTECCIÓN DE ÚLTIMA GENERACIÓN					
Cortafuegos de aplicaciones web	X			X	X
Control de aplicaciones web	X	X	Modelos más grandes	X	X
Sistema de prevención de intrusiones	X	X	X	X	X
Filtrado de datos HTTPS	X	Limitado	Modelos más grandes	Limitado	
CONEXIÓN DE USUARIOS Y OFICINAS REMOTAS					

VPN IPSec y SSL	X	X	Limitado	X	X
Portal VPN	X				
Redes de malla inalámbrica	X			X	X
Portal de autoservicio para usuarios	X			X	
Protección de oficinas remotas lista para usar (RED)	X			X	
FACILIDAD DE USO E IMPLEMENTACIÓN					
Creación predeterminada de informes, para la revisión diaria del rendimiento	X	X	X	X	X
Clúster activo-activo con equilibrio integrado de cargas	X	X	X	X	X
Cuadrante mágico de Gartner de soluciones de UTM	Líder	Líder	Líder	Líder	Líder
LICENCIAS Y SOPORTE					
Conjunto uniforme de funciones en todos los modelos	X	X	X	X	X
Posibilidad de añadir módulos de licencias adicionales según las necesidades	X	X	X	X	Modelos más grandes
Varias opciones de soporte técnico	X	X	X	X	X

Tabla 5.1.3 Comparación de productos UTM

Fuente: Sophos (2013)

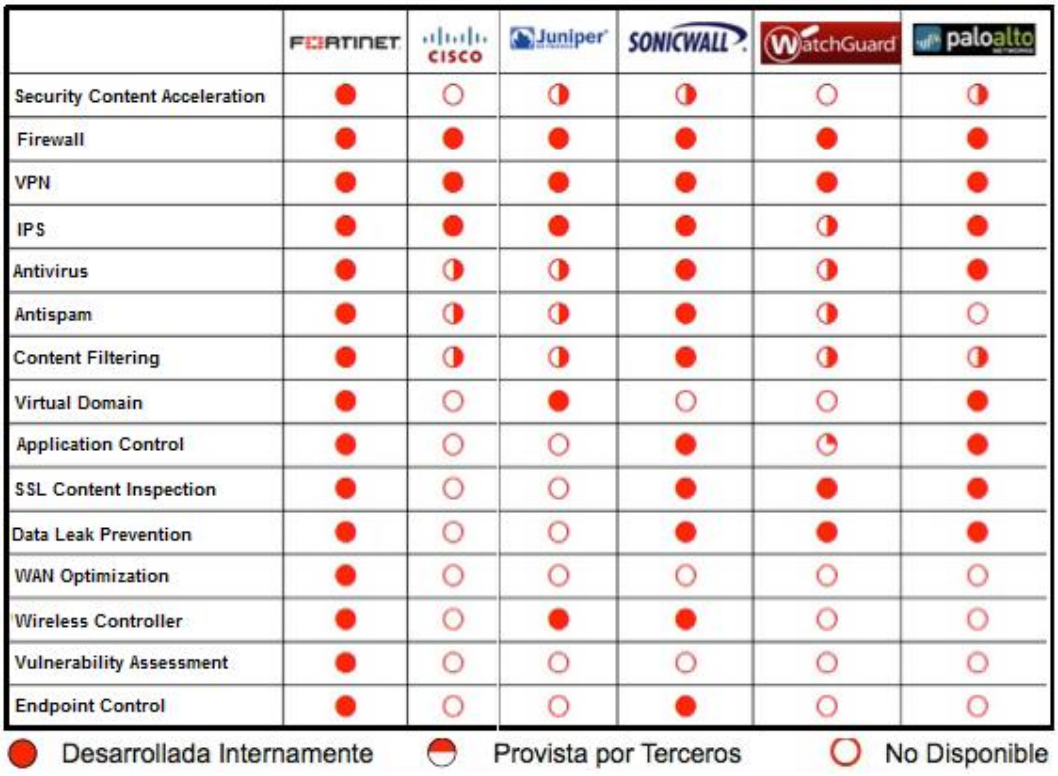


Figura 5.1.4 Comparación funcionalidades de proveedores de dispositivos UTM.

Fuente: Fortinet (2013)

Figura 5.1.5 Comparación Certificaciones de los proveedores dispositivos UTM.

Fuente: Fortinet (2013)

Una vez analizada la información de los cuadros comparativos de los principales proveedores de dispositivos UTM y tomando los resultados del cuadrante mágico de Gartner del año 2013 (Figura 5.1.5 Cuadrante Mágico de

Gestión de Amenazas Unificadas) como un respaldo para la selección de la marca, se aprecia que:

- La tecnología ofrecida por las empresas Juniper, Sonicwall, WatchGuard y Check Point y Palo Alto se presentan como una alternativa de seguridad pero no se consideran en la propuesta debido a que varias funcionalidades son provistas por terceros o simplemente no las ofrecen, por lo tanto son productos de seguridad aislados. (Ver figura 5.4.6 y tabla 5.1.3).

- La tecnología ofrecida por Cisco se presenta como una alternativa de conectividad más que como una alternativa de seguridad; 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 la gestión unificada de amenazas (UTM).
- Se encuentran en el cuadrante de líderes las empresas: Fortinet, Check Point Technologies, Dell, WatchGuard, Sophos, por lo tanto las marcas que no se encuentran en el cuadrante mágico de Gartner no han sido consideradas.

- El actual dispositivo de seguridad de ANT es marca Sophos (Anteriormente llamada Astaro Security Gateway) no cumplió con las expectativas técnicas y debido a los problemas técnicos presentados hasta la presente fecha como se indicó en el capítulo cuatro (descripción de la situación actual de la red) sirven para descartar la marca Sophos debido a la mala experiencia.

- La tecnología ofrecida por la empresa Fortinet se presenta como la más apropiada al momento de hablar de gestión unificada de amenazas, siendo este proveedor el que lidera actualmente el mercado y posicionada por Gartner quinto año en el cuadrante de Líderes en Gestión Unificada de Amenazas.

Por lo tanto se selecciona la marca Fortinet para el diseño del sistema de seguridad perimetral de la Agencia Nacional de Tránsito debido a que Fortinet es el fabricante pionero y líder de soluciones de Seguridad Integral de redes en

tiempo real. Fortinet ofrece una completa gama de productos (software y hardware), servicios de subscripción y soporte que trabajan conjuntamente para proporcionar soluciones de seguridad; sus plataformas de seguridad con aceleración ASIC ofrecen protección multinivel integrando todas las aplicaciones de seguridad esenciales, como firewall, VPN, Antivirus, IDS/IPS, filtrado de contenidos web, antispam y calidad de servicio. [51]

Fortinet dispone del más completo portafolio de seguridad, tanto integral de redes como específica de aplicaciones (correo electrónico, bases de datos, etc.) que satisfacen los requerimientos más exigentes con funcionalidades líderes en el mercado y con el mayor de los rendimientos, es así que ofrece a sus clientes (Ver el Anexo 3 para tener mayor detalle de las funcionalidades):

5.1.4.1 Equipamiento de alto rendimiento

Los equipos de seguridad Fortinet constituyen una nueva generación de equipos de seguridad de muy alto rendimiento que garantizan la protección completa de nuestros sistemas en tiempo real. [51]

Las plataformas de seguridad FortiGate, líderes del mercado UTM, proveen una solución integrada de seguridad compuesta por las funcionalidades más necesarias para tener una protección completa de nuestras comunicaciones como son: Firewall, VPN (IPSEC y SSL), Antivirus, Sistemas de Detección/Prevención de Intrusiones, Filtrado Web, Antispam, Anti-Spyware, Control de Aplicaciones, Inspección de Contenido en SSL etc. Además, todas las funcionalidades de seguridad se integran de forma conjunta con funcionalidades añadidas como Traffic Shaping, Alta Disponibilidad, Balanceo de carga, Aceleración WAN, Enrutamiento dinámico. [51]

El gran abanico de equipos FortiGate existente permite diseñar soluciones adaptadas a las diferentes necesidades de cada entorno, disponiendo en todos ellos de las mismas funcionalidades gracias a la homogeneidad del Sistema Operativo FortiOS, que es similar en todos los equipos FortiGate, independientemente de la gama a la que pertenezcan. [51]

Los equipos FortiGate pueden considerarse como equipos todo en uno, configurados para proporcionar todo el conjunto de funcionalidades de seguridad disponibles en el mercado de una forma sencilla, pero también pueden ser considerados como un appliance de seguridad especializado en una o varias de las funcionalidades de las que dispone, obteniendo un equipo de alto rendimiento y prestaciones sin competencia. [51]

La familia de equipos Fortinet se extiende con equipos que complementan las funcionalidades de los equipos FortiGate:

- La plataforma FortiManager, que permite la gestión, administración, configuración y actualización de firmas desde un único punto centralizado de miles de equipos FortiGate que estén distribuidos en nuestro entorno de comunicaciones.
- Los equipos FortiAnalyzer, que nos proveen de una potente herramienta de gestión y análisis de logs, generación periódica y automatizada de informes configurables por el administrador, así como herramientas complementarias de análisis forense, análisis de vulnerabilidades, scanning de red y correlación de eventos.
- FortiMail, que proporciona una plataforma de seguridad de correo con equipos que pueden actuar como servidor de correo puro, como MTA (Relay de correo) o en modo transparente (Proxy SMTP transparente). Proporcionando las técnicas necesarias para garantizar la completa seguridad del correo electrónico.
- El software FortiClient, como completo agente de seguridad para el puesto de usuario, dotado de las funcionalidades de Firewall, Antivirus, AntiSpam, Web Filter, siendo cliente VPN IPSec para el establecimiento de túneles con los equipos FortiGate, y siendo posible su administración centralizada desde una plataforma FortiManager.

5.1.4.2 Servicios Fortinet

Fortinet ofrece de forma conjunta con su equipamiento servicios profesionales que garantizan el soporte, la actualización y el correcto mantenimiento de los niveles de servicio demandados. [51]

Gracias a los equipos técnicos distribuidos a lo largo de todo el mundo, Fortinet es capaz de ofrecer soporte internacional con cobertura 24x7x365, actualizando en tiempo real las bases de datos de firmas de antivirus e IDS/IPS y los motores de estas aplicaciones, así como actualizando de forma continuada las bases de datos en las que se apoyan los servicios Fortiguard Web Filtering y Fortiguard AntiSpam. [51]

El Servicio FortiProtect Distribution Network (FDN) se encarga de la distribución de estas actualizaciones a lo largo de todo el mundo, existiendo el compromiso con aquellos clientes que contratan el servicio FortiProtect Premier Services de disponer de la firma correspondiente a cualquier nuevo ataque en menos de 3 horas. [51]

Por otra parte, los equipos de soporte y desarrollo velan de forma continua para dar respuesta a los servicios FortiCare de mantenimiento hardware, actualizaciones y desarrollo de nuevas versiones de firmware, y soporte vía telefónica o email. Los centros de soporte y desarrollo están distribuidos por todo el mundo, si bien todos cuentan con un servicio 24x7, garantizándose de este modo que el soporte siempre se ofrece a nuestros clientes desde el punto más cercano regionalmente. [51]

Además, Fortinet cuenta con Ingenieros de Sistemas en cada una de sus más de 40 oficinas repartidas a lo largo de todo el mundo, lo que le permite ser capaz de prestar asistencia técnica in situ en los países más importantes, apoyándose en sus partners certificados para cubrir el resto del mundo. [51]

Figura 5.1.6 Mapa de localización de la red Fortiprotect Distribution Network (FDN).
Fuente: Fortinet (2013)

5.1.4.3 Reconocimiento de la industria.

Gracias al constante foco en seguridad, la continua inversión en investigación y la calidad de los productos, la tecnología Fortinet es reconocida por los más altos estándares del mundo de la seguridad y ha sido capaz de conseguir las más prestigiosas certificaciones independientes del mercado en cada una de las funcionalidades de seguridad que implementa. [51]

Entre las certificaciones conseguidas destacan:

- NSS: Certificación UTM
- ICSA: 6 certificaciones ICSA. Para cada funcionalidad y en varios productos
- Common Criteria EAL-4+: Certificación como equipo de comunicaciones seguras.
- Virus Bulletin: Certificación para FortiClient como Antivirus de puesto de trabajo.
- AV comparatives: Calificando el motor de antivirus en la categoría Advanced.

Destacan también la obtención de varios premios en revistas especializadas de la industria que reconocen la calidad de los productos Fortinet en cada una de sus múltiples funcionalidades de forma independiente. [51]

5.2 DEFENSA DE LA RED

Los equipos de seguridad perimetral (Fortigate y FortiAnalyzer) serán instalados en el edificio matriz de ANT y estarán configurados para trabajar en clúster de alta disponibilidad y las funcionalidades activas son:

a) Alta Disponibilidad (HA)

Esta funcionalidad permitirá suplir las falencias del equipamiento de seguridad actual, la mayor parte de problemas en la red de ANT se han ocasionado por no contar con equipamiento de backup que permitan configurar un sistema de alta disponibilidad.

La capacidad de trabajar en clúster de alta disponibilidad dota a los equipos de redundancia ante fallos. Además el clúster puede configurarse en modo activo-activo haciendo balanceo de carga del tráfico o en modo activo/pasivo en la que un único equipo procesa el tráfico de la red y es monitorizado por los demás para sustituirle en caso de caída.

b) Modalidad Router o Transparente

Uno de los principales problemas de la red de ANT es la exposición de su red interna, por lo que se requiere que el dispositivo permita controlar el tráfico que va entre la red interna (privada) y la red externa (Internet), adicionalmente la red interna permanecerá oculta al configurar Traducción de Dirección de Red.

Los equipos deben poseer la capacidad de trabajar en dos modalidades diferentes de funcionamiento: modo Router/NAT o modo Transparente.

- **Modo Router (NAT):** Trabajando en modo router el equipo actúa como un dispositivo de nivel 3, enrutando los paquetes entre los diferentes interfaces físicos y/o lógicos del equipo, con la capacidad de realizar NAT.

- **Modo Transparente:** Trabajando en modo transparente el equipo se comporta como un bridge, dejando pasar los paquetes a través el mismo en función de las políticas definidas. El equipo no tiene direcciones IP en sus interfaces (solamente posee una IP para su administración y actualización). De este modo, el equipo puede ser introducido en cualquier punto de la red sin necesidad de realizar ninguna modificación sobre ningún otro dispositivo.

c) Autenticación de Usuarios

Uno de los principales problemas detectados es la existencia de cuentas habilitadas que no se encuentran en uso y el acceso a ciertos servicios mediante cuentas predeterminadas y con perfil de uso privilegiado. Por lo que se requiere que la plataforma soporte la autenticación de usuarios.

Esta autenticación puede realizarse contra una base de datos local creada en el propio equipo, o bien contra el servidor de Active Directory, pudiendo realizarse con este último una autenticación transparente de los usuarios del dominio de ANT.

d) Firewall

Debido a la cantidad de puertos TCP/UDP y servicios levantados innecesariamente en los dispositivos de red de ANT se requiere que los equipos obligatoriamente posean la funcionalidad de firewall, esto permitirá clasificar, controlar y gestionar el tráfico generado por las aplicaciones y los datos que pasan a través de la red.

El firewall deberá contar con las siguientes funcionalidades:

- **Políticas de Firewall:** Deberá permitir establecer políticas de firewall en base a los criterios de:
  - Interfaces de entrada y salida del flujo.
  - Direcciones o grupos de direcciones IP origen y destino.
  - Protocolo, servicio o puertos TCP/UDP.

La política definirá la acción a tomar con aquellos paquetes que cumplan los criterios definidos. Entre las acciones a realizar deberán estar:

- Permitir la conexión.
- Denegar la conexión.
- Requerir autenticación antes de permitir la conexión.
- Procesar el paquete como perteneciente a una conexión tunelizada mediante IPSec.
- Realizar traducción de direcciones.
- Aplicar reglas de gestión de ancho de banda.
- Analizar el tráfico mediante funcionalidades adicionales de seguridad, como Antivirus, AntiSpam, Detección/Prevención de Intrusiones, filtrado Web, etc. mediante la definición de un perfil de protección.

A cada política se le podrá definir un horario, tanto único como recursivo, que permite acotar la aplicación de la regla a un espacio temporal determinado en función de la hora, el día de la semana, mes o año.

- **Inspección SSL**

Dentro del perfil de protección se podrá aplicar la configuración necesaria para poder efectuar inspección dentro de protocolos seguros basados en SSL, como HTTPS, SMTPS, POP3S e IMAPS.

De esta forma será posible aplicar túneles SSL que atraviesen la plataforma inspección de contenidos.

- **Calidad de Servicio (QoS)**

Mediante la aplicación de técnicas de Calidad de Servicio la red provee un servicio prioritario sobre el tráfico más sensible al retardo o bien limitar el ancho de banda de aquellas aplicaciones que hagan un uso intensivo de los recursos de la red. Una adecuada gestión de la calidad de servicio nos permitirá la utilización de aplicaciones sin recurrir a una ampliación innecesaria del ancho de banda, reservando el ancho de banda necesario y priorizando este tipo de tráfico ante otros menos sensibles al retardo como pueda ser el correo o el tráfico ftp.

e) Red Privada Virtual (VPN)

Esta funcionalidad solventará el problema de conexión con terceros y usuarios internos que necesiten movilidad y acceso a los recursos de red ya que permite realizar autenticación de usuarios locales en el equipo y realizar conexiones cifradas al poder utilizar los protocolos de tunelización (IPSec, SSL, PPTP y L2TP) analizados en el capítulo 3, de esta forma, las sucursales y empleados que se encuentran fuera de la red de ANT podrán establecer comunicaciones privadas sobre redes públicas garantizando la confidencialidad e integridad de los datos trasmitidos por Internet.

Adicionalmente el tráfico VPN puede ser analizado por el módulo Firewall así como por las funcionalidades adicionales (antivirus, IPS, web filtering, antispam).

f) Antivirus

Dentro de los problemas detectados en la red de ANT son estaciones de trabajo y servidores infectados con software malicioso (virus), con la base de firmas de antivirus desactualizadas lo cual causa que en la red exista la proliferación de código malicioso.

La solución deberá contar con sistema antivirus perimetral para detectar la existencia de un archivo infectado en una transmisión, el archivo será eliminado o guardado en cuarentena, y podrá ser sustituido por un mensaje de alerta configurable por el administrador. Para una protección extra, el motor antivirus deberá ser capaz de bloquear ficheros de un tipo específico (.bat, .exe, etc) que potencialmente sean contenedores de virus, o bien bloquear aquellos archivos adjuntos de correo electrónico que sean de un tamaño superior al límite de filtrado.

El filtrado antivirus deberá proteger la navegación web (protocolo http), la transferencia de archivos (protocolo ftp) y los contenidos transmitidos por correo electrónico (protocolos IMAP, POP3 y SMTP), siendo posible escanear estos protocolos en puertos diferentes a los habitualmente empleados, e incluso en múltiples puertos.

g) Detección y Prevención de Intrusión (IDS/IPS)

A pesar de las vulnerabilidades encontradas durante el análisis de la red, ANT no ha sido víctima de intrusiones pero existen servicios mal configurados en los servidores de ANT posibilitando el uso no autorizado y exponiendo la red, por lo que la funcionalidad IPS/IDS permitirá detectar y prevenir los siguientes tipos de ataques:

- Ataques de Denegación de Servicio (DoS).
- Ataques de Reconocimiento.
- Exploits.
- Ataques de Evasión.
- Anomalías estadísticas de tráfico TCP, UDP e ICMP, como son:
    - Flooding: Si el número de sesiones apunta a un solo destino en un segundo está sobre el umbral, el destino está experimentando flooding.
    - Scan: Si el número de sesiones desde un origen único en un segundo está sobre el umbral, el origen está siendo escaneado.
    - Source: Si el número de sesiones concurrentes desde un único destino está sobre los umbrales, el límite de sesiones por origen está siendo alcanzado.
    - Destination session limit: Si el número de sesiones concurrentes a un único destino está sobre el umbral, el límite de sesiones por destino está siendo alcanzado.

h) Control de Aplicaciones y Filtrado de Tráfico Web

Los módulos de filtrado de contenido y filtrado web permitirán realizar un control efectivo, estos módulos controlarán aplicaciones evasivas o que cambien de puerto con frecuencia ya que actualmente personal de ANT hace evasión del control ya que el equipamiento actual no controla de manera adecuada la navegación y utilización de aplicaciones que causan el excesivo uso de ancho de banda.

En la actualidad hay infinidad de aplicaciones que fluyen por la red, siendo algunas de ellas productivas y otras no. Con el control de aplicaciones es posible verificar el tráfico basándose en las propias aplicaciones que lo generan y no en el puerto utilizado.

i) AntiSpam

Uno de los principales problemas de ANT es la recepción diaria de spam, el equipamiento antispam permitirá realizar el análisis en tiempo real del correo electrónico para los protocolos SMTP, POP3 e IMAP gracias al análisis y comparación con servidores externos y con servicios de listas negras.

Se podrán aplicar filtros antispam a los mensajes de correo y basar su control por origen del mensaje y por el contenido del mismo.

j) Prevención de Fuga de Información

La característica de Prevención de Fuga de Información o DLP (Data Leak Prevention) ofrece la posibilidad de evitar que la información categorizada como sensible o confidencial salga fuera de la organización a través de la plataforma.

Es posible llevar a cabo esta protección en diferentes protocolos de transferencia de datos utilizados usualmente, como smtp, ftp o http, con reglas o grupos de reglas predefinidas, un buen ejemplo es una de ellas que inspecciona en busca de números de tarjetas de crédito, o reglas totalmente personalizables.

k) Gestión de los Equipos

Los equipos podrán ser gestionados localmente mediante acceso http, https, telnet o SSH, siendo estos accesos configurables por interfaz, además se deberá poder definir diferentes perfiles de administración con objeto de limitar las tareas y posibilidades de cada usuario con acceso al equipo.

l) Registro de Logs

Los equipos deberán contar con la capacidad de registro de eventos, tráfico y aplicaciones y podrá ser habilitada tanto a nivel global como en cada una de las políticas definidas a nivel de firewall.

Estos registros podrán ser almacenados localmente o bien en un servidor externo como pueden ser un syslog o la plataforma propia.

m) Registro centralizado y gestión de informes

Se deberá contar con una plataforma dedicada al registro centralizado de logs y la gestión y tratamiento de los mismos detallando los eventos registrados a nivel de Firewall, ataques, virus, VPN, utilización web, análisis forense, etc.

