REPÚBLICA DEL ECUADOR
Escuela Politécnica Nacional
"E SCIENTIA HOMINIS SALUS"

La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del (los) autor(es).

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.

- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.

- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS DE LAS CARACTERÍSTICAS TÉCNICAS MÍNIMAS DE LOS EQUIPOS DE SEGURIDAD, PARA EMPRESAS DE MEDIANA ESCALA, ENFOCADOS A AMENAZAS EXTERNAS A LA INTRANET.

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

JUAN PABLO GALLARDO VELÁSQUEZ

jpablogv86@gmail.com

DIRECTOR: ING. CARLOS ROBERTO EGAS ACOSTA

carlos.egas@epn.edu.ec

Quito, febrero 2019

DECLARACIÓN

Yo, Juan Pablo Gallardo Velásquez declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

Juan Pablo Gallardo Velásquez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Juan Pablo Gallardo Velásquez bajo mi supervisión.

Ing. Carlos Roberto Egas Acosta
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

A Dios, ante todo, que me ha bendecido con una gran familia, que me ha apoyado durante toda mi vida, a mis amigos que han estado en los buenos y malos momentos, y por último a los profesores que han guiado mi camino en la EPN.

DEDICATORIA

Dedico este trabajo a mi familia, especialmente a mi querido Abuelito Juan, que ha sido el principal responsable para que estudie en esta prestigiosa Universidad.

CONTENIDO

CAPÍTULO I: FUNDAMENTO TEÓRICO 2

1.1 Introducción 2

1.2 Red de Área Local 2

1.2.1 Redes LAN Conmutadas 3

1.2.2 Redes LAN Inalámbricas 4

1.3 Equipos activos actuales en una LAN 6

1.3.1 Enrutador (Router) 7

1.3.2 Conmutador (Switch) 8

1.3.3 Servidores 11

1.3.4 Teléfonos IP 11

1.3.5 Puntos de acceso a la red (access points). 12

1.4 Seguridad para una LAN 13

1.4.1 Cuadrante Mágico de Gartner para firewall de redes, aplicable a empresas grandes y medianas. 14

1.4.2 Cortafuegos (Firewall) 17

1.4.3 Sistema de detección de intrusos (IDS). 18

1.4.4 Sistema de prevención de intrusos (IPS) 19

1.4.5 Generalidades de las zonas delimitarizadas (DMZ) 20

1.4.6 Redes Privadas Virtuales (VPN) 21

1.4.7 Antivirus o antimalware 21

1.4.8 Control de acceso AAA 22

CAPÍTULO II: ANÁLISIS DE AMENAZAS A LA RED CONOCIDAS 24

2.1 Vulnerabilidades 24

2.2 Amenazas 24

2.3 Tipos de atacantes 24

2.3.1 Hacker 24

2.3.2 Craker 25
2.3.3 Phreaker 25
2.3.4 Spammers 25
2.3.5 Carders 25
2.3.6 Script kiddies 25
2.3.7 Phisher 26
2.4 Tipos de ataques 26
2.4.1 Denegación de servicio (DOS) 26
2.4.2 Remote to local (R2L) 26
2.4.3 Remote to user (R2U) 26
2.4.4 Remote to root (R2R) 26
2.4.5 Remote disk read (rdr) 26
2.4.6 Remote disk WRITE (rdW) 27
2.4.7 User to root (U2R) 27
2.4.8 Surveillance / probing o scan - probe (s/p) 27
2.5 Amenazas a la red 27
2.5.1 Virus 27
2.5.2 Caballos de Troya 28
2.5.3 Gusanos 28
2.5.4 Ransomware 29
2.5.5 Spyware 29
2.5.6 Adware 30
2.5.7 Scareware 30
2.5.8 Phishing 30
2.5.9 Rootkits 31
2.6 Amenazas más comunes en Empresas de Mediana Escala (encuesta) 31
2.6.1 Amenazas reportadas en sitio oficial del ecuador 39

2.7 ¿Cómo actuar ante un ataque de red? 40

2.8 Plan de Continuidad de Negocios (Business Continuity Plan-BCP) y plan de contingencia. 41

2.9 Actualidad en seguridad informática 42

CAPÍTULO III: CARACTERÍSTICAS DE LAS EMPRESAS DE MEDIANA ESCALA 45

3.1 Empresa de Mediana Escala 45

3.1.1 Servicios que presta una empresa de Mediana Escala 45

3.2 PYMES 46

3.2.1 Fortalezas de las PYMES 47

3.2.2 Debilidades de las PYMES 47

3.2.3 PYMES Ecuador 47

3.2.4 Información que debe ser protegida 48

3.3 Ataques a empresas pequeñas y medianas 49

3.4 Empresa modelo, basada en las estadísticas de la encuesta 50

3.4.1 Condiciones iniciales 50

3.4.2 Topología 51

3.4.3 Cálculo de tráfico de red referencial 51

3.4.4 Mejores prácticas para acceso a la red empresarial 54

CAPÍTULO IV: PLANTEAMIENTO DE SOLUCIONES DE SEGURIDAD 55

4.1 Características técnicas mínimas que debe cumplir la solución de segurida 55

4.2 Propuesta de Solución de Seguridad 57

4.2.1 Propuesta de Solución con software de firewall licenciado o libre 59

4.2.2 propuesta de solución con hardware dedicado de firewall 63

4.2.3 Condiciones de aplicación de la solución 66

4.2.4 Personal técnico para administración de la seguridad 67

4.3 Proformas de seguridad obtenidas 68

4.4 Costo inicial referencial de una solución de seguridad, incluidos los equipos de conectividad. 72

4.5 Generalidades del Plan de Contingencia 77

4.5.1 Plan de contingencia ante ataques de red por una amenaza externa para una empresa de mediana escala. 79

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES 81

REFERENCIAS BIBLIOGRÁFICAS 83

ANEXOS ..... A

Anexo A.- Encuesta de seguridad de redes ..... A

Anexo B.- Ficha de datos de equipos de seguridad. ..... E

Anexo C.- Incidentes y vulnerabilidades reportados en el 2016 según ecucert. . M

ÍNDICE DE FIGURAS

Figura 1.1 Configuración de red típica en oficinas [5] 3
Figura 1.2 Configuración de una LAN inalámbrica [5] 5
Figura 1.3 Familia IEEE 802.11 [7]..... 5
Figura 1.4 IEEE 802.11 actualidad [8]..... 6
Figura 1.5 Modelo de red jerárquico [10]..... 7
Figura 1.6 Router Cisco [11]..... 7
Figura 1.7 Conmutador D-Link [13] 8
Figura 1.8 Teléfono analógico vs teléfono IP [19]. 12
Figura 1.9 Punto de Acceso Cisco [20] 13
Figura 1.10 Modelo de Cuadrante Mágico [22] 14
Figura 1.11 Cuadrante Mágico de Gartner 2016 [21] 16
Figura 1.12 Firewall [25] 18
Figura 1.13 Sistema de detección de intrusos..... 19
Figura 1.14 Sistema de prevención de intrusos 20
Figura 1.15 Configuración básica de una DMZ 20
Figura 2.1 Porcentaje de empresas víctimas de ataques cibernéticos..... 32
Figura 2.2 Tiempo de interrupción de los servicios 34
Figura 2.3 Plataformas usadas para seguridad..... 34
Figura 2.4 Servicios de red de una empresa de mediana escala..... 35
Figura 2.5 Amenazas más comunes en una red 35
Figura 2.6 Herramientas de seguridad 36
Figura 2.7 Firewalls más usados en Ecuador..... 36
Figura 2.8 Porcentaje de empresas con plan de contingencia 37
Figura 2.9 Inversión en seguridad de las empresas de mediana escala 38
Figura 2.10 Conocimiento de los técnicos acerca de las tendencias en equipos de seguridad.....38
Figura 3.1 Actividades comerciales que se desempeñan en el Ecuador [47]. . 46
Figura 3.2 Algunas empresas de mediana escala [47]..... 48
Figura 3.3 Topología Empresa modelo 51
Figura 4.1 Esquema de solución con firewall virtual licenciado..... 60
Figura 4.2 Esquema de solución propuesto 64
Figura 4.3 Proforma de Firewall ASA 5506 69

Figura 4.4 Proforma de firewall ASA 5506H 70
Figura 4.5 Firewall UTM Cyberoam 71
Figura 4.6 Proforma #1 de equipos de conectividad y seguridad 74
Figura 4.7 Proforma #2 de equipos de conectividad y seguridad 75
Figura 4.8 Proforma #3, equipos de comunicación 76
Figura 4.9 Proforma #3, equipo de seguridad 77
Figura 4.10 Interacción entre las fases de planificación de un plan de contingencia [68] 79

ÍNDICE DE TABLAS

Tabla 1.1. Características de LAN [5]..... 4
Tabla 2.1 Ataques de red en el último año..... 33
Tabla 3.1 Índice de simultaneidad..... 52
Tabla 4.1. Características mínimas de seguridad de red 56
Tabla 4.2. Características del antivirus 56
Tabla 4.3. Características mínimas para el firewall 57
Tabla 4.4. Equipos utilizados en la solución de seguridad 60
Tabla 4.5. Ventajas y desventajas del firewall virtual 61
Tabla 4.6. Algunas empresas proveedoras de firewall virtual 62
Tabla 4.7 Equipos utilizados en la solución de seguridad con hardware dedicado de firewall 64
Tabla 4.8 Pros y contras de la solución con hardware específico 65
Tabla 4.9 Pros y contras del personal que va a operar la solución de seguridad 67
Tabla 4.10 Detalle de la propuesta de seguridad en base a proforma. 69
Tabla 4.11 Detalle de la propuesta de seguridad en base a proforma. 70
Tabla 4.12 Detalle de la propuesta de seguridad en base a proforma. 72
Tabla 4.13. Equipos para solución inicial de seguridad..... 73

RESUMEN

En el presente trabajo de titulación se ha realizado un estudio de las amenazas que podrían ocasionar que una empresa de mediana escala se vea afectada en su giro de negocio, para lo cual se define las empresas que se pueden considerar como de mediana escala, así como del tipo de redes que son implementadas en estas empresas.

El estudio está enfocado en las amenazas externas a la intranet, por lo que la solución consta de equipos de seguridad acordes a las necesidades de este tipo de empresas.

Los equipos de seguridad y conectividad perimetral serán escogidos de acuerdo con la empresa tipo propuesta para este trabajo de titulación, considerando los parámetros mínimos de seguridad que se ilustran en el cuarto capítulo del presente trabajo. Además, se dan las pautas para realizar un plan de contingencia en caso de que la solución que el usuario escoja llegue a fallar.

Muchos de los análisis se hicieron con base en el resultado de una encuesta a los administradores de red de algunas empresas de mediana escala en Ecuador, cuya información es parecida a los análisis hechos por empresas dedicadas a dar soluciones de seguridad en la región.

Al final se proponen las características mínimas que debe cumplir la solución de seguridad que se va a implementar en una empresa de mediana escala. Cabe señalar que este es un estudio general, y que la solución puede variar según el giro de negocio de la empresa.

PRESENTACIÓN

En el primer capítulo se hace una introducción a las redes de área local (LAN[1]), donde se conceptualiza el funcionamiento de los equipos activos actuales de una LAN, y de los equipos que tradicionalmente se usan para proteger la red. En este capítulo, además, se observa qué equipos de seguridad se encuentran en el cuadrante mágico de Gartner[2].

El segundo capítulo se concentra en investigar los distintos tipos de amenazas a una red, el tipo de atacantes, las amenazas más comunes en nuestro medio, y en definir lo que es un plan de contingencia. Se plantea una encuesta a los administradores de red de empresas de mediana escala, cuyos resultados serán clave en el desarrollo del presente trabajo.

El tercer capítulo se enfoca en definir el objeto de aplicación de este proyecto de titulación, descubrir hacia qué tipo de empresas va dedicado este trabajo, se plantea la empresa tipo escogida para este trabajo de titulación y se genera una encuesta de seguridad de red que permita descubrir las amenazas más comunes de este tipo de empresas.

La solución planteada se encuentra en el cuarto capítulo, donde, con base en los capítulos anteriores, se definen las características técnicas mínimas que debe cumplir una solución de seguridad para que sea escalable en el tiempo. Asimismo, se plantea una topología referencial donde se va a aplicar la solución propuesta, y se dejan las pautas de un plan de contingencia para cuando la red se vea amenazada.

Por último, en el capítulo final se incorporan las conclusiones, las cuales han sido expuestas según los objetivos específicos del plan de titulación.

---

[1] Red de Área Local

[2] Cuadrante mágico de Gartner. - es una referencia gráfica del estado de un producto tecnológico en un instante de tiempo. Se estudiará más adelante.

1 CAPÍTULO I: FUNDAMENTO TEÓRICO

1.1 INTRODUCCIÓN

En el presente trabajo de titulación se pretende analizar los parámetros mínimos de seguridad que debe tener una empresa de mediana escala, para lo cual se hace uso de las recomendaciones de seguridad que han sido publicadas hasta la actualidad en diferentes medios escritos y digitales, y también de una encuesta.

Se investigan las amenazas presentes en la red conocidas, ya sean virus, intrusiones o ataques de denegación de servicio, así como la forma de mitigarlas. Para esto se utilizan equipos de seguridad, cuyas características se acoplen al presupuesto de una empresa de mediana escala, que según CISCO es una empresa que maneja de 100 a 1.000 usuarios [1]. Otra forma de categorizar una empresa de mediana escala en nuestro país es aquella que dispone de un ingreso bruto anual entre $1.000.001,00 y $5.000.000,00 y que además maneje un personal de entre 50 a 199 colaboradores [2].

Hoy en día las redes corporativas son más importantes para los objetivos de negocio que nunca. En consecuencia, una mayor cantidad de datos sensibles atraviesan las redes cableadas e inalámbricas por donde fluye gran cantidad de datos valiosos para la empresa, lo cual atrae a un número cada vez mayor de hackers[3] y aplicaciones de malware[4] [3].

Cada nodo, aplicación, certificado, dispositivo interno o externo, y usuario que accede a la red, corren el riesgo de ser comprometidos con software malicioso si no se han tomado las medidas de seguridad adecuadas para detectar y remediar al menos las amenazas de red actualmente conocidas. El malware u otro vector de

---

[3] Nombre común que se les da a los expertos informáticos que acceden a un determinado sistema sin autorización.

[4] Término que engloba todo tipo de programa o código informático malicioso. Es la abreviación de Malicious Software.

ataque podría propagarse rápidamente a través de la red por lo que una de las nuevas tendencias de seguridad es, interconectar a los equipos de red de tal manera que se conviertan en sensores de anomalías, convirtiendo así a la red en una estructura inteligente, que de manera proactiva permite tomar acciones frente a los ataques y violaciones que sufre la red [3].

Las primeras soluciones de red se dieron en los años de 1960, pero es hasta el año 2000 que se tuvo un paquete de soluciones bien definido, cuyo objetivo era prevenir los esfuerzos de los hackers por vulnerar las redes de computación y tratar los problemas actualmente existentes [4].

Las organizaciones de redes de seguridad han creado comunidades donde se forman profesionales en seguridad, y donde se enseñan protocolos para prevención de amenazas. Esta fuerza de trabajo se especializa en prevenir ataques, y estos profesionales son los contratados por las grandes empresas para que manejen su infraestructura de seguridad.

A los profesionales de seguridad que se encargan de prevenir ataques, encontrar vulnerabilidades, plantear soluciones y colaborar para prevenir daños a la red se los conoce comúnmente como hackers blancos. Son profesionales cuyo objetivo es ayudar al bienestar de la información segura.

1.2 RED DE ÁREA LOCAL

“Una LAN es una red de comunicaciones que interconecta varios dispositivos y que proporciona un medio para el intercambio de información entre ellos [5]”. La cobertura de una LAN es pequeña, pudiendo llegar a abarcar algunos edificios. Las ventajas son: alta velocidad de los datos y administración interna de la red. Las configuraciones típicas son las redes conmutadas y las redes inalámbricas como se muestra en la figura 1.1.

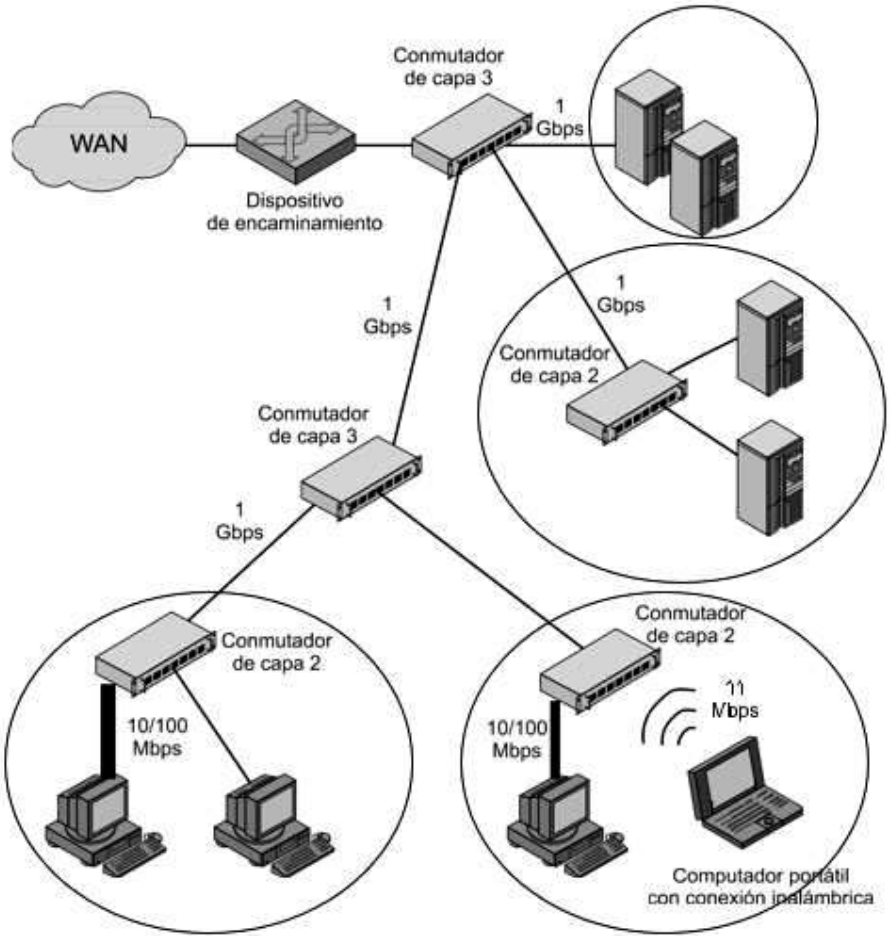


Figura 1.1 Configuración de red típica en oficinas [5]

1.2.1 REDES LAN CONMUTADAS

Entre las más populares se tiene la LAN Ethernet, constituida por un único conmutador, o por un conjunto de conmutadores interconectados entre sí; también están las redes ATM, que usan la tecnología de red ATM en un entorno local; y como último se tienen las LAN con canal de fibra óptica. En la tabla 1.1 se muestra un resumen de las características de las LAN de alta velocidad.

"Los años recientes han sido testigos de cambios vertiginosos en aspectos como la tecnología, el diseño y las aplicaciones comerciales de las redes de área local (LAN, Local Area Network). Una de las principales características de esta evolución es la introducción de toda una gama de nuevos esquemas en las redes locales de alta velocidad. Los distintos enfoques para el diseño de LAN de alta velocidad se han

plasmado en productos comerciales con objeto de dar solución a las continuas necesidades del mercado [5]".

Tabla 1.1 Características de LAN [5]

	Fast Ethernet	Gigabit Ethernet	Canal de fibra	LAN inalámbrica
Velocidad de datos	100 Mbps	1 Gbps, 10 Gbps	100 Mbps-3,2 Gbps	1 Mbps-54 Mbps
Medio de transmisión	UTP, STP, fibra óptica	UTP, cable apantallado fibra óptica	Fibra óptica cable coaxial, STP	Microondas 2,4 GHz, 5 GHz
Método de acceso	CSMA/CD	Conmutado	Conmutado	CSMA/Sondeo
Estándar	IEEE 802.3	IEEE 802.3	Asociación del canal de fibra	IEEE 802.11

1.2.2 REDES LAN INALAMBRICAS

Las redes inalámbricas son de gran utilidad en toda empresa, sus aplicaciones son diversas, y llegan a convertirse en un complemento fundamental para las redes LAN.

Cuando se necesita movilidad, versatilidad y facilidad de comunicación, las redes inalámbricas toman mucha importancia, la más usada de las tecnologías inalámbricas está definida en el estándar IEEE 802.11.

Conforme pasan los años, este tipo de tecnología ha ido superando sus limitaciones iniciales, que eran costos altos, velocidades de transmisión bajas, corto alcance y frecuencias de transmisión muy ocupadas. Hoy en día podemos tener equipos inalámbricos muy económicos, dependiendo del fabricante y con características apropiadas para trabajar con gran número de usuarios.

En la figura 1.2 se observa un ejemplo de una configuración de red con presencia de equipos conectados mediante tecnología inalámbrica.

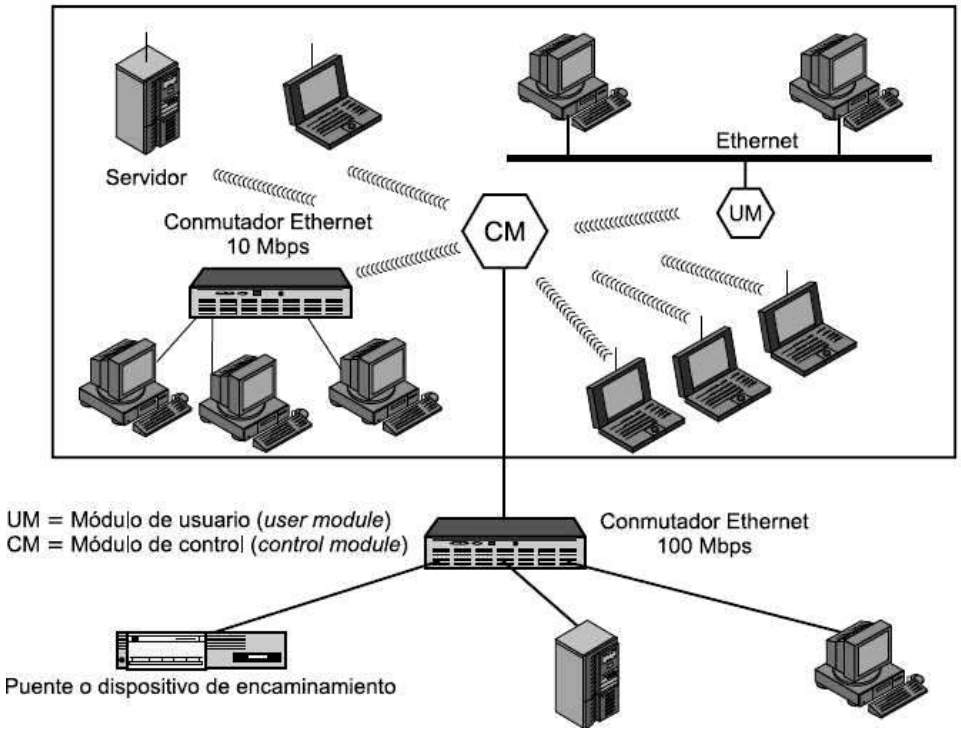


Figura 1.2 Configuración de una LAN inalámbrica [5]

Se presenta en la figura 1.3 un cuadro comparativo de los estándares IEEE 802.11 usados en la actualidad.

	802.11 legacy	802.11b	802.11a	802.11g	802.11n
Banda	2.4Ghz / 850-950nm	2.4GHz	5Ghz	2.4GHz	2.4GHz / 5GHz
Capa física	FHSS / DSSS / IR	DSSS	OFDM	DSSS / OFDM	MIMO / OFDM
	GFSK / DPSK	DPSK sin/con CCK o PBCC	PSK / QAM	DPSK / PSK / QAM	
Tasa máxima	2 Mbps	11Mbps	54 Mbps	54 Mbps	600 Mbps
Throughput (*)	0.9 Mbps	4.5 Mbps	23 Mbps	20 Mbps	135 Mbps
Alcance interior (*)	20m	40m	35m	40m	70m
Alcance exterior (*)	100m	150m	120m	150m	300m
Año	1997	1999	1999	2003	2008
Uso	En desuso	Muy extendido	Poco extendido	Extendido y creciente	En desarrollo
Rendimiento	Buen rendimiento	Rendimiento medio	Mejor rendimiento	Rendimiento medio	Máximo rendimiento
Consumo	Bajo consumo	Bajo consumo	Mayor consumo	Bajo consumo	
Canales sin solapamiento	No	3 canales simultáneos	12 canales simultáneos		
Compatibilidad		Incompatible con 802.11a	Incompatible con 802.11b	Compatible con 802.11b	Compatible con todos
Interferencias	Bluetooth, microondas, DECT, ...			Bluetooth, microondas, ...	
Otras			Necesita licencia en algunos países		

(*) Valores aproximados

Figura 1.3 Familia IEEE 802.11 [7]

Por otro lado en la figura 1.4 se puede observar los estándares actuales, mismos que en Ecuador aún no están implementados, según el listado de equipos homologados y permitidos en el país por el Consejo Nacional de Telecomunicaciones (CONATEL) hasta octubre del 2017 [6].

	WIFI AC	WIFI AD	WIFI HALOW
BANDA DE FRECUENCIAS	5 GHz (mantiene compatibilidad con 2,4 GHz)	60 GHz (mantiene compatibilidad con 2,4 y 5 GHz)	900 MHz (mantiene compatibilidad con 2,4 y 5 GHz)
VELOCIDADES MÁXIMAS	7 Gbps	4,6 - 7 Gbps ahora, pero ya se habla de hasta 100 Gbps	Por determinar
COBERTURA TÍPICA	30 metros	5-10 metros	Más de 60 metros
APLICACIONES	Conexión dispositivos multimedia e Internet en todas las habitaciones del hogar, video streaming UHD	Transferencia de datos a alta velocidad y corta distancia. Transmisión de video sin compresión sin cables	Internet de las cosas, conexión de sensores y equipos domóticos.

Figura 1.4 IEEE 802.11 actualidad [8]

1.3 EQUIPOS ACTIVOS ACTUALES EN UNA LAN

Para el propósito del presente trabajo de titulación es necesario analizar los diferentes equipos activos que intervienen en la comunicación hacia la red externa, por lo que se verán breves descripciones de equipos como:
enrutadores, conmutadores de capa 2 y 3, dispositivos de red inalámbricos, equipos de telefonía IP y servidores. Los equipos de seguridad se analizarán más adelante.

La metodología de CISCO para empresas de mediana y gran escala recomienda un modelo de red jerárquico por capas, lo que simplifica el diseño de la red, y por lo tanto la administración e implementación de la misma [9]. Para una mediana empresa este modelo jerárquico se abrevia a dos capas, la capa de acceso y la capa de núcleo o de core[5], en la figura 1.5 se observa el modelo jerárquico de tres capas.

[5] Core, hace referencia al núcleo de un dispositivo de red, por ejemplo: switch de core, se refiere al conmutador principal o de núcleo de la red.

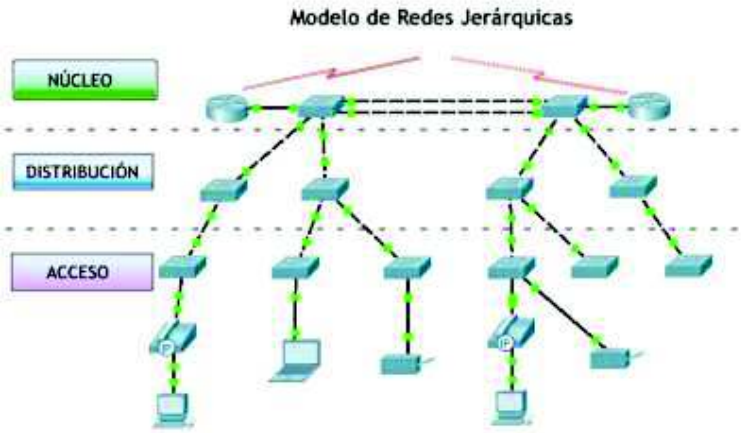


Figura 1.5 Modelo de red jerárquico [10]

A continuación, se describe la funcionalidad de los equipos de comunicación que intervienen en las capas de esta distribución jerárquica.

1.3.1 ENRUTADOR (ROUTER)

Figura 1.6 Router Cisco [11]

El enrutador es un dispositivo de capa 3 del modelo ISO/OSI. Su función es conectar varias redes, analizar los datos que se van a enviar a una red, empaquetar datos y enviarlos dependiendo del tipo de medio de trasporte a las diferentes redes, también ayudan a distinguir el tipo de tráfico y la prioridad que este tiene para ser entregado a determinado usuario, además brindan seguridad a la información que por ellos circula [12].

Las prestaciones que ofrecen estos equipos son diversas; entre las más comunes están:

- Permiten el enrutamiento de VLANs[6].
- Aceptan grandes velocidades de transmisión de datos.
- Soportan diversas tecnologías de conexión.
- Dan soporte de seguridad, protocolo IPsec y VPN[7].
- Admiten protocolos de enrutamiento.
- Permiten configurar la calidad del servicio (QoS).
- Dan soporte de Zonas Desmilitarizadas (DMZ).

No todos los equipos incluyen estos servicios, por lo general lo hacen los que están dedicados a interconectar grandes o medianas empresas, debido a los requerimientos en conectividad, calidad de servicio y seguridad que estas empresas necesitan.

1.3.2 CONMUTADOR (SWITCH)

Figura 1.7 Conmutador D-Link [13]

Es un dispositivo que pertenece a la capa 2 del modelo ISO/OSI. Permite conmutar paquetes de un usuario a otro evitando colisiones en el medio físico. Cada conexión a un punto de este dispositivo se considera un dominio de colisión.

Las dos formas en que el tráfico es reenviado de un puerto a otro son:

---

[6] Son redes de área local virtuales usadas para crear redes lógicas independientes dentro de una misma red física.

[7] Una VPN es una red privada virtual, usada para proveer mayor seguridad en el intercambio de información.

- Almacenamiento y envío (store-and-forward switch). Toda la trama se almacena en una memoria temporal llamada buffer, y una vez que se verifica la validez de la trama esta es reenviada hasta su destino.

- Conmutador rápido. "El conmutador aprovecha que la dirección de destino se encuentra al comienzo de la trama MAC (control de acceso al medio) para retransmitir la trama entrante sobre la línea de salida correspondiente tan pronto como sabe la dirección de destino [5]".

En la práctica se utiliza un modelo de conmutadores jerárquicos, en el nivel superior se encuentran los equipos que brindan conexión con la red externa y que permiten el enrutamiento de paquetes, un nivel más abajo se encuentran los conmutadores de distribución, que son los encargados de interconectar a la empresa de mediana escala, y por último se tiene a los conmutadores de acceso, que son los que brindan la conexión final a los usuarios.

1.3.2.1 Conmutadores de la capa Acceso

Estos conmutadores deben brindar los servicios de conectividad, seguridad y además opciones de tecnología avanzada.

El servicio de conectividad se encarga de conectar a los dispositivos de los usuarios finales con la LAN, además se necesitan protocolos que permitan la redundancia de enlaces, evitando lazos de información, y siempre tener un mecanismo de administración de estos dispositivos usando las Lan-Virtuales, el servicio de seguridad tiene que ver con las funciones que recuperan las configuraciones del dispositivo , como el bloqueo de puertos de ser el caso, las características avanzadas tienen que ver con la agregación de enlaces y el soporte de protocolos avanzados como OpenFlow[8] (SDN), y por último tener el servicio que permita identificar el tipo de tráfico y darle prioridad, en el caso de voz y video concretamente, es decir que estos equipos deben permitir calidad de servicio (QoS) [9].

---

[8] Openflow, protocolo utilizado en redes definidas por software (SDN).

Algunas características técnicas que poseen estos equipos son:

- Pueden ser modulares o apilables
- Soportar tecnología PoE[9].
- Puertos entre 24 y 48 para empresas de mediana escala.
- Puertos de fibra óptica para los enlaces ascendentes.
- Seguridad con SPAN[10] y BPDU[11] Guard [14].

1.3.2.2 Conmutadores de la capa de Distribución.

La capa de distribución es el medio de comunicación entre la capa de acceso y el core, lo que ayuda para la disponibilidad y redundancia, además aquí se produce el enrutamiento y tiene entre sus principales funciones la seguridad, las políticas de red, el filtrado de paquetes, el acceso a la red WAN, la redistribución entre protocolos de ruteo, el ruteo entre VLANs [15].

Por otro lado, las características técnicas principales de los equipos de esta capa son:

- Puertos de 10/40/100 GE
- Capacidad de conmutación máxima de 600Gbps.
- Rendimiento de 1.44 billones de paquetes por segundo en adelante.
- Soporte de SNMP (Protocolo de administración de red simple) [16].

1.3.2.3 Conmutadores de la capa de Núcleo.

"Su función principal es llevar grandes cantidades de tráfico de manera confiable y veloz, donde la latencia y velocidad son factores primordiales en esta capa." [15].

Un conmutador de esta capa debe ser rápido, escalable y seguro, por lo que algunas características de estos equipos son las siguientes:

---

[9] PoE, Power over Ethernet, característica de los equipos de poder ser energizados por tecnología ethernet.

[10] SPAN, Serial Port Analyzer, función de supervisar los puertos.

[11] BPDU Guard, unidad de datos de protocolo puente, detecta bucles en una red.

- Densidad de Puertos de alta velocidad, Gigabit-Ethernet y puertos de fibra óptica.
- Posee protocolos de Gateway exterior (BGP).
- Velocidades de hasta 100Gbps
- Fuentes de poder adicionales
- Soporte de hasta 8000 listas de control de accesos (ACLs).
- Máximo número de interfaces virtuales (VLANs) 3967.
- Soporte agrupación de enlaces.
- Permite la redundancia de equipos mediante el protocolo HSRP.
- Hasta 1023 entradas NAT.

1.3.3 SERVIDORES

"Un servidor es un computador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada: desde archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc." [17].

1.3.4 TELÉFONOS IP

Son dispositivos de comunicación que se utilizan para enviar y recibir voz y datos a través del Protocolo Internet, deben estar sincronizados y configurados mediante una consola de administración centralizada.

Se han convertido en uno de los principales dispositivos para comunicación dentro y fuera de las empresas, convirtiéndose así en una gran ayuda para redes convencionales LAN, ya que permiten a largo plazo abaratar costos, comparando con los dispositivos de telefonía convencional (analógica), tanto en el cableado estructurado como en las líneas telefónicas que se arriendan para que toda una empresa pueda gozar de un servicio de telefonía [18].

En figura 1.8 se muestra como es la conexión de un teléfono IP vs un teléfono tradicional analógico.

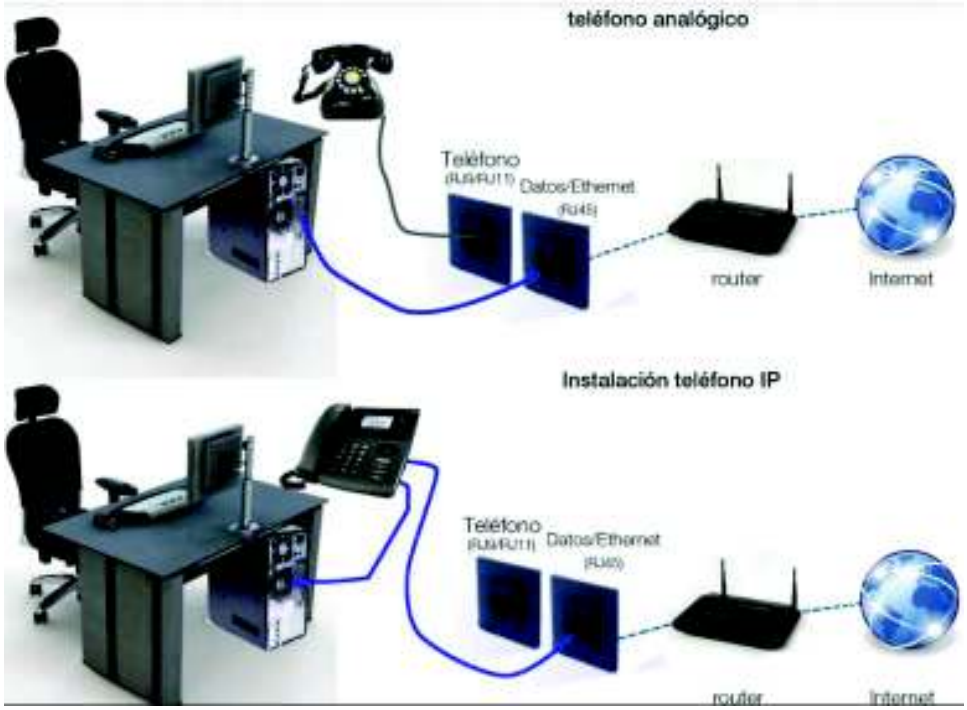


Figura 1.8 Teléfono analógico vs teléfono IP [19].

1.3.5 PUNTOS DE ACCESO A LA RED (ACCESS POINTS).

Para que en una empresa se tenga acceso a la red, interna o externa, desde cualquier lugar físico donde el usuario se encuentre, es necesario ayudarse de la tecnología inalámbrica, que actualmente soporta grandes velocidades de transmisión de datos.

Para este propósito se utilizan los equipos de conectividad llamados puntos de acceso (Access Points en inglés, AP). Cuando se tiene una red inalámbrica pequeña, configurar un Access point no es problema, pero a medida que la red crece éste trabajo no es tan sencillo, debido a que, si se realiza cualquier cambio, se deberá realizar el mismo en cada equipo, mientras que, si se dispone de un dispositivo central que configure a estos puntos de acceso (controladora inalámbrica), basta con enviar la orden desde el controlador y todos los equipos reciben y ejecutan la instrucción.