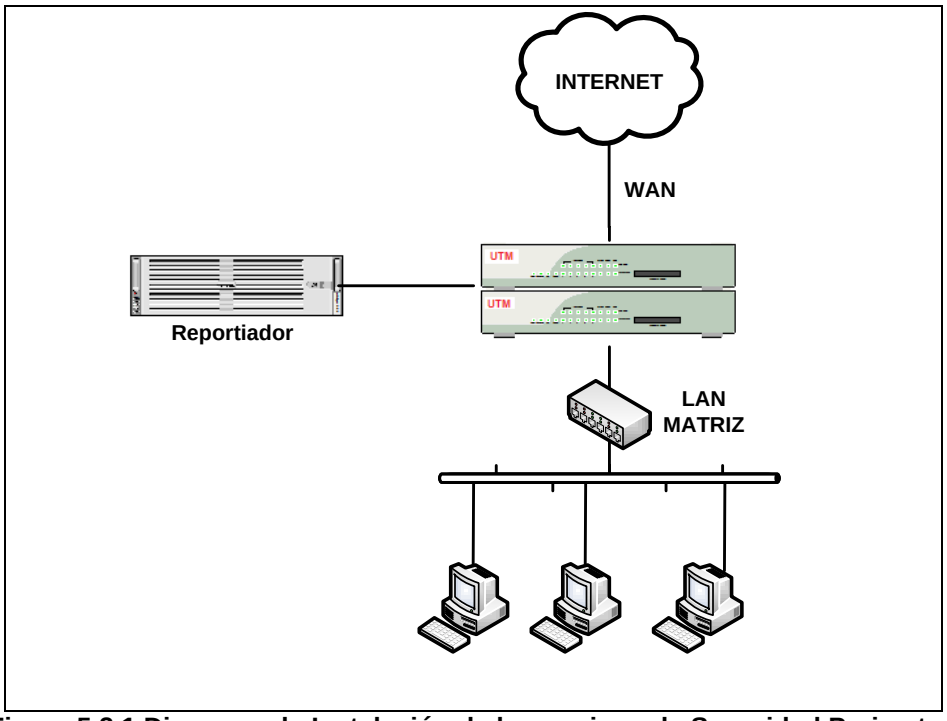


Figura 5.2.1 Diagrama de Instalación de los equipos de Seguridad Perimetral (Reportiador y Seguridad Informática)

Fuente: Chicaiza, D. (2014)

5.3 DEFENSA DEL CLIENTE

Como se apreció en el capítulo cuatro (descripción de la situación actual de la red) los equipos de escritorio cuentan con un nivel de seguridad medio, por lo que es necesario complementar con:

- Contar con un sistema operativo original así como paras las soluciones ofimáticas en uso. El contar con un sistema operativo original garantiza el funcionamiento de hardware, software, periféricos y servicios que se

necesitan con total seguridad y permite contar con servicio técnico de ser necesario.

- Desactivar algunos servicios de Windows ya que no son necesarios y consumen recursos de la computadora. Ejemplos de ellos son: Windows Search (WSearch), Archivos sin conexión (CscService), entre otros.
- Instalar navegadores web confiables y mantenerlos con las versiones más actuales que ofrezca el proveedor.
- Realizar respaldos frecuente a los archivos y al estado de sistema.
- Actualmente se permite la utilización de dispositivos personales, por lo tanto se debe especificar qué dispositivos están permitidos.
- Activar el firewall del sistema operativo.
- Agregar todos los dispositivos de la institución al dominio, esto permitirá controlar el acceso a los mismos y mantener las políticas actualizadas.
- Instalar el software antivirus, mantenerlo activado y actualizado.
- La implementación de dispositivos UTM permitirá mejorar la seguridad de los host al utilizar los siguientes módulos:
    - Autenticación de usuarios permitirá llevar un mejor del acceso a los servicios ya la autenticación puede realizarse contra una base de datos local creada en el propio equipo, o bien contra el servidor de Active Directory.
    - VPN, la utilización de redes privadas virtuales solventará el problema de conexión de los usuarios internos que necesitan movilidad pero requieren de recursos de red de la institución ya que permite realizar autenticación de usuarios locales en el equipo y realizar conexiones cifradas al poder utilizar los protocolos de tunelización.
    - Antivirus, este permitirá detectar y bloquear ficheros de un tipo específico (.bat, .exe, etc) que potencialmente sean contenedores de virus, o bien bloquear aquellos archivos adjuntos de correo electrónico que sean de un tamaño superior al límite de filtrado.
    - Control de Aplicaciones y Filtrado de Tráfico Web, estos módulos ayudaran con el control de aplicaciones evasivas ya que actualmente personal de ANT hace evasión del control y se tiene excesivo uso de ancho de banda.

- Prevención de Fuga de Información, este módulo ofrecerá la posibilidad de evitar que la información categorizada como sensible o confidencial salga fuera de la organización a través de la plataforma.

5.4 DEFENSA DEL SERVIDOR

A fin de estar preparados para enfrentar las diferentes amenazas de seguridad es necesario realizar varias adquisiciones para mejorar la capacidad de la red y la disponibilidad de los servicios, a continuación se describe los requerimientos de la red LAN, WAN y servidores:

5.4.1 LAN (Edificio matriz)

Es indispensable contar con respaldo de los principales dispositivos y medios de transmisión a fin de que las comunicaciones no se vean afectadas ante posibles incidentes:

- Adquirir un switch core de las mismas características del equipamiento actual.
- Instalar el backbone de fibra óptica desde los cuartos de distribución hacia el cuarto de comunicación principal, con la finalidad que se pueda activar contingencia automática.

En la figura 5.4.1 se aprecia la topología de red que permitiría contar con respaldo de los principales dispositivos de comunicación y medios de transmisión.

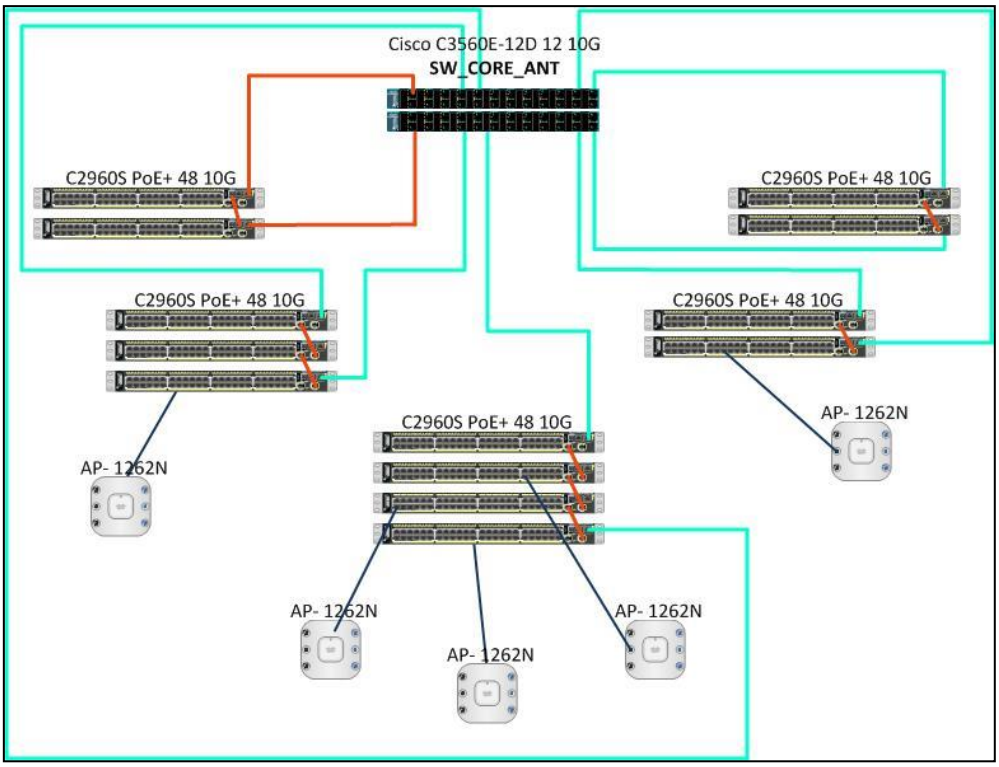


Figura 5.4.1 Diseño LAN Redundante - Edificio matriz

Fuente: Chicaiza, D. (2014)

Como se describió en el capítulo cuatro, los equipos de comunicaciones cuentan con un nivel de seguridad aceptable pero es necesario complementar dicha seguridad, para lo cual se sugiere los siguientes procesos que recomienda el fabricante[15]:

- Documentar la red mediante esquemas de los enlaces de datos, Internet, redes locales, ubicación de dispositivos.
- Actualización de la versión de sistemas operativos a la última versión estable ofrecida por el fabricante.
- Limitar el número de intentos de login.
- Bloquear la recuperación de password (no service password-recovery), al utilizar el comando debemos recordar almacenar una copia de la configuración de cada dispositivo, así como un registro de los password usados y guardarlos en un lugar seguro, ya que no habrá posibilidad de recuperar los password si son perdidos.
- Debemos desactivar los servicios de TCP o UDP que no estén en uso, tales como:

[15] http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

- echo (port number 7)
- discard (port number 9)
- daytime (port number 13)
- chargen (port number 19)
- Adicionalmente los servicios no usados como: Finger, BOOTP, DHCP, MOP, DNS, http server, service config, lldp, etc.

- Limitar el tiempo que una sesión de administración está activa: Usar keepalives para mantener sesiones de TCP activas, y cuando el extremo remoto no esté disponible la sesión sea terminada, evitando que haya un hueco de seguridad.

5.4.2 WAN (Enlaces)

Es necesario realizar una serie de trabajos e inversiones para mejorar la calidad de gestión de las redes WAN, es crítico que se realicen con la finalidad de que sea posible que el conjunto de aplicaciones de ANT tengan apropiados tiempos de respuesta.

- Solicitar a CNT la revisión de modelos, versiones de IOS, capacidades y configuraciones de los ruteadores que se están instalando para atender los requerimientos de ANT.
- Solicitar a CNT que priorice los tráficos en los ruteadores por la aplicación de configuraciones que utilicen Calidad de Servicio (QoS).
- Afinar los Acuerdos de Nivel de Servicio (SLA) con CNT. Actualmente se cuenta con un SLA que garantiza una disponibilidad del 99,6% para los servicios de datos e internet que no cuentan con backup.
- De ser posible contratar otro proveedor de servicios para enlaces de contingencia a los puntos críticos a fin de contar con un mayor porcentaje de disponibilidad.

5.4.3 Equipos Servidores

Como se apreció en el capítulo cuatro (descripción de la situación actual de la red) es necesario adquirir un nuevo chasis IBM Blade Server H para mejorar la disponibilidad de los servidores. Actualmente en el chasis mencionado se

ejecutan 14 servidores virtuales y 6 servidores físicos, por lo que un daño en una cuchilla y peor aún el chasis mismo, afectaría el despacho de servicios informáticos. Es urgente instalar equipos para contingencia de servicios DNS, DHCP, Mail y Active Directory.

Existe un nivel intermedio de seguridad implementada en los servidores de ANT, pero es necesario complementar dicha seguridad, por lo tanto se sugiere instalar los equipos de protección de correo electrónico y el actual dispositivo de seguridad (Astaro Security Gateway) en el centro de datos de CNT E.P.

Re utilizar el módulo Firewall del dispositivo Astaro Security Gateway para controlar el flujo de datos desde las Oficinas de Atención al Usuario, Matriz de ANT y demás dependencias que mantienen una conexión con la red LAN de servidores que se encuentran en el centro de datos de CNT. El dispositivo Astaro cuenta con una suite de herramientas denominada Astaro Network Security que incluye funciones totalmente integradas como: firewall, IDS/IPS, VPN y un sistema de protección contra intrusiones y denegaciones de servicio.

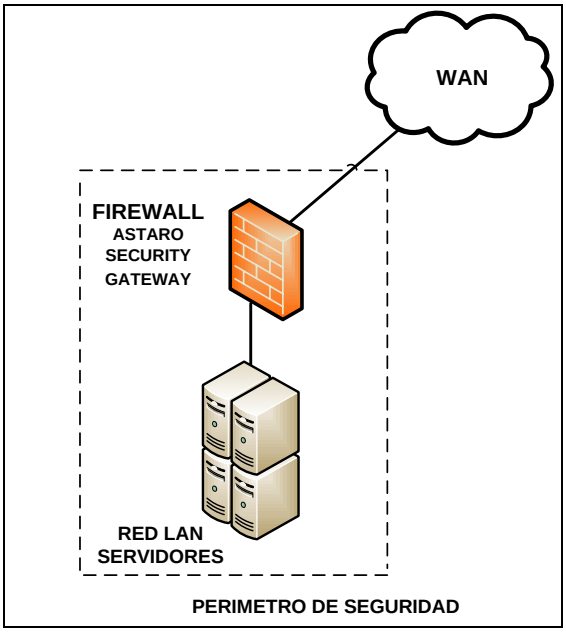


Figura 5.4.2 Diagrama de Instalación de Astaro Security Gateway

Fuente: Chicaiza, D. (2014)

Astaro Security Gateway estará configurado para trabajar de la siguiente manera:

- Modo Transparente, ya que no se realizará NAT.

- Filtrado de paquetes:
    - Por protocolo utilizado (TCP, UDP, ICMP, etc.).
    - Por direcciones fuente y destino.
- Monitoreo de la actividad de la red.

El dispositivo de protección de correo electrónico estará configurado para trabajar de la siguiente manera:

- Cluster de alta disponibilidad.
- Modo Gateway, así se comportará como un sistema securizado de relay SMTP, llevando a cabo las labores de inspección del correo en busca de ataques dirigidos contra el servidor de correo, así como la inspección antivirus y antispam y las labores de enrutamiento de correo necesarias cubiertas por un sistema con un muy elevado rendimiento.
- Protección Antispam:
    - Protección contra correo entrante y saliente.
    - Protección a nivel de conexión IP.
    - Protección y análisis a nivel de aplicación SMTP.
    - Inspección total de cabeceras.
    - Listas blancas/negras por usuario o globales.
- Gestión de Antivirus y Antispam por usuario mediante atributos de LDAP o por políticas.
- Protección ante denegaciones de servicio o ataques:
    - Protección Anti Mail Bombing.
    - Protección antiphising.
    - Recipient Address Attack.
    - Bounce Attack.
    - Email Rate Limiting.
    - Reverse DNS Check para Anti-Spoofing.
- Almacenamiento basado en políticas de correos entrantes o salientes con posibilidad de backup a un sistema de almacenamiento remoto.
- Generador de notificaciones diarias sobre cuarentenas.

- Soporte y gestión de colas de correo.

Adicionalmente es necesario realizar en los servidores las siguientes tareas:

- Reducir el ámbito de ataque, es necesario quitar o deshabilitar todas las aplicaciones o servicios innecesarios para minimizar las vías desde las que atacante podría aprovechar el sistema de forma malintencionada.
- Aplicar actualizaciones de seguridad de los sistemas operativos.
- Instalar software antivirus y mantener habilitado el software en todos los equipos.
- Realizar pruebas con un escáner de vulnerabilidades periódicamente para garantizar que no aparecen puntos débiles para la seguridad.
- Restringir aplicaciones no autorizadas.
- Gestión periódica de parches.
- Manejar políticas de auditoría, esto implica auditar inicios de sesión, auditar cambios de políticas y auditar acceso a los equipos.
- Limitar el acceso a sistemas de ficheros, esto evita el robo de credenciales (lectura) y el uso de exploits y backdoors (escritura/ejecución).
- Deshabilitar la ejecución automática (Autorun).
- Prohibir la instalación de drivers no firmados.
- Activar el firewall de los sistemas operativos.
- Realizar el borrado periódico del historial de comandos.
- Realizar copias de seguridad frecuentemente y comprobar dichas copias de seguridad para asegurarse de que se pueden restaurar correctamente.
- Manejar el inicio de sesión único para los usuarios finales.
- Establecer de manera formal los procedimientos para instalación y configuración de servidores (MS Windows y Unix/Linux).
- Adquirir licenciamiento de sistemas operativos para los servidores.
- Para precautelar la información es necesario depurar las cuentas creadas en el servidor de dominio. Se encontraron 1,546 cuentas creadas, de las cuales 493 están deshabilitadas, 51 son administradores, 196 nunca han ingresado al dominio, 24 no han ingresado desde el año 2011, 157 no han ingresado desde el año 2012, y quedan 625 que están activas y sin inconvenientes.

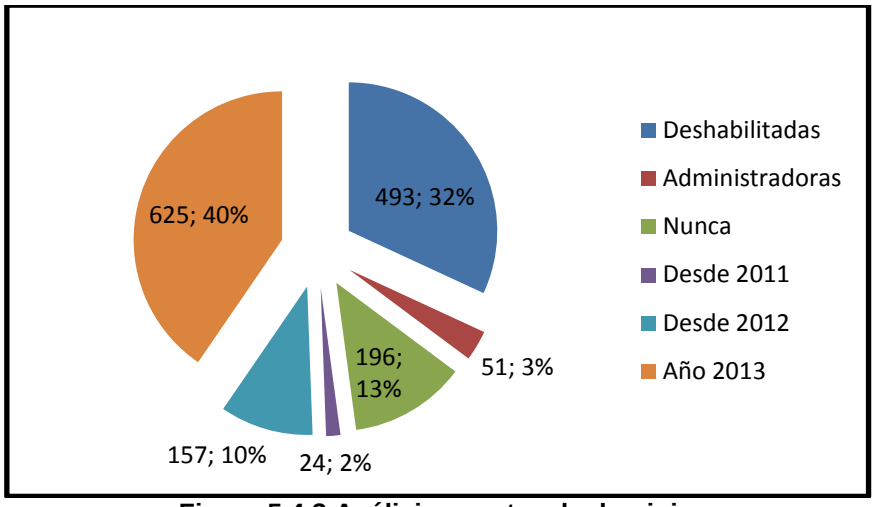
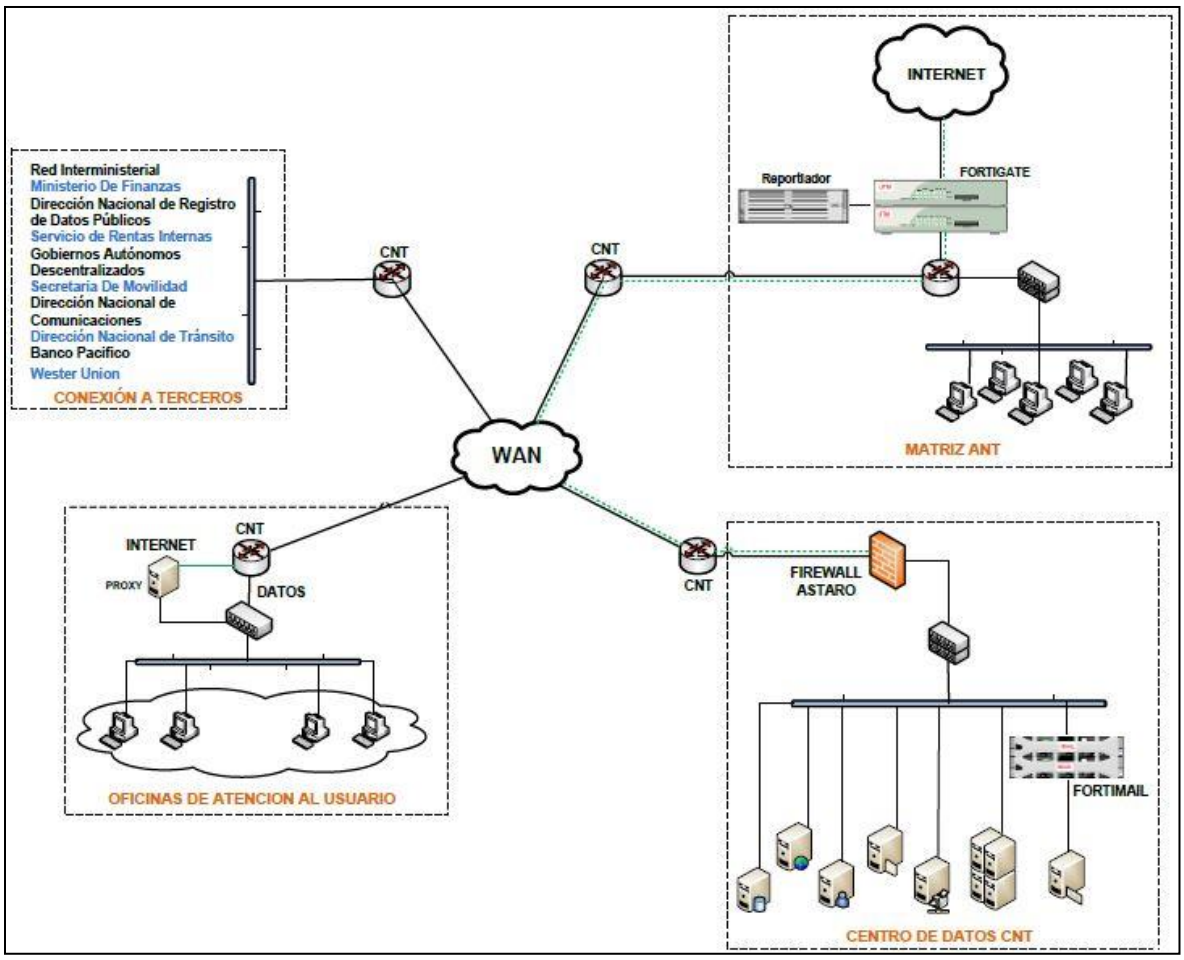


Figura 5.4.3 Análisis cuentas de dominio

Fuente: Chicaiza, D. (2014)

A continuación se muestra el esquema de red que se desea implementar para brindar seguridad configurado para trabajar de la siguiente manera:



5.4.4 Diagrama de Instalación de los equipos de Seguridad Perimetral ANT

Fuente: Chicaiza, D. (2014)

5.4.1 LAN (Sucursales)

Como se pudo observar en el capítulo cuatro, existe una falencia en el equipamiento switch de las agencias debido a que se encuentran obsoletos, por lo tanto es necesaria la adquisición de nuevo equipamiento que permita:

- Manejar segmentación (VLAN).
- Administración remota por protocolo SSH.
- Monitoreo por protocolo SNMP.
- Puertos FastEthernet y Gigabith Ethernet de acuerdo a la cantidad de dispositivos finales.
- Manejo de POE.

Es necesario utilizar el diseño jerárquico de red (capa de núcleo, distribución y acceso), pero debido a la baja cantidad de usuarios se considera que el equipamiento de la capa de acceso es suficiente para ofrecer los recursos más utilizados por los usuarios.

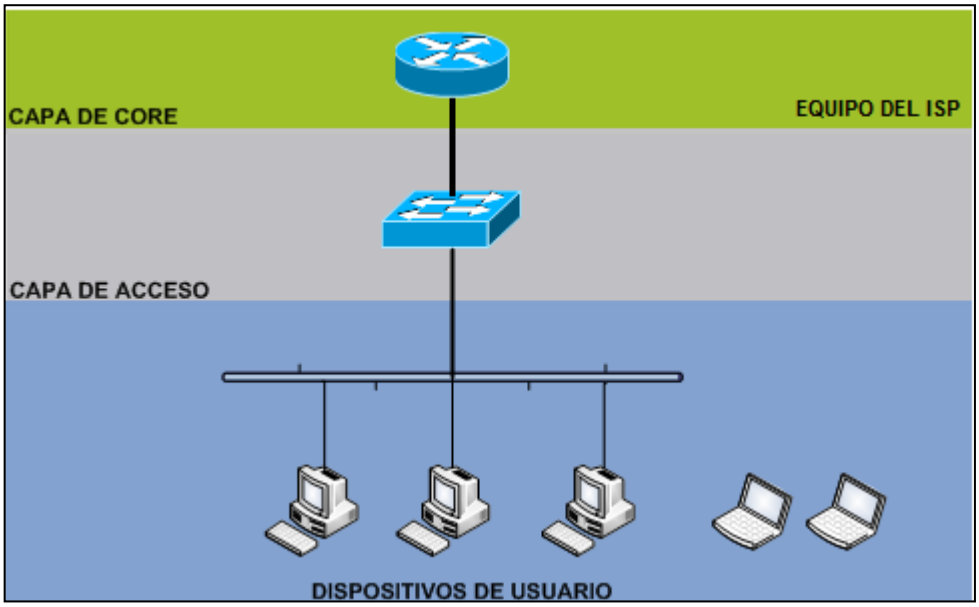


Figura 5.4.5 Arquitectura de RED Sucursales ANT

Fuente: Chicaiza, D. (2014)

La seguridad de los equipos de comunicación deberá cumplir con los normas mínimas implementadas en la matriz y estar basadas en las buenas prácticas que proporciona el proceso de fortalecimiento.