En la figura 1.9 se muestra un AP de marca CISCO el cual es recomendado por el fabricante para empresas de mediana escala.

Figura 1.9 Punto de Acceso Cisco [20]

1.4 SEGURIDAD PARA UNA LAN

Son todos los procesos y equipos activos que harán que la red LAN sea segura. Este trabajo de titulación se enfoca en las amenazas externas a la intranet, por lo que describir la función de equipos de seguridad, como cortafuegos o antivirus, que hacen que la red sea lo más segura posible, es imprescindible para proponer más adelante una solución de seguridad de red para la LAN.

Se mencionará algunas herramientas de protección, que ayudan a prevenir intrusiones, como son los IDS[12] e IPS[13], pero antes de mencionar esta herramienta conviene hacer un análisis del cuadrante mágico de Gartner en cuanto a cortafuegos se refiere, ya que es la herramienta que se considera como la primera barrera ante las amenazas externas a la intranet que tiene una empresa de mediana escala [21].

---

[12] IDS, Intrusion Detection System, que significa sistema de detección de intrusos

[13] IPS, Intrusion Prevention System, que significa sistema de prevención de intrusos

1.4.1 CUADRANTE MÁGICO DE GARTNER PARA FIREWALL DE REDES, APLICABLE A EMPRESAS GRANDES Y MEDIANAS.

Gartner, Inc. es una compañía de investigación, información de tecnología y consultoría líder a nivel mundial. Entrega todos los días la visión relacionada con la tecnología necesaria para sus clientes en la toma de decisiones correctas al momento de adquirir una determinada solución de seguridad.

Para presentar sus investigaciones, Gartner utiliza lo que llama cuadrantes mágicos, que consisten en clasificar a los proveedores de equipos de seguridad de acuerdo a ciertas categorías: líderes, retadores o aspirantes, visionarios, jugadores de nicho.

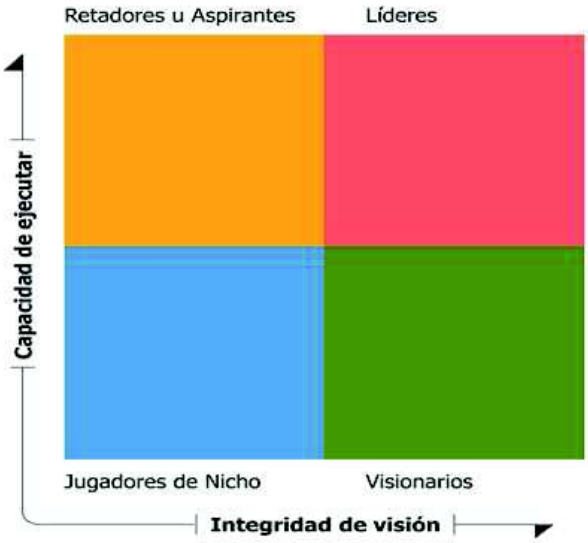


Figura 1.10 Modelo de Cuadrante Mágico [22]

Haciendo referencia a la página web oficial de Gartner se encuentra una leve descripción de lo que significan estas categorías, la cual se menciona a continuación.

Líderes. - Ejecutan bien su visión de negocio, están bien posicionados en el mercado.

Visionarios. - Entienden la tendencia del mercado o tener visión para cambiar las reglas del mercado, pero aún no se consolidan por completo.

Retadores u aspirantes. – Su software se ejecuta bien, dominan un largo segmento de mercado, pero aún no demuestran un total entendimiento de la dirección de su mercado.

Jugadores de Nicho. – Se enfocan con éxito en un segmento pequeño, o no están enfocados y no innovan o superan a otros.

Criterio de inclusión

Las empresas de seguridad, para ser incluidas en el cuadrante de Gartner deben cumplir con las siguientes condiciones:

- Tener la capacidad para competir en el mercado del firewall.
- Integrar sucesivamente listas cortas de ventas.
- Tener una presencia competitiva en lo corporativo y en las ventas.
- Haber alcanzado por los vendedores en el correr del último año ventas de productos de firewall por más de diez millones de dólares [21].

Las compañías que integran este mercado están centradas principalmente en iniciativas empresariales. A medida que el mercado de firewall sigue desarrollándose, los NGFW (firewalls de próxima generación) van agregando nuevas características que les permitan aplicar mejor las políticas de aplicación y control del usuario, así como detectar nuevas amenazas [23].

A la fecha de elaboración de este documento, se ha tomado como referencia el informe de Gartner publicado el 25 de mayo del 2016, donde muestra a las empresas: Palo Alto Networks, Check Point Software Technologies, Fortinet y Cisco como las empresas líderes en el mercado.

Las empresas que integran el cuadrante mágico del mercado de firewall según el último informe son las siguientes:

- Check Point Software Technologies
- Intel Security (McAfee)
- AhnLab

- Barracuda Networks
- Cisco
- Dell SonicWALLF5
- Fortinet
- Hillstone Networks
- HP
- Huawei
- Juniper Networks
- Palo Alto Networks
- Sangfor
- Sophos
- Stormshield
- WatchGuard. [21]

Figura 1.11 Cuadrante Mágico de Gartner 2016 [21]

1.4.2 CORTAFUEGOS (FIREWALL)

Estos dispositivos son encargados de proteger la red, encargados de permitir o bloquear el acceso a ella en base a reglas configurables y demás criterios de seguridad predefinidos. En un inicio se consideraba que un cortafuego era un conjunto de reglas de control de acceso; luego la tecnología evolucionó hasta tener equipos que hacen filtrado de paquetes IP, apertura y cierre de sesiones, entre otras.

En el mercado existen diversos tipos de firewall, en versiones que pueden ser:

- Virtuales (en software licenciado y software libre). - son implementados mediante instaladores a un equipo de computación que sea capaz de soportar un trabajo ininterrumpido durante todo el tiempo que se utilice esta solución.
- Como una parte de las aplicaciones de un equipo de red. - existen algunos fabricantes de dispositivos de red que traen incorporado la función de firewall como un módulo adicional, es decir que además de enrutar o conmutar un paquete se podría hacer trabajar a ese equipo como un firewall.
- Montadas sobre un hardware dedicado solo para ese propósito (Appliance). - ejecuta un sistema operativo propietario del fabricante del equipo, se acompaña de soluciones de otros fabricantes para realzar la seguridad [24].

Las empresas consideradas pequeñas que usan soluciones de seguridad lo hacen a través del software que viene embebido en los equipos de conectividad contratados, un ejemplo claro se tiene en los servicios de internet doméstico o pequeños negocios, donde el equipo que realiza las funciones de enrutar, conmutar, también realiza las funciones de firewall.

En la siguiente figura 1.12, se muestra el concepto de un cortafuego o firewall gráficamente.

Figura 1.12 Firewall [25]

1.4.3 SISTEMA DE DETECCIÓN DE INTRUSOS (IDS).

Es un software de seguridad que monitorea pasivamente la red, es decir, copia el tráfico y lo analiza, lo compara con software malicioso. Si el tráfico copiado lleva algún tipo de virus no puede eliminarlo por sí solo, necesita de un router y un firewall para mitigar la amenaza.

El IDS reporta la amenaza encontrada para que otra aplicación tome medidas al respecto.

En la figura 1.13 se ilustra en el paso 1 como el paquete se copia hacia el IDS, en el paso 2 se analiza en busca de amenazas, y el paso 3 se administra la herramienta para tomar una decisión, se puede informar que el paquete está infectado y que se debe mitigar inmediatamente o se puede informar que el paquete analizado no contiene ninguna amenaza conocida.

Esta herramienta es muy útil para detectar la infección de cualquier tipo de virus conocido hasta la actualidad hacia la red de trabajo y gracias a esto es posible que el firewall pueda mitigar las amenazas tan rápido como sea posible.

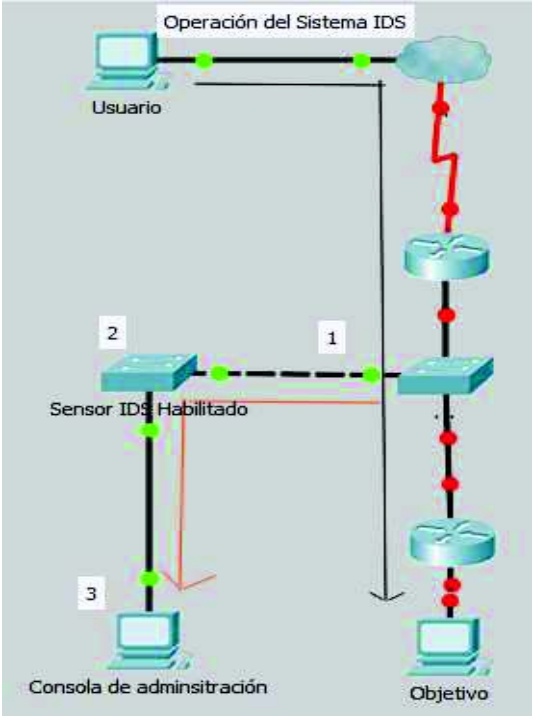


Figura 1.13 Sistema de detección de intrusos

1.4.4 SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)

Es una tecnología de seguridad de red implementada en línea, es decir, el tráfico de datos debe pasar a través de este dispositivo antes de llegar a su destino final, examina el flujo de tráfico de red para detectar y prevenir explotaciones de vulnerabilidades, si el tráfico analizado no es confiable, lo descarta.

Los datos son analizados y comparados con bases de datos de firmas digitales, además el IPS se basa en perfiles y protocolos de análisis de detección de intrusos, en conclusión el trabajo del IPS es, identificar, parar y bloquear el ataque [26].

En la figura 1.14 se explica de manera gráfica el funcionamiento de IPS, en el paso 1, se genera un determinado tráfico que va dirigido hacia la red interna, como segundo paso se analiza el tráfico en el IPS, en el paso 3 se toma la decisión de permitir el paso del paquete o desecharlo, en este ejemplo se puede ver como en el punto 4 se descarta el paquete porque en el punto anterior se lo consideró como amenaza y no se permitió el tránsito hacia el equipo final.

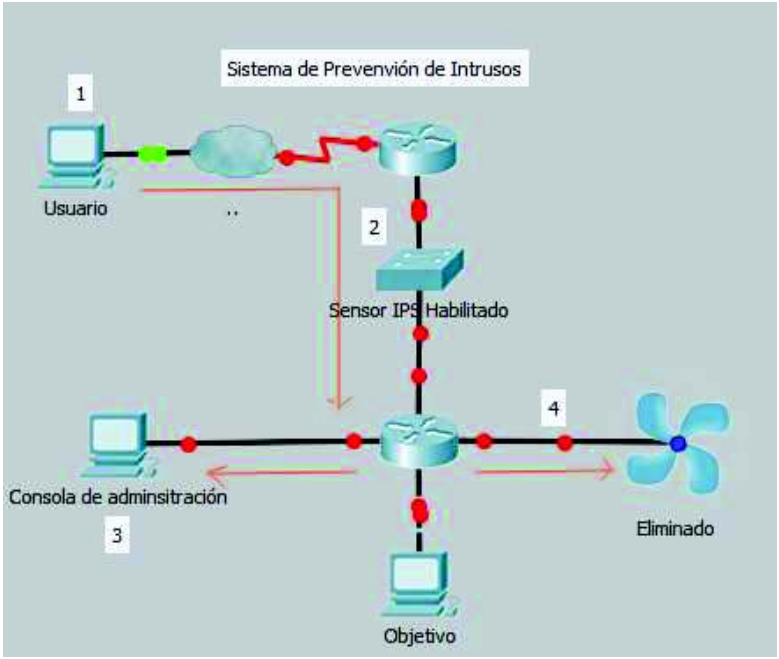


Figura 1.14 Sistema de prevención de intrusos

1.4.5 GENERALIDADES DE LAS ZONAS DESMILITARIZADAS (DMZ)

Como describe TP-Link a DMZ: es un diseño conceptual de red donde los servidores de acceso público se colocan en un segmento separado, aislado de la red. La intención de DMZ es asegurar que los servidores de acceso público no puedan comunicarse con otros segmentos de la red interna, en el caso de que un servidor se encuentre comprometido [27].

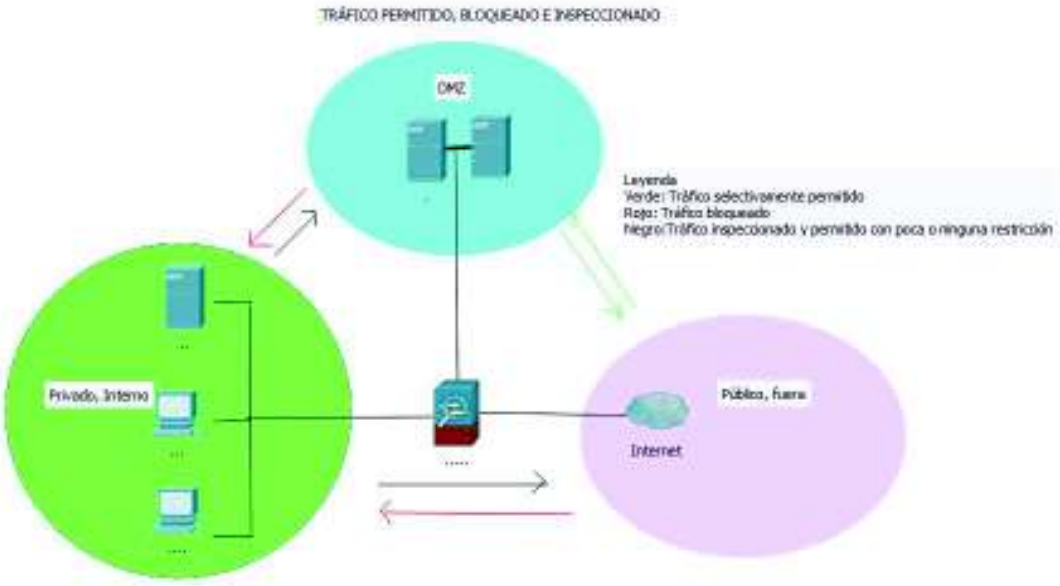


Figura 1.15 Configuración básica de una DMZ

En la figura 1.15 se observa de manera gráfica las opciones que se tiene al configurar una DMZ, el tráfico proveniente de la red privada puede ir hacia internet o hacia la DMZ sin restricciones, mientras que el tráfico que retorna desde la DMZ o de internet hacia la red interna es inspeccionado y permitido.

El tráfico que se genera en la DMZ hacia la red interna es bloqueado, pero si va hacia la red externa es selectivamente permitido; depende de los servicios requeridos configurados previamente.

El tráfico que fluye desde internet hacia la DMZ es selectivamente permitido e inspeccionado y el tráfico que retorna desde la DMZ a internet es dinámicamente permitido, es decir que solo es en respuesta a un paquete recibido.

El tráfico de internet permitido es solo aquel que es en respuesta a una solicitud de la red, nada ingresa a la red a menos que se solicite [28].

1.4.6 REDES PRIVADAS VIRTUALES (VPN)

Una VPN, es una red privada creada a través de una red pública, usualmente mediante internet. Utiliza conexiones virtuales enrutadas por internet hasta la red remota.

Crea grupos de usuarios separados de otros usuarios de la red, permitiéndoles comunicarse como si estuvieran en una misma red privada, este nivel de separación es seguro, cifrado, y existen diferentes tipos de protocolos que se utilizan para lograr la comunicación segura de los usuarios que pueden usar su propia infraestructura o una red pública.

Las VPN pueden ser de capa 2 o capa 3 y dependiendo de su aplicación se utilizan diferentes protocolos [29].

1.4.7 ANTIVIRUS O ANTIMALWARE

Hoy en día al mencionar una protección contra amenazas externas de red, se piensa en un antivirus como un concepto muy general, pero en realidad no solo protege de virus a un equipo computacional, sino también de cualquier tipo de

software malicioso (malware), los virus están incluidos en el concepto de malware.

Muchas veces escuchamos el término antimalware, que sería una protección global contra software malicioso pero, en la actualidad los llamados antivirus en realidad protegen de todo tipo de software malicioso, virus, gusanos, caballos de Troya, etc., de los cuales se hablará más adelante [30].

En el mercado existen antivirus diversos, que se los puede obtener de acuerdo al nivel de confianza que se han ganado y de la facilidad para obtenerlos, los cuales van desde versiones gratuitas a soluciones pagadas, los más populares se menciona los a continuación:

- Kaspersky
- Eset
- Avira
- Panda
- Symantec
- Trend Micro
- McAfee.

1.4.8 CONTROL DE ACCESO AAA

Como medida de seguridad en una LAN se usa una autenticación AAA, de las siglas en inglés (Autorization, Authentication, Accounting), que quiere decir que para permitir un determinado acceso a un dispositivo se debe evaluar estos tres parámetros, donde se verifique quién es la persona que ingresa, los permisos que este tiene para realizar alguna acción y los procesos que realiza en el equipo.

1.4.8.1 Autenticación

Proceso en el que un cliente se identifica antes de obtener acceso a la red y servicios en general, se lo realiza mediante credenciales de identificación como: usuario y contraseña, desafíos, certificados digitales, entre otras [31].

1.4.8.2 Autorización

“Define los servicios o recursos a los que el usuario puede acceder una vez que su ingreso a la red ha sido concedido” [31]. Por ejemplo: si dispone o no permiso para cambiar la configuración de un dispositivo, si puede o no hacer uso de los servicios de impresión, etc.

1.4.8.3 Contabilización

La contabilización (Accounting), permite almacenar información acerca de las actividades en la red por parte de los usuarios, esta información es útil para administración, planificación, facturación, auditorías, etc., [31].

2 CAPÍTULO II: ANÁLISIS DE AMENAZAS A LA RED CONOCIDAS

Debido a que la información es cada vez más valiosa y la forma de almacenamiento está cambiando, es necesario que esta información sea protegida de manera adecuada, evitando que algún virus, gusano o cualquier tipo de software malicioso afecte la seguridad de la información.

Es por eso que se debe tener claro lo que es una vulnerabilidad y una amenaza en las redes actuales. Adicional a esto se mencionará el tipo de atacantes cibernéticos y las amenazas de red reportadas en el Ecuador en el año 2016.

2.1 VULNERABILIDADES

¨Es una debilidad inherente a toda red y dispositivo, incluyendo routers, switches, computadoras de escritorio, servidores, e incluso los propios dispositivos de seguridad¨ [32].

2.2 AMENAZAS

Es una potencial violación de seguridad de una red, cuando las condiciones se prestan, es decir que exista una acción, circunstancia o evento que podría causar daño explotando una vulnerabilidad de la red [4].

2.3 TIPOS DE ATACANTES

Se considera atacante a una persona que, con conocimiento de causa y utilizando herramientas informáticas, obtiene acceso a la información de una empresa o persona con fines ilícitos, con el objeto final de obtener algún tipo de beneficio económico o perjudicar al elemento infiltrado.

A continuación, se detallan los diferentes tipos de atacantes conocidos:

2.3.1 HACKER

Experto programador en computadoras que accede sin autorización a los recursos

de una red, la finalidad puede ser variada, pero aún no se considera una amenaza hasta que causa daños a la red ingresada, por ejemplo: realizar un test de penetración para dar recomendaciones de seguridad a la empresa vulnerada [32].

2.3.2 CRAKER

Individuo que, tras romper la seguridad de un sistema, modifica el software original y causa daño al sistema ingresado [32].

2.3.3 PHREAKER

Persona que manipula la red telefónica haciendo que esta funcione a su conveniencia. Se podría dar el caso de que una llamada internacional cueste lo mismo que una llamada local.

2.3.4 SPAMMERS

Usualmente este tipo de atacantes usa virus para tomar el control de un equipo y enviar gran cantidad de correos electrónicos a nombre de la persona infectada, evitando así que los verdaderos involucrados en este tipo de ataque sean detectados.

2.3.5 CARDERS

Su objetivo es obtener acceso a las tarjetas bancarias de las personas infectadas con algún tipo de virus recolector de información, estudian el método de trabajo de estas tarjeras y si encuentran alguna vulnerabilidad atacan de inmediato.

2.3.6 SCRIPT KIDDIES

Son principiantes en el mundo del hacking, que por diversión o por querer involucrarse un poco más en el ambiente de hacking, utilizan la red de internet para buscar información sobre cómo crear ataques, y usan programas que están destinados a crear virus pequeños que podrían causar algún daño a un determinado sistema informático.

2.3.7 PHISHER

El phisher trata de adquirir información personal para provocar daño económico a un individuo. Puede usar mails para obtener información confidencial propia de cada persona o cualquier otro tipo de medio, incluyendo las redes sociales para obtener información relevante de contraseñas o tarjetas bancarias.

2.4 TIPOS DE ATAQUES

Son clasificados según su función, es decir, del daño que causan a las redes internas de alguna organización.

2.4.1 DENEGACIÓN DE SERVICIO (DoS)

También llamado ataque DoS; se da cuando el atacante obtiene acceso a la red y degrada un determinado servicio, haciéndolo inaccesible a los usuarios legítimos.

2.4.2 REMOTE TO LOCAL (R2L)

El atacante, sin contar con cuenta en la máquina de la víctima, es capaz de enviar paquetes a dicha máquina y obtener acceso local [33]. Utiliza para este propósito herramientas digitales que descubren alguna vulnerabilidad para permitir el acceso [32].

2.4.3 REMOTE TO USER (R2U)

El atacante consigue acceso a una cuenta de usuario de la máquina de la víctima [33].

2.4.4 REMOTE TO ROOT (R2R)

El atacante tiene el control total de la máquina de la víctima [33].

2.4.5 REMOTE DISK READ (RDR)

El atacante es capaz de leer ficheros de datos privados de la máquina de la víctima, sin necesidad de la autorización de su propietario [33].

2.4.6 REMOTE DISK WRITE (RDW)

El acatante es capaz de escribir ficheros de datos privados en la máquina de la víctima, sin necesidad de la autorización de su propietario [33].

2.4.7 USER TO ROOT (U2R)

El usuario local de una máquina es capaz de obtener los privilegios que normalmente son reservados para el root Unix o super-usuario [33].

2.4.8 SURVEILLANCE / PROBING O SCAN - PROBE (S/P)

Programas que pueden explorar automáticamente una red de máquinas, recogiendo información o identificando vulnerabilidades conocidas; con esto, se tiene un mapa de las máquinas y servicios y una identificación de los puntos débiles de una red, útiles para ataques más peligrosos [33].

2.5 AMENAZAS A LA RED

Es importante conocer los tipos de malware que afectan nuestros dispositivos, y que los reconozcamos, ya que los hackers o criminales en línea utilizan a los usuarios finales para que instalen los programas maliciosos sin que estos ni siquiera se den cuenta.

2.5.1 VIRUS

Es un código malicioso que viene adjunto a un archivo ejecutable. Muchas veces necesita que el usuario autorice la ejecución. Cuando el virus se ejecuta, analiza el disco duro infectando archivos. Puede provocar daños severos como borrar o modificar archivos, o daños leves como cambiar la imagen de la pantalla. Muchos de estos virus se pueden colocar en una memoria flash o en un CD/DVD. A través de correo electrónico también se puede transmitir un virus.

Mitigación*:* instalación de un firewall y un antivirus que puedan controlar el tráfico de información entrante, instalación de software, además examinación periódica para detectar y mitigar virus [34].

2.5.2 CABALLOS DE TROYA

Hacen alusión a la leyenda griega, que narra la historia de un enorme caballo de madera ofrecido al pueblo de Troya por sus enemigos, del cual salieron los soldados griegos mientras los troyanos dormían para poder atacar por fin la ciudad.

Es la ilustración de un engaño encubierto. De igual forma, este tipo de amenazas esconden códigos maliciosos en aplicaciones supuestamente confiables, en software libre que se puede descargar desde internet, chats y mensajería electrónica son algunas de las fuentes comunes de infección, son muy difíciles de detectar [35].

Mitigación: una herramienta preventiva o reactiva es el software antivirus, que detecta y elimina virus, gusanos y caballos de Troya, el cual debe ser instalado en todas las maquinas conectadas a la red [36]. También se puede utilizar un dispositivo de gestión unificada de amenazas (UTM) como el Secure Service Gateway (SSG) 50 de Juniper Networks, que ofrece protección contra amenazas a equipos de escritorio y servidores, dado que posee un conjunto de funciones de seguridad con contrafuegos e inspección de estado, VPN IPSec, IPS, antivirus, antispam y filtrado web [36].

2.5.3 GUSANOS

Los gusanos se replican así mismos, y exploran vulnerabilidades de la red. Usualmente una de las consecuencias es que la red se vuelva lenta. Una vez que el equipo es infectado no necesita del usuario, la infección se replica sola por la red.

Mitigación: al igual que con los caballos de Troya, una forma de protección es el uso de una suite de seguridad o antivirus, la cual debe mantenerse actualizada teniendo los archivos adecuados para la correcta detección de amenazas dado que, al no mantener actualizado el antivirus, el equipo está vulnerable a gusanos desconocidos [37] .

2.5.4 RANSOMWARE

Niega el acceso a la información del dispositivo infectado. Para remover esta restricción el virus demanda un pago económico.

Mitigación: controlar los ficheros que se sobrescriben, dadas las preferencias de los ransomware [38] de encriptar archivos personales de los usuarios, se puede monitorizar archivos que tengan extensiones doc, txt, jpeg, pdf, etc. [39]. También se debe tomar medidas de aislamiento del sistema que eviten que se propague, por lo que se debe realizar lo siguiente [39]:

- Desmontar todas las unidades
- Desconectar todas las interfaces, incluyendo las de red para impedir una conexión.

2.5.5 SPYWARE

Este malware es usado para obtener información del usuario y enviarla a algún lugar remoto para su análisis, obviamente sin autorización del usuario, está ejecutándose en segundo plano.

Mitigación. – las técnicas de detección de spyware para prevenir una infección en un sistema de cómputo se basan en cuatro parámetros importantes.

1. Detección en base a firmas digitales.
2. Detección basada en el comportamiento.
3. Detección basada en las especificaciones.
4. Detección basada en minería de datos.

Y la solución que engloba a estos cuatro diferentes puntos de análisis es un antispyware basado en patrones de diseño de software de seguridad.

Un antivirus moderno es capaz de detectar un malware por medio de una cadena característica extraída de su código, y la almacena en una base de datos, por lo que es necesario que el antivirus se encuentre actualizado [40]. Con ello, el antivirus puede establecer niveles para limitar el acceso a las acciones y opciones de configuración de interface local [40].

También se puede utilizar un antispyware, ya que este es capaz de reducir los efectos causados por el spyware, incluyendo el uso no autorizado de la información privada [41].

2.5.6 ADWARE

Es el responsable de desplegar propaganda fastidiosa mientras se navega por internet en un dispositivo. Es utilizado por algunas empresas de ventas para determinar las preferencias del usuario, y así enviar publicidad que podría ser de interés del comprador.

Mitigación: el software antispyware también posee aplicaciones que incluyen la detección, eliminación de cookies y adware, asimismo evita instalaciones futuras [36].

2.5.7 SCAREWARE

Malware muy peligroso que incluye herramientas de escaneo. Crea ansiedad en el usuario ya que este cree que la información que le brinda esta amenaza es real. Esto se logra con base en ingeniería social, la cual analiza los gustos, preferencias, lugares, amigos, etc., del usuario, haciendo seguimiento de sus redes sociales.

Mitigación: Un antivirus está en la capacidad de establecer niveles que limitan el acceso a las acciones, opciones de configuración de interface local, y a información privada, cuando se detecta una amenaza [40].

2.5.8 PHISHING

Se basa en una técnica de ingeniería social, que trata de convencer al usuario de proporcionar información personal y almacenarla en páginas web falsas, tomando el nombre de alguna entidad real para engañar al usuario.

Por ejemplo: puede llegar un correo electrónico del banco de su confianza, pidiendo que actualice sus datos y brinde información de sus cuentas bancarias. Con esta información el atacante cibernético puede hacer transacciones en su nombre y robar su dinero, o hacer que usted pague por algo que no recibió [42].

Mitigación: esta técnica encaja en una estafa común, mas no en un fraude informático, dado que son casos donde se realiza una transferencia patrimonial con un engaño evidente, a pesar de que la comunicación se realiza por medios informáticos, un buen antivirus podría limitar el accionar de estas amenazas [43].

2.5.9 ROOTKITS

Es un programa que oculta la presencia de malware en el sistema, se instala y se mantiene oculto, pero otorga permisos de administrador al atacante, con lo que puede generar daños de cualquier tipo.

Mitigación: Microsoft Forefront Client Security Brinda protección unificada frente a software malicioso como spyre, rootkits, virus, gusanos y troyanos, trabajando en tiempo real o de forma programada, esta es una de las maneras de protegernos ante esta amenaza [44].

2.6 AMENAZAS MÁS COMUNES EN EMPRESAS DE MEDIANA ESCALA (ENCUESTA)

Se planteó una encuesta a administradores de red, personas que tienen una formación técnica especializada en seguridad perimetral de redes y/o que trabajan en esta área y tienen experiencia en el campo, con el objetivo de recopilar información acerca de las empresas de mediana escala en Ecuador, para saber: cómo se manejan en cuanto a seguridad se refiere, qué infraestructura disponen para este cometido, las amenazas más comunes a las qué se enfrentan y qué técnicas y/o herramientas usan para mitigar estas amenazas.

La información obtenida de cada empresa es totalmente confidencial, por lo que se ha visto la necesidad de no incluir en la encuesta nombres de técnicos y de empresas para las que prestan sus servicios.

Las personas encuestadas en mención son aspirantes a un certificado CCNP[14],

---

[14] CCNP, Cisco Certified Network Professional: es un certificado profesional en el manejo de redes otorgado por Cisco.

cuyo perfil es el siguiente: capaces de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y extendidas, así como trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, redes inalámbricas y video.

Habiendo analizado el perfil de las personas encuestadas, se decidió aplicar la encuesta a los aspirantes a este certificado de la Academia Cisco con sede en la Universidad San Francisco de Quito. Esta encuesta se realizó con la ayuda de un formulario gratuito de Google. Cabe mencionar que por seguridad esta encuesta fue proporcionada por los técnicos de seguridad de forma anónima y voluntaria, conociendo la finalidad de la misma.

La encuesta planteada se encuentra en anexo A. las respuestas fueron tabuladas automáticamente por el formulario gratuito de Google.

Respuestas tabuladas automáticamente.

1.

Figura 2.1 Porcentaje de empresas víctimas de ataques cibernéticos

Se puede verificar que cerca del 40% de las empresas de mediana escala han sufrido algún tipo de ataque cibernético en el último año.

2.

Tabla 2.1 Ataques de red en el último año

Si su respuesta anterior fue afirmativa, describa como afectó el normal funcionamiento de su empresa. (25 respuestas)
Me negó el acceso al servidor de datos y se encriptó la información.
Mediante correo invade malware solo al computador en el que se abrió correo, replica innumerables veces un archivo, satura el PC y replica el correo. Esto ocurrió solo en POS específicos aislados
Página web.
Correo.
Degradación de servicios.
Lentitud en la comunicación.
Sin documentación para ventas.
Servicio web.
Virus zepto.
No existió afectación, se controló el evento.
Saturación en interfaces de tx.
Spam que congestiona el servidor correo.
Denegación de servicios.
Se detuvo el servicio de Internet.
Demora en los trámites internos con los clientes.
Ransomware en dos equipos.
Al implementar el servicio de correo corporativo, el servidor fue atacado por robots spam, lo que ocasionó que coloquen en lista negra a la IP de nuestra institución.
Caída del sistema, modificación de registros de la base de datos.
Se paró producción hasta limpiar lo encriptado.
Tiempo fuera de servicio de aplicativos.
Cifrado de datos.
Pérdida de datos sensibles a la empresa.
Lentitud en el servicio.
Tiempo fuera de servicio.
Borrado de configuración de firewall, intentos persistentes de acceso.

3.

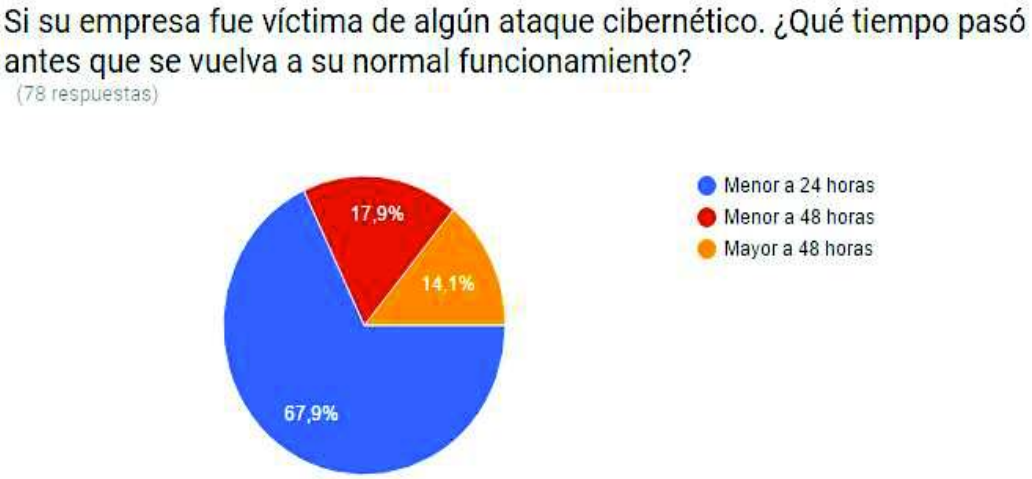


Figura 2.2 Tiempo de interrupción de los servicios

Un gran porcentaje de empresas tiene la capacidad de recuperarse de un ataque en menos de 24 horas, pero no es el caso de todas las empresas.

4.

Figura 2.3 Plataformas usadas para seguridad

Se observa que la infraestructura de las empresas es mixta; en su mayoría combinan los sistemas operativos, lo que quiere decir que el personal humano que hace seguridad de redes en las empresas está en la capacidad de manejar diferentes sistemas operativos y diferentes configuraciones, todo con el fin de que la red sea más segura.

5.

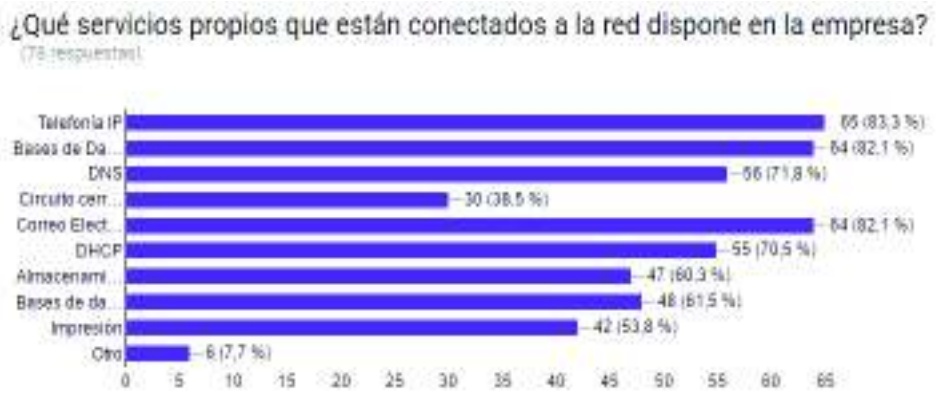


Figura 2.4 Servicios de red de una empresa de mediana escala

Una empresa de mediana escala dispone de algunos servicios de red que son muy importantes para su funcionamiento. La prioridad de un servicio frente a otro depende en gran medida del giro del negocio. En la figura 2.4 se describen los servicios básicos e importantes que se deben proteger en una red de mediana escala.

6.

Figura 2.5 Amenazas más comunes en una red

La figura evidencia las amenazas reales que enfrenta una empresa de mediana escala en el día a día. Esta información será tomada como base para la propuesta de seguridad que se realizará en el capítulo cuarto de este trabajo de titulación.

7.

. ¿Qué herramienta de seguridad dispone en su empresa?

78 respuestas

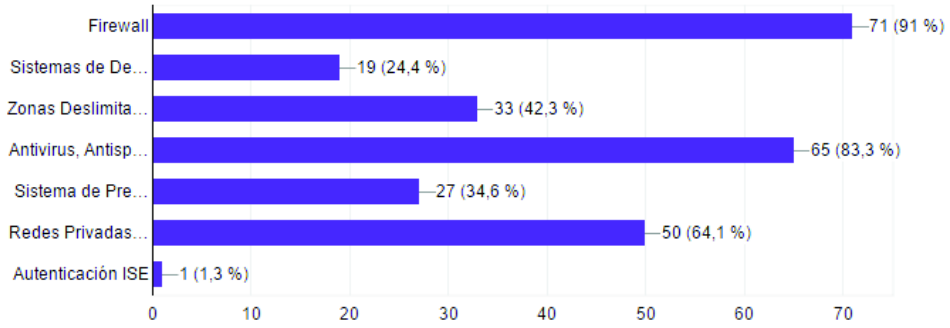


Figura 2.6 Herramientas de seguridad

Se puede observar que la gran mayoría de empresas de mediana escala tiene un firewall y un antivirus configurado en su solución de seguridad, adicional se ayudan de redes privadas virtuales para garantizar la integridad de los datos al conectarse remotamente a la empresa.

8.