Adicionalmente, es necesaria la estandarización del sistema de cableado horizontal de acuerdo a las características del sistema Cableado Horizontal utilizado en la matriz, es decir que cumple con:

- Par trenzado con blindaje (STP).
- Categoría 6A.
- 2 salidas (datos, voz) por área de trabajo.
- Etiquetas en los patch panel y salidas de área de trabajo.
- No tener puentes, derivaciones y empalmes a lo largo de todo el trayecto del cableado.
- No supera la máxima longitud permitida (100m = 90 m + 3 m usuario + 7 m patch pannel).

La seguridad de las estaciones de trabajo de las agencias cumple los mismos estándares que en el edificio matriz pero se debe garantizar que:

- Todas las estaciones de trabajo se encuentren dentro del dominio, esto permitirá controlar el acceso a los mismos y mantener las políticas actualizadas.
- Autenticación de usuarios en las estaciones de trabajo a través del ingreso del usuario y contraseña otorgado por el Directorio Activo de la Institución.
- Todas las máquinas deberán contar con asignación de IP estática.
- Instalar el software antivirus, mantenerlo activado y actualizado.
- Deshabilitar la ejecución automática (Autorun).
- Restringir aplicaciones no autorizadas.
- Quitar o deshabilitar todas las aplicaciones innecesarias para minimizar las vías desde las que atacante podría aprovechar el sistema de forma malintencionada.
- Aplicar actualizaciones de seguridad de los sistemas operativos.
- Activar el firewall del sistema operativo.

5.5 DIRECTIVAS, PROCEDIMIENTOS Y CONCIENCIACIÓN

Las políticas de seguridad constituyen una herramienta para hacer frente a futuros problemas, fallos de sistemas, imprevistos o posibles ataques

informáticos. Sin embargo, se puede incurrir en una falsa sensación de seguridad si las políticas de seguridad no se han implantado correctamente en toda la organización.

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.

5.5.1 Objetivos.

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.

Los beneficios directos de implantar políticas de seguridad son:

- Administración de riesgos.
- Asegurar la continuidad del negocio.
- Definición de responsabilidades, expectativas y comportamientos aceptables.
- Asegurar la integridad y confidencialidad de la información.

5.5.2 Justificación.

Las políticas de seguridad permitirán cubrir los requerimientos de seguridad y ayudaran a evitar pérdidas económicas, degradación del prestigio de la institución y brindar un mejor servicio a la ciudadanía. Además son necesarias para brindar protección adecuada al activo informático más importante de la institución, la información.

Debido a la naturaleza de la organización, los principales aspectos o elementos de seguridad a considerarse son:

- **Disponibilidad:** Que los servicios de ANT estén disponibles para su uso en todo momento en que sean necesarios, de modo que se satisfaga las necesidades de los usuarios (internos y externos).
- **Confidencialidad:** Que los servicios de ANT sean accesibles únicamente a los usuarios autorizados.
- **Capacidad:** Que provea a los usuarios herramientas para hacer eficiente y eficaz su trabajo, con flexibilidad para adaptarse a las necesidades cambiantes del día a día.

5.5.3 Alcance.

La creación de políticas y desarrollo de procedimientos permitirá cumplir con la normativa establecida por la Secretaría Nacional de la Administración Pública para la Gestión de Seguridad de la Información a través del Segundo Suplemento del Registro Oficial No. 88 Acuerdo 166 del 25 de septiembre de 2013.

5.5.4 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 (Director Ejecutivo y Directores Departamentales), ya que es vital contar con su apoyo para establecer medidas preventivas y de recuperación para el sistema.

- Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información en conjunto con la Dirección de Tecnologías de la Información (Director y Personal Técnico), ya que es el organismo encargado de llevar a cabo el procedimiento de investigación, desarrollo, implementación y control de las políticas de seguridad.

- Personal de la institución en general, ya que son los responsables del acatamiento (conocimiento, aceptación, predisposición y ejecución) de las normas de seguridad en lo que respecta a la correcta utilización de los recursos TI; 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.

5.5.5 Políticas de Seguridad

5.5.5.1 Control de acceso

- **Identificación.**

1. Es necesario formalizar el procedimiento que actualmente se realiza de forma empírica para la activación de una cuenta (acceso). Este procedimiento requiere la entrega del formulario denominado “Solicitud de Creación de Usuarios de Acceso a Red” en el cual se debe proporcionar la siguiente información:

   - Nombres y Apellidos completos.
   - Cédula de Identidad.
   - Grupo de usuarios al que pertenece.
   - Cargo que desempeña.
   - Fecha de creación de cuenta.
   - Horario en el que necesita el acceso.
   - Autorizaciones y accesos requeridos.
   - Departamento al que pertenece.

   El formulario debe ser escrito con letra legible y/o a computadora y deberá contar con la firma del funcionario, Jefe de Área y del Responsable de la Dirección de Tecnologías encargado de la cración.

Agencia Nacional de Tránsito	SOLICITUD DE CREACIÓN DE USUARIOS DE ACCESO A RED	GT-ST-FOR-001-2011 Versión: 1.0

INGRESO	ADICION	ELIMINACION	BLOQUEO	RE-ASIGNACION	FECHA
X					

NOMBRES Y APELLIDOS DEL SOLICITANTE	CEDULA	CARGO

EDIFICIO/No. DE PISO	DIRECCION	DEPARTAMENTO
	Av. Mariscal Sucre y Jorge Sánchez	

LOGIN	PERIODICIDAD (<30 DIAS)	VALIDO HASTA DIA	VALIDO HASTA MES	VALIDO HASTA AÑO	IDENTIFICACION PC

DIAS	HORARIO DESDE	HORARIO HASTA	ROL	SISTEMA
T/D			Otorgado por el Active Directory	
L - V				

USUARIO	COORDINADOR o JEFE DE AREA	GESTION TECNOLOGICA
Nombre:	Nombre:	Nombre:
Fecha:	Fecha:	Fecha: 03/06/2014

NOTA: Llenar con letra imprenta.
El usuario declara conocer las políticas y normas del uso de los recursos informáticos y acepta sus responsabilidades por el uso correcto o incorrecto de las claves a él asignadas. Las claves de usuario son confidenciales y personales.

Figura 5.5.1 Formulario de Creación de Usuario de Red

Fuente: Chicaiza, D. (2014)

2. Es necesario tener la comunicación formal mediante documento escrito o correo electrónico por parte de la Dirección de Talento Humano, 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.
3. La desactivación de una cuenta requiere la entrega del formulario de cierre de cuentas; este documento debe contener la siguiente información:
    - Nombres y Apellidos completos.
    - Fecha de anulación de cuenta.
    - Plazos para la separación del funcionario.

Agencia Nacional de Tránsito

REGISTRO PARA CIERRE DE APLICATIVOS Y RESPALDOS

DTIC-CR-FOR-001
Revisión 2
22/10/2012

1. DATOS DEL FUNCIONARIO SALIENTE

Nombres:		Apellidos:		Cédula N°:	
Provincia:		Agencia / Área:			
Cargo/ Función:		Fecha de Salida:			

2. DATOS DE FUNCIONARIO SUPERIOR / JEFE DE AREA

Nombres:		Apellidos:		Cédula N°:	
Agencia		Área:			

3. CONTROL PARA CIERRE DEAPLICATIVOS
(SELECCIONAR APLICATIVOS A LOS QUE TENÍA ACCESO.)

Aplicativos	Fecha de Aplicación/ Verificación	Observaciones/ Usuario Asignado	Sumilla
☐ *Correo Electrónico*			
☐ *Red Institucional*			
☐ *Sistema Quipux*			
☐ *Intranet Institucional*			
☐ *Sistema Sitcon*			
☐ *Sistema Axis*			
☐ *Sistema Esigef*			
☐ *Sistema Silo*			
☐ *Sistema Rol de Pagos*			
☐ *Otro Aplicativo*			

4. INFORMACIÓN DEL RESPALDO
(LLENAR EN CASO DE DEJAR RESPALDOS EN FORMATO DIGITAL)

Fecha de Notificación TH		Fecha de Respaldo	
Persona Encargada del Respaldo		Sumilla:	
Tipo de Equipo Respaldado	☐ *Desktop* ☐ *Pórtatil* ☐ *Servidor* ☐ *Otro*		
Tamaño del Respaldo (Mb o Gb)		Medio Respaldado	☐ *CD* ☐ *DVD* ☐ *Disco Externo* ☐ *Red* ☐ *Otro (Especificar)*
Funcionamiento del Respaldo	☐ *SI* ☐ *NO*	CUSTODIO DEL RESPALDO (Nombres, Apellidos y Dependencia)	

Figura 5.5.2 Formulario de Cierre de Aplicativos

Fuente: Chicaiza, D. (2014)

- **Cuenta y contraseña.**

El establecimiento de cuentas y contraseñas debe seguir las siguientes reglas y características:

1. La institución debe manejar un convenio de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos en orden y completos. Se adjunta el formato para el Convenio de Confidencialidad (Anexo 1).
2. La contraseña del usuario debe seguir las siguientes normas y recomendaciones:

    - Debe contener al menos 8 caracteres.

- Se recomienda utilizar dígitos, letras y caracteres especiales.
- Tiempo de expiración 3 meses como máximo.
- En lo posible no debe estar formada por información característica del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento, organización o cargo.
- Bloquear al usuario luego de cinco intentos de ingreso de contraseña fallidos.
- El usuario puede modificar su contraseña pero con notificación al administrador.
- Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios.
- No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad o de acceso público.

3. Se debe forzar el cambio de contraseña en el primer inicio de sesión.
4. Es necesario generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información.
5. Se debe mantener un registro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.

5.5.5.2 Seguridad Física

1. Es necesario realizar mantenimiento de los equipos, para lo cual se debe contemplar:
   - Mantenimientos periódicos.
   - Considerar las especificaciones y recomendaciones del proveedor.
   - Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.
   - Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.
2. Es necesario asegurar los equipos fuera de las instalaciones, se debe tomar en cuenta los siguientes aspectos:

- Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución.
- Establecer una cobertura adecuada del seguro, para proteger los equipos que se encuentran fuera de las instalaciones.
- Tener autorización previa para el retiro de cualquier equipo, información o software.
- Identificar a los empleados, contratistas y usuarios de terceras partes, que tienen la autorización para el retiro de activos de la institución.
- Registrar cuando el equipo o activo sea retirado y cuando sea devuelto.

5.5.5.3 Gestión de los incidentes de la seguridad de la información.

1. Es necesario llevar un reporte sobre los eventos de seguridad de la información, estos deberán contemplar:
    - Un punto de contacto (Oficial de Seguridad de la Información) para el reporte de los eventos de seguridad.
    - Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden:
        - Identificar el incidente.
        - Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.
        - Notificar al Oficial de Seguridad de la Información de la institución.
        - Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
        - Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
        - Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de

que el incidente ocurra, recreando el incidente para identificar sus posibles causas.

- Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes.
- Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.
- Resolver y restaurar el servicio afectado por el incidente debido a la paralización de un equipo o sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.
- Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a Resuelto. Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.

5.5.5.4 Conexiones externas

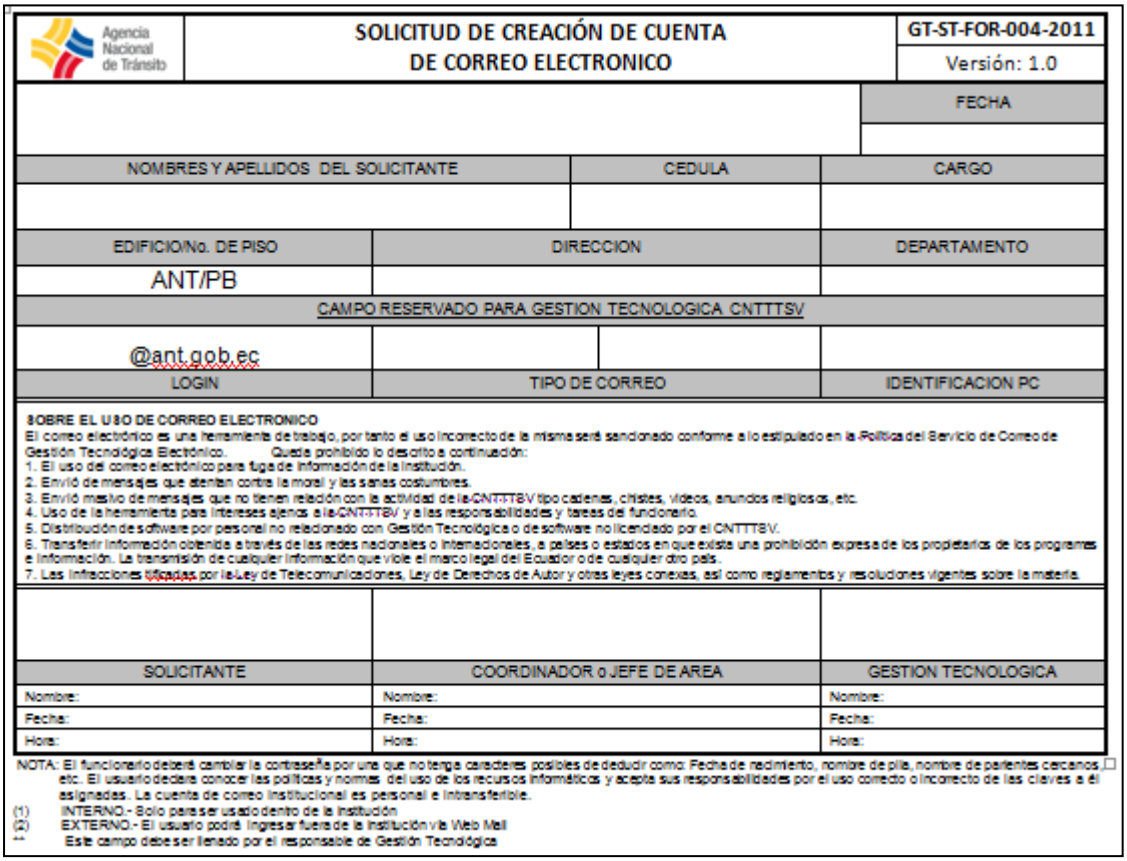
1. Las conexiones que vienen desde redes públicas (Internet y sucursales) deben estar bajo un estricto monitoreo y control de las actividades, es necesario utilizar métodos de encriptación para proteger los datos que se trasmiten por las conexiones remotas.

2. Establecimiento del servicio de Internet bajo explícita solicitud del Director de cada departamento, es responsabilidad de cada funcionario:
   - Utilizar el recurso para propósitos institucionales.
   - No descargar ni instalar software ajeno a la organización o sin el consentimiento y supervisión del personal encargado de los asuntos TI.
   - No utilizar el recurso para actividades de entretenimiento como descargas (música, video), juegos, chat, navegación improductiva y demás actividades que no corresponden al trabajo operacional.
3. Es necesario concienciar a los funcionarios sobre la funcionalidad, riesgos y medidas de seguridad que se deben adoptar para el uso correcto y eficiente de internet.

4. Es indispensable mantener 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 transitan por la red, además este dispositivo debe brindar capacidades de filtrado (paquetes y web) para facilitar el análisis de los eventos suscitados.
    - Prohibir el acceso a sitios y ejecución de aplicaciones que no se encuentre autorizado de acuerdo al perfil de navegación de cada funcionario.

5.5.5.5 Correo electrónico

1. La Creación de cuenta de correo electrónico se realizará bajo petición formal a través del formulario denominado “solicitud de Creación de Cuenta de Correo Electrónico”.



Agencia Nacional de Tránsito	SOLICITUD DE CREACIÓN DE CUENTA DE CORREO ELECTRONICO	GT-ST-FOR-004-2011 Versión: 1.0

		FECHA

NOMBRES Y APELLIDOS DEL SOLICITANTE	CEDULA	CARGO

EDIFICIO/No. DE PISO	DIRECCION	DEPARTAMENTO
ANT/PB		

CAMPO RESERVADO PARA GESTION TECNOLOGICA CNTTTSV		
@ant.gob.ec		
LOGIN	TIPO DE CORREO	IDENTIFICACION PC

SOBRE EL USO DE CORREO ELECTRONICO
El correo electrónico es una herramienta de trabajo, por tanto el uso incorrecto de la misma será sancionado conforme a lo estipulado en la Política del Servicio de Correo de Gestión Tecnológica Electrónico. Queda prohibido lo descrito a continuación:
1. El uso del correo electrónico para fuga de información de la institución.
2. Envió de mensajes que atenten contra la moral y las sanas costumbres.
3. Envió masivo de mensajes que no tienen relación con la actividad de la CNTTTSV tipo cadenas, chistes, videos, anuncios religiosos, etc.
4. Uso de la herramienta para intereses ajenos a la CNTTTSV y a las responsabilidades y tareas del funcionario.
5. Distribución de software por personal no relacionado con Gestión Tecnológica o de software no licenciado por el CNTTTSV.
6. Transferir información obtenida a través de las redes nacionales o internacionales, a países o estados en que exista una prohibición expresa de los propietarios de los programas e información. La transmisión de cualquier información que viole el marco legal del Ecuador o de cualquier otro país.
7. Las infracciones tipificadas por la Ley de Telecomunicaciones, Ley de Derechos de Autor y otras leyes conexas, así como reglamentos y resoluciones vigentes sobre la materia.

SOLICITANTE	COORDINADOR o JEFE DE AREA	GESTION TECNOLOGICA
Nombre:	Nombre:	Nombre:
Fecha:	Fecha:	Fecha:
Hora:	Hora:	Hora:

NOTA: El funcionario deberá cambiar la contraseña por una que no tenga caracteres posibles de deducir como: Fecha de nacimiento, nombre de pila, nombre de parientes cercanos, etc. El usuario declara conocer las políticas y normas del uso de los recursos informáticos y acepta sus responsabilidades por el uso correcto o incorrecto de las claves a él asignadas. La cuenta de correo institucional es personal e intransferible.
(1) INTERNO.- Solo para ser usado dentro de la institución
(2) EXTERNO.- El usuario podrá ingresar fuera de la institución vía Web Mail
** Este campo debe ser llenado por el responsable de Gestión Tecnológica

Figura 5.5.3 Solicitud de Creación de Cuenta de Correo Electrónico

Fuente: Chicaiza, D. (2014)

- El correo electrónico es una herramienta de trabajo, por tanto el uso incorrecto de la misma será sancionado conforme a lo estipulado en la Política del Servicio de Correo Electrónico. Queda prohibido lo descrito a continuación:
- El uso del correo electrónico para fuga de información de la institución.
- Envió de mensajes que atentan contra la moral y las sanas costumbres.
- Envió masivo de mensajes que no tienen relación con la actividad de la ANT tipo cadenas, chistes, videos, anuncios religiosos, etc.
- Uso de la herramienta para intereses ajenos a la ANT y a las responsabilidades y tareas del funcionario.

2. Es indispensable fomentar el reconocimiento de los mensajes de correo electrónico empresarial como documentos formales.
3. A fin de optimizar la capacidad de almacenamiento se debe asignar a cada cuenta de correo una capacidad de almacenamiento fija (100 MB) y establecer la reasignación de capacidad bajo petición formal.

5.5.5.6 Antivirus

1. Es indispensable la implementación del mecanismo de protección en todos los dispositivos de la red.
2. Permitir que el mecanismo de actualización sea automático.
3. Se debe analizar de forma automática al conectar los dispositivos USB en los computadores de la institución.
4. Se debe realizar la ejecución obligatoria de un escaneo periódico al sistema de forma automática.
5. Es necesario concienciar al personal de la institución acerca del problema de los virus y cómo proceder frente a los mismos.
6. Ante la presencia de un virus en el sistema se deberá proceder de la siguiente manera:
    - Dar notificación al departamento de sistemas.
    - No ejecutar el archivo que contiene al virus.

5.5.5.7 Seguridad de Aplicaciones

1. Es indispensable la separación de las instancias de Desarrollo, Pruebas y Producción.
    - Se debe controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada por el administrador de red.
    - Se requiere implantar ambientes de prueba, iguales en capacidad, a los ambientes de producción.
    - El acceso al entorno de producción, se debe realizar únicamente en caso de extrema necesidad, con la autorización explícita correspondiente.
2. Es necesario la gestión de los cambios en los servicios ofrecidos por terceros.
    - Se debe coordinar el proceso de cambio cuando se necesita realizar cambios o mejoras a las redes y uso de nuevas tecnologías en los servicios ofrecidos por terceros.
    - Se debe coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por terceros.

5.6 SEGURIDAD FÍSICA

La Agencia Nacional de Tránsito posee una protección física aceptable, ya que cuenta con vigilancia las 24 horas, zonas de acceso restringidas y protegidas por llave. Sin embargo, se podría complementar la seguridad con la adquisición de un sistema de video seguridad IP para el edificio matriz a fin de contar con un esquema de monitoreo y administración centralizado.

El vídeo IP, a menudo conocido como vigilancia IP para determinadas aplicaciones en el ámbito de la vigilancia en seguridad y la monitorización remota, es un sistema que ofrece a los usuarios la posibilidad de controlar y grabar en vídeo a través de una red IP (LAN/WAN/Internet). [48]

El vídeo IP puede utilizarse en un número ilimitado de situaciones; no obstante, la mayoría de aplicaciones se incluyen en una de las dos categorías siguientes:

- **Vigilancia y seguridad**

La avanzada funcionalidad del vídeo IP lo convierte en un medio muy adecuado para las aplicaciones relacionadas con la vídeo vigilancia y seguridad. La flexibilidad de la tecnología digital permite al personal de seguridad proteger mejor a las personas, las propiedades y los bienes. Por tanto, dichos sistemas constituyen una opción especialmente interesante para las instituciones que requieren proteger sus instalaciones. [48]

- **Monitorización remota**

El vídeo IP permite a los usuarios la posibilidad de reunir información en todos los puntos clave de una operación y visualizarla en tiempo real, lo que la convierte en la tecnología perfecta para la monitorización remota y local de equipos, personas y lugares. [48]

Figura 5.6.1 Sistema de Video Seguridad IP

Fuente: AXIS (2013)

Este diagrama muestra un sistema de video IP, donde la información del video se transmite de forma continua a través de una red IP, utilizando cámaras IP. Los sistemas de vídeo IP incorporan funciones de grabación y usan discos duros convencionales para el almacenamiento de las imágenes. Hay dos

beneficios principales derivados de esta circunstancia. Por una parte que la información esté almacenada en formato digital supone que es mucho más rápida y sencilla su localización usando mecanismos de búsqueda avanzados y, por otra parte, que el almacenamiento se realiza a través de la red y por tanto no es imprescindible que se lleve a cabo allí donde esté el sistema sino que por razones de seguridad o conveniencia estas grabaciones se pueden llevar a cabo en lugares remotos.

- **Gestión de video**

La calidad de las cámaras IP depende directamente de la selección y configuración de los sistemas de gestión de vídeo que las controlan. Los sistemas deberán permitir a los usuarios controlar, analizar y almacenar eficazmente la salida de vídeo. Los sistemas que se basan en una plataforma de vídeo IP resultan adecuados para la integración en otros sistemas tales como el control de acceso o la gestión de edificios, y la información de esos sistemas puede ser utilizada para activar funciones en el sistema de vídeo IP, como por ejemplo, almacenar imágenes relativas a eventos. [49]

- **Plataformas de hardware**

Existen las plataformas de grabación de vídeo en red (NVR), un NVR se presenta como una caja de hardware con la funcionalidad de gestión de vídeo pre instalada. Por definición, está dedicado a tareas específicas de grabación, análisis y reproducción de vídeo IP. El NVR no permite que ninguna otra aplicación se conecte a éste. El propio hardware de NVR se bloquea con esta aplicación y la unidad en raras ocasiones puede modificarse para alojar algún componente fuera de su especificación original. [49]

Un NVR es un verdadero sistema digital que recibe imágenes digitales y transmisiones de vídeo a través de la red y las graba en un disco duro en un formato digital. Un NVR no dispone de un monitor y un teclado exclusivos. Toda la visualización y gestión del NVR tiene lugar de forma remota a través de la red. [49]

5.6.1 Diseño del Sistema

La Agencia Nacional de Tránsito presta sus servicios a la ciudadanía en general de la provincia de Pichincha atendiendo en las oficinas del edificio matriz. El edificio de ANT está construido en hormigón, gypsum con cubierta de estructura de hierro y consta de tres plantas:

- **Planta Baja:** Información, Comedor, Archivo Nacional, Dirección Ejecutiva, Comunicación Social, Dirección Administrativa Financiera.
- **Primera Planta:** Atención al Usuario, Oficinas Administrativas, Dirección de Tecnologías.
- **Segunda Planta:** Sin utilizar.

Estas plantas se encuentran conectadas entre sí por gradas eléctricas, gradas normales y por el ascensor; existen espacios de parqueo en los sectores Norte (Funcionarios) y Sur (Público General) del edificio.

Su zona perimetral está constituida por una reja en la parte frontal y lateral, en este sector es donde se ubican las entradas (vehicular y peatonal) para el público en general.

Figura 5.6.2 Reja frontal y lateral edificio matriz ANT

Fuente: Chicaiza, D. (2014)

5.6.2 Determinación de las zonas a vigilar

Para nuestro estudio dividiremos al edificio en zonas:

- Zona 1: PB lado sur.
- Zona 2: PB lado norte.
- Zona 3: Primera Planta lado norte.
- Zona 4: Primera Planta lado sur.
- Zona 5: Perímetro.

La distribución eficaz de los puntos de video vigilancia se establecerán en base a:

- Valorización del material y equipo en cada dependencia.
- Cantidad de tráfico en cada zona.
- Nivel de seguridad existente.

- **Zona 1 (PB lado sur)**

En esta zona están ubicadas las oficinas de Comunicación social, Dirección Ejecutiva, Dirección Administrativa Financiera y Bodega. Se estima un bajo tráfico de personas. El nivel de seguridad es óptimo, se realiza el control de entrada y salida con la presencia de guardias de seguridad en el único corredor de acceso a dichas oficinas. Adicionalmente las oficinas de Dirección Ejecutiva cuentan con la presencia de dos guardias de seguridad.

El principal riesgo radica en la posible sustracción de equipos de las oficinas. Para obtener un óptimo nivel de vigilancia se establecerán 3 puntos de video vigilancia.

Figura 5.6.3 Guardias de Seguridad corredor PB Sur
Fuente: Chicaiza, D. (2014)

- **Zona 2: PB lado norte:**

En esta zona se destaca la puerta de ingreso del público, se cuenta con el counter de información con 6 puestos de trabajo, el área para entrega de documentación del archivo nacional, por lo tanto se estima una alta circulación de personas.

Figura 5.6.4 Guardias de Seguridad Atención al Usuario

Fuente: Chicaiza, D. (2014)

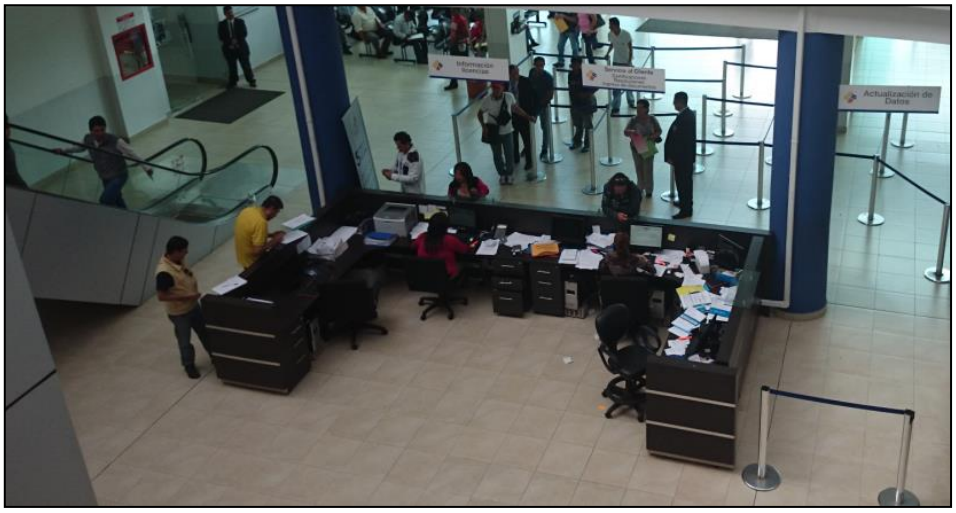


Figura 5.6.5 Guardias de Seguridad Atención al Usuario

Fuente: Chicaiza, D. (2014)

El nivel de seguridad es alto ya que se dispone de 3 guardias distribuidos de la siguiente manera: 1 en el counter de información, 1 en la puerta de ingreso, 1 en el área de entrega de documentación. Los riesgos en este caso radicarían en la continua circulación de personas y la posible infiltración de elementos

indeseables por el cerramiento en especial en la noche. Para solventar estos problemas se establecerán 3 puntos de video vigilancia.

- **Zona 3: Primera Planta lado norte:**

En esta zona se destacan los corredores de acceso a las oficinas de Planificación y Desarrollo, Talento Humano, Dirección de Tecnologías de la Información, Dirección Provincial de Pichincha, se estima una baja circulación de personas.

Figura 5.6.6 Acceso corredor 1 Norte Primer Planta

Fuente: Chicaiza, D. (2014)

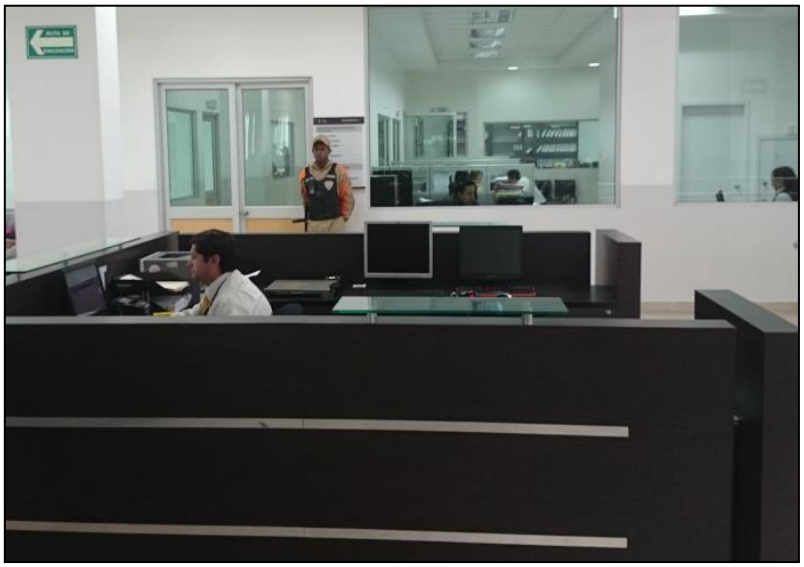


Figura 5.6.7 Acceso corredor 2 Norte Primer Planta

Fuente: Chicaiza, D. (2014)

El nivel de seguridad es medio ya que se dispone de 2 guardias distribuidos en cada corredor de acceso. Los riesgos en este caso radicarían en la sustracción de equipos de las oficinas. Para solventar estos problemas se establecerán 2 puntos de video vigilancia.

- **Zona 4: Primera Planta lado sur:**

En esta se encuentra el acceso principal para el acceso del público en general y se constituye en el principal nexo entre las oficinas de Atención al Usuario, Secretaría General y demás Oficinas Administrativas. La circulación por la zona será a gran escala en virtud de lo cual existe el riesgo de que se produzca la sustracción de equipos de las oficinas.

Figura 5.6.8 Atención al Usuario Primera Planta Sur

Fuente: Chicaiza, D. (2014)

El nivel de seguridad es medio existe el control de 2 guardias en las áreas de Atención al Usuario, 1 guardia en el corredor hacia las oficinas administrativas. En esta zona se establecerán 4 puntos de video vigilancia.

- **Zona 5: Perímetro.**

En esta zona se encuentra el acceso principal, los parqueaderos para el público en general, parqueadero para funcionarios por lo que se requiere proteger todos los accesos al edificio matriz. El nivel de seguridad es medio existe el control de guardias en los alrededores del edificio, en las entradas a los parqueaderos, en total se cuenta con 6 guardias. En esta zona se establecerán 4 puntos de video vigilancia.

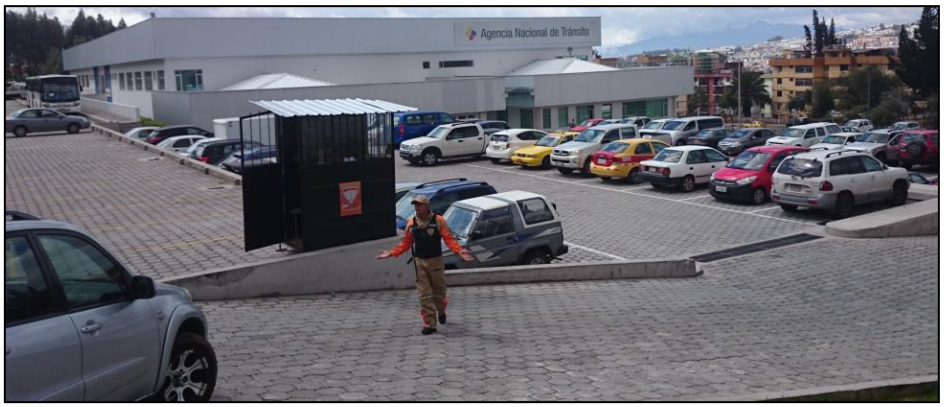


Figura 5.6.9 Seguridad Perímetro Sur Ingreso al Parqueadero Público

Fuente: Chicaiza, D. (2014)

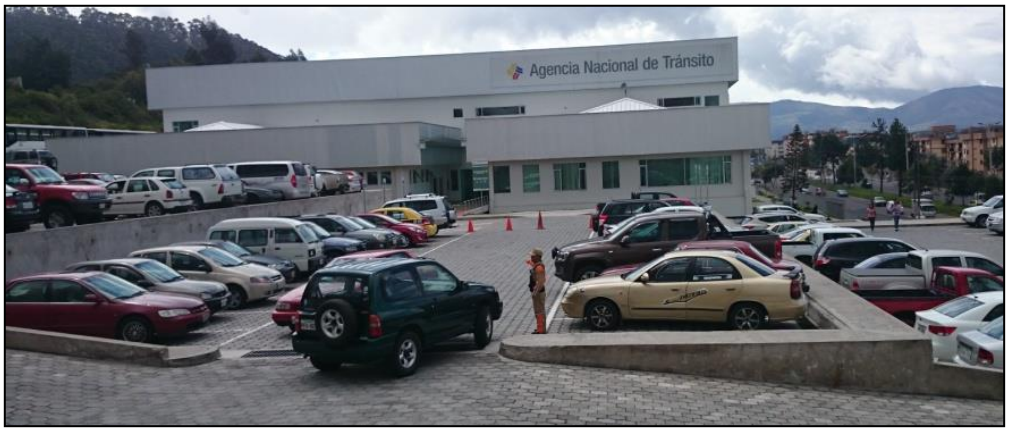


Figura 5.6.10 Seguridad Perímetro Sur Parqueadero Público

Fuente: Chicaiza, D. (2014)

En resumen, se ha determinado la colocación de 16 cámaras IP en apoyo a la seguridad del edificio matriz de ANT.

5.6.3 Consideraciones sobre las cámaras

El sistema de vigilancia por vídeo debe constar de la utilización de cámaras IP, sistema de grabación de video de red (NVR) que se encuentran disponibles en el mercado en diversos modelos que satisfacen una amplia variedad de necesidades.

- **Número de cámaras:** Se proyecta la colocación de 16 cámaras, 4 exteriores y 12 interiores.
- **Fuente de energía:** La energía es suministrada a través del cable de red (UTP cat.6A) utilizando POE.
- Sistema de grabación de red: Basado en hardware especializado.

- **Cámaras Exteriores**

Se recomiendan las cámaras IP Domo PTZ, estas son cámaras con movimiento vertical/horizontal/zoom (PTZ) poseen la ventaja de obtener una visión panorámica, inclinada, alejada o de cerca de una imagen manual o automáticamente. La cámara PTZ puede por ejemplo utilizarse para seguir los movimientos de una persona en un determinado sector (control manual).

Figura 5.6.11 Cámara IP DOMO PTZ

Fuente: Chicaiza, D. (2014)

Se colocarán 4 cámaras exteriores cuya ubicación se detalla a continuación:

- **Cámara 1:** Se ubicará en la cornisa ubicada al Nororiente.
- **Cámara 2:** Se ubicará en la cornisa ubicada al Noroccidente.
- **Cámara 3:** Se ubicará en la cornisa ubicada al Suroriente.
- **Cámara 4:** Se ubicará en la cornisa ubicada al Suroccidente.

Estas cámaras deberán ser instaladas en las esquinas del edificio, en dicha posición permitirán obtener vistas panorámicas de 270° por lo tanto resultan ideales para la vigilancia perimetral del edificio y estacionamientos.

Las cámaras deberán ser compatibles con visión diurna/nocturna, audio bidireccional, ranura para tarjetas de memoria, cuatro puertos de entrada/salida configurables para dispositivos externos, la posibilidad de utilizar alimentación de 24 VCC o alimentación a través de POE, deberán contar con carcasas a fin de tener protección frente al polvo, la humedad o los actos vandálicos.

- **Cámaras Interiores**

Se sugiere para interiores el uso de cámaras IP fijas tipo domo con zoom y enfoque remotos.

Figura 5.6.12 Cámara IP fija tipo domo

Fuente: Chicaiza, D. (2014)

Se ha considerado en el diseño la colocación de 12 cámaras interiores distribuidas de la siguiente forma:

- **Cámara 5, 6 y 7:** Se ubicará en la Zona 1.
- **Cámara 8, 9 y 10:** Se ubicará en la Zona 2.
- **Cámara 11 y 12:** Se ubicará en la Zona 3.
- **Cámara 13, 14, 15 y 16:** Se ubicará en la Zona 4.

Se han considerado las cámaras de red IP tipo domo a prueba de agresiones, estas deberán ser fijas y contar con visión diurna/nocturna, admitir movimiento horizontal/vertical y zoom digital que permita la transmisión de una vista de la imagen completa para su visualización o grabación.

Este tipo de cámara es la solución perfecta para video vigilancia de los pasillos y oficinas de ANT.

- **Plataforma de hardware para Gestión de Video**

Un grabador de vídeo en red se presenta como una caja de hardware con funcionalidades de gestión de vídeo preinstaladas. Un hardware de NVR normalmente está patentado y diseñado específicamente para gestión de vídeo. Está dedicado a sus tareas específicas de grabación, análisis y reproducción de vídeo en red y normalmente no permite que ninguna otra aplicación se conecte a éste. El sistema operativo puede ser Windows, UNIX/Linux o patentado. [49]

Un NVR está diseñado para ofrecer un rendimiento óptimo para un conjunto de cámaras y normalmente es menos escalable que un sistema basado en servidor de PC. Esto permite que la unidad resulte más adecuada para sistemas más pequeños donde el número de cámaras se encuentra dentro de los límites de la capacidad de diseño de un NVR. Normalmente, un NVR es más fácil de instalar que un sistema basado en una plataforma de servidor de PC. [49]

El NVR al ser un dispositivo modular se ajusta al requerimiento inicial del proyecto de video seguridad de ANT ya que permite la integración de más cámaras si el crecimiento de la institución lo requiere.

Las características técnicas que debe cumplir el NVR son:

- Sistema modular.
- Soporte de hasta 64 canales.
- Grabaciones de cámaras de red de 100 Mbps.
- Soporte H.264, MPEG-4 y MJPEG.
- Resolución desde VGA a 5 megapíxeles.
- Almacenamiento interno: hasta 8 discos duros SATA.
- Sistema operativo incorporado basado en Linux.
- Compatible con los métodos de compresión H.264, MPEG-4 y MJPEG.
- Compatible con las cámaras HD y megapíxel de Samsung, AXIS, Panasonic y Sony que cumplen con el estándar ONVIF.
- Modo de búsqueda: fecha/hora, evento.
- Función de reproducción: Avance rápido / Retroceso rápido, Avanzar un paso / Retroceder un paso.
- Soporte de protocolos: TCP/IP, UDP/IP, RTP (UDP), RTP (TCP), RTSP, NTP, HTTP, DHCP, PPPoE, SMTP, ICMP, IGMP, ARP, DNS, DDNS, UPnP, ONVIF.
- Usuarios remotos (máximos): Búsqueda 3 / Unicast directo 10 / Multicast directo 20.
- Seguridad: Filtrado de dirección IP, registro de acceso de usuarios, autenticación 802.1x.
- Puertos: 2 RJ-45 10/100/1000 Base-T, 2 puertos eSATA.

- Tensión de entrada: 100 ~ 240 VCA.
- Visualización multipantalla: 1/4/9/16, Secuencia.
- Modo de grabación: Manual, Programación (Continua/Evento), Evento (Pre/Post).

A continuación se describen los dispositivos que permiten cubrir los requerimientos de video seguridad:

ITEM	DESCRIPCIÓN	CANTIDAD
1	Cámaras IP Tipo PTZ.	4
2	Cámaras IP tipo domo.	12
3	Grabador de video de Red.	1

Tabla 5.6.1 Cantidad de equipos de Video Seguridad.

Fuente: Chicaiza, D. (2014)

- **Presupuesto**

El presupuesto estimado para el proyecto es de $ 54.500,00 (cincuenta y cuatro mil quinientos con 00/100 dólares americanos) más impuestos.

Descripción	Cantidad	Precio Unitario	Precio Total
DETALLE DE EQUIPOS			
Cámaras IP Tipo PTZ.	4	2.500,00	10.000,00
Cámaras IP tipo domo.	12	750,00	9.000,00
Grabador de video de Red (NVR-4TB).	1	3.000,00	3.000,00
DETALLE DE SERVICIOS			
Servicio de Instalación de Equipos de Video Seguridad	1	10.500,00	10.500,00
Servicio de Soporte y Mantenimiento	3	6.500,00	19.500,00
Servicio de Capacitación de la Solución.	1	2.500,00	2.500,00
		SUBTOTAL	**54.500,00**
		IVA	6.540,00
		TOTAL	**61.040,00**

Tabla 5.6.2 Presupuesto Referencial Video Seguridad

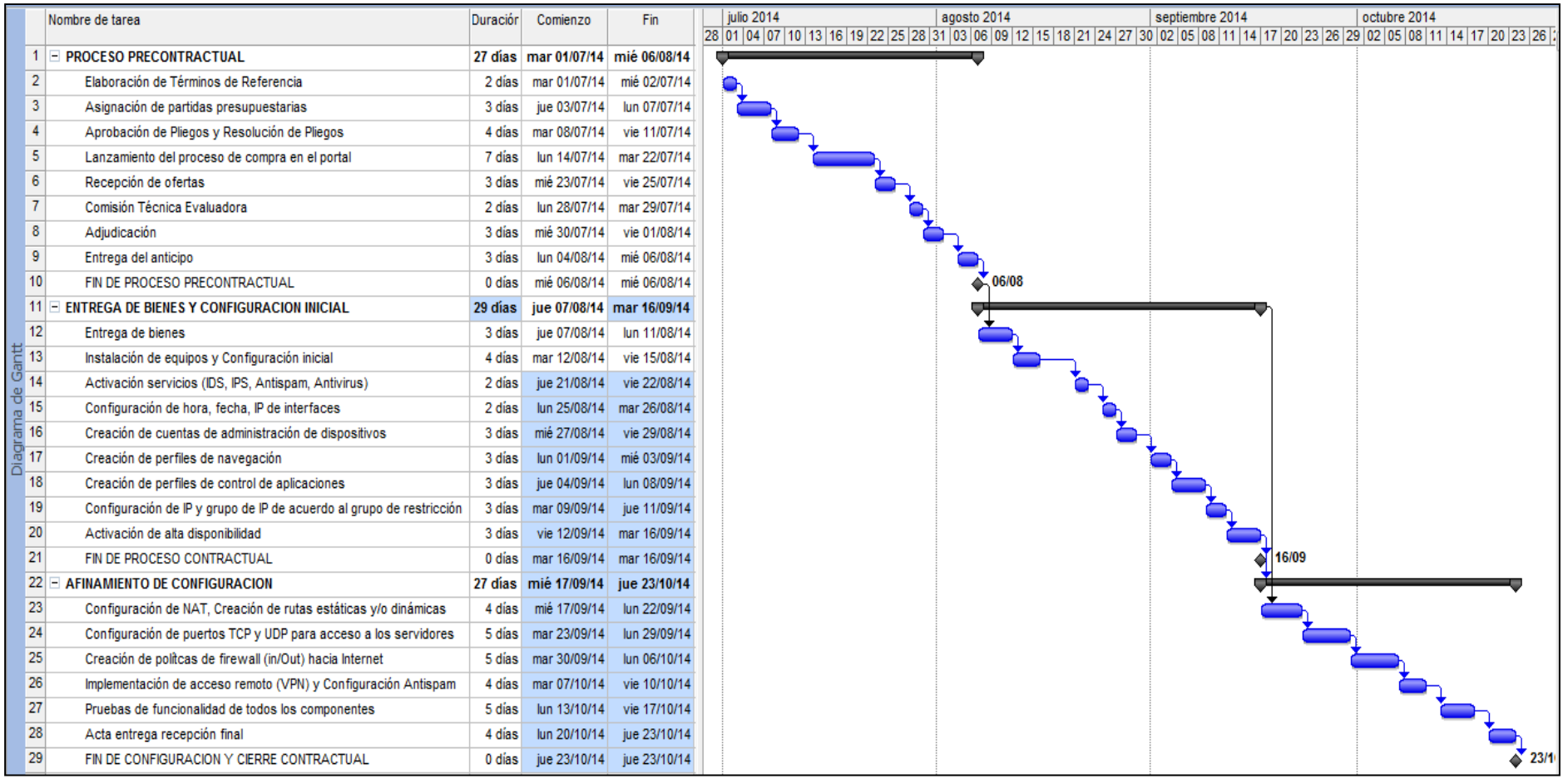
Fuente: Chicaiza, D. (2014)

5.7 CRONOGRAMA DE IMPLEMENTACIÓN.

El tiempo estimado para la ejecución total de implementación y funcionamiento del sistema de seguridad perimetral será de 90 días calendario aproximadamente.

Cronograma estimado de Ejecución del proyecto:

Este cronograma es referencial, mismo que se podrá modificar al momento de realizar la adquisición de los dispositivos.