¿Cuál de los siguientes firewall es utilizado para proteger su red? (78 respuestas)

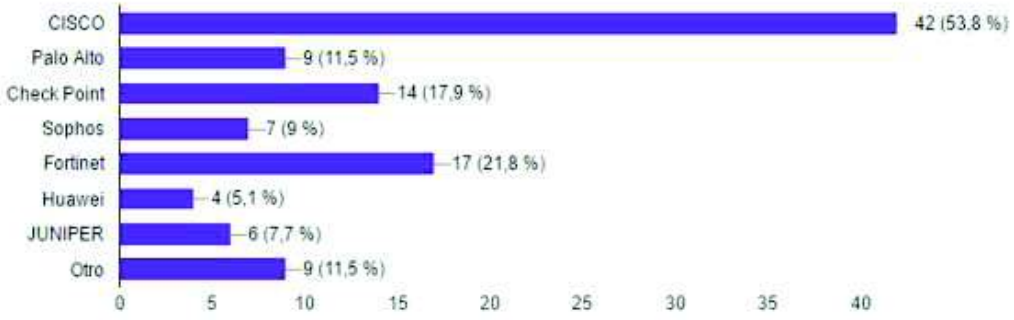


Figura 2.7 Firewalls más usados en Ecuador

Se hizo esta pregunta para investigar el mercado local. Se puede ver que proveedores de equipos como Cisco o Fortinet tienen mayor preferencia en los usuarios, pese a que empresas como Checkpoint o Palo Alto son las marcas de equipos que dominan a nivel mundial según la información del cuadrante mágico de Gartner.

Al preguntar informalmente, los usuarios manifiestan que eligen estos equipos porque en la región tienen más opción de capacitación en el manejo de los mismos, además de un fácil acceso a soporte de operación por parte de los proveedores de estos equipos.

Cisco incluso tiene a nivel mundial una rama dedicada a la enseñanza, que certifica a sus estudiantes en el manejo de conceptos y uso de equipos de red.

9.

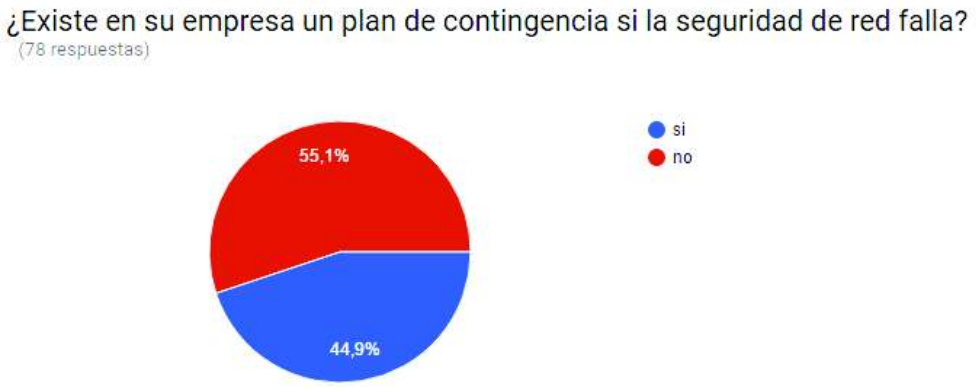


Figura 2.8 Porcentaje de empresas con plan de contingencia

Más de la mitad de empresas de mediana escala no cuentan con un plan de contingencia cuando la red falla. Lo que se hace en la actualidad es corregir los daños en la marcha. Esto da pie a que eventualmente no se puedan recuperar todos los servicios de manera efectiva, o que la información no sea íntegra nunca más.

Los motivos para que esto suceda pueden ser varios, desde el factor económico hasta un desconocimiento de los pasos que se deben seguir para implementar un buen plan de contingencia. En este proyecto de titulación se dejarán las pautas para que se pueda implementar un plan de contingencia.

10.

Figura 2.9 Inversión en seguridad de las empresas de mediana escala

Se puede verificar en la gráfica que la mayoría de las empresas encuestadas invierten menos de $ 10.000 en seguridad. Las empresas en este estudio son las consideradas de mediana escala, y la actividad de las mismas se detalla en el capítulo siguiente.

11.

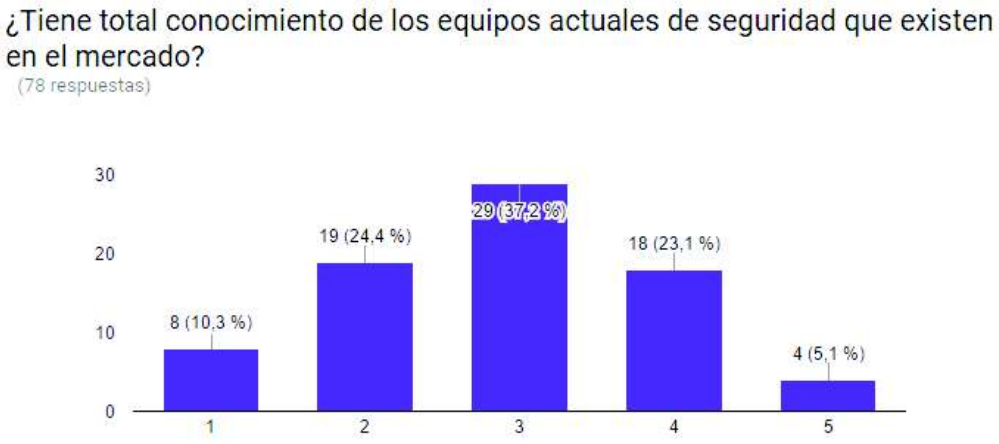


Figura 2.10 Conocimiento de los técnicos acerca de las tendencias en equipos de seguridad

La tecnología avanza cada día, por lo que es muy importante que el personal encargado de la seguridad de la red esté al tanto de los nuevos equipos o tecnologías que se ofrecen en el mercado.

2.6.1 AMENAZAS REPORTADAS EN SITIO OFICIAL DEL ECUADOR

Según el centro de respuestas a incidentes informáticos del Ecuador (ECUCERT), en el año 2016 se reportaron los siguientes incidentes.

- Drones_Botnet. - conjunto de hosts conectados a internet, que interactúan para realizar una tarea específica, sin el consentimiento ni conocimiento de los propietarios, al host se lo conoce como zombi.
- Sinkhole_HTTP_IPv6.
- Sinkhole_HTTP.
- Microsoft_Sinkhole.

  Estos 3 incidentes son del tipo pasivo, un sinkhole es un sistema al que se dirigen las IPs malintencionadas, es como crear un campo de pruebas de análisis, hacia donde se dirige al atacante que intenta obtener información de conexión, se emula diferentes protocolos para hacer creer que el sitio al que se accede es real, los protocolos que se intentaron atacar fueron HTTP e IPv6, adicional el sistema operativo de Microsoft.
- Bruteforce. - este tipo de ataque consiste en ir probando y combinando uno por uno diferentes caracteres de texto, numéricos o alfanuméricos, hasta que alguna combinación de resultado, para esto se necesita un diccionario completo.
- Compromised_website. - son sitios web comprometidos utilizados para el envío de spam, ataques DDoS, etc.
- Phishing. - como se explicó anteriormente, se trata de un engaño al usuario para que provea información personal con fines de lucro.
- CC_Server. - representa los problemas que han tenido los usuarios para conectarse al servidor CC de la suite de programas de Adobe, debido a las actualizaciones desfasadas, se presentan vulnerabilidades que pueden convertirse en amenazas cuando son explotadas por un atacante.

Esta información fue solicitada vía mail a Ecucert, ya que no se encuentra disponible al público en general, el mail se encuentra adjunto en el anexo C.

2.7 ¿CÓMO ACTUAR ANTE UN ATAQUE DE RED?

En el capítulo anterior se determinó los mecanismos que se utilizan para mantener una red segura, pero el momento que la red se ve atacada por un agente externo (amenaza de red), es cuando la red debe mitigar o contrarrestar esa amenaza, para lo cual se debe seguir los pasos mencionados a continuación:

1.- Definir el Alcance. - Estimar el impacto del ataque, cuantificar el daño ocasionado, se debe valorar si el impacto es alto en la empresa o tiene un rango bajo-tolerable en función de los servicios que presta la empresa. Identificar la amenaza, recopilar toda la información que exista de la amenaza, recopilar reportes de los equipos de seguridad y configuraciones de software.

2.- Garantizar la continuidad del servicio. - Cuando se detecta el equipo que está infectado, se lo debo inhabilitar y activar su respaldo inmediatamente para que las operaciones de la empresa no se vean afectadas, también se debe verificar cuentas abiertas, conexiones en proceso, y dar de baja estos servicios.

3.- Contener la infección. - Aislar la zona de impacto de la amenaza, se debe evitar a toda costa que el ataque se siga esparciendo por la red, por consiguiente, hay que tomar medidas necesarias para lograr este objetivo, por ejemplo, un simple bloqueo de puertos hasta un apagado de cierto equipo, además se debe estar en constante monitoreo de movimientos inusuales sobre los datos del servicio vulnerado.

Por otro lado, si se generó una infección en un equipo y este se encuentra cifrado, se deberá aplicar un proceso de ingeniería inversa para obtener las claves criptográficas. Pero si el ataque es a través de protocolos como HTTP, se podrá identificar con mayor facilidad los comandos utilizados por el atacante.

En cualquiera de los casos se podrá identificar los equipos infectados y así también patrones de tráfico que deberán generarse para crear una barrera de defensa.

4.- Disminuir la infección y eliminar el vector del ataque. - Eliminar el origen del ataque es un proceso complejo, se requiere un análisis detallado del código para entender cómo funciona y desde ahí iniciar una desinfección, ya sea de forma manual o automática con un sistema de antivirus.

Los ataques deben ser eliminados completamente, caso contrario la empresa será víctima de nuevos ataques con otros vectores. La primera acción es aislar la falla que permitió el ingreso al sistema para luego eliminarla, al mismo tiempo se recomienda cambiar las contraseñas de todos los equipos de comunicación en la red, pues estos son los objetivos predilectos para los ataques.

5.- Revisar las lecciones aprendidas. - Los ataques son situaciones donde se pone a prueba la red, por tanto, se debe aprender de estas experiencias y fortalecer los puntos débiles que se encuentre, asimismo analizar las debilidades de las políticas de seguridad que se tiene implementado y mejorarlas, como resultado de estas acciones en un futuro será más fácil encontrar los puntos de riesgo, la información que es más atacada será protegida e incluso las zonas que no eran consideradas objetivo de ataque ahora serán tomadas en cuenta dentro del plan de seguridad, concluyendo en una red más segura [45].

2.8 PLAN DE CONTINUIDAD DE NEGOCIOS (BUSINESS CONTINUITY PLAN-BCP) Y PLAN DE CONTINGENCIA.

El plan de continuidad de negocio (BCP por sus siglas en inglés) es la respuesta prevista por una empresa ante aquellas situaciones de riesgo que le pueden afectar de forma crítica, es decir, impedir la operación tecnológica que soporta los procesos de negocio más importantes.
Toda empresa, sin importar su tamaño, sea grande, mediana, pequeña o micro debe tener un BCP para garantizar su continuidad.

El plan de continuidad de negocio es aplicable a todos los tipos de negocios, con más énfasis en aquellos donde la disponibilidad de la información es su mayor activo. A partir del 11 de septiembre de 2001, cuando fue el atentado a las torres

gemelas en Estados Unidos, los planes de continuidad de negocio cobraron importancia, dando mayor cobertura a compañías del sector financiero y sus asociados donde hoy en día tienen su mayor aplicación.

Los aspectos que se deben tener en cuenta cuando se planifica un BCP son:

- Identificar los recursos más importantes e imprescindibles que hacen que la empresa funcione adecuadamente.
- Calendarizar respaldos de los recursos irremplazables.
- Desarrollar procedimientos en caso de una interrupción en el normal funcionamiento de la empresa.
- Hacer pruebas y mantenimiento constante a los sistemas de respaldo, de modo que se verifique su normal funcionamiento.

En cambio, un plan de contingencia hace referencia a las acciones que se deben tomar una vez que la empresa se ha visto perjudicada. En este trabajo se hace referencia al funcionamiento de la red de datos, para que las pautas del plan de contingencia sean enfocadas al giro de negocio de la mediana empresa afectada.

Cabe señalar que todo plan de continuidad de negocios tiene incorporado un plan de contingencia, pieza importante para la prevención de una interrupción en la línea de producción de una empresa.

2.9 ACTUALIDAD EN SEGURIDAD INFORMÁTICA

En relación con la seguridad actual en una red se debe comenzar explicando que los ataques ya no solo afectan a las empresas grandes, sino también a las empresas medianas y pequeñas, debido a que al atacante le resulta más sencillo vulnerar las pocas o nulas defensas [46].

La evolución del malware es sin duda una de las grandes preocupaciones para los defensores de red, como el malware de auto propagación (cryptoworms ransomware), Wanna Cry y Nyetya son dos ejemplos de este tipo de malware, que en el 2017 explotaron una vulnerabilidad de Microsoft Windows llamada EternalBlue causando grandes daños a las empresas y recibieron a cambio pagos de dinero en

criptomonedas como rescate por la información eliminada, pero según el Gobierno de EEUU creen que estos ataques en realidad lo que buscaban era eliminar información antes que pedir rescate por ella [46].

Por otra parte, el abuso de servicios en la nube y otros recursos legítimos como: Google, Dropbox, Github, etc., que dan soporte a aplicaciones, datos e identidades que se trasladan a la nube, de ahí que los equipos de seguridad deben gestionar el riesgo que implica perder el control del perímetro de la red tradicional. Además, la constante evolución, crecimiento del entorno virtual (nube) y IoT dificultan la defensa en los equipos de seguridad, en consecuencia, los atacantes están sacando provecho de este hecho [46].

“Una razón es la falta de claridad sobre quién es exactamente el responsable de proteger esos entornos” [46].

Como resultado de este gran desafío, “las empresas pueden necesitar aplicar una combinación de mejores prácticas, tecnologías de seguridad avanzadas como machine learning e incluso algunas metodologías experimentales” [46], según los servicios que son necesarios para su giro de negocio y la constante evolución de las amenazas.

Por otro lado, el 50% del tráfico web global se encriptó a partir de octubre de 2017, con la encriptación se pretende mejorar la seguridad, de ahí que, los atacantes con sus eficaces herramientas entran en el juego de encriptar sus actividades y causar más daño inclusive, por tanto, se está utilizando la inteligencia artificial y aprendizaje mecanizado para detectar patrones inusuales en el tráfico web encriptado [46].

Continuando con las tendencias de comunicación enfocados a seguridad de redes, no se puede quedar fuera el concepto de traiga su propio dispositivo (BYOD)[15], con lo cual ganamos movilidad en la red y ahorro en las empresas de mediana escala,

---

[15]BYOD.- del inglés Bring Your Own Device, que quiere decir, traiga su propio dispositivo.

los celulares inteligentes, las computadoras portátiles, son algunos de los dispositivos que se podrían usar en el trabajo siendo de pertenencia del trabajador. Con lo cual lleva un nuevo riesgo de seguridad, la tendencia es tener una administración centralizada para control de estos dispositivos. Lo que se hace es enviar a estos equipos por una red especial hacia internet, de manera que cuando quieran ingresar a un recurso interno de la red, sea necesario que pasen por todos los filtros como un paquete normal de internet, con lo cual, si el dispositivo es autorizado y no se detecta alguna amenaza podrá ingresar a la intranet, caso contrario se descarta el paquete [1].

3 CAPÍTULO III: CARACTERÍSTICAS DE LAS EMPRESAS DE MEDIANA ESCALA

3.1 EMPRESA DE MEDIANA ESCALA

El decreto ejecutivo 757, en la Sección II, Capítulo I, Artículo 106, literal C, del reglamento al código orgánico de la producción, comercio e inversiones, con fecha 29 de diciembre 2010 manifiesta que: “Una mediana empresa es aquella unidad de producción que tiene de 50 a 199 trabajadores y un valor de ventas o ingresos brutos anuales entre un millón (1.000.001,00) y cinco millones (5.000.000,00) de dólares”.

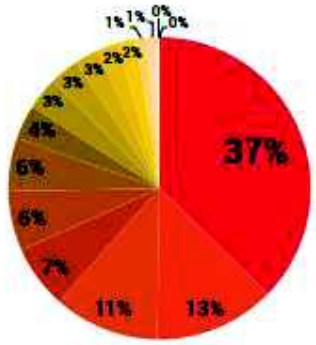
3.1.1 SERVICIOS QUE PRESTA UNA EMPRESA DE MEDIANA ESCALA

Según datos publicados en la revista EKOS del presente año, las pequeñas y medianas empresas en Ecuador representan el 75% de las compañías en Ecuador y concentran más del 70% de los empleos [47].

Esta revista hace un análisis desde el año 2013, donde se experimentó un incremento de 1.565 empresas medianas generando que su número ascienda a un total de 9.604. Igualmente, sus niveles de ingresos, utilidades y rentabilidad han aumentado en este último año. No obstante, el ingreso promedio refleja una tendencia negativa.

Su composición en 2013 presenta una gran influencia del sector comercial (37,28%) seguido de las actividades inmobiliarias, empresariales y de alquiler (12,99%), de las industrias manufactureras (11,26%) y del trasporte, almacenamiento y comunicaciones (11,26%). Según el nivel de desempeño, las empresas medianas registraron un 18,4% de crecimiento entre 2012 y 2013, en las que las mayores tasas de crecimiento ocurren en los segmentos de construcción (55,6%) y pesca (39,9%) [47].

A continuación, en la Figura 3.1 se muestra un resumen de las actividades comerciales que se desempeñan en Ecuador [47].



- Comercio
- Actividades inmobiliarias y de servicios
- Manufactura
- Transporte y almacenamiento
- Construcción
- Agropecuario
- Otras actividades de servicios
- Intermediación financiera
- Pesca
- Servicios sociales y de salud
- Enseñanza
- Hoteles y restaurantes
- Administración publica y defensa
- Explotación de minas y canteras
- Suministro de electricidad, gas y agua
- Organizaciones y órganos extraterritoriales

Figura 3.1 Actividades comerciales que se desempeñan en el Ecuador [47].

3.2 PYMES

Se define una PYME como un conjunto de pequeñas y medianas empresas, con características distintas a las grandes corporaciones. Las PYMES constituyen un pilar fundamental en la economía de cualquier país, ya que son las responsables de generar la gran mayoría de puestos de empleo y en muchos de los casos no se necesita un gran capital de inversión para estar en funcionamiento [47]. Un negocio de venta de repuestos automotrices se puede considerar una pequeña empresa que, con el tiempo puede crecer, tener sucursales, manejar un determinado volumen de personal y capital, y convertirse en una mediana empresa como lo hizo Abilenecorp S.A. [48], donde su giro de negocio depende cada vez más de la tecnología, ya que la tendencia de negocios está orientándose cada día a la red global. Si su seguridad informática se ve vulnerada puede causar pérdidas significativas. En algunos casos estas empresas pueden incluso desaparecer, ya que sus ingresos son fluctuantes.

3.2.1 FORTALEZAS DE LAS PYMES

Algunas fortalezas de las pequeñas y medianas empresas son su poder de adaptarse al mercado, la personalización de productos, y su gran diversidad de producción de bienes y servicios [47]. Otra gran ventaja es que sus empleados son muy leales, reflejando el compromiso y la personalidad del fundador [49], debido a su tamaño que permite una mayor proximidad entre la comunidad donde desarrollan sus actividades, lo que conlleva a conocer cuáles son las necesidades de sus trabajadores y su ambiente social [50].

La mayoría de la fuerza laboral del mundo se encuentra produciendo para las pequeñas y medianas empresas, representando el 95% de las unidades productivas [47].

3.2.2 DEBILIDADES DE LAS PYMES

Al ser empresas pequeñas y medianas, resulta poco probable que establezcan una infraestructura tecnológica capaz de competir con las grandes empresas. Falta de fomento en la cantidad de créditos otorgados de modo que, en la mayoría de casos, no puedan ofrecer sueldos competitivos y deban contar con personal poco capacitado [47] , y que no se tenga una infraestructura tecnológica adecuada para responder a las presiones de los clientes y competir con las grandes empresas a nivel mundial [49].

3.2.3 PYMES ECUADOR

Una investigación publicada en el diario El Comercio de la ciudad de Quito, el 19 de julio de 2015, declara que el 68% de las PYMES ecuatorianas cuenta con ordenadores, el 88% tiene servicio de Internet, y el 99% accede a la red a través de la banda ancha fija [51].

Esto evidencia que no se está explotando en su totalidad las capacidades de la red mundial para generar intercambios comerciales. Algunas causas pueden ser: miedo a realizar transacciones en Internet, temor a que los datos de la organización sean vulnerados, excesivo recelo al uso de tecnología, entre otras [52].

Algunas de las empresas consideradas de mediana escala se muestran a continuación. Estas empresas son analizadas hasta el año 2013. Se ha tomado esta fecha como referencia ya que una empresa debe mantenerse en el tiempo, actualmente estas empresas siguen liderando los distintos tipos de mercado, con leves variaciones en las posiciones que ocupan en el ranking mostrado.

TOP 100 EMPRESAS MEDIANAS						
Rk	Razón Social	Sector	Total Ingresos		Var. %	IMP. RENTA CAUSADO 2012 (USD miles)
			2011 (USD millones)	2012 (USD millones)		
1	ZAVATO S.A.	Manufactura	4.428,59	4.996,86	12,83%	81,77
2	ORENAS S.A.	Minas y canteras	4.089,54	4.996,73	22,18%	124,96
3	PROVEEDORA ANDINA DE PAPEL ANDIPAPEL S.A.	Comercio	5.179,16	4.987,91	-3,69%	5,77
4	HYDRIAPAC S.A.	Servicios	3.186,13	4.981,30	56,34%	12,52
5	ACERDFERRETER Y CONSTRUCCIONES CIA. LTDA	Construcción	4.491,12	4.980,95	10,91%	9,96
6	ESTACION DE SERVICIOS ROJAS CIA. LTDA. SERVIROJAS	Comercio	4.814,34	4.980,92	3,46%	25,25
7	CORPORACION ZEDECUADOR S.A.	Servicios	3.143,15	4.978,41	58,39%	135,05
8	DROESTIBA S.A ESTIBADORES DE EL ORO	Transporte	4.194,09	4.972,75	18,57%	41,07
9	SISTEMA DE EXTRACCION DE PALMISTE SIEXPAL S.A.	Alimentos y bebidas	11.544,12	4.971,58	-56,93%	58,46
10	TRAUMAMED S.A.	Comercio	4.392,84	4.971,08	13,16%	157,89
11	COMERCIALIZADORA VIVANCO COBOS VICOSA CIA. LTDA.	Comercio	5.084,02	4.970,83	-2,23%	22,65
12	MINDCORP S.A.	Construcción	4.014,00	4.969,78	23,81%	2,49
13	XUK S.A.	Pesca y elaborados	4.459,25	4.955,40	11,13%	117,81
14	ENATIN S.A.	Construcción	4.576,14	4.955,33	8,29%	35,96
15	ARROYO AGUIRRE CONSTRUCTORES Y SERVICIOS CIA. LTDA.	Construcción	1.676,60	4.952,02	195,36%	76,06
16	DICARNES AGUBICAB S.A.	Comercio	4.555,40	4.950,77	8,68%	2,74
17	OLEAGINOSAS TROPICALES OLYTRASA S.A.	Alimentos y bebidas	4.312,66	4.950,63	14,79%	0,00
18	ESCOBAR RUIZ CIA. LTDA.	Manufactura	4.325,09	4.948,73	14,42%	14,00
19	ZAPEC S.A.	Comercio	1.731,34	4.947,36	185,75%	49,53
20	PASTIFICIO TOMEBAMBA CIA. LTDA.	Alimentos y bebidas	3.316,77	4.946,71	49,14%	18,83

Figura 3.2 Algunas empresas de mediana escala [47].

3.2.4 INFORMACIÓN QUE DEBE SER PROTEGIDA

Tomando información de la encuesta de seguridad de redes, realizada a personas encargadas de la administración de seguridad de red, para las empresas de mediana escala, los servicios más importantes que deberían protegerse en una empresa de mediana escala son los siguientes:

- Acceso a Internet
- Correo electrónico

- Telefonía IP
- Directorio activo
- Bases de datos
- Servicios de aplicaciones
- Servicio DNS
- Servicio DHCP

Estos servicios están entre los más importantes, según la encuesta realizada en el capítulo anterior.

Dependiendo del giro de negocio de la empresa, el que se afecte un determinado servicio perjudica directamente en la economía de la misma.

3.3 ATAQUES A EMPRESAS PEQUEÑAS Y MEDIANAS

Al analizar información especializada de sitios relacionados con tecnologías de información a nivel latinoamericano, se obtienen los siguientes datos:

- 40% de las empresas medianas han sufrido intrusiones.
- Nicaragua, Guatemala y Ecuador ocupan los tres primeros lugares en incidentes por ataques de código malicioso.
- El phishing ocupa un 16% del total de los incidentes de seguridad informática.
- El 35% de las empresas han iniciado campañas de educación y concientización a sus usuarios acerca de los riesgos de seguridad a los que podrían exponerse.

Todos estos datos fueron obtenidos por la empresa de seguridad informática ESET, mediante encuestas realizadas a 3000 profesionales de la región [53]. Además, esta información concuerda con los datos obtenidos en la encuesta planteada en el capítulo segundo, donde se pregunta a administradores de redes sobre las amenazas que enfrentan cada día y se obtuvo que el 38.5% de las empresas encuestadas fueron víctimas de ataques cibernéticos en el último año.

3.4 EMPRESA MODELO, BASADA EN LAS ESTADÍSTICAS DE LA ENCUESTA

Como se ha mencionado a lo largo de este trabajo, se va a definir una empresa de mediana escala tipo, que puede servir de base para una implementación real, en la cual influye mucho el giro de negocio de la misma, se realizará el cálculo de tráfico solo como ejemplo, ya que en la actualidad ya no se realizan dichos cálculos, simplemente se realiza un test con el proveedor de servicios de internet (ISP), hasta llegar a la capacidad necesaria para trabajar adecuadamente, como lo hacen Netlife [54], CNT [55], entre otros.

3.4.1 CONDICIONES INICIALES

- Número de usuarios conectados. - una empresa de mediana escala puede tener hasta 199 colaboradores y cada uno de ellos puede disponer de 2 a 3 dispositivos capaces de conectarse a la red, se realiza el diseño para la cantidad máxima de usuarios con un solo dispositivo cada uno.

- Servicios de la red de mediana escala. - en base a análisis anteriores, una empresa de mediana escala ofrece los siguientes servicios básicos:

  Acceso a Internet o navegación web
  Correo Electrónico
  Telefonía IP
  Aplicativos propios (antivirus, aplicaciones, servicio DNS, servicio DHCP, bases de datos), se agrupa todos estos servicios para que sea representativo el tráfico de red estimado que se calcula.

3.4.2 TOPOLOGÍA

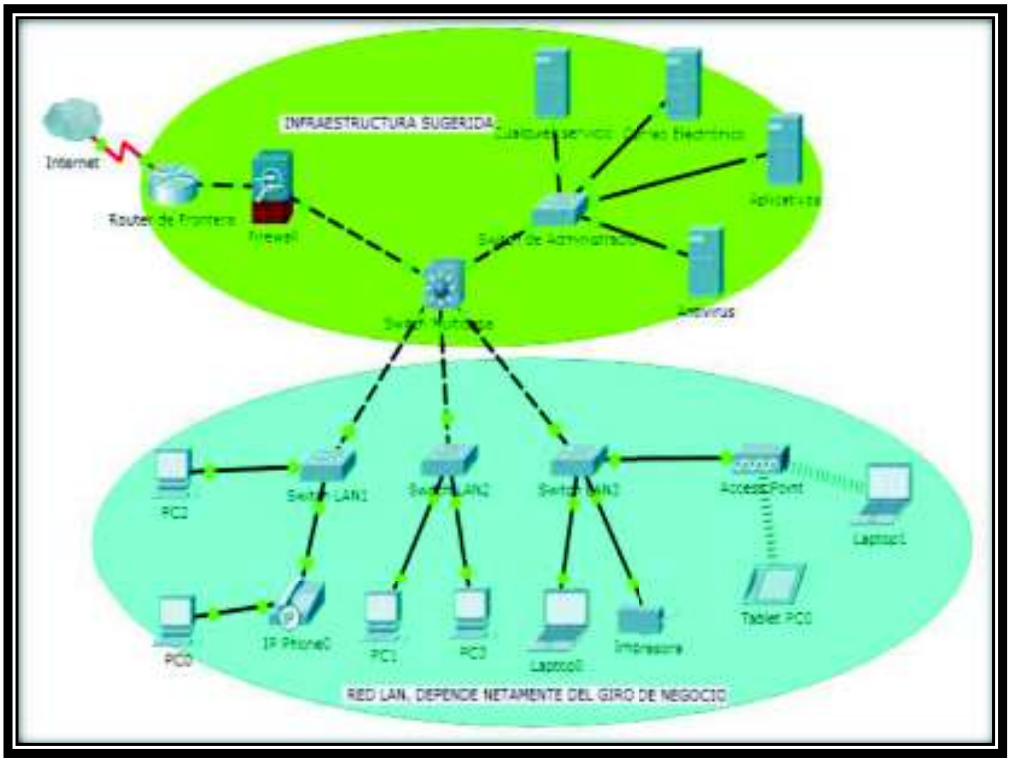


Figura 3.3 Topología Empresa modelo

Se plantea un diseño referencial para la empresa de mediana escala, siguiendo las recomendaciones de Cisco en la distribución de los equipos de comunicación, donde consta la infraestructura sugerida para administración y control de la información [56]: dispositivo firewall (seguridad), servicios que presta la empresa (Correo, DHCP, aplicativos, antivirus, etc.); Además de la red interna (conectividad), que depende netamente del giro de negocio de la empresa, donde se ha considerado equipos conmutadores de capa 2.

3.4.3 CÁLCULO DE TRÁFICO DE RED REFERENCIAL

Lo primero que se debe determinar es el índice de simultaneidad, que indica la cantidad de usuarios que están haciendo uso de una determinada aplicación al mismo tiempo.

Cabe indicar que estos cálculos son referenciales, los datos reales se obtienen haciendo pruebas en la red ya en funcionamiento. Por lo que algunos datos serán sacados de la bibliografía especializada [57].

Tabla 3.1 índice de simultaneidad

	Aplicación	Usuarios	Índice de simultaneidad (%)	Usuarios simultáneos
Internet	Descargas	199	20	40
	Navegación	199	20	40
Intranet	Correo Electrónico	199	20	40
	Telefonía IP	199	20	40
	Aplicativos propios	199	20	40
	Total	199	100	

3.4.3.1 Capacidad de descarga de archivos

Una descarga se realiza cada 30 segundos y tiene un tamaño promedio de 500 Kbps, y teniendo 40 usuarios simultáneos se obtiene los siguientes resultados [57].

$$C_{DA} = \frac{500Kbps}{1\ descarga} x \frac{8bits}{1\ Byte} x \frac{1descarga}{30s} x\ 40\ u.s = 5.3Mbps$$

C_{DA}: Capacidad de descarga de archivos

3.4.3.2 Capacidad de páginas web.

Se obtiene que en promedio la navegación web tiene un tamaño de 320Kbytes, y suponiendo que se visite 10 páginas web por hora y con 40 navegantes simultáneos se obtiene el siguiente resultado [57].

$$C_{PW} = \frac{320Kbps}{1\ Página} x \frac{8bits}{1\ Byte} x \frac{10\ Páginas}{3600s} x\ 40\ u.s = 0.284Mbps$$

C_{PW}: Capacidad de páginas web

3.4.3.3 Capacidad de correo electrónico

Ahora se va a calcular la capacidad de ancho de banda requerida para el tráfico de correo electrónico. Donde se estima que el tamaño promedio de un correo es de 500Kbps y que se revisa 10 correos cada 30 minutos, con 40 usuarios simultáneos [57].

$$C_{ce} = \frac{500Kbps}{1\ Página} x \frac{8bits}{1\ Byte} x \frac{10\ Correos}{30min} x \frac{1min}{60s}\ x40\ u.s = 0.889Mbps$$

C_{ce}: Capacidad de correo electrónico

3.4.3.4 Capacidad telefonía IP

Se hace referencia a que utilizando el protocolo UDP [16]se obtiene un tamaño de cabecera de la trama de 58 bytes y el tamaño de un paquete de voz es de 20 bytes, a una velocidad de transmisión de 8 Kbps, y con 40 usuarios simultáneos se obtiene una capacidad total de [57]:

$$C_{TIP} = Vtx\ x \frac{Tamaño\ cabecera + Tamaño\ paquete\ de\ voz}{Tamaño\ paquete\ de\ voz} x\ usuarios\ simultáneos$$

Vtx: velocidad de transmisión

C_{TIP}: capacidad de telefonía IP

$$C_{TIP} = 8Kbps\ x \frac{58\ Bytes + 20\ Bytes}{20\ Bytes} x40\ u.s = 1{,}248Mbps$$

3.4.3.5 Capacidad de aplicactivos propios

En el diseño tipo se considera que el conjunto de aplicaciones propias de la empresa como: antivirus, bases de datos, impresión, etc., generan un tráfico de 200kbps cada 10min, y teniendo 40 usuarios simultáneos se obtiene [57]:

$$C_{APP} = \frac{200Kbps}{1\ C.App} x \frac{8bits}{1\ Byte} x \frac{1\ C.App}{10min} x \frac{1min}{60s}\ x40\ u.s = 0.106Mbps$$

C_{APP}: Capacidad de aplicativos propios

Con lo cual tenemos un tráfico total de la red de: internet + intranet

Total (Mbps): (5.3+ 0.284) + 0.889+ 1.248+ 0.106= 7.8Mbps

El enlace que se debería contratar es de 10Mbps dedicados, debido a que se necesita alrededor de 8Mbps para su normal funcionamiento, se deja un poco de holgura al tráfico de datos en la red y se contrata 10Mbps, según los cálculos hechos, pero recordando siempre que estos análisis son netamente referenciales, con lo que se evidencia que el tráfico total que circulará por la red será de 7.8Mbps.

---

[16] Protocolo UDP, trabaja en la capa 4 del modelo de referencia OSI, rápido y su desempeño es en base al mejor esfuerzo, es no confiable.

3.4.4 MEJORES PRÁCTICAS PARA ACCESO A LA RED EMPRESARIAL

Las pequeñas y medianas empresas podrán realizar las siguientes acciones para lograr mitigar los principales problemas de seguridad [58]:

- Utilizar una contraseña para iniciar sesión en un equipo de cómputo. Las contraseñas son el mecanismo de entrada para gran parte de sistemas informáticos, por lo que si no se cuenta con una configuración segura el sistema es vulnerable.
- Contraseñas robustas. Las contraseñas deben cumplir características que las hagan difíciles de descifrar, como no utilizar contraseña en blanco, no utilizar palabras que se encuentren en un diccionario, no utilizar información personal, debe estar conformada por letras mayúsculas, letras minúsculas y caracteres, y por último debe tener como mínimo ocho caracteres.
- Utilizar cuentas con privilegios limitados. Las cuentas con privilegios administrativos únicamente son necesarias cuando se requiere instalar programas o modificar la configuración del equipo.
- Utilizar software de seguridad. Es necesario que se tenga instalado un software que evite que la información se dañe o altere, o incluso que el equipo pueda ser controlado de manera remota. Se debe contar con al menos software antivirus, antispyware y un firewall personal. De esta manera se tiene el equipo protegido mientras se navega por internet o aun cuando se esté desconectado.
- Actualizar el sistema operativo del equipo. Con las actualizaciones se puede contar con actualizaciones de seguridad importantes. Con ello, se debe tener activadas las actualizaciones automáticas de acuerdo con la programación que se defina.
- Cambiar las configuraciones predeterminadas. Las configuraciones predeterminadas pueden contener vulnerabilidades de seguridad, por lo que inicialmente se debe cambiar los nombres de cuenta y contraseñas por defecto y aplicar los parches de seguridad [59].
- Apagar o desconectar el ordenador de la red cuando no se lo utilice. Con esto, un atacante no puede ingresar al equipo [59].

4 CAPÍTULO IV: PLANTEAMIENTO DE SOLUCIONES DE SEGURIDAD

4.1 CARACTERÍSTICAS TÉCNICAS MÍNIMAS QUE DEBE CUMPLIR LA SOLUCIÓN DE SEGURIDAD

La encuesta realizada fue de gran utilidad, permitió identificar cuáles son las amenazas más comunes en una red para empresas de mediana escala, con lo cual se plantean los parámetros mínimos que deben cumplir los equipos para una solución de seguridad de red.

Si solamente se toma la información de la encuesta de seguridad, se necesitaría básicamente un buen antivirus para tener solventada temporalmente la solución, como se mostró en la sección 2.5; sin embargo, entre los procedimientos de seguridad que recomiendan los expertos además de un buen antivirus [60], un firewall bien configurado es imprescindible para tener una barrera entre los dispositivos propios del usuario y los atacantes [61]. Por esta razón se incluye en la solución un dispositivo firewall, cuyas características mínimas de cumplimiento se detallan más adelante en la tabla 4.3.

Hoy en día es muy común que el usuario final no solo se conecte a la red desde su computador de escritorio, sino que lo haga también desde dispositivos móviles, con lo cual puede estar conectado simultáneamente desde dos o más dispositivos. Al considerar una empresa de mediana escala con alrededor de 200 personas conectadas desde diferentes dispositivos, y teniendo en cuenta también que estas representan el 95% de empresas generando un alto volumen de empleo [62], se prevé que la solución abarque un licenciamiento de entre 300 y 500 dispositivos, tanto para el antivirus como para el firewall.

Además, con la tendencia de las empresas a incorporar el concepto de BYOD, es necesario tener una DMZ donde vaya todo el tráfico generado por dispositivos móviles y portátiles, obligando así a este tráfico que ingresa a la red pasar por el filtro de firewall y de antivirus, en este proyecto de titulación solo se muestra

gráficamente como sería la topología con la DMZ incluida, ya que la configuración de la misma corresponde netamente a la intranet, lo cual se encuentra fuera del alcance de este proyecto.