	Nombre de tarea	Duración	Comienzo	Fin
1	**PROCESO PRECONTRACTUAL**	**27 días**	**mar 01/07/14**	**mié 06/08/14**
2	Elaboración de Términos de Referencia	2 días	mar 01/07/14	mié 02/07/14
3	Asignación de partidas presupuestarias	3 días	jue 03/07/14	lun 07/07/14
4	Aprobación de Pliegos y Resolución de Pliegos	4 días	mar 08/07/14	vie 11/07/14
5	Lanzamiento del proceso de compra en el portal	7 días	lun 14/07/14	mar 22/07/14
6	Recepción de ofertas	3 días	mié 23/07/14	vie 25/07/14
7	Comisión Técnica Evaluadora	2 días	lun 28/07/14	mar 29/07/14
8	Adjudicación	3 días	mié 30/07/14	vie 01/08/14
9	Entrega del anticipo	3 días	lun 04/08/14	mié 06/08/14
10	FIN DE PROCESO PRECONTRACTUAL	0 días	mié 06/08/14	mié 06/08/14
11	**ENTREGA DE BIENES Y CONFIGURACION INICIAL**	**29 días**	**jue 07/08/14**	**mar 16/09/14**
12	Entrega de bienes	3 días	jue 07/08/14	lun 11/08/14
13	Instalación de equipos y Configuración inicial	4 días	mar 12/08/14	vie 15/08/14
14	Activación servicios (IDS, IPS, Antispam, Antivirus)	2 días	jue 21/08/14	vie 22/08/14
15	Configuración de hora, fecha, IP de interfaces	2 días	lun 25/08/14	mar 26/08/14
16	Creación de cuentas de administración de dispositivos	3 días	mié 27/08/14	vie 29/08/14
17	Creación de perfiles de navegación	3 días	lun 01/09/14	mié 03/09/14
18	Creación de perfiles de control de aplicaciones	3 días	jue 04/09/14	lun 08/09/14
19	Configuración de IP y grupo de IP de acuerdo al grupo de restricción	3 días	mar 09/09/14	jue 11/09/14
20	Activación de alta disponibilidad	3 días	vie 12/09/14	mar 16/09/14
21	FIN DE PROCESO CONTRACTUAL	0 días	mar 16/09/14	mar 16/09/14
22	**AFINAMIENTO DE CONFIGURACION**	**27 días**	**mié 17/09/14**	**jue 23/10/14**
23	Configuración de NAT, Creación de rutas estáticas y/o dinámicas	4 días	mié 17/09/14	lun 22/09/14
24	Configuración de puertos TCP y UDP para acceso a los servidores	5 días	mar 23/09/14	lun 29/09/14
25	Creación de políticas de firewall (in/Out) hacia Internet	5 días	mar 30/09/14	lun 06/10/14
26	Implementación de acceso remoto (VPN) y Configuración Antispam	4 días	mar 07/10/14	vie 10/10/14
27	Pruebas de funcionalidad de todos los componentes	5 días	lun 13/10/14	vie 17/10/14
28	Acta entrega recepción final	4 días	lun 20/10/14	jue 23/10/14
29	FIN DE CONFIGURACION Y CIERRE CONTRACTUAL	0 días	jue 23/10/14	jue 23/10/14

Figura 5.7.1 Cronograma estimado de Ejecución del proyecto

Fuente: Chicaiza, D. (2014)

A continuación se detallan las actividades y responsables de cada una:

PROCESO PRECONTRACTUAL	
TAREA	**RESPONSABLES**
Elaboración de Términos de Referencia	Proyectos Tecnológicos
Asignación de partidas presupuestarias	Dirección Financiera
Aprobación de Pliegos y Resolución de Pliegos	Dirección de Contratación Pública
Lanzamiento del proceso de compra en el portal	
Recepción de ofertas	
Comisión Técnica Evaluadora	Dirección de Contratación Pública, Planificación y Seguridad Informática
Adjudicación	Dirección de Contratación Pública
Entrega del anticipo	Dirección Financiera
ENTREGA DE BIENES Y CONFIGURACION INICIAL	
TAREA	**RESPONSABLES**
Entrega de bienes	Empresa Adjudicada, Abastecimientos, Comité de Recepción
Instalación de equipos y Configuración inicial	Empresa Adjudicada, Infraestructura Tecnológica
Activación servicios (IDS, IPS, Antispam, Antivirus)	Empresa Adjudicada, Infraestructura Tecnológica y Oficial de Seguridad de la Información
Configuración de hora, fecha, IP de interfaces	
Creación de cuentas de administración de dispositivos	
Creación de perfiles de navegación	
Creación de perfiles de control de aplicaciones	
Configuración de IP y grupo de IP de acuerdo al grupo de restricción	
Activación de alta disponibilidad	
AFINAMIENTO DE CONFIGURACION	
TAREA	**RESPONSABLES**
Configuración de NAT, Creación de rutas estáticas y/o dinámicas	Empresa Adjudicada, Infraestructura Tecnológica y Oficial de Seguridad de la Información
Configuración de puertos TCP y UDP para acceso a los servidores	
Creación de polítcas de firewall (in/Out) hacia Internet	
Implementación de acceso remoto (VPN) y Configuración Antispam	
Pruebas de funcionalidad de todos los componentes	
Acta entrega recepción final	

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- ✓ Se identificó que la infraestructura tecnológica de la Agencia Nacional de Tránsito presenta vulnerabilidades y existen falencias en torno a la transferencia de información entre sucursales ya que no se utiliza ninguna herramienta de encriptación que permita dar confidencialidad a la información.

- ✓ La red de ANT posee mecanismos de seguridad como el software antivirus Kaspersky y el dispositivo Astaro Security Gateway (punto único de protección y de falla), los mismos que constituyen una herramienta muy fuerte para la protección de la red, pero que no permiten ejercer controles 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.
    - 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 de confianza y los que representan inseguridad y peligro.

- Finalmente carece de políticas que permitan controlar, administrar y monitorear las operaciones que se suscitan en la red, lo cual conlleva a la ineficiencia e inseguridad de la red.

✓ La mayoría de los ataques de suplantación de identidad y programas maliciosos se llevan a cabo a través de Internet, al restringir el acceso a determinados sitios web utilizando tecnología de filtrado de direcciones o contenido web permite que las empresas puedan reducir los riesgos de que los usuarios se conviertan en víctimas de estos ataques.

✓ El establecimiento de Redes Privadas Virtuales basadas en protocolos de tunelización (IPSec SSL, PPTP y L2TP) permite que oficinas pequeñas puedan establecer comunicaciones privadas sobre redes públicas garantizando la confidencialidad e integridad de los datos trasmitidos por Internet.

✓ Utilizar técnicas de autenticación a través de políticas de Firewall (Interfaces de entrada y salida, direcciones IP origen y destino, protocolo, servicio o puertos TCP/UDP) permitirán llevar un mejor control del tráfico que circula por nuestra red.

✓ Contar con sistema de seguridad que maneje un esquema de alta disponibilidad permitirá que la Agencia Nacional de Tránsito cuente siempre con las aplicaciones que apoyan sus operaciones principales, pues la falta de disponibilidad de las mismas puede repercutir en costos, tiempos, esfuerzos y por supuesto en la confianza e insatisfacción de los usuarios.

✓ Una adecuada gestión de calidad de servicio nos permitirá la utilización de aplicaciones susceptibles a retardos (voz y aplicaciones multimedia) sin recurrir a una ampliación innecesaria del ancho de banda, reservando el ancho de banda necesario y priorizando este tipo de tráfico ante otros menos sensibles al retardo como pueda ser el correo o el tráfico ftp.

✓ El Sistema de Detección de Intrusión constituye un sensor de red en tiempo real que utiliza definiciones de firmas de ataques y detección de

comportamientos anómalos para detectar y prevenir tráfico sospechoso y ataques de red como los ataques de denegación de servicio (DoS) y ataques de reconocimiento.

- ✓ Las soluciones UTM modernas deben adaptarse de forma flexible a las necesidades actuales y futuras de las empresas. Estas deben permitir la integración de dispositivos adicionales en una única consola de gestión, esto creará una instalación más potente que funcione como un todo. El disponer de diferentes opciones de expansión permiten ahorrar tiempo y dinero.

- ✓ Los sistemas de gestión unificada de amenazas (UTM), combinan varias funcionalidades (firewall, VPN, antivirus, IDS, IPS y filtrado de contenidos) en un sólo dispositivo, siendo esta tecnología la más popular entre las empresas con redes remotas u oficinas distantes ya que permiten garantizar la seguridad centralizada con control completo sobre sus redes distribuidas globalmente.

- ✓ La tecnología Fortinet es una poderosa combinación de software y hardware basada en el uso de circuitos integrados de aplicación específica, conocidos por sus siglas en inglés como ASIC, a través de la cual permite el análisis del contenido del tráfico en tiempo real, satisfaciendo todas las necesidades de protección a nivel de aplicación sin impactar en el rendimiento de la red.

- ✓ La solución de seguridad planteada mediante el uso de dispositivos UTM de la marca Fortinet ayudarán a proteger los activos informáticos, además permitirá brindar seguridad a las comunicaciones entre sucursales y al Internet.

- ✓ La clave para tener un entorno más seguro es lograr que los empleados entiendan su responsabilidad personal al momento de utilizar nuevas tecnologías o tener acceso a información institucional, una lista concreta de lo que debe y no debe hacerse es la forma más eficaz de comunicar las políticas y habilitar su uso responsable.

- ✓ Las contraseñas débiles presentan una vulnerabilidad importante para los sistemas de autenticación. Se necesita emplear contraseñas de al menos, una combinación de letras y números además de especificar una largura mínima, el historial de la clave, bloqueos de cuenta y expiración de claves para forzar a los usuarios a crear contraseñas robustas.

- ✓ Las tecnologías biométricas son la forma segura de identificación inequívoca de las personas: identificación con el propio cuerpo, que va siempre con nosotros, nada que perder (tarjetas), nada que olvidar (contraseñas). Los rasgos biométricos son invariables, salvo en contadas excepciones y siempre van con la persona. Ni se pierden ni se olvidan.

6.2 RECOMENDACIONES

- ✓ El escaneo de puertos es una técnica usada por hackers pero también puede ser utilizada por los administradores de red, es indispensable realizar un análisis de nuestra red utilizando software especializado en detección de vulnerabilidades con el fin de saber qué puertos están abiertos o cerrados, los servicios que son ofrecidos, verificar el estado de los principales equipos de red, esto nos dará una mejor idea de que tan segura es nuestra red y de cómo aprovechar los resultados para asegurar la misma.

- ✓ El indispensable utilizar procedimientos de fortalecimiento (hardening) para reducir la mayor cantidad de riesgos y minimizar la cantidad de vulnerabilidades sobre nuestros sistemas, de esta forma podremos garantizar la continuidad de los servicios.

- ✓ Es indispensable contar con mecanismos de protección como:
    - o Un firewall para restringir o permitir las conexiones y servicios de forma específica.
    - o Encriptación para proteger la información sensible en tránsito mediante el uso de VPN y en almacenamiento.
    - o 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.

✓ Es indispensable dar a conocer que el equipo de seguridad de la información incluye a todos los empleados, inculcar buenas prácticas de seguridad al personal de la institución puede lograr que mediante capacitación e implementación de tecnología de seguridad perimetral la red sea más segura.

✓ El factor económico no debe ser una limitante al momento de invertir en tecnologías que permitan desarrollar e implementar políticas de seguridad, contar con mecanismos de control, administración y monitoreo de los dispositivos que conforman la red (Servidores, estaciones de trabajo, equipos de comunicación, etc.) ya que permitirán que la red sea menos vulnerable a intrusiones y denegación de servicio.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Wikiversidad (2007), Seguridad en Redes de Computadores/Ataques contra las redes, http://es.wikiversity.org/wiki/Seguridad_en_Redes_de_Computadores/Ataques_contra_las_redes. Último Acceso el 06 de noviembre de 2013.

- [2] Álvaro Primo Guijarro (2012), Seguridad Perimetral, http://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf. Último Acceso el 06 de noviembre de 2013.

- [3] Joaquín García Alfaro (2011), Ataques contra redes TCP/IP, http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01769.pdf Último Acceso el 10 de noviembre de 2013.

- [4] INTECO (2013), Centro de Alerta Temprana sobre Virus y Seguridad Informática. Fraude en Internet. http://www.inteco.es/Formacion/Fraude_en_Internet/. Último Acceso el 15 de noviembre de 2013.

- [5] Diario el Telégrafo (2011), Ataques hacker a redes de Ecuador, http://www.telegrafo.com.ec/noticias/tecnologia/item/mas-paginas-web-oficiales-hackeadas.html. Último Acceso el 15 de noviembre de 2013.

- [6] Agencia Nacional de Tránsito (2013), Visión, Misión y Objetivos, http://www.ant.gob.ec/index.php/ant/vision-mision-y-objetivos#.Ur2tr_t0ncw Último Acceso el 16 de noviembre de 2013.

- [7] Ramos, L., Seguridad de la Información, Normas ISO 27000, disponible en: http://www.cpciba.org.ar/archivos/adjuntos/seguridad.pdf, consultado febrero 2014.

- [8] Sandoval, D., Ciencia, Tecnología e Industrias Intermedias, Superintendencia de Servicios de Certificación Electrónica, disponible en: http://www.sunai.gob.ve/images/stories/PDF/Ponencias/EF/3_Daniel_sandoval.pdf.

- [9] Seguridad Informática, (2009), Conceptos básicos de Seguridad Informática, disponible en: http://seguridadinformaticas.blogspot.com/. Último Acceso el 15 de noviembre de 2013.

- [10] Costas, J. (2010), Seguridad Informática. RA-MA S.A. Editorial y Publicaciones. España.

- [11] López & San Valero, (20), Paradigmas, Seguridad Informática, disponible en: http://www.wilucha.com.ar/Sistemas/S_SegInform.html

- [12] Rodriguez, D. Seguridad de la Informacion y Iso 27001, disponible en: http://es.scribd.com/doc/214542899/Seguridad-de-La-Informacion-y-Iso-27001.

- [13] Universidad Nacional de Lujan, Argentina. Amenazas a la Seguridad de la Información, disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12.

- [14] Castro, L. (2014), Conoce qué es hacker y cómo están clasificados, disponible en: http://aprenderinternet.about.com/od/ConceptosBasico/g/Que-Es-Hacker.htm, consulta en mayo 2014.

- [15] San Miguel, A. (2011), Tipos De Hackers Que Debes Conocer, disponible en: http://axelsanmiguel.com/8-tipos-de-hackers-que-debes-conocer/, consulta en mayo 2014.

- [16] Alulema, D. (2008), 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, Escuela Politécnica Nacional, Ciudad Quito, Ecuador.

- [17] Firtman, S. (2005), Seguridad Informática: Las amenazas y vulnerabilidades más peligrosas, al desnudo. MP Ediciones.

- [18] Wikipedia, (2013), Defensa en Profundidad. Disponible en: http://es.wikipedia.org/wiki/Defensa_en_profundidad

- [19] Gómez, A. (2006), Enciclopedia de la Seguridad Informática. Alfaomega Ra-Ma. España.

- [20] Alveniz, (2011), Virus y Programas Maliciosos. Disponible en: http://albeniz-2011-informatica.wikispaces.com/Virus.

- [21] Blockspot, (2010), Tipos de Virus. Disponible en: http://tiposdeviruss.blogspot.com/.

- [22] Wikipedia, (2014), Bomba lógica, Disponible en: http://es.wikipedia.org/wiki/Bomba_l%C3%B3gica.

- [23] Cyclopaedia, (2012), Ataque de Fuerza Bruta, Disponible en: http://es.cyclopaedia.net/wiki/Ataque-de-fuerza-bruta.

- [24] Wikipedia, (2014), Transport Layer Security, Disponible en: http://es.wikipedia.org/wiki/Bomba_l%C3%B3gica.

- [25] GlobalSign, Centro de Información SSL, Disponible en: https://www.globalsign.es/centro-informacion-ssl/quien-necesita-ssl.html.

- [26] Conocimientos Informáticos, Razones para segmentar una LAN, Disponible en: http://ordenador.wingwit.com/Redes/localnetworks/71822.html#.U4FVlSjyRXk

- [27] Katz, M. (2013), Redes y Seguridad. Alfaomega Grupo Editor. México.

- [28] Wordpress, (2012), Algoritmos de Encriptación Simétrica y Asimétrica. Disponible en: http://mariiss15.wordpress.com/2012/11/14/algoritmos-de-encriptacion-simetrica-y-asimetrica/.

- [29] Scribd, (2014), Firewall. Disponible en: http://es.scribd.com/doc/210605170/Firewall-1-1-Final.

- [30]Soler, S. (2011), Las Redes VPN y Sus Beneficios. Disponible en: http://prezi.com/tc0qztssvmzk/las-redes-vpn-y-sus-beneficios/

- [31] Mitre, H. (2012), Artículo Autenticación. Disponible en: http://www.slideshare.net/hmitre17/autenticacin.

- [32] Wikipedia. (2014), Criptografía. Disponible en: http://es.wikipedia.org/wiki/Contrase%C3%B1a

- [33] Wikipedia. (2014), Tarjeta Inteligente. Disponible en: http://es.wikipedia.org/wiki/Tarjeta_inteligente.

- [34] Umanick. (2013), Hablemos de biometría: ventajas y desventajas. Disponible en: http://www.umanick.info/2013/07/hablemos-de-biometria-ventajas-y.html.

- [35] Slideshare. (2009), Qué es un virus. Disponible en: http://www.slideshare.net/chaidez13/un-virus-1142640

- [36] Plusesmas. (2011), Qué es y cómo funciona un programa antivirus. Disponible en: http://www.plusesmas.com/nuevas_tecnologias/articulos/seguridad_virus/que_es_y_como_funciona_un_programa_antivirus/17.html

- [37] Sánchez, B. (2013), Ventajas de un Antivirus. Disponible en: http://www.ehowenespanol.com/ventajas-antivirus-lista_94954/.

- [38] Infocode.(2011), Ventajas y Desventajas de los Antivirus para PC y los Antivirus Online. Disponible en: http://info-code.blogspot.com/2011/05/ventajas-y-desventajas-de-los-antivirus.html

- [39] Salinas, R. (2005), Actualidad TIC, Revista del Instituto Tecnológico de Informática. Disponible en http://www.iti.es/media/about/docs/tic/06/2005-02-intrusos.pdf

- [40] Rangel, S. (2011), Un sistema de prevención de intrusos. Disponible en: http://prezi.com/7dso0f0irqti/un-sistema-de-prevencion-de-intrusos-o-por-sus-siglas-en-in/

- [41] Networkworld. (2008), Prevención de intrusiones. Disponible en: http://www.networkworld.es/seguridad/prevencion-de-intrusiones

- [42] Rabadán, M. (2007), Cryptex Seguridad de la Información. Disponible en: http://seguridad-informacion.blogspot.com/2007/12/seguridad-perimetral-gestin-unificada.html

- [43] Cyclopaedia. (2013), Unified Threat Management. Disponible en: http://es.cyclopaedia.net/wiki/Unified-Threat-Management

- [44] Catalaa, J. (2010), Guía de Dimensionamiento Firewall/UTM. Disponible en: http://www.adexsus.com/v2/pdf/Recursos/Sonicwall/UTM%20Sizing%20Document_ESP42010.pdf

- [45] Beab. (2007), El cuadrante mágico de gartner. Disponible en: http://elprincipiodeincertidumbre.net/blog/2007/10/29/el-cuadrante-magico-de-gartner/

- [46] Wikipedia. (2014), Nessus. Disponible en: http://es.wikipedia.org/wiki/Nessus.

- [47] Technet. (2014), Guía de defensa en profundidad antivirus. Disponible en: http://technet.microsoft.com/es-es/library/cc162791.aspx

- [48] AJB. (2010), Qué es el Video IP. Disponible en: http://tacticasenseguridad.net/foro/13-software-y-camaras-ip/19-que-es-el-video-ip/fb_pdf.html

- [49] Axis. (2013), Plataformas de hardware. Disponible en: http://www.axis.com/es/products/video/about_networkvideo/platforms.htm

- [50] Samsung. (2012), Samsung presenta una solución NVR modular http://www.samsungsecurity.es/es-es/newsandevents/news/samsung%20introduce%20a%20building%20block%20nvr%20solution.aspx?IN=32

- [51] Fortinet. (2009). Seguridad Integral en Tiempo Real. Disponible en: http://www.fortinet.com/

- [52] Fortinet. (2013). High Performance Multi-Threat Security Solutions. Disponible en: http://www.fortinet.com/.

- [53] Safenet. (2014). Safenet es clasificada como líder en autenticación en el cuadrante mágico de Gartner. Disponible en: http://prosupply.ec/safenet-

es-clasificada-como-lider-en-autenticacion-en-el-cuadrante-magico-de-gartner/

- [54] CA Technologies. (2014). CA Technologies Acerca de nosotros. Disponible en: http://www.ca.com/es/about-us.aspx

- [55] Daboweb. (2013). Sistemas IDS/IPS open source. Disponible en: http://www.daboweb.com/2011/03/14/smooth-sec-sistema-ids-ips-con-motor-suricata-e-interface-snorby/

- [56] Steffens, H. (2010). ENDIAN: Una solución Open Source de seguridad perimetral. Disponible en: http://liacolombia.com/2010/07/endian-una-solucion-open-source-de-seguridad-perimetral/

- [57] CISCO. (2014). Informe Anual de Seguridad de CISCO 2014. Disponible en: http://www.hacking-etico.com/wp-content/uploads/2014/03/cisco2014_infosec_report.pdf

- [58] Wikipedia. (2014). Herramientas que permiten realizar el monitoreo de la actividad. Disponible en: http://es.wikipedia.org

- [59] Wiens, J. (2013). UTM al rescate. Disponible en: http://www.informationweek.com.mx/networking/utm-al-rescate/

ANEXOS

Anexo 1. Convenio de confidencialidad

En la ciudad de XXXX, a los xxx días del mes de xxxx del año xxxx comparecen a la celebración del presente Convenio por una Parte, el Ing. xxxxx, en su calidad de Director Ejecutivo y representante legal de la **Agencia Nacional de Regulación y Control del Transporte Terrestre, Tránsito y Seguridad Vial**, en adelante ANRCTTTSV, según consta en el nombramiento que forma parte de este convenio en documento debidamente certificado, y; por otra, el Señor (a) XXXXXXX, ecuatoriano, mayor de edad, de estado civil xxxx, domiciliado en esta ciudad de xxxxxx, hábil y capaz de obligarse, por sus propios y personales derechos, a quién en adelante y para efectos del presente contrato se le conocerá como "EL SERVIDOR PÚBLICO". Ambas partes acuerdan celebrar el presente convenio al tenor de las siguientes cláusulas:

CLÁUSULA PRIMERA: ANTECEDENTES.-

1. La ANRCTTTSV es una institución de derecho público, misma que ejerce la rectoría en todos los aspectos relacionados con el transporte terrestre, tránsito y seguridad vial, cuyas facultades son constitucional y legalmente establecidas, y en derecho tiene capacidad plena y suficiente para realizar todo acto o contrato tendiente a garantizar el cumplimiento de sus fines.

2. La ANRCTTTSV requiere, para el cumplimiento de sus objetivos y actividades, de ciudadanos profesionales calificados que aporten en la ejecución de las labores relacionadas con sus fines.

3. EL SERVIDOR PÚBLICO, fue contratado para prestar sus servicios en la ANRCTTTSV, mediante contrato de (servicios ocasionales – profesionales, según sea el caso) suscrito a los XX días del mes de xxxxx del año xxxx, mediante el cual se compromete a prestar sus servicios profesionales a la ANRCTTTSV.