En la siguiente tabla se detallan las necesidades básicas de una red en cuanto a seguridad, con lo cual se puede decir que la red se encuentra protegida contra amenazas externas a la intranet. La solución debe tener por lo menos protección contra las siguientes amenazas. (Ver Tabla 4.1)

Tabla 4.1 Características mínimas de seguridad de red

Protección contra:	Virus
	Ataques DoS
	Phishing
	Malware
	Spyware
	Gusanos
	Troyanos
Servicios que deben ser protegidos:	Correo electrónico
	Telefonía IP
	Bases de datos
	DNS
	DHCP
	Directorio activo
	Aplicativos
	Almacenamiento de información
	Acceso a internet

Las características que se espera de un antivirus son:

Tabla 4.2 Características del antivirus

Bloqueo de sitios web	Prevención proactiva
Anti malware	Control de aplicaciones
Administración centralizada	Navegación segura
Licenciamiento para 300 usuarios	Anti spam
Protección contra software de secuestro informático.	Protección contra virus, gusanos, spyware, troyanos.
Soporte técnico	Anti phishing

Las características que debe tener un firewall de red como mínimo para que la solución sea escalable son [63]**:**

Tabla 4.3 Características mínimas para el firewall

Características técnicas que debe cumplir el equipo de firewall para proteger la red de la empresa de mediana escala, por lo menos tres años.	Licenciamiento para 300 dispositivos
	Protocolos de red: DHCP, IP estática, PPPoE, PPTP, L2TP, STP, DDNS
	Protocolo NAT
	Borde de red (DMZ)
	Soporte VLAN: VLAN basadas en puertos y 802.1q basadas en etiquetas, enrutamiento entre VLAN
	Número de VLAN: 16 VLAN activas (rango 1-4096)
	802.1x supplicant: Protocolo de Autenticación Extensible (EAP), MD5, EAP Protegido (PEAP).
	Soporte VPN
	Actualizaciones periódicas
	Control de acceso basado en MAC, enlace IP/MAC, perfiles inalámbricos
	Gestión segura: HTTPS, nombre de usuario / contraseña, certificados X.509 v3
	Antivirus incorporado
	Baja latencia
	Compatibilidad con cualquier sistema operativo en el dispositivo final. OS X, Windows, Linux, Android, etc.
	Soporte IPv6
	4 puertos Uplink 10/100/1000 Mbps

4.2 PROPUESTA DE SOLUCIÓN DE SEGURIDAD

Con base en los resultados obtenidos de las encuestas y del análisis hecho en los capítulos previos, se plantea la siguiente solución de seguridad para una empresa de mediana escala, tomando en cuenta costos y funcionalidad de los equipos.

Además, considerando que una empresa está bien administrada y en constante crecimiento, el criterio de diseño de la parte de seguridad de la red debe sugerir un equipo de firewall para protección externa, aparte de un antivirus potente que

cumpla con los requisitos establecidos anteriormente.

Como se mostrará más adelante en las topologías sugeridas, el firewall se instala a continuación del enrutador de frontera, aislando a la granja de servidores de la empresa en donde están los servicios dedicados que prestan a la misma, ya sea correo electrónico, almacenamiento de información, etc.

Dentro de los servicios dedicados que se proponen para la empresa debe estar el servidor de antivirus, desde donde se puedan administrar las licencias, actualizaciones y las tareas hacia los equipos de la red empresarial, a fin de que todo el tiempo la empresa se encuentre protegida.

Una gran ayuda para proteger la red es que el equipo de firewall haga un primer bloqueo de amenazas, ya sea por bloqueo de cierto tráfico o por acción del antivirus incorporado. Cuando un virus pasa el primer filtro se espera que el antivirus elimine esta amenaza.

Para el tráfico generado por los dispositivos internos de tipo móviles y portátiles se recomienda incorporar una DMZ, para que todo este tráfico sea previamente analizado por los filtros del firewall y del antivirus. La implementación de esta DMZ está fuera del alcance de este proyecto de titulación, ya que se considera parte de la infraestructura interna de la red.

Se sugiere además la incorporación de las mejores prácticas que se detallaron en el capítulo anterior (3.4.4).

Cabe destacar que ningún antivirus asegura una protección del 100%. Todos los días surgen nuevas amenazas, por lo que se requiere que el software que se elija como antivirus y firewall tengan soporte y actualizaciones permanentes. Por tal motivo se indica las características de un plan de contingencia en caso de que la red se vea vulnerada.

Adicional se debe considerar también la opción de utilizar mecanismos de

protección como IPS e IDS incorporados en el firewall, estos son aconsejables en las redes dedicadas a proteger a la mediana empresa, por lo que se propone la incorporación de estos mecanismos en la protección de la red. Ya que se necesita estar monitoreando la red en todo momento y estar alerta ante cualquier anomalía, con estas características se asegura combatir y más que nada prevenir en tiempo real las intrusiones no autorizadas a la red.

Las razones por las que se deben aplicar IPS e IDS son:

- Prevenir problemas de la red al disuadir a individuos hostiles.
- Detectar ataques y otras violaciones de la seguridad que no son prevenidas por otras medidas de protección.
- Detectar preámbulos de ataques (normalmente pruebas de red y otras actividades) [64].

Como se mencionó en el primer capítulo de este trabajo de titulación, un firewall puede ser implementado de tres maneras:

1. Virtuales (en software licenciado o software libre)
2. Como una parte de las aplicaciones de un equipo de red.
3. Hardware dedicado solo para ese propósito

La opción 2 que se menciona es recomendable solamente para empresas consideradas pequeñas, por lo que la propuesta que se hace en este trabajo es con base a un firewall por software, o un hardware dedicado para ese propósito, es decir las opciones 1 y 3.

4.2.1 PROPUESTA DE SOLUCIÓN CON SOFTWARE DE FIREWALL LICENCIADO O LIBRE

En la actualidad es una tendencia que las empresas comiencen a tener soluciones de red y seguridades híbridas, es decir, una parte física y otra virtual, con lo cual se gana disponibilidad de los servicios.

Esta opción sugiere utilizar un firewall, montado sobre una máquina virtual. Además de los equipos de conectividad necesarios se incorpora la protección de un antivirus. La siguiente figura 4.1 muestra una topología base para esta propuesta de solución.

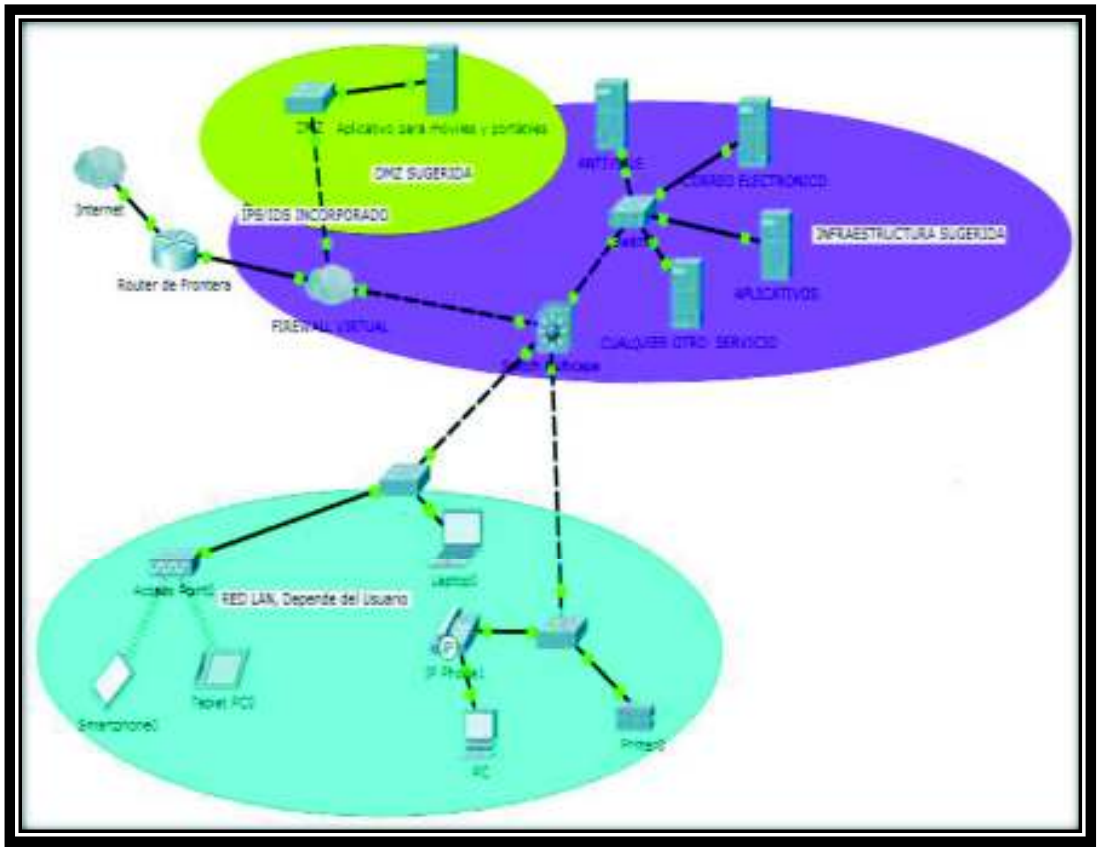


Figura 4.1 Esquema de solución con firewall virtual licenciado

Los equipos que se utilizan para esta solución de seguridad se los mencionará a continuación, no se pretende orientar a la compra de una u otra marca, como ejemplo se ha colocado algunos equipos que se ofertan en el mercado local:

Tabla 4.4 Equipos utilizados en la solución de seguridad

Router de frontera: Con capacidad de soportar enlaces de alta velocidad, podría ser un Cisco 800 Series o un Alcatel Lucent 7750 SR-e, por ejemplo. En los anexos se incluyen las especificaciones de estos equipos a manera de ejemplo.

Servidor de antivirus: Los requisitos del diseño de este servidor vienen dados por las características y necesidades del software de antivirus.
Switch multicapa: Recomendado que sea multicapa [65] para proveer grupos de trabajo separados por vlans y que se puedan direccionar paquetes de información [66] sin la necesidad de un router.
Máquina para instalar el software de firewall: Dependiendo del proveedor de la solución podría ser una máquina con características especiales o incluso puede ser una conexión a la nube donde radique el software.

Existen en el mercado algunos proveedores de seguridad con software de firewall que podrían cumplir con los parámetros mínimos sugeridos en la solución de seguridad, pero se debe hacer un análisis de las ventajas y desventajas de estas soluciones.

Esta información ha sido obtenida consultando varios sitios de internet, sin embargo, al no ser confiables en su totalidad y al no haber encontrado una fuente bibliográfica se ha cotizado esta información con expertos de seguridad de la Universidad San Francisco de Quito, donde mencionan lo siguiente:

Tabla 4.5 Ventajas y desventajas del firewall virtual

VENTAJAS	DESVENTAJAS
Gratis.	Las versiones gratis no disponen de soporte técnico dedicado.
Mayor disponibilidad de las soluciones que se ofertan en la nube.	Personal altamente capacitado para la configuración del software de firewall.
Menor inversión en infraestructura.	Límite en el uso de recursos, las soluciones virtuales a gran escala son muy costosas.
Constante incorporación en el mercado, nueva tendencia en seguridad.	
Software libre, se puede modificar a las necesidades del programador.	

El IDS que va a ser implementado en esta solución es gratuito y viene como una aplicación del sistema operativo de libre distribución LINUX.

Para mayor referencia se han consultado a algunas empresas que proveen este tipo de soluciones, y que pueden cumplir con los parámetros mínimos requeridos mostrados en las tablas 4.2 y 4.3.

Tabla 4.6 Algunas empresas proveedoras de firewall virtual

EMPRESA	ENLACES DE DESCRIPCIÓN DE LA SOLUCIÓN
IBM	http://www.ibm.com/cloud-computing/ec/es/platform/?S_PKG=&cm_mmc=Search_Google-_-Bluemix+Program_IBM+Cloud-_-ILA_AR-_-+firewall_Broad_&cm_mmca1=000006TS&cm_mmca2=10001882&mkwid=fcea3f7c-f14b-4625-af54-8e3504bbd3fc|937|18216
PFSENSE	https://www.pfsense.org/
FORCEPOINT	https://www.forcepoint.com/sites/default/files/resources/files/datasheet_forcepoint_ngfw_en.pdf
PANDA	http://www.pandasecurity.com/spain/enterprise/solutions/gatedefender-eSeries/GateDefender%20eSeries.htm

IBM. - provee un servicio de almacenamiento en la nube, con toda la información totalmente protegida, incluso los servicios se los ofrece desde la nube, la seguridad y el almacenaje se paga por dispositivo y tiempo de permanencia del contrato.

PFSENSE. - una de las soluciones más usadas a nivel mundial, se encuentran lanzando su nuevo producto orientado a la nube, donde las aplicaciones y la conectividad son controladas desde el internet, ayudándose del nuevo producto de Microsoft Azure, que pretende administrar todos los recursos de red, almacenamiento de información y acceso a servicios, todo mediante el acceso a una nube privada. Se plantea como un competidor directo de Cisco en seguridad, se promueve como una solución de tal manera, que se puede hacer la misma configuración de los ASA de Cisco.

FORCEPOINT. - software que provee gran versatilidad, puede ser implementado sobre un equipo dedicado o sobre una máquina virtual (KVM, VMware), se encuentra en crecimiento, en el cuadrante de Gartner se ubica entre los visionarios más prominentes, este software inspecciona todos los protocolos y las capas del modelo OSI[17], tiene motores dedicados a inspeccionar Anti-Botnet, de gran utilidad para las incidencias en Ecuador.

PANDA. – la solución en seguridad tiene el nombre de Gatedefender, cuya característica principal es la de filtrado de conexiones, mediante WIFI al contenido de la red. La gestión es centralizada y vía web, se puede implementar en versión de software, virtual o sobre un hardware dedicado.

4.2.2 PROPUESTA DE SOLUCIÓN CON HARDWARE DEDICADO DE FIREWALL

Al ser una solución dedicada a empresas de mediana escala, muchas de las cuales con proyección a ser clasificadas como grandes, se espera que la solución sea óptima, adaptable a las necesidades reales de la empresa. Por lo cual se plantea una solución de seguridad con un equipo dedicado netamente a proteger la red, haciendo de primera barrera ante los ataques externos.

Se propone una topología donde la primera barrera ante las amenazas externas sea el firewall dedicado, con características de IPS e IDS incorporadas. Luego el tráfico de red debe pasar por un análisis de un potente antivirus antes de llegar al usuario final como se muestra en la Figura 4.2.

[17] OSI, siglas en inglés, que representan al sistema de interconexión abierto.

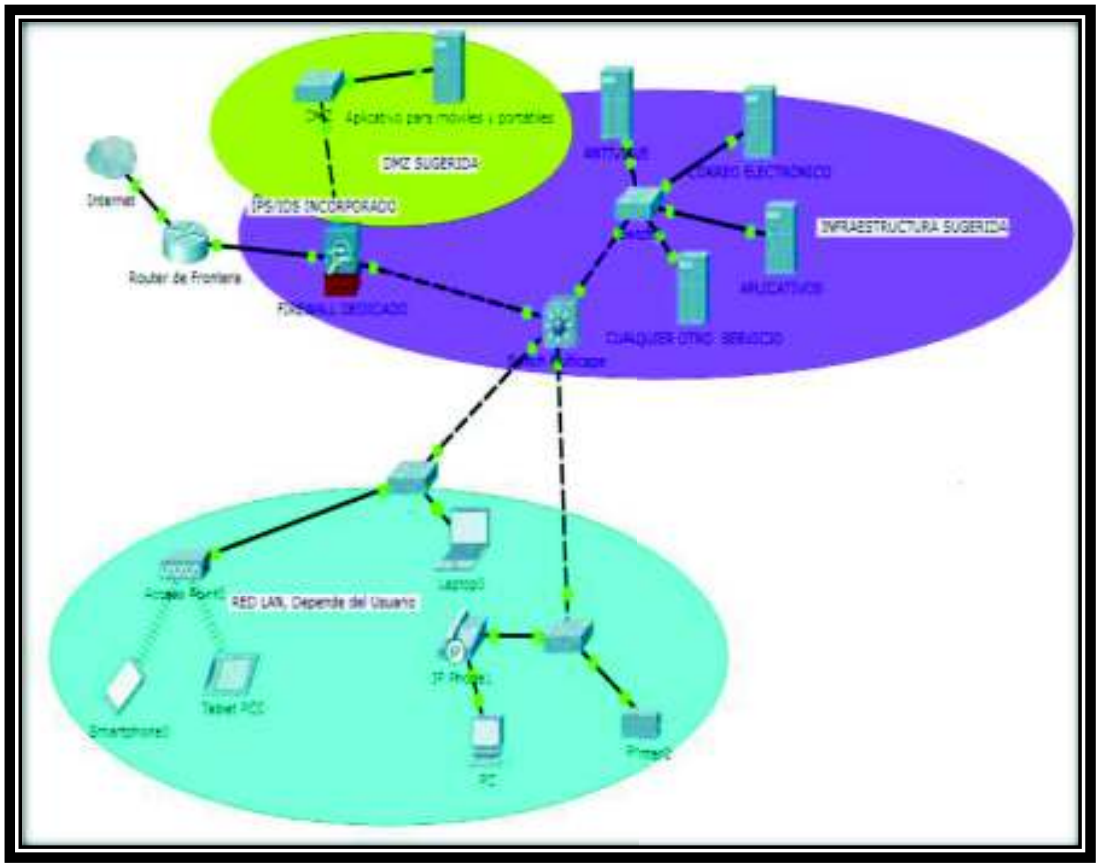


Figura 4.2 Esquema de solución propuesto

Al enfocarnos solamente en la prevención de amenazas externas a la intranet estamos hablando netamente del equipo firewall y del antivirus contratado. Las características que deben poseer estos equipos ya fueron establecidas.

Al momento de decidir implementar un proyecto de seguridad para una empresa de mediana escala se debería analizar la mejor opción de los equipos que nos propongan, teniendo presentes los requisitos mínimos de las tablas 4.2 y 4.3 que necesitamos para que nuestra red esté segura.

Tabla 4.7 Equipos utilizados en la solución de seguridad con hardware dedicado de firewall

Router de Frontera: Con capacidad de soportar enlaces de alta velocidad, podría ser un Cisco 800 Series o un Alcatel Lucent 7750 SR-e. Por ejemplo, en los anexos se incluyen las especificaciones de estos equipos de ejemplo.
Servidor de antivirus: Los requisitos del diseño de este servidor vienen dados por las características y necesidades del software de antivirus.