4. Por la naturaleza de las funciones asignadas a EL SERVIDOR PÚBLICO por parte de la ANRCTTTSV, es imprescindible la suscripción del presente Convenio de Confidencialidad, como contrato subsidiario al contrato principal de (servicios ocasionales – profesionales, según sea el caso), a fin de garantizar el secreto y reserva de la información a la que tendrá acceso y conocimiento EL SERVIDOR PÚBLICO en ejercicio de sus funciones.

CLÁUSULA SEGUNDA: OBJETO

El objeto del presente contrato es garantizar el sigilo y protección de los datos y archivos informáticos y no informáticos que, si bien es cierto son públicos, la ANRCTTTSV es la única responsable de su administración y manejo por su condición de entidad rectora de las actividades relacionadas con el transporte terrestre, tránsito y seguridad vial. Por lo tanto, EL SERVIDOR PÚBLICO en virtud de que prestará sus servicios a la ANRCTTTSV y por la naturaleza de sus

labores y cargo tendrá acceso a información secreta, confidencial, patrimonial, estratégica, información técnica y comercial de carácter reservado, de propiedad de la ANRCTTTSV, de sus usuarios, conductores, contratistas, subcontratistas, asociaciones, cooperativas, compañías y en fin de cualquier tercero involucrado con la actividad del transporte terrestre, tránsito y seguridad vial en el país. EL SERVIDOR PÚBLICO se compromete y obliga a no divulgar y guardar reserva al respecto de toda la información a la que tenga conocimiento por medios orales, escritos, electrónicos, gráficos u otros.

CLÁUSULA TERCERA: DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL

Para efectos del presente convenio, se considera como "Información Confidencial" a cualquier dato o conjunto de datos transferidos por escrito o en forma verbal o visual a través de cualquier medio, e ingresados en las bases de datos administradas por la ANRCTTTSV, así como también aquellos marcados como "De Propiedad Confidencial" o cualquier otro aviso similar; junto con notas, análisis, hojas de trabajo, estudios o cualquier otro documento preparado por EL SERVIDOR PÚBLICO, o cualquiera de los demás empleados, servidores o funcionarios de la ANRCTTTSV, el cual contenga, refleje, estén basados o sean generados por tal información; igualmente toda información de carácter societaria, técnica, financiera, comercial, estratégica, de planificación, potenciales resoluciones internas de la entidad, es de ser publicadas, información y proyecciones de planes de negocios, datos, registros de negocios, listas de clientes y proveedores, contratos con proveedores, planes estratégicos, lista de empleados, políticas y procedimientos, información relacionada con los procesos, técnicas, tecnologías, programas de software, códigos fuente, esquemas, diseños o teorías y en general toda la información que se relacione con los servicios y actividades que realiza la ANRCTTTSV, su matriz, las unidades provinciales, delegaciones, agencias y departamentos, y/o cualquier información relacionada con la estructura organizacional de estas.

En todo caso, aún cuando la información no estuviera marcada con una nota de que se trata de Información Confidencial, EL SERVIDOR PÚBLICO reconocerá este carácter a toda la información descrita en el párrafo anterior. En consecuencia, EL SERVIDOR PÚBLICO queda obligado a consultar por escrito a través de los mecanismos de comunicación interna establecidos si el contenido de la información que ostente estas características corresponden o no a Información catalogada como Confidencial, previo a la divulgación, entrega o comunicación de cualquier información que directa o indirectamente haya sido solicitada, y de ser así deberá, previo a la entrega efectiva, esperar el consentimiento por escrito por parte de su Jefe inmediato superior.

Todas la copias impresas o electrónicas, anotaciones, resúmenes o extractos de esta información deberán ser tratadas como tal.

CLÁUSULA CUARTA: EXCEPCIONES

No obstante, no constituirá "Información Confidencial" para efectos de este Convenio:

i. La que la ley no reconozca como aquella que requiera de sigilo.

ii. Información que es o se resuelva de conocimiento o dominio público de manera

diferente a la de ser revelada directa o indirectamente por la ANRCTTTSV**.**

iii. La información Confidencial que haya sido requerida por autoridad competente y de acuerdo a la Ley. En este evento, EL SERVIDOR PÚBLICO deberá comunicar inmediatamente y por escrito a la Dirección de la ANRCTTTSV acerca de dicho requerimiento y previa autorización por escrito cooperar con la ANRCTTTSV para que tome las acciones tendientes a la protección de la Información o limitar la naturaleza y alcance del requerimiento. La ANRCTTTSV deberá continuar protegiendo como confidencial y privativa toda la Información revelada en respuesta a una orden de autoridad competente.

Bajo ninguna circunstancia, por el hecho de que la información declarada en este instrumento como confidencial cayera en manos de terceros no autorizados por la ANRCTTTSV, adquirirá el carácter de pública, pues la calidad de información pública solo puede ser declarada de manera expresa, por escrito y por la ANRCTTTSV.

CLÁUSULA QUINTA: DECLARACIONES

EL SERVIDOR PÚBLICO, admite y consiente que toda la Información Confidencial que recibe de la ANRCTTTSV, es propiedad exclusiva de ésta y que se la da a conocer únicamente con el propósito de obtener la correcta prestación de servicios contratados. Por lo que en ningún momento el presente Convenio se entiende como cesión, otorgamiento de licencia, transmisión o transferencia de la propiedad, derechos de propiedad industrial, ni otros derechos de propiedad intelectual, de la "Información Confidencial", a EL SERVIDOR PÚBLICO ni a terceras personas que la adquieran por intermedio de este.

CLÁUSULA SEXTA: PLAZO

a) Este Convenio tendrá una duración de un año, contados a partir de la fecha de suscripción, y deberá ser renovado, si el contrato de (servicios ocasionales, profesionales, según el caso etc.) suscrito por las partes se renueva también. No obstante, las obligaciones previstas en el presente Convenio estarán vigentes hasta (4) cuatro años después de la finalización del mismo.

b) Ante la terminación de este Convenio, EL SERVIDOR PÚBLICO el SERVIDOR PÚBLICO inmediatamente no tendrá acceso al uso de las claves y accesos entregados, así como a los textos, archivos, documentos, equipos y toda la Información Confidencial a su cargo, misma que se revertirá bajo custodia inmediata de la ANRCTTTSV, y sin realizar ningún tipo de copia o registro. Ante el pedido de ANRCTTTSV, el SERVIDOR PÚBLICO EL SERVIDOR PÚBLICO certificará por escrito que ha cumplido con esta obligación.

c) Sin perjuicio de la terminación de este Convenio, las obligaciones de el SERVIDOR PÚBLICO EL SERVIDOR PÚBLICO respecto de la Información Confidencial a la que tuvo acceso y conocimiento durante el tiempo que prestó sus servicios en la ANRCTTTSVANRCTTTSV, sobrevivirán a tal terminación, conforme lo previsto en el literal a) de la presente Cláusula.

d) En Consecuencia, aún en el caso de haber terminado sus relaciones laborales con la ANRCTTTSV, el SERVIDOR PÚBLICO El SERVIDOR PÚBLICO será responsable de la divulgación de la Información Confidencial cuando la revele a sus socios, colaboradores, administradores, dependientes, empleados o compañías que tengan relación con el ex SERVIDOR PÚBLICO que prestó sus servicios en la ANRCTTTSV EL SERVIDOR PÚBLICO, así como a sus clientes y demás empresas vinculadas directa o indirectamente con este, y que llegaren a tener acceso a la información clasificada como confidencial de propiedad de ANRCTTTSV, de conformidad a lo establecido en el literal a) de la presente cláusula.

CLÁUSULA SÉPTIMA: DEBER DE RESERVA.-

Con el fin de guardar la reserva de la "Información Confidencial" que se suministre en el desarrollo de este Convenio, el SERVIDOR PÚBLICO El SERVIDOR PÚBLICO deberá:

a) Custodiar con reserva la "Información Confidencial" recibida o a la que tenga acceso de la ANRCTTTSV.

b) No utilizar la información recibida en detrimento de la ANRCTTTSVANRCTTTSV o para obtener información privilegiada frente a otros individuos.

c) Utilizar la Información Confidencial exclusivamente en relación con lo estipulado en este Convenio.

Cuando el SERVIDOR PÚBLICO conozca de cualquier pérdida, uso no autorizado o revelación de la Información Confidencial de la ANRCTTTSV, el SERVIDOR PÚBLICO deberá notificar inmediatamente por escrito a sus jefes inmediatos superiores de tal pérdida, uso no autorizado o revelación. La ANRCTTTSV mediante el departamento correspondiente remediará tal uso no autorizado o revelación de la Información Confidencial.

En caso de que el SERVIDOR PÚBLICO, necesitare revelar la Información Confidencial a sus compañeros, subalternos o cualquier tercero, requerirá autorización expresa y escrita de la Dirección Ejecutiva de la ANRCTTTSV. Una vez obtenida la autorización correspondiente el SERVIDOR PÚBLICO tendrá la obligación de, previamente a la divulgación de la Información Confidencial, suscribir los correspondientes Convenios de Confidencialidad que garanticen el debido cumplimiento de lo señalado en el presente documento.

CLÁUSULA OCTAVA: AUSENCIA DE LICENCIAS.-

Ni la ejecución de este Convenio, ni el suministro de información en virtud del mismo, se interpretará, directa o indirectamente, como otorgamiento al SERVIDOR PÚBLICO o a sus subalternos, dependientes, consultores y/o asesores, o cualquier otro tercero, de licencia alguna o derecho para utilizar Información Confidencial para su propio beneficio o beneficio de cualquier otra persona natural o jurídica y en este sentido, el SERVIDOR PÚBLICO se compromete expresamente a no utilizarla de este modo.

CLÁUSULA NOVENA: MEDIDAS DE PROTECCIÓN.-

La ANRCTTTSV tomará las precauciones necesarias para que la Información no sea revelada a cualquier persona que no esté autorizada conforme lo previsto en este documento, y tomará todas las medidas iguales o similares a aquellas utilizadas para proteger su propia Información.

CLÁUSULA DÉCIMA: DEVOLUCIÓN DE LA INFORMACIÓN.-

El SERVIDOR PÚBLICO se compromete a devolver inmediatamente que ha concluido su contrato, toda la Información con la que haya trabajado sin mantener en su poder ningún tipo de copia de esa Información. La ANRCTTTSVANRCTTTSV deberá exigir la entrega de una certificación firmada por el SERVIDOR PÚBLICO el SERVIDOR PÚBLICO garantizando la entrega completa de la Información, así como de las obligaciones de confidencialidad y restricción estipuladas en este Convenio, conforme la Cláusula Quinta.

CLÁUSULA UNDÉCIMA: CLÁUSULA PENAL.-

El incumplimiento total o parcial de los compromisos aquí asumidos por el SERVIDOR PÚBLICO**,** dará lugar al pago de la parte incumplida a favor de la parte cumplida, de una pena equivalente a (500) Quinientos Salarios Básicos Unificados Mensuales Vigentes. Dicha pena se aplicará sin perjuicio de que se pueda exigir, igualmente, el cumplimiento de la obligación principal y la correspondiente indemnización de perjuicios. Se estipula que el presente acuerdo presta mérito ejecutivo.

Si se detectare y demostrare el mal uso de la información confidencial por parte del SERVIDOR PÚBLICO, se procederá inmediatamente a la recisión del contrato principal y su correspondiente destitución, así como también se iniciarán las causas penales correspondientes ante el Ministerio Público.

CLÁUSULA DUODÉCIMA: RESOLUCION DE CONTROVERSIAS.-

LAS PARTES acuerdan que toda controversia será sometida ante los Tribunales de Jurisdicción Contencioso Administrativa, de la ciudad de Quito.

CLÁUSULA DÉCIMA TERCERA: ACUERDO COMPLETO.-

Este documento constituye el Convenio de Confidencialidad en su totalidad y anula/reemplaza cualquier acuerdo o negociación previa, escrita, verbal y/o electrónica, sobre este tema.

Revisado este Convenio **LAS PARTES** manifiestan su acuerdo, en constancia de lo cual se firma en la ciudad de XXXXX () a los xx días de XXXXX de xxxx en dos ejemplares originales, de similar contenido.

_____	**_____**
Ing. Paola Carvajal	**(Nombres y Apellidos**
Directora Ejecutiva de la ANRCTTTSV	**C.I.)**
	SERVIDOR PÚBLICO EL SERVIDOR PÚBLICO

Anexo 2. Evaluación de los Dispositivos FORTINET [52]

A continuación se describen las funcionalidades que ofrecen los dispositivos Fortinet, mismas que se ajustan a los requerimientos de ANT y que permitirán mitigar las vulnerabilidades detectadas y las falencias del actual equipamiento de seguridad de la Agencia Nacional de Tránsito.

Fortinet encontró lo siguiente:

La tecnología Fortinet es una poderosa combinación de software y hardware basada en el uso de circuitos integrados de aplicación específica, conocidos por sus siglas en inglés como ASIC, a través de la cual es capaz de ofrecer el procesamiento y análisis del contenido del tráfico de la red sin que ello suponga ningún impacto en el rendimiento de las comunicaciones. "Ibíd."

La tecnología incluye el Procesador FortiASIC™ y el Sistema Operativo FortiOS™ los cuales forman el núcleo de los equipos FortiGate y son la base del alto rendimiento ofrecido por los equipos. "Ibíd."

El procesador FortiASIC™, diseñado por Fortinet, posee un motor propietario de análisis de contenido que acelera los intensivos procesos de análisis requeridos por la seguridad a nivel de aplicación (Antivirus, filtrado de contenidos y procesos relacionados), estos procesos tendrían un rendimiento mucho más bajo si fueran llevados a cabo por procesadores de propósito general. FortiASIC™ también contiene un motor de aceleración para el cifrado que permite realizar filtrado Antivirus en tiempo real del tráfico de los túneles VPN. "Ibíd."

La exclusiva arquitectura basada en ASIC empleada por los equipos Fortinet permite el análisis del contenido del tráfico en tiempo real, satisfaciendo todas las necesidades de protección a nivel de aplicación sin impactar en el rendimiento de la red. El procesador FortiASIC™ posee múltiples características que hacen posible su alto rendimiento: "Ibíd."

- Contiene un motor hardware que acelera el análisis de las cabeceras de cada paquete y del contenido ensamblado de los paquetes de una conexión, acelerando de este modo los procesos del motor del

Firewall y del motor de IDS/IPS al ser capaz de identificar a velocidad de línea el flujo al que pertenece cada paquete. "Ibíd."

- Posee un potente motor de comparación de firmas que permite comparar el contenido del tráfico de una sesión contra miles de patrones de firmas de virus, ataques de intrusión, u otros patrones sin comprometer el rendimiento de la red. Este motor de análisis reensambla los paquetes pertenecientes a un mismo mensaje en memoria, carga las firmas necesarias y realiza una búsqueda por comparación de patrones, todos estos procesos se realizan a nivel de hardware con la ganancia en velocidad que eso supone. "Ibíd."
- El chip FortiASIC™ incluye también un motor de aceleración de cifrado que permite realizar cifrado y descifrado de alto rendimiento para el establecimiento de las Redes Privadas Virtuales o VPN. "Ibíd."

FortiOS™

El sistema operativo FortiOS™ fue diseñado con objeto de soportar funcionalidades de conmutación de alto rendimiento. El núcleo de FortiOS™ es un kernel dedicado, optimizado para procesamiento de paquetes y trabajo en tiempo real. Provee además de un interfaz homogéneo para cada una de las funcionalidades ofrecidas. Este sistema operativo funciona sobre diversos modelos de procesadores de propósito general, contando con biprocesadores en los equipos de gama alta. Esta flexibilidad permite emplear el mismo sistema operativo en todos los equipos FortiGate. "Ibíd."

a) Modalidad Router o Transparente

Los equipos FortiGate poseen la capacidad de trabajar en dos modalidades diferentes de funcionamiento: modo Router/NAT o modo Transparente. "Ibíd."

Modo Router (NAT): Trabajando en modo router el equipo actúa como un dispositivo de nivel 3, enrutando los paquetes entre los diferentes interfaces físicos y/o lógicos del equipo, con la capacidad de realizar NAT. "Ibíd."

Modo Transparente: Trabajando en modo transparente el equipo se comporta como un bridge, dejando pasar los paquetes a través el mismo en función de las políticas definidas. El equipo FortiGate no tiene direcciones IP en

sus interfaces (solamente posee una IP para la gestión del propio equipo y actualización de firmas). De este modo, el equipo puede ser introducido en cualquier punto de la red sin necesidad de realizar ninguna modificación sobre ningún otro dispositivo. "Ibíd."

El equipo FortiGate soporta las mismas funcionalidades en ambos modos de funcionamiento (firewall, antivirus, IPS, web filtering, antispam), con la única salvedad de que trabajando en modo transparente no se puede hacer NAT. "Ibíd."

Para el caso de ANT, se ha seleccionado el modo router (NAT) ya que permitirá controlar el tráfico que va entre la red interna (privada) y la red externa (Internet), adicionalmente la red interna permanecerá oculta al configurar Traducción de Dirección de Red.

b) Dominios Virtuales

Los equipos FortiGate permiten la utilización de Dominios Virtuales, de modo que sobre una única plataforma física podemos configurar hasta 500 Equipos virtuales, completamente independientes entre sí y con todas las funcionalidades que posee cada plataforma física. "Ibíd."

Todos los equipos FortiGate disponen en su configuración básica de la capacidad de definición de hasta 10 dominios virtuales, siendo posible ampliar el número de éstos en los equipos de gama alta (a partir de la gama FG3000), llegando hasta 500 Dominios Virtuales. Cada uno de estos dominios virtuales representan de forma lógica una máquina independiente del resto, asignándoles interfaces lógicos (VLAN’s) o físicos con la posibilidad de trabajar en modo router o transparente, aplicar diferentes perfiles y políticas sobre cada máquina, etc. "Ibíd."

c) Routing

Los equipos FortiGate pueden trabajar con enrutamiento dinámico, soportando RIP (v1 y v2), OSPF y BGP, además de trabajar con enrutamiento estático y ofrecer la posibilidad de realizar policy routing. "Ibíd."

- **Enrutamiento Estático Redundante**

Para cada ruta estática definida en el equipo es posible añadir diferentes gateways. De este modo, cuando la puerta de enlace definida como primaria no esté disponible, el equipo FortiGate encaminará los paquetes por el segundo gateway definido. Para poder detectar la caída de cualquiera de los elementos que componen el camino de salida definido con el gateway principal, cada interfaz posee la funcionalidad llamada Ping Server que nos permite monitorizar el estado de dicho camino mediante el envío de paquetes ICMP contra cualquier nodo de ese camino. "Ibíd."

Si el equipo FortiGate no recibe respuesta al ping definido, considera que dicho camino no está disponible y comienza a utilizar el siguiente gateway definido. De este modo podemos emplear la plataforma FortiGate para configurar múltiples conexiones a Internet, soportando redundancia entre ellas. "Ibíd."

- **Policy Routing**

Utilizando la funcionalidad de Policy Routing la plataforma FortiGate amplía el abanico de posibilidades de enrutamiento, permitiendo que el encaminamiento de los paquetes no se realice únicamente en función de la red de destino, sino teniendo en cuenta también los siguientes parámetros: "Ibíd."

- Interfaz Origen
- Protocolo, servicio o rango de puertos
- Interfaz y dirección destino

De este modo se podría, por ejemplo, hacer que el tráfico http (usando el puerto 80) fuese redirigido hacia un interfaz, mientras que el resto del tráfico es dirigido hacia otro, logrando de este modo balancear la carga entre dos interfaces de conexión a Internet, sin perder la redundancia de los mismos. "Ibíd."

- **Enrutamiento Dinámico**

Los equipos FortiGate soportan enrutamiento dinámico mediante los protocolos RIP (v1 y v2), OSPF y BGP, así como enrutamiento Multicast, PIM en sus dos versiones Sparse Mode yDense Mode, de modo que se permite la integración de las plataformas en entornos de red avanzados. "Ibíd."

d) Alta Disponibilidad

La capacidad de trabajar en cluster de alta disponibilidad (HA) dota a los equipos FortiGate de redundancia ante fallos. Además el cluster puede configurarse en modo activo-activo haciendo balanceo de carga del tráfico o en modo activo/pasivo en la que un único equipo procesa el tráfico de la red y es monitorizado por los demás para sustituirle en caso de caída. "Ibíd."

- Los equipos FortiGate pueden ser configurados en cluster, proporcionando escenarios de alta disponibilidad mediante la utilización de varios equipos redundantes entre sí, empleando un protocolo específico para la sincronización del cluster.
- El cluster puede estar formado hasta por 32 equipos
- La funcionalidad de Alta Disponibilidad está soportada por todas las plataformas FortiGate a partir del equipo FortiGate50B inclusive
- Cada miembro del cluster debe ser del mismo modelo hardware así como tener instalada la misma versión del Sistema Operativo.
- La funcionalidad de Alta Disponibilidad está soportada tanto en modo router como en modo transparente.

- **HA Heartbeat**

Los miembros del cluster se comunican entre ellos a través de un protocolo propietario denominado HA heartbeat. Este protocolo se utiliza para:

- Sincronizar la configuración entre los equipos.
- Sincronizar la tabla de sesiones activas tanto de firewall como de VPN.
- Informar a los otros miembros del cluster del estado del equipo y sus enlaces.

Los interfaces empleados para el intercambio de información entre los equipos del cluster son definidos por el administrador del equipo, sin necesidad de que sean enlaces dedicados a esta función y permitiendo que dichos enlaces sean empleados para transmitir tráfico de producción. "Ibíd."

Dado que los equipos que forman parte del cluster se intercambian información sobre las sesiones Firewall y VPN activas, la caída de un equipo o un enlace no afecta a estas sesiones, realizándose una protección ante fallos completamente transparente. "Ibíd."

El administrador puede definir aquellos interfaces cuyo estado quiere monitorizar con objeto de determinar cuándo debe cambiarse el equipo que actúa como activo en el cluster. "Ibíd."

- **Modos Activo-Activo y Activo-Pasivo**

Los equipos configurados en alta disponibilidad pueden trabajar en modo activo-activo o en modo activo-pasivo. Ambos modos de funcionamiento son soportados tanto en modo transparente como en modo router. "Ibíd."

- **Clúster activo-pasivo:** Consiste en un equipo FortiGate primario que procesa todo el tráfico y uno o más equipos subordinados que están conectados a la red y al equipo primario, pero no procesan tráfico alguno. "Ibíd."

- **Modo activo-activo:** Permite balancear la carga de tráfico entre las diferentes unidades que componen el cluster. Cada FortiGate procesa activamente las conexiones existentes y monitoriza el estado de los otros nodos del cluster. El nodo primario procesa el tráfico y redistribuye el tráfico entre los diferentes equipos que forman parte del cluster. "Ibíd."

Esta funcionalidad permitirá suplir las falencias del equipamiento de seguridad actual, la mayor parte de problemas en la red se han ocasionado por no contar con un sistema de alta disponibilidad. En el caso de ANT se ha seleccionado el modo clúster activo pasivo a fin de que el equipo pasivo cuente con las mismas configuraciones y nivel de rendimiento que el equipo en estado activo. Esta permitirá restablecer en pocos segundos los servicios manteniendo la integridad de los datos, permitirá que los usuarios no se percaten que se ha producido un problema.

e) Optimización WAN

La optimización o aceleración WAN posibilita la mejora y el incremento de rendimiento y seguridad en comunicaciones a través de redes de área extensa, como puede ser el caso de Internet o MacroLans. Esta función está disponible por VDOM (firewall virtual) configurándose de manera independiente para cada uno de ellos, lo que dota de mucha flexibilidad sobre todo en entornos con varias localizaciones dispersas o servicios gestionados. "Ibíd."

La tecnología de compresión utilizada es propiedad de Fortinet, con lo que no es compatible con aceleradores de terceros, aunque sí lo es con el cliente Forticlient WAN Optimization. "Ibíd."

Las principales funcionalidades aportadas son la optimización de la comunicación, reducción del ancho de banda consumido, gracias a la optimización del protocolo de comunicación utilizado, byte caching, web caching y la posible securización de la comunicación cliente/servidor a través de la red WAN gracias al establecimiento de un túnel seguro. Con esto se reducen latencias, se incrementa el rendimiento y se garantiza la privacidad en las transacciones. "Ibíd."

f) Autenticación de Usuarios

Las plataformas FortiGate soportan la autenticación de usuarios en diferentes funcionalidades, como son:

- **Autenticación a través de políticas de Firewall o Identity based Policy:** Cuando un determinado tráfico es identificado por una política definida en el Firewall que tiene habilitada la opción de autenticación, el equipo decide si dicho tráfico es permitido o no en función del usuario del que se trate, de esta forma la granularidad de las reglas puede llevarse a cabo en función del origen del tráfico o en función del grupo de usuarios que generen el tráfico. Esta autenticación puede realizarse contra una base de datos local creada en el propio equipo, o bien contra servidores externos RADIUS, TACACS +, LDAP o Active Directory, pudiendo realizarse con este último una autenticación transparente de los usuarios que pertenezcan al Directorio Activo de Microsoft. "Ibíd."

- **Autenticación de usuarios VPN:** Cuando un usuario intenta acceder la red interna a través del servicio de acceso remoto VPN provisto por los equipos FortiGate, ya sea IPSec o SSL la tecnología empleada, el equipo solicita la autenticación del usuario de forma previa a establecer la conexión. Esta autenticación se puede realizar mediante una base de datos local, o bien mediante la utilización de servidores externos (RADIUS, LDAP, AD, etc.). "Ibíd."

Fortinet dispone de un protocolo propietario denominado FSAE (Fortinet Server Authentication Extension) que interactúa con el Servidor de Directorio Activo. El protocolo FSAE se basa en la utilización de un agente ligero software que se instala en el servidor AD y que desde ese momento establece un diálogo con el equipo FortiGate. Así, cada vez que un usuario se valida en el servidor AD, el agente FSAE informa al equipo FortiGate de qué usuario se ha validado, a qué grupo pertenece y que dirección IP le ha sido asignada. A partir de ese momento, cada vez que el usuario realice alguna operación que implique validación por parte del Firewall contra el Directorio Activo, como puede ser el acceso a Internet, la validación se realiza de forma transparente gracias a la información que se han intercambiado el servidor AD y el equipo FortiGate. "Ibíd."

Con esta funcionalidad se solucionan los problemas de autenticación, pues permitirá realizar el control de usuarios al poder filtrar por dirección IP, ID de red y el acceso por VPN y su validación por parte del Firewall contra el Directorio Activo.

g) Firewall

Los equipos FortiGate poseen la funcionalidad de firewall basada en tecnología Stateful Inspection Packet. Esto le permite hacer un análisis exhaustivo de la cabecera de cada paquete, identificando la sesión a la que pertenece, chequeando el correcto orden de los paquetes y realizando control sobre el tráfico de la red. "Ibíd."

Las políticas del firewall controlan todo el tráfico que atraviesa el equipo FortiGate. Cada vez que el Firewall recibe un nuevo paquete, analiza la cabecera de este para conocer las direcciones origen y destino, el servicio al que

corresponde ese paquete, y determina si se trata de una nueva sesión o bien pertenece a una sesión ya establecida y llega en el orden correcto. "Ibíd."

Este análisis de la cabecera es acelerado mediante el Circuito Integrado de Aplicación Específica FortiASIC, lo que permite a las plataformas FortiGate alcanzar un rendimiento mayor y un número de nuevas sesiones por segundo superior al de cualquier solución basada en la utilización de una CPU de propósito general. "Ibíd."

Las políticas de seguridad son definidas en el firewall en base a los interfaces origen y destino. Este modo de definición de las políticas permite optimizar el rendimiento y el procesamiento de cada uno de los flujos, ya que para cada uno de los paquetes es identificado su origen y su destino y enviado entonces al módulo de routing. Esta organización permite que el paquete sea tan solo comparado contra las reglas definidas entre esos interfaces, comenzando por la superior de todas y descendiendo hasta encontrar aquella con que coincida en función de los diferentes parámetros configurables para cada política (par origen/destino, servicio, calendario, etc.). Si no se encontrara ninguna regla que coincidiera con el paquete analizado, éste sería descartado. Al tener que comparar contra un grupo menor que el total de las reglas definidas, el tiempo requerido disminuye, lo que agregado a la utilización de la tecnología FortiASIC confiere a los equipos FortiGate un rendimiento inigualable como firewall. "Ibíd."

- **Definición de Políticas**

  Las políticas del firewall se definen en base a los siguientes criterios: "Ibíd."

  - Interfaces de entrada y salida del flujo. Puede referirse tanto a Interfaces Físicos del equipo como a interfaces lógicos definidos como VLAN Interface, siguiendo el estandar 802.1Q para marcado de tramas de cada VLAN, o pueden establecerse como Any para que se utilice cualquier interfaz de entrada o salida.
  - Direcciones o grupos de direcciones IP origen y destino.
  - Protocolo, servicio o puertos TCP/UDP.

La política define la acción a tomar con aquellos paquetes que cumplan los criterios definidos. Entre las acciones a realizar están:

- Permitir la conexión.
- Denegar la conexión.
- Requerir autenticación antes de permitir la conexión. La validación de usuario puede realizarse contra usuarios registrados en local, o bien haciendo uso de servidores externos que pueden ser RADIUS, LDAP y/o Directorio Activo.
- Procesar el paquete como perteneciente a una conexión tunelizada mediante IPSec.
- Realizar traducción de direcciones.
- Aplicar reglas de gestión de ancho de banda.
- Analizar el tráfico mediante funcionalidades adicionales de seguridad, como Antivirus, AntiSpam, Detección/Prevención de Intrusiones, filtrado Web, etc. mediante la definición de un perfil de protección.

A cada política se le puede definir un horario, tanto único como recursivo, que permite acotar la aplicación de la regla a un espacio temporal determinado en función de la hora, el día de la semana, mes o año. "Ibíd."

Cada política permite realizar traducción de direcciones mediante NAT, permitiendo realizar una traducción estática de direcciones, o bien utilizar grupos de direcciones con objeto de realizar NAT dinámico, y así mismo definir traducciones de puertos (PAT). "Ibíd."

En cada política se puede habilitar el seguimiento de aquellas conexiones que atraviesan el firewall de acuerdo a la política definida, con objeto de poder hacer un registro de las conexiones establecidas a través del equipo. "Ibíd."

- **Inspección SSL**

Dentro del perfil de protección se podrá aplicar la configuración necesaria para poder efectuar inspección dentro de protocolos seguros basados en SSL, como HTTPS, SMTPS, POP3S e IMAPS. "Ibíd."

De esta forma será posible aplicar dentro de los túneles SSL que atraviesen la plataforma inspección de contenidos, así como inspección Antivirus, IPS o control de aplicaciones. "Ibíd."

- **Balanceo de carga multiplexación http y aceleración SSL**

Los dispositivos FortiGate permiten la configuración de IP's virtuales (VIP's) de manera que estas ofrecen balanceo de carga de servidores, teniendo la capacidad de que las peticiones realizadas a la IP virtual puedan ser atendidas por un grupo de servidores habilitados para ese efecto. La distribución del balanceo de carga puede ser configurado a nivel de puertos TCP o UDP, con la posibilidad de tener varios servicios desplegados en la misma IP y atendidos por grupos de servidores distintos. Cada uno de los servidores que componen grupo de balanceo, puede ser monitorizado a nivel ICMP, TCP o http de manera que ente el fallo de un servidor, el servicio continúa activo en el resto de equipos, dotando a la plataforma de alta disponibilidad. "Ibíd."

- **Calidad de Servicio (QoS)**

Mediante la aplicación de técnicas de Calidad de Servicio la red provee un servicio prioritario sobre el tráfico más sensible al retardo. Los equipos FortiGate permiten aplicar técnicas de priorización de tráfico y Calidad de Servicio (QoS), reservar ancho de banda para aquellas aplicaciones que sean más sensibles al retardo, o bien limitar el ancho de banda de aquellas aplicaciones que hagan un uso intensivo de los recursos de la red. "Ibíd."

La Calidad de Servicio es una funcionalidad fundamental para poder gestionar el tráfico generado por la transmisión de voz y las aplicaciones multimedia. Estos tipos de tráfico son enormemente sensibles al retardo y a la variación del mismo (jitter). Una adecuada gestión de la calidad de servicio nos permitirá la utilización de estas aplicaciones sin recurrir a una ampliación innecesaria del ancho de banda de la red, reservando el ancho de banda necesario y priorizando este tipo de tráfico ante otros menos sensibles al retardo como pueda ser el correo o el tráfico ftp. "Ibíd."

Los equipos FortiGate proveen calidad de servicio para todos los servicios soportados, incluyendo H.323, SIP, TCP, UDP, ICMP o ESP.

La Calidad de Servicio es implementada en las plataformas FortiGate del siguiente modo:

- La gestión de ancho de banda se realiza mediante la utilización de buffers que permiten regular los diferentes flujos de tráfico en base a la velocidad de transmisión de los paquetes. Lo que se consigue de este modo es evitar que los paquetes sean descartados, haciendo que se almacenen en el buffer hasta su transmisión, retrasando su envío hasta que sea posible. Los equipos FortiGate usan la técnica Token Bucket para garantizar y limitar el ancho de banda. "Ibíd."
- La bufferización se realiza en función de la prioridad asignada a cada flujo, pudiendo variar entre prioridad alta, media o baja. Si el ancho de banda no es suficiente para el envío de todos los paquetes almacenados, se transmiten en primer lugar los de prioridad alta. "Ibíd."
- La tecnología DiffServ permite modificar los parámetros DSCP, siguiendo las normas RFC 2474 y 2475. Así, aquellos componentes de la red compatibles con DiffServ, son capaces de interpretar la prioridad de los paquetes transmitidos inspeccionando las cabeceras de los paquetes y clasificando, marcando, y gestionando el tráfico en base a esta información. "Ibíd."

- **Calidad de Servicio Basada en Políticas**

Los equipos FortiGate aplican la calidad de servicio de manera diferenciada en cada una de las políticas definidas en el firewall a través de perfiles previamente definidos. Una vez que el flujo de tráfico ha sido identificado por alguna de las políticas existentes, los parámetros QoS definidos en dicha política se aplican sobre ese flujo particular de tráfico. "Ibíd."

- **Gestión del Ancho de Banda (Traffic Shaping) a nivel de políticas**

Los parámetros de configuración del ancho de banda nos permiten definir un ancho de banda mínimo o un límite máximo para el tráfico identificado con esa política. El ancho de banda definido no puede superar el ancho de banda total disponible, pero puede ser empleado para mejorar la calidad del uso de este

ancho de banda por aquellas aplicaciones que hagan un uso intensivo del mismo, o bien aquellas aplicaciones sensibles al retardo. "Ibíd."

- **Gestión del Ancho de Banda (Traffic Shaping) a nivel de Interfaces**

Igual que a nivel de políticas, los dispositivos FortiGate permiten la gestión de ancho de banda a nivel de interfaz, permitiendo definir un ancho de banda máximo asociado a una interfaz específica, de esta forma se consigue limitar el tráfico entrante a una interfaz determinada pudiendo hacer control del ancho de banda disponible por interfaz. Esta técnica aplica tanto a interfaces físicas como a interfaces lógicas, tipo VLAN o VPN. "Ibíd."

- **Soporte DiffServ**

La funcionalidad DiffServ puede ser configurada en el equipo FortiGate con objeto de modificar los valores DSCP (Differentiated Services Code Point) para todos los paquetes a los que se aplica una política en particular. "Ibíd."

Cada política se puede configurar para aplicar esos valores en cada uno de los sentidos del flujo, siendo independientes ambos parámetros entre sí. "Ibíd."

- **Soporte VoIP**

Los equipos FortiGate incorporan soporte para los protocolos más demandados de VoIP (H323, SIP, SCCP, SIMPLE) aplicando sobre estos los mayores controles de seguridad y reporting a través de los protección profiles. Entre las funcionalidades soportadas cabe destacar. "Ibíd."

- Escaneo Antivirus para transferencias de ficheros realizadas sobre IM vía protocolos SIP/SIMPLE.
- Application layer gateway para SIP basado en SCTP y TCP.
- Compresión/descompresión de cabeceras SIP.
- Mantenimiento de la información IP original incluso cuando está presente NAT.
- Conversión entre SIP basado en TCP y SIP basado en SCTP y viceversa.
- Limitación del número de mensajes.

Como se aprecia la funcionalidad de firewall ofrecida por Fortinet permitirá solventar la falta de control en la red (cantidad de puertos TCP y UDP abiertos innecesariamente), esto permitirá ejercer un control adecuado de acceso a los servicios y servidores de ANT y así poder hacer un registro de las conexiones establecidas a través del equipo.

h) VPN

Los equipos FortiGate soportan el establecimiento de Redes Privadas Virtuales basadas en protocolos IPSec y SSL, además de PPTP y L2TP. De esta forma, oficinas pequeñas, medias, corporaciones e ISPs pueden establecer comunicaciones privadas sobre redes públicas garantizando la confidencialidad e integridad de los datos trasmitidos por Internet. "Ibíd."

Al estar integrada la funcionalidad VPN en la propia plataforma FortiGate, el tráfico VPN puede ser analizado por el módulo de Firewall así como por las funcionalidades adicionales antivirus, IPS, web filtering, antispam, etc. "Ibíd."

- **Internet Protocol Security (IPSec)**

Un marco de trabajo para el intercambio seguro de paquetes a nivel de la capa IP, nivel 3. Las unidades FortiGate implementan el protocolo Encapsulated Security Payload (ESP) en modo túnel. Los paquetes cifrados aparecen como paquetes ordinarios que pueden ser enrutados a través de cualquier red IP. "Ibíd."

Para el establecimiento de redes privadas virtuales basadas en IPSec, FortiGate cumple el estándar IPSec y soporta:

- Algoritmos de cifrado: DES, 3DES y AES 128, 192 y 256
- NAT Transversal
- DPD (Dead Peer Detección, detección de caída del nodo remoto)
- Autenticación basada en pre-shared key con usuarios definidos en una base de datos local o en un servidor externo (LDAP, RADIUS, Directorio Activo), certificados X.509, autenticación extendida XAuth.
- Interoperabilidad con otros fabricantes IPSec Compliant (Cisco, Checkpoint, etc.).
- Alta disponibilidad de enlaces VPN desde un único equipo.

- Posibilidad de definir hasta 3 puertas de enlace diferentes para cada túnel para resistencia ante fallos.
- Soporte de acceso redundante a Internet.

- **Point-to-Point Tunneling Protocol (PPTP)**

Este protocolo habilita la interoperabilidad entre las unidades FortiGate y los clientes PPTP Windows o Linux. PPTP utiliza protocolos de autenticación PPP; de este modo clientes Windows o Linux PPTP pueden establecer un túnel PPTP contra un equipo FortiGate que ha sido configurado para trabajar como un servidor PPTP. Como alternativa, el equipo FortiGate puede ser configurado para reencaminar paquetes PPTP a un servidor PPTP en la red. Para la autenticación de los clientes, FortiGate soporta PAP, CHAP y autenticación de texto plano. "Ibíd."

Los clientes PPTP son autenticados como miembros de un grupo de usuarios. El protocolo PPTP ofrece un grado menor de seguridad que IPSec, ya que el canal de control de mensajes PPTP no es autenticado y su integridad no está protegida. Además, los paquetes encapsulados PPP no son criptográficamente protegidos y pueden ser leídos o modificados. "Ibíd."

- **VPN SSL**

Las Soluciones VPN SSL aportan un sistema de acceso remoto seguro a nuestra red que, garantizando en todo momento la confidencialidad e integridad de la información, constituye un sistema con una implantación, administración y mantenimiento simplificado. Dado que las VPN SSL usan cifrado SSL, no es necesaria la instalación de ningún software específico en los ordenadores remotos, sino que resulta accesible desde cualquier navegador, lo que supone un gran avance frente a las tradicionales VPN basadas en IPSec, en lo que a sistemas de acceso de usuario se refiere. De este modo, se ofrece un método de acceso a los sistemas de información de cualquier organización que no requiere de la implantación de ninguna aplicación específica en los ordenadores remotos con lo que se permite un acceso controlado a los recursos, con total garantía de seguridad. "Ibíd."

Todas las plataformas FortiGate incorporan la posibilidad de ser utilizadas como servidor de túneles SSL, con una configuración sencilla que permite la autenticación de usuarios mediante sistemas de autenticación robusta y la personalización del servicio de acceso remoto. "Ibíd."

Adicionalmente se cuentan con características habituales en este tipo de solución, como posibilidad de establecer conexiones mediante clientes pesados (descargando un ActiveX) o personalizar al completo el portal de acceso SSL que se le presenta a los usuarios. "Ibíd."

Esta funcionalidad solventa el problema de conexión con terceros ya que permite realizar autenticación de usuarios locales en el equipo o permitirá realizar conexiones cifradas al poder utilizar los protocolos de tunelización soportados por los equipos Fortigate y la interoperabilidad con otros fabricantes (Cisco, Checkpoint, etc.).

Esta funcionalidad solventa el problema de conexión con terceros ya que permite realizar autenticación de usuarios locales en el equipo o permitirá realizar conexiones cifradas al poder utilizar los protocolos de tunelización soportados por los equipos Fortigate y la interoperabilidad con otros fabricantes. Adicionalmente el tráfico VPN puede ser analizado por el módulo Firewall así como por las funcionalidades adicionales (antivirus, IPS, web filtering, antispam).

i) Antivirus

FortiGate ofrece el sistema antivirus perimetral de mayor rendimiento gracias a su optimizada arquitectura y configuración. Los componentes principales del sistema antivirus de FortiGate son:

- La arquitectura hardware basada en FortiASIC.
- Su optimizado sistema operativo FortiOS.
- La infraestructura FortiProtect, los laboratorios y centros de desarrollo distribuidos a lo largo de todo el mundo.

Si el sistema FortiGate detecta la existencia de un archivo infectado en una transmisión, el archivo es eliminado o guardado en cuarentena, y es sustituido por un mensaje de alerta configurable por el administrador. Además, el equipo

FortiGate guarda un registro del ataque detectado, y puede configurarse el envío de un correo de alerta o un trap SNMP. "Ibíd."

Para una protección extra, el motor antivirus es capaz de bloquear ficheros de un tipo específico (.bat, .exe, etc) que potencialmente sean contenedores de virus, o bien bloquear aquellos archivos adjuntos de correo electrónico que sean de un tamaño superior al límite de filtrado. "Ibíd."

El filtrado antivirus de FortiGate protege la navegación web (protocolo http), la transferencia de archivos (protocolo ftp) y los contenidos transmitidos por correo electrónico (protocolos IMAP, POP3 y SMTP), siendo posible escanear estos protocolos en puertos diferentes a los habitualmente empleados, e incluso en múltiples puertos. "Ibíd."

j) Detección y Prevención de Intrusión (IDS/IPS)

El Sistema de Detección de Intrusión de FortiGate constituye un sensor de red en tiempo real que utiliza definiciones de firmas de ataques y detección de comportamientos anómalos para detectar y prevenir tráfico sospechoso y ataques de red. "Ibíd."

El motor IDS provee seguridad hasta la capa de aplicación, sin mermar por ello el rendimiento de la red. La capacidad de IDS de los equipos FortiGate se basa en el modulo de routing, el modulo de firewall y la capa de aplicación. De esta forma el sistema de detección de intrusiones no se limita únicamente a la detección de ataques de nivel de red ni tampoco al análisis individual de cada paquete. FortiGate reensambla el contenido de los paquetes en línea y lo procesa para identificar ataques hasta el nivel de aplicación. "Ibíd."

Cada sensor (Red, IP, Transporte, Aplicación) es un programa que genera un tráfico ínfimo. Elsensor utiliza el hardware FortiASIC para acelerar la inspección del tráfico y chequear patrones de tráfico que concuerden con las firmas y anomalías especificadas. La arquitectura hardware asistida de detección de intrusión provee a los equipos FortiGate de rendimientos excepcionales únicos en el mercado. "Ibíd."

La funcionalidad IPS de FortiGate detecta y previene los siguientes tipos de ataques:

- Ataques de Denegación de Servicio (DoS).
- Ataques de Reconocimiento.
- Exploits.
- Ataques de Evasión de Sondas IDS.

- **Métodos de Detección**

Las estrategias mediante las que las que la plataforma FortiGate es capaz de realizar las tareas de detección y prevención de intrusión son dos: detección de firmas y seguimiento de comportamientos anómalos. "Ibíd."

- **Detección de Firmas**

Las firmas de ataques se encuentran en el núcleo del modulo de detección de intrusiones FortiGate (más de 3600 firmas soportadas). Las firmas son los patrones de tráfico que indican que un sistema puede estar bajo un ataque. Funcionalmente, las firmas son similares a las definiciones de virus, con cada firma diseñada para detectar un tipo de ataque particular. "Ibíd."

Tanto las firmas predefinidas como el motor IPS, son actualizables a través de FortiProtect Distribution Network (FDN), de un modo similar al que se actualizan las definiciones de antivirus.

- **Detección de Anomalías de Tráfico**

Los equipos FortiGate analizan las secuencias de paquetes y el establecimiento de sesiones de acuerdo a los patrones de tráfico definidos en los diferentes protocolos estándar. FortiGate IPS identifica a su vez anomalías estadísticas de tráfico TCP, UDP e ICMP, como son: "Ibíd."

- Flooding: Si el número de sesiones apunta a un solo destino en un segundo está sobre el umbral, el destino está experimentando flooding.
- Scan: Si el número de sesiones desde un origen único en un segundo está sobre el umbral, el origen está siendo escaneado.

- Source: Si el número de sesiones concurrentes desde un único destino está sobre los umbrales, el límite de sesiones por origen está siendo alcanzado.
- Destination session limit: Si el número de sesiones concurrentes a un único destino está sobre el umbral, el límite de sesiones por destino está siendo alcanzado.

Los umbrales pueden ser configurados por el usuario para tener capacidad de contemplar situaciones excepcionales, como la existencia de un proxy en la red, etc. "Ibíd."

- **Prevención de Intrusiones en Tiempo Real**

Cuando los ataques son detectados, el sistema toma acciones las acciones necesarias para prevenir daños. Cualquier ataque detectado puede ser bloqueado, ya sean ataques basados en firmas, ataques basados en anomalías, o ataques personalizados. "Ibíd."

Debido a que el módulo IDS está completamente integrado con el motor de firewall, los equipos FortiGate proveen detección y prevención de intrusiones en tiempo real. El módulo IDS posee un enlace específico en el modulo de firewall que permite que una vez el sensor identifica un ataque, el modulo firewall rápidamente toma acción para bloquear el tráfico impidiendo que el ataque tenga éxito. Los equipos FortiGate permiten definir diferentes acciones a realizar en función del ataque detectado: "Ibíd."

- Pass: FortiGate permite que el paquete que activó (triggered) la firma pase a través del firewall.
- Drop: El equipo FortiGate descarta el paquete que activó la firma.
- Reset: El equipo descarta el paquete que activó la firma, envía un reset al cliente y al servidor, y borra la sesión de la tabla de sesiones del equipo FortiGate.

- **Actualizaciones de la Base de Datos de Firmas de Ataques y Motor de Escaneo**

En las actualizaciones del servicio IPS/IDS se actualiza la base de datos de ataques y anomalías reconocidas y el motor de escaneo, los cuales son continuamente renovados por Fortinet y distribuidos mediante la red FortiProtect tan pronto como nuevas formas de ataque son encontradas y difundidas. "Ibíd."

- **Actualizaciones automáticas**

Los equipos FortiGate son dinámicamente actualizados gracias la red FortiProtect Distribution Network (FDN). Los servidores FDN se encuentran distribuidos a lo largo de todo el mundo con disponibilidad 24x7 para entregar nuevas firmas y motores para los dispositivos FortiGate. "Ibíd."

Todos los equipos FortiGate están programados con una lista de servidores FDN más cercanos de acuerdo a la zona horaria configurada en el equipo. Así mismo, las plataformas de gestión FortiManager pueden actuar como un nodo de la red FDN para los equipos que gestiona. "Ibíd."

Los dispositivos FortiGate soportan dos modos de actualización:

- **Pull updates:** Los equipos pueden comprobar automáticamente si existen en la red FDN nuevas definiciones de virus disponibles y, si encuentran nuevas versiones, descargarlas e instalarlas automáticamente, así como los motores de antivirus actualizados. Estas comprobaciones pueden ser programadas para su realización en periodos horarios, diarios o semanales. "Ibíd."

- **Push updates:** Cada vez que un nuevo motor de antivirus o un nuevo fichero de definiciones es publicado, los servidores que forman parte de la red FDN notifican a todos los equipos FortiGate configurados para push updates que una nueva actualización está disponible. En 60 segundos desde la recepción de una notificación push, el equipo FortiGate se descargará la actualización desde la FDN. "Ibíd."

- **Actualizaciones Manuales**

A parte de los métodos de actualizaciones expuestos anteriormente, los equipos FortiGate poseen la opción de realizar actualizaciones manuales. El administrador del equipo FortiGate puede iniciar la actualización manual simplemente seleccionando la opción de “Update now” desde la consola de gestión del equipo FortiGate. "Ibíd."

k) Control de Aplicaciones

Los módulos de filtrado de contenido y filtrado web permitirán realizar un control efectivo, estos módulos controlarán aplicaciones evasivas o que cambien de puerto con frecuencia ya que actualmente personal de ANT hace evasión del control ya que el equipamiento actual no controla de manera adecuada la navegación y utilización de aplicaciones que causan el excesivo uso de ancho de banda.

En la actualidad hay infinidad de aplicaciones que fluyen por la red, siendo algunas de ellas productivas y otras no. Con el control de aplicaciones es posible verificar el tráfico basándose en las propias aplicaciones que lo generan y no en el puerto utilizado. De esta forma es posible permitir el tráfico en el puerto 80, pero controlar programas de mensajería instantánea o P2P que habitualmente hacen uso de este puerto como medida evasiva. "Ibíd."

Las principales ventajas que aporta el control de aplicaciones son las siguientes:

- Ir más allá del control tradicional de nivel 3 de los firewalls convencionales, pudiendo así controlar aplicaciones evasivas o que cambien de puerto con frecuencia. "Ibíd."
- Uno de los vectores de infección de malware más habitual es el intercambio de ficheros a través de uno de los protocolos más utilizados como es http, por ello surge la necesidad de poder controlar las distintas aplicaciones que hacen uso de este mecanismo común.
- Obtener una mayor visibilidad de la red, de forma que sea posible conocer en profundidad y con detalle el uso que se hace de este recurso por parte de los usuarios de una organización. "Ibíd."

En la actualidad se cuenta con más de 1000 aplicaciones soportadas, adicionalmente y apoyándose en el motor IPS, se prevé catalogar nuevas aplicaciones que se irán incluyendo. "Ibíd."

l) Filtrado de Tráfico Web (URL Web Filtering)

La distribución y visualización de contenido no autorizado supone un riesgo importante para cualquier organización. Para las empresas, la monitorización del uso que sus empleados hacen de los accesos a Internet y la prevención de visualización de contenidos web inapropiados o no autorizados se ha convertido en algo necesario, justificado por los costes financieros y las implicaciones legales que conlleva la pasividad en este aspecto. "Ibíd."

El servicio FortiGate web filtering puede ser configurado para escanear toda la cadena del contenido del protocolo http permitiéndonos filtrar direcciones URL potencialmente no asociadas al desarrollo de la normal actividad laboral, contenidos embebidos en las propias páginas web o scripts basados en java, activeX o cookies, contenidos potencialmente peligrosos. "Ibíd."

La funcionalidad de filtrado web puede definirse mediante listas creadas por el propio usuario, o bien mediante la utilización del servicio FortiGuard Web Filtering. "Ibíd."

- **URL Filtering mediante uso de listas locales**

El filtrado de URL puede implementarse utilizando bases de datos locales con listas black/white list definidas por el usuario que contienen URLs cuyo acceso está permitido o denegado. El acceso a URLs específicas puede ser bloqueado añadiéndolas a la lista de bloqueo de URLs. El dispositivo FortiGate bloquea cualquier página web que coincida con la URLs especificada y muestra un mensaje de sustitución de la misma al usuario. "Ibíd."

- **Filtrado de Contenido mediante listas locales**

Los dispositivos FortiGate pueden ser configurados para bloquear aquellas páginas web que contengan palabras o frases clave incluidas en la lista de Banned Words. Cuando una página web es bloqueada, un mensaje de alerta que

sustituye a la web original generado por FortiGate es mostrado en el navegador del usuario. "Ibíd."

Las palabras clave pueden ser añadidas una por una, o importadas utilizando un fichero de texto. Estas palabras pueden ser palabras individuales o una cadena de texto de hasta 80 caracteres de longitud. Las palabras pueden estar en varios lenguajes utilizando los sistemas de caracteres Western, Simplified Chinese, Traditional Chinese, Japanese, Thaï o Korean. "Ibíd."

Las palabras y expresiones pueden ser configuradas utilizando comodines o expresiones regulares perl. "Ibíd."

- **Filtrado de Java / Scripts / Cookies**

El filtrado de contenido web también incluye características de filtrado de scripts y códigos maliciosos que puede ser configurado para bloquear contenido web inseguro tal y como Java Applets, Cookies y ActiveX. "Ibíd."

m) AntiSpam

Uno de los principales problemas de ANT es la recepción diaria de spam, el equipamiento de Fortinet permitirá realizar el análisis en tiempo real del correo electrónico para los protocolos SMTP, POP3 e IMAP gracias al análisis y comparación con servidores externos propios de FortiGuard y con servicios de listas negras.

La funcionalidad AntiSpam de los equipos FortiGate permite gestionar los correos no solicitados detectando los mensajes de spam e identificando esas transmisiones. Los filtros antispam se configuran de un modo global, si bien son aplicados en base a perfiles de protección, al igual que el resto de funcionalidades del equipo. "Ibíd."

La funcionalidad AntiSpam ofrecida por los equipos FortiGate consiste en la aplicación de diferentes filtros sobre el tráfico de intercambio de correo electrónico (protocolos SMTP, POP3 e IMAP). Aquellos filtros que requieren la conexión con servidores externos (FortiGuard Antispam o los servicios de Listas Negras en tiempo real) se ejecutan de forma simultánea con los otros filtros, optimizando el tiempo de respuesta del análisis de los mensajes. Tan pronto como alguno de los

filtros aplicados identifica el mensaje como spam se procede a realizar la acción definida para cada filtro que podrá ser: "Ibíd."

- Marcar el mensaje como Spam (Tagged): El mensaje quedará identificado como Spam y en el perfil de protección podremos decidir si se deja pasar, identificándolo como Spam y pudiendo incluir en la cabecera del mismo o en el encabezamiento MIME un mensaje identificativo, o bien si preferimos descartar el mensaje (solo sobre SMTP). "Ibíd."
- Descartar (Discard): En este caso el mensaje es desechado, en el caso de SMTP es posible sustituirlo con un mensaje predefinido que advierta al usuario del envío de Spam. "Ibíd."

Los filtros antispam aplicados por la plataforma FortiGate a los mensajes de correo se basan en el control por origen del mensaje y el control por el contenido del mismo. "Ibíd."

n) Data Leak Prevention

Cambiando el enfoque tradicional de las plataformas de seguridad perimetrales cuyo objetivo histórico ha sido evitar que el malware y los intrusos accedan a la red interna o protegida, la característica de Prevención de Fuga de Información o DLP (Data Leak Prevention) ofrece la posibilidad de evitar que la información categorizada como sensible o confidencial salga fuera de la organización a través de la plataforma. "Ibíd."

Es posible llevar a cabo esta protección en diferentes protocolos de transferencia de datos utilizados usualmente, como smtp, ftp o http, con reglas o grupos de reglas predefinidas, un buen ejemplo es una de ellas que inspecciona en busca de números de tarjetas de crédito, o reglas totalmente personalizables. "Ibíd."

o) Gestión de los Equipos FortiGate

Cada equipo FortiGate puede ser gestionado localmente mediante acceso http, https, telnet o SSH, siendo estos accesos configurables por interfaz, Además

existe la posibilidad de definir diferentes perfiles de administración con objeto de limitar las tareas y posibilidades de cada usuario con acceso al equipo. "Ibíd."

Fortinet cuenta además con una plataforma de gestión global centralizada para múltiples equipos denominada FortiManager™. El sistema FortiManager™ es una plataforma integrada para la gestión centralizada de equipos FortiGate a través del cual pueden configurarse múltiples dispositivos FortiGate de forma simultánea, creando grupos de equipos y plantillas de configuración y permitiendo monitorizar el estado de estos dispositivos. "Ibíd."

- **Gestión Centralizada con FortiManager**

FortiManager es la plataforma de gestión centralizada de Fortinet. FortiManager permite la centralización de las acciones que se han de llevar a cabo en los equipos FortiGate permitiendo un rápido despliegue de los proyectos de seguridad, el mantenimiento y actualización de los distintos dispositivos FortiGate y su monitorización en tiempo real. "Ibíd."

Además, con FortiManager se puede gestionar la suite de PC FortiClient y el gestor de logging y reporting FortiAnalyzer, presentando una única interfaz de gestión para todos los elementos de seguridad. Así mismo, la plataforma FortiManager se puede utilizar como servidor de actualización de firmas de los equipos FortiGate, como si fueran un nodo más de la red FDN, pero que forma parte de la red del usuario, pudiendo de esta manera centralizar la gestión de las descargas de seguridad de los equipos. "Ibíd."

- **Registro de Logs**

La capacidad de registro de eventos, tráfico y aplicaciones puede ser habilitada tanto a nivel global como en cada una de las políticas definidas a nivel de firewall y en cada protection profile, permitiéndonos configurar con un elevado nivel de detalle y de forma independiente cada uno de los registros que se requieren. "Ibíd."

Estos registros pueden ser almacenados localmente (en memoria o en disco, en aquellas unidades que disponen de él) o bien en un servidor externo como pueden ser un syslog o la plataforma FortiAnalyzer. "Ibíd."

- **Registro centralizado y gestión de informes con FortiAnalyzer**

FortiAnalyzer es una plataforma dedicada al registro centralizado de logs y la gestión y tratamiento de los mismos. FortiAnalyzer posee la capacidad de generar más de 350 informes diferentes que nos aportan información detallada sobre los eventos registrados a nivel de Firewall, ataques, virus, VPN, utilización web, análisis forense, etc. Entre los posibles informes cabe destacar: "Ibíd."

- Informes de ataques: ataques registrados por cada equipo FortiGate, señalando el momento en el que son registrados, e identificados a las fuentes más comunes de ataque.
- Informes de virus: top virus detectados, virus detectados por protocolo.
- Informe de Eventos: eventos propios de la máquina, de administración de la misma, etc.
- Informe de utilización del correo electrónico: usuarios más activos en envío y recepción, ficheros adjuntos bloqueados identificados como sospechosos.
- Informe de utilización del tráfico web: usuarios web top, sitios bloqueados, usuarios de mayor frecuencia de intento de acceso a sitios bloqueados, etc.
- Informe de utilización de ancho de banda: informes de uso del ancho de banda por usuario, día, hora y protocolo.
- Informes por protocolo: Protocolos más utilizados, usuarios ftp /telnet top.
- FortiAnalyzer incluye un registro histórico y en tiempo real del tráfico de cada uno de los equipos FortiGate gestionados, así como una herramienta de búsqueda en los logs.

Aparte de la capacidad de generación de informes y de la gestión de los logs de las distintas plataformas FortiGate, FortiAnalyzer puede actuar como gestor de alertas bajo determinadas condiciones configurables por el administrador de seguridad. De esta forma se centralizan las alertas de seguridad en un único dispositivo evitando la dispersión y las dificultades de gestión asociadas a esta. Como elementos de análisis de la red FortiAnalyzer cuenta con un monitor de

tráfico en tiempo real y un escáner de vulnerabilidades que permiten conocer en todo momento el estado de la seguridad en el entorno aportando la capacidad de actuar sobre los puntos débiles o las vulnerabilidades detectadas. Para facilitar al máximo las tareas de búsqueda de logs, existen módulos de análisis forense y de correlación de eventos que permiten encontrar la información necesaria sin la pérdida de tiempo típicamente asociada a la búsqueda en ficheros de log independientes y descentralizados. "Ibíd."

Anexo 3. Especificaciones técnicas dispositivos UTM

Equipos de Seguridad Informática

a) Especificaciones generales

- Tipo: Administración Unificada de Amenazas (UTM). Appliance de propósito específico.
- Fabricado en el año 2013, no usado, no re manufacturado, no End Of Live.
- Basado en tecnología ASIC.
- El equipo podrá ser configurado en modo gateway o en modo transparente en la red.
- Instalado en rack estándar.
- Deberá tener fuente redundante de energía.

b) Especificaciones de Hardware

- Fuente de alimentación AC: 100–240 VAC.
- Deberá soportar mínimo 10 millones de sesiones concurrentes.
- IPS Throughput (HTTP) >= 6 Gbps.
- IPSec Throughput >= 17 Gbps.
- SSL-VPN Throughput >= 500 Mbps.
- Sesiones nuevas por segundo >= 200,000
- Firewall throughput >= 40 Gbps.
- Total número de interfaces será de : Mínimo 8 x 10-GbE SFP+ y 10 x SFP con tecnologia ASIC-accelerated port, 2 x 10/100/1000 port
- Debe tener al menos 2 SFP incluidos.

- Poseer la posibilidad de integración con un equipo reporteador y de administración centralizada del mismo fabricante.
- Ilimitado número de licencias para los usuarios.
- Garantía y soporte 8x5, por tres años.

c) Características del sistema operativo incluido

- Específico para seguridad que sea compatible con el appliance.
- Servidor DNS incluido en el sistema operativo, el cual permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.

d) Funcionalidades

- **Firewall**

- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- El firewall podrá especificar políticas tomando en cuenta puerto físico fuente y destino.
- Las reglas del firewall deberán tomar en cuenta dirección IP fuente (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Podrá definirse reglas de firewall para servicios sobre protocolo SCTP.
- Reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino. Podrán tener limitantes y/o vigencia en base a tiempo.
- Soportar reglas de firewall en IPv4 e IPv6 configurables tanto por CLI como por Interface Gráfica de Usuario.
- Capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Capacidad de hacer traslación de direcciones estático, NAT.

- Capacidad de hacer traslación de direcciones dinámico, PAT.

- **VPN IPSec/L2TP/PPTP/SSL**

- Soportar la configuración de túneles L2TP.
- Soportar la configuración de túneles PPTP.
- Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
- Soportar longitudes de llave para AES de 128, 192 y 256 bits.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.
- La VPN IPSec deberá poder ser configurada en modo interface.
- Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.
- Capacidad de realizar SSL VPNs.
- Soporte de autenticación de dos factores.
- Soporte de renovación de contraseñas para LDAP y RADIUS.
- Soporte a asignación de aplicaciones permitidas por grupo de usuarios.
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.

- **Antivirus**

- Antivirus en tiempo real, integrado a la plataforma de seguridad.
- Configuración en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP.
- Capacidad de poner en cuarentena archivos infectados encontrados.
- Capacidad de actualización automática de firmas.
- Los centros de actualización y firmas de antivirus deberán ser propietarios del fabricante.
- El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
- Configuración en modo Proxy y modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer

la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.

- **Filtro Web**

- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías.
- Las consultas de categorización de URLs deberán ser hechas a centros de actualización propietarios del fabricante.
- Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad.
- Configurable directamente desde la interfaz de administración del dispositivo appliance.
- Los mensajes entregados al usuario por parte del URL Filter deberán ser personalizables.
- La solución de Filtraje de Contenido debe soportar el forzamiento de Búsqueda Segura independientemente de la configuración en el browser del usuario.

- **Conectividad y Sistema de ruteo**

- Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
- Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP Y multicast routing.
- Soporte a ruteo dinámico RIPng, OSPFv3.
- Soporte a ruteo de multicast.

- **Mecanismos de detección de ataques**

- Detección de ataques de RPC (Remote procedure call).
- Protección contra ataques de Windows o NetBios.
- Protección contra ataques de SMTP, IMAP, Sendmail o POP.

- Protección contra ataques DNS (Domain Name System).
- Protección contra ataques de ICMP (Internet Control Message Protocol).
- Protección contra ataques a FTP, SSH, Telnet.

- **Control de Aplicaciones**

- La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.
- Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
- Podrá analizar el tráfico de red para detectar el tráfico de aplicaciones, incluso si el tráfico Utiliza los puertos no estándar o protocolos.
- Deberá poder prevenir el envío y recepción de archivos utilizando el sistema de mensajería instantánea.
- Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.

- **Alta Disponibilidad**

- Soporte e implementación de Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.
- Alta disponibilidad en modo Activo-Pasivo.
- Alta disponibilidad en modo Activo-Activo.
- Se podrá asignar un nombre de grupo al clúster, un grupo id, un password para identificar el clúster.
- La Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.

- **Virtualización**

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante Virtual Systems, Virtual Firewalls o Virtual Domains.

- La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus.
- La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
- Se podrá definir distintos servidores de log (syslog) para cada instancia virtual.
- Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.

- **Inspección de Contenido SSL**

- Debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
- La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.

- **Prevención de Fuga de Información (DLP)**

- Ante la detección de una posible fuga de información deben poder aplicarse el menos las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento.
- La solución debe soportar la capacidad de generar logs de por un acontecimiento de bloqueo y realizar el bloqueo de la IP utiliza para este envío.
- La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.

- **Administración**

- Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS.
- Interface basada en línea de comando (CLI) para administración de la solución.

- Comunicación cifrada y autenticada con username y password, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet).
- El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o HTTPS.
- Soporte de SNMP versión 2 y versión 3.

- **Métodos de notificación**

- Alertas vía correo electrónico.
- Alarmas mostradas en la consola de administración del appliance.
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos.

Equipo de análisis y almacenamiento de logs

a) Especificaciones generales

- Deberá soportar la funcionalidad de crear reportes mediante un equipo appliance dedicado al análisis de logs que deben ser enviados a él por el equipo appliance de filtrado de contenido y control de antispam.
- Formato tipo appliance (dispositivo de propósito específico).
- Sistema operativo propietario.
- Interface de administración gráfica (GUI) vía Web (HTTP y HTTPS)
- Interface de administración vía CLI (Línea de comando) vía telnet, SSH y consola serial.
- Reemplazo de discos duros sin necesidad de apagar del equipo
- La visualización de logs se podrá hacer tanto en tiempo real como de los registros guardados anteriormente en los discos duros.
- Filtrados en base a datos específicos como por ejemplo dirección IP, para que toda la información almacenada de dicha dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.

- Se podrá hacer una personalización de la información que se desea visualizar al momento de crear los reportes.
- El resultado, u output, será un archivo PDF, MS WORD, HTML, Texto, MHT o XML.
- Capacidad para acceder a todos los reportes generados.
- Capacidad de personalización de los formatos de presentación y filtrado de logs.

b) Especificaciones de Hardware

- Capacidad almacenamiento >= 2x2TB.
- Velocidad de recepción de datos >= 12Mbps.
- Número mínimo de interfaces: 6 puertos x 10/100/1000.
- Número de clientes no restringido.
- Capacidad de recibir al menos 3000 logs por segundo.
- Debe tener fuente redundante de poder.
- Voltaje AC: 100-240VAC.
- Debe tener la capacidad de almacenar al menos 75 GB por día de logs.

Equipo de protección de correo electrónico

a) Especificaciones generales

- Fabricado en el año 2013, no usado, no re manufacturado, no End Of Live.
- La solución de seguridad de correo electrónico deberá soportar la funcionalidad mediante un equipo appliance dedicado al control de correo spam y antivirus.
- Proteger el correo electrónico entrante (desde Internet) y correo saliente (hacia Internet), detectando palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
- Protección de al menos 90,000 virus diferentes y 30,000,000 de firmas antispam.

- Capacidad incluida de conectarse en tiempo real a una base de datos centralizada propietaria del fabricante para descargar actualizaciones de antispam y consultas de direcciones IP y dominios.
- Protección contra ataques de negación de servicio por Mail Bombing.
- Verificaciones de DNS en reversa para proveer protección tipo Anti-Spoofing.
- Posibilidad de establecer políticas por destinatario/receptor de correo electrónico por dominio, para correo entrante o correo saliente.
- Posibilidad de funcionar como SMTP mail gateway para servidores de correo electrónico existentes.
- Capacidad de hacer autenticación para SMTP a través de LDAP, RADIUS, POP3 o IMAP.
- Filtraje de archivos anexos y contenido de mensaje de correo.
- Filtraje por palabra prohibida.
- Soporte a listas negras de terceros.
- Debe funcionar en modo transparente (bridge), en modo Gateway (relay) o en modo servidor (Donde soporte cuentas locales de correo electrónico con acceso SMTP, POP3, IMAP).
- Utiliza un Agente de Transferencia de Correo (MTA) basado en estándares optimizado para proveer altos niveles de desempeño.
- El sistema debe ser de propósito específico basado en un sistema operativo pre-endurecido/asegurado.

b) Protección Antispam

- Número de Interfaces Requeridas Al menos 4 interfaces de 10/100/1000 Mbps.
- Almacenamiento Al menos 2X1 TB de disco duro incluido.
- Perfiles Antivirus para el filtraje de correos por sistema >= 200.
- Perfiles AntiSpam para el filtraje de correos definibles por equipo >= 200.
- Número de Políticas basadas en receptor de correo para correo entrante por dominio de correo (incoming)>= 600.
- Número de políticas basadas en receptor de correo para correo saliente (outgoing)>= 3000.

- Desempeño en mensajes para correo por hora definibles a un tamaño promedio de mensaje de 3 KB en modo reenvío de correo solamente (Sin AntiSpam ni Antivirus)>= 400,000.
- Desempeño en mensajes para correo por hora definibles a un tamaño promedio de mensaje de 3 KB en modo de filtraje AntiSpam >= 350,000.
- Modo servidor-MAILBOXES >= 1,000

La instalación y configuración de todos los equipos se realizarán durante horarios nocturnos, fines de semana y feriados de ser necesario, de tal forma de afectar el menor tiempo posible los servicios tecnológicos de la ANT.

Anexo 4. Catálogos de equipos Fortinet