Switch Multicapa: Recomendado que sea multicapa para proveer grupos de trabajo separados por vlans y que se puedan direccionar paquetes de información sin la necesidad de un router.
Firewall dedicado: Debe ser un equipo que se acople a las necesidades de la empresa. Se sugiere que se utilice uno de los equipos que se considera de mejores prestaciones. Según el Cuadrante de Gartner analizado en capítulos anteriores, se podría escoger equipos de marca Cisco, Palo Alto, CheckPoint, Fortinet, etc., siempre y cuando el dinero no sea un limitante, se puede encontrar en el mercado otras soluciones en otras marcas no tan reconocidas.

Al igual que la solución anterior, las fuentes de internet no son todas confiables, por lo cual, para realizar un cuadro comparativo de ventajas y desventajas de la presente solución, se consultó con los expertos en seguridad perimetral de la Universidad San Francisco de Quito. (Msc. Jose Luis Medina e Ing. Galo Pérez).

Tabla 4.8 Pros y contras de la solución con hardware específico

VENTAJAS	DESVENTAJAS
Software y hardware dedicado a dar protección a la red.	Costo y mantenimiento de los equipos elevado, necesitan redundancia.
Mantenimiento periódico	Pago de licencias periódicas
Seguridad controlada por el administrador	Si el equipo se daña afecta al normal funcionamiento de la red
Firewalls de administración de amenazas unificado (UTM), con excelentes características	Cambio de equipos cada cierto tiempo, debido a que las amenazas cada vez evolucionan y se necesita mayor capacidad en los equipos de protección.

Se aconseja que los técnicos que van a implementar una determinada solución de seguridad con cualquiera de los equipos dedicados de firewall analicen si cumplen con los parámetros mínimos requeridos, y evalúen la parte económica.

También se debe considerar el monto de inversión en equipos el primer año, así como el pago de las licencias de utilización del software incorporado en el equipo, ya sea cada uno, tres o cinco años.

4.2.3 CONDICIONES DE APLICACIÓN DE LA SOLUCIÓN

Ante todo, las condiciones de aplicación de cualquiera de estas soluciones propuestas dependen del giro del negocio de la empresa de mediana escala, por lo cual se propone las siguientes opciones:

a. Se dispone de una infraestructura de red en la nube o mixta, es mejor escoger una solución de seguridad por software, dado que no se tiene control de los recursos del proveedor de estos servicios. Además, el factor económico pesa bastante, pero si se dispone de un técnico altamente capacitado en software libre se recomienda esta opción.

b. Se utiliza infraestructura con diversos sistemas operativos, como se pudo observar en la encuesta realizada, la mayoría de empresas de mediana escala utiliza infraestructura con diversos sistemas operativos. Aquí se recomienda una solución por hardware. Cuando la información a proteger es sumamente valiosa y el giro de negocio de la empresa depende netamente de estar conectados a la red externa, es imprescindible que se tenga equipos dedicados, con personal altamente capacitado, planes de contingencia para levantar el servicio lo más rápido posible, pero, ante todo, siempre tratar de prevenir intrusiones. Se recomienda altamente una solución con equipos dedicados, infraestructura propia y personal adecuado para su operación, el factor económico no es un obstáculo en esta solución.

Otro punto a analizar es la parte de costos y nuevas tendencias. Se debe evaluar si es rentable tener una infraestructura propia que dure algunos años, frente a alquilar una infraestructura de seguridad. Las nuevas tendencias son las tecnologías NFV[18] y SDN[19] que en el futuro podrían revolucionar la forma en que se administran y controlan las redes. Estas tecnologías están fuera del alcance de

---

[18] NFV, Network Function Virtualization es una iniciativa para virtualizar los servicios de red que ahora son realizados por hardware dedicado.

[19] SDN, Software Defined Networking es una manera de abordar la creación de redes donde el control se desprende del hardware y se le da a una aplicación de software llamada controlador.

estudio de este trabajo de titulación, pero es importante que se analice su función en un futuro.

4.2.4 PERSONAL TÉCNICO PARA ADMINISTRACIÓN DE LA SEGURIDAD

Si bien es cierto el presente trabajo es orientado a empresas que aún no cuentan con un departamento técnico especializado en las configuraciones de seguridad de red, es necesario conocer el perfil del talento humano que se encargará de administrar estas soluciones.

Se puede pensar en dos escenarios posibles que podrían ser factibles dependiendo del giro del negocio y de la seriedad con que se quiera manejar la seguridad perimetral de la empresa.

Una propuesta es preparar al personal de la empresa con conocimientos técnicos de seguridad y de manejo de redes, que además adquiera las herramientas para operar cualquier tipo de firewall, asimismo que sepa administrar un antivirus y que al mismo tiempo proponga políticas de seguridad para la empresa. Para quién este documento es de mucha ayuda.

La otra propuesta es contratar una empresa que ofrezca soluciones de seguridad y mantenimiento de la solución, que actué fuera de la empresa.

A continuación, una tabla que resume las ventajas y desventajas de ambas propuestas:

Tabla 4.9 Pros y contras del personal que va a operar la solución de seguridad

CAPACITAR A PERSONAL		**CONTRATAR UNA EMPRESA DEDICADA AL MANTENIMIENTO DE LA SEGURIDAD**	
Ventajas	**Desventajas**	**Ventajas**	**Desventajas**
Disponibilidad inmediata.	Capacitación continua de los técnicos de seguridad. Costos.	Mayor conocimiento y accionar ante amenazas.	La disponibilidad podría no ser inmediata.

Mantenimiento de equipos permanente.	Inversión en un equipo de trabajo.	Costo anual, inferior a tener personal propio de la empresa.	El usuario no sería exclusivo.
Minimizar riesgos de intrusos.	Rubro mensual en sueldos del personal de seguridad de red.		Programación de cualquier cambio en la seguridad con anticipación; depende de los términos del contrato.
Adopción de políticas personalizadas.	Contratar auditorías externas periódicas.		Servicio reactivo, es decir, cuando haya una emergencia entran en funcionamiento.
Cambios al instante.			
Técnico familiarizado con la estructura de la empresa.			
Tiempo de respuesta corto o inmediato.			

4.3 PROFORMAS DE SEGURIDAD OBTENIDAS

Se ha logrado conseguir proformas de algunos equipos, entre ellos equipos de marcas poco conocidas pero que tienen buenas prestaciones.

A continuación, las proformas obtenidas:

1.- Firewall ASA NGFW 5506

CLIENTE: *Juan Pablo Gallardo*
FECHA: *23 de diciembre de 2016*
DETALLE: *ASA*

ITEM	P/N	DESCRIPCIÓN	CANTIDAD	PRECIO Unitario	PRECIO TOTAL
Productos					
1	ASA5506-FPWR-BUN	ASA 5506-X with FirePOWER Svcs. Chassis and Subs. Bundle	1	$ -	$ -
	ASA5506-K9	ASA 5506-X with FirePOWER services, 8GE, AC, 3DES/AES	1	$ 1,679.06	$ 1,679.06
	CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	1	$ -	$ -
	SF-ASA-K-9.6-K8	ASA 9.6 Software Image for ASA 5506/5508/5516 series	1	$ -	$ -
	SF-ASA-FPS.4.1-K9	Cisco FirePOWER Software v5.4.1 for ASA 5500-X	1	$ -	$ -
	ASA5506-CTRL-LIC	Cisco ASA5506 Control License	1	$ -	$ -
	ASA5506-SSD	ASA 5506-X SSD	1	$ -	$ -
	ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	1	$ -	$ -
	ASA5506-PWR-AC	ASA 5506-X Power Adaptor	1	$ -	$ -
	L-ASA5506-TAC=	Cisco ASA5506 FirePOWER IPS and URL Licenses	1	$ -	$ -
	L-ASA5506-TAC-1Y	Cisco ASA5506 FirePOWER IPS and URL 1YR Subs	1	$ 590.63	$ 590.63
				SUBTOTAL:	$ 2,269.69

Figura 4.3 Proforma de Firewall ASA 5506

Detalle de la propuesta:

Tabla 4.10 Detalle de la propuesta de seguridad en base a proforma.

Requerido	Propuesta
Licenciamiento para 300 dispositivos	✓
IPS-IDS	✓
Soporte VPN	✓
Actualizaciones periódicas	✓
Soporte DMZ	✗
Antivirus incorporado	✓
Baja latencia	✓
Compatibilidad con cualquier sistema operativo en el dispositivo final. OS X, Windows, Linux, Android, etc.	✓

Soporte IPv6	✓
2 puertos Uplink de 1G o 10G	✓

Esta es una solución que cumple con la gran mayoría de requisitos para un óptimo sistema de seguridad. La licencia es anual, es decir que cada año se debe pagar $590.63 dólares. El resto de costos solo se paga el primer año.

2.- Firewall ASA NGFW 5506H

Date: 21-Dec-2016 **Estimate ID:** MS60842561VS
Deal ID: NA

All prices are shown in USD

Part Number	Description	Service Duration (Months)	Lead Time	Unit List Price	Qty	Unit Net Price	Extended Net Price
ASA5506H-FPWR-BUN	ASA 5506H Firepower Threat Defense	—	N/A	0.00	1	0.00	0.00
ASA5506H-SP-BUN-K9	ASA 5506H-X SEC PLUS Bundle	—	42	2,995.00	1	2,995.00	2,995.00
CAB-AC2	AC Power cord North America	—	14	0.00	1	0.00	0.00
SF-ASA-K-9.6-K8	ASA 9.6 Software image for ASA	—	14	0.00	1	0.00	0.00
SF-ASA-FP5.4.1-K9	Cisco FirePOWER Software v5.4.1 for	—	14	0.00	1	0.00	0.00
ASA5506H-CTRL-LIC	Cisco ASA5506H-X Control License	—	14	0.00	1	0.00	0.00
ASA5506H-SSD	ASA 5506H-X SSD	—	14	0.00	1	0.00	0.00
ASA5506H-SEC-PL	ASA 5506H-X Sec. Plus License	—	2	0.00	1	0.00	0.00
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License	—	14	0.00	1	0.00	0.00
ASA5506H-PWR-AC	ASA 5506H-X Power Adaptor	—	14	0.00	1	0.00	0.00
L-ASA5506H-TAMC=	Cisco ASA5506H-X FirePOWER IPS,	—	2	0.00	1	0.00	0.00
FS-VMW-2-SW-K9	Cisco Firepower Management	—	2	500.00	1	500.00	500.00
CON-SNT-ASA5506H	SNTC-8X5XNBD ASA 5506H-X SEC	12	N/A	493.63	1	493.63	493.63
CON-SAU-VMWSW2	SW APP SUPP + UPGR Cisco	12	N/A	100.00	1	100.00	100.00
L-ASA5506H-TAMC-3Y	Cisco ASA5506H-X IPS, AMP, URL	36	N/A	4,313.00	1	4,313.00	4,313.00

Valid through:
FOB Point: None

Product Total	3,495.00
Service Total :	593.63
Subscription Total	4,313.00
Total Price:	8,401.63

Figura 4.4 Proforma de firewall ASA 5506H

Detalle de la propuesta:

Tabla 4.11 Detalle de la propuesta de seguridad en base a proforma.

Requerido	Propuesta
Licenciamiento para 300 dispositivos	✓
IPS-IDS	✓
Soporte VPN	✓
Actualizaciones periódicas	✓
Soporte DMZ	✓
Antivirus incorporado	✓

Baja latencia	✓
Compatibilidad con cualquier sistema operativo en el dispositivo final. OS X, Windows, Linux, Android, etc.	✓
Soporte IPv6	✓
2 puertos Uplink de 1G o 10G	✓

Esta propuesta de seguridad tiene un costo total inicial de $8401,63. Cada año se debe renovar el soporte técnico del equipo, que tiene un costo de $493,63 y cada 3 años se debe renovar la licencia del módulo AMP[20], IPS, y el filtrado por aplicación URL que tiene un costo de $4313.

3.- Firewall UTM Cyberoam CR200iNG

El costo de este equipo incluye la instalación, configuración y adiestramiento de 2 técnicos locales de la empresa, es un firewall de nueva generación UTM que viene incluido la licencia de operación para 3 años, como se muestra en la siguiente figura 4.5.

Descripción	Cantidad	Valor Unitario	Valor Total
Venta, instalación y configuración de: -Hardware: UTM marca Cyberoam modelo CR200iNG -Software: licencia de Total Value Suscription, valida por **36 meses** contados a partir de la fecha de su instalación. Incluye: Web and Aplication Filter, Intrusion Prevention System, Gateway Antivirus, Gateway Anti-Spam. -Soporte 8x5 para el hardware y software (no incluye las configuraciones) via e-mail o chat -Instalación y configuración del equipo en las instalaciones de su empresa en la ciudad de Quito -Capacitación para 2 personas de la empresa, durante el proceso de instalación y configuración.	1	9.730,00	9.730,00
		Subtotal	9.730,00
		12% del IVA	1.167,60
		Total	10.897,60

Figura 4.5 Firewall UTM Cyberoam

[20] AMP, de sus siglas en inglés: Anti-Malware-Protection, que significa protección ante software malicioso.

Detalle de la propuesta:

Tabla 4.12 Detalle de la propuesta de seguridad en base a proforma.

Requerido	Propuesta
Licenciamiento para 300 dispositivos	✓
IPS-IDS	✓
Soporte VPN	✓
Actualizaciones periódicas	✓
Soporte DMZ	✓
Antivirus incorporado	✓
Baja latencia	✓
Compatibilidad con cualquier sistema operativo en el dispositivo final. OS X, Windows, Linux, Android, etc.	✓
Soporte IPv6	✓
2 puertos Uplink de 1G o 10G	✓

4.4 COSTO INICIAL REFERENCIAL DE UNA SOLUCIÓN DE SEGURIDAD, INCLUIDOS LOS EQUIPOS DE CONECTIVIDAD.

Se consiguió algunas cotizaciones para una solución de seguridad. Sospechando que se necesitarán incluso los equipos de conectividad, se solicitó la proforma de equipos para una empresa donde se conecten 300 dispositivos a la red.

Un proveedor manifiesta que la marca que más se vende para soluciones empresariales es CISCO, pero se ha recibido cotizaciones en otras marcas también. Dependiendo de las necesidades de la empresa se puede incluso mezclar marcas de equipos, ya que la operación de interconectividad está regulada por organismos internacionales de estandarización.

Se plantean los siguientes equipos:

Tabla 4.13 Equipos para solución inicial de seguridad

EQUIPO	CANTIDAD
Switch de core	1
Router de frontera	1
Firewall	1
Switch de acceso	5x 48Puertos + 4x24Puerto

Proforma 1:

Price Estimate

Ing. Pablo Rojas

TELCO DYNAMICS CIA LTDA
AV ZOILO RODRIGUEZ ENTRE VIRGILIO A,0
LOJA, 0-0

ECUADOR

Ph no:+593 593987842700

TELCO DYNAMICS

LOJA,LOJA-
ECUADOR

Ph no:+593 593987842700

Price Estimate for planning and information purposes only and is not a binding offer from Cisco.

Date: 17-Mar-2017

Estimate ID: CB70345119UK

Deal ID: NA

All prices are shown in USD

Part Number	Description	Service Duration (Months)	Lead Time	Unit List Price	Qty	Unit Net Price	Disc(%)	Extended Net Price	Equipo
WS-C4506-E	Cat4500 E-Series 6-Slot Chassis, fan, no ps	---	14	4,995.00	1	4,995.00	0.00	4,995.00	SW de core
CON-SNT-C4506E	SNTC-8X5XNBD Cat4500 E-Series 6-Slot Chassis, fan, no	12	N/A	2,667.50	1	2,667.50	0.00	2,667.50	
S45EU-S8-38E	CAT4500e SUP8e Universal Image	---	14	0.00	1	0.00	0.00	0.00	
C4K-SLOT-CVR-E	Catalyst 4500 E-Series Family Slot Cover	---	14	0.00	4	0.00	0.00	0.00	
C4500E-IPB	Paper IP Base License	---	14	0.00	1	0.00	0.00	0.00	
WS-X45-SUP8-E	Catalyst 4500 E-Series Supervisor 8-E	---	21	19,995.00	1	19,995.00	0.00	19,995.00	
WS-X4712-SFP+E	Catalyst 4500 E-Series 12-Port 10GbE (SFP+)	---	14	26,995.00	1	26,995.00	0.00	26,995.00	
PWR-C45-1400AC	Catalyst 4500 1400W AC Power Supply (Data Only)	---	14	1,495.00	1	1,495.00	0.00	1,495.00	
CAB-US520-C19-US	NEMA 5-20 to IEC-C19 14ft US	---	14	0.00	2	0.00	0.00	0.00	
PWR-C45-1400AC/2	Catalyst 4500 1400W AC Power Supply Redundant(Data Only)	---	14	1,495.00	1	1,495.00	0.00	1,495.00	

C2911-AX/K9	Cisco 2911 AX Bundle w/ AppSEC Lic.	---	14	4,945.00	1	4,945.00	0.00	4,945.00	Router de Frontera
CON-SSSNT-C2911AX9	SOLN SUPP 8X5XNBD Cisco 2911 AX Bundle w/ AppSEC Lic.	12	N/A	994.13	1	994.13	0.00	994.13	
MEM-2900-512U2.5GB	512MB to 2.5GB DRAM Upgrade (2GB+512MB) for Cisco 2901-2921	---	14	0.00	1	0.00	0.00	0.00	
FL-C2911-WAASX	WAASX Feature License RTU (Paper) for 2911	---	14	0.00	1	0.00	0.00	0.00	
PWR-2911-AC	Cisco 2911 AC Power Supply	---	14	0.00	1	0.00	0.00	0.00	
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	---	14	0.00	1	0.00	0.00	0.00	
HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR	---	14	0.00	4	0.00	0.00	0.00	
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	---	21	0.00	1	0.00	0.00	0.00	
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR	---	14	0.00	1	0.00	0.00	0.00	
SL-29-IPB-K9	IP Base License for Cisco 2901-2951	---	14	0.00	1	0.00	0.00	0.00	
SL-29-SEC-K9	Security License for Cisco 2901-2951	---	14	0.00	1	0.00	0.00	0.00	
SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	---	14	0.00	1	0.00	0.00	0.00	
WAAS-RTU-1300	WAAS and VWAAS Right to Use for 1300 connections	---	14	0.00	1	0.00	0.00	0.00	
CON-ECMUS-WS1300	SOLN SUPP SWSS WAAS and VWAAS Right to Use for 1300 con	12	N/A	73.60	1	73.60	0.00	73.60	
SL-29-DATA-APP-K9	DATA features for 2900 series APP license	---	14	0.00	1	0.00	0.00	0.00	
SL-1300-WAAS/K9	WAAS and/or vWAAS 1300 TCP Connection RTU on a single router	---	14	0.00	1	0.00	0.00	0.00	
S29UK9-15403M	Cisco 2901-2921 IOS UNIVERSAL	---	14	0.00	1	0.00	0.00	0.00	
SL-29-APP-K9	AppX License with: DATA and WAAS for Cisco 2900 Series	---	14	0.00	1	0.00	0.00	0.00	
ASA5506-K9	ASA 5506-X with FirePOWER services, 8GE, AC, 3DES/AES	---	14	995.00	1	995.00	0.00	995.00	Firewall ASA
CON-SNT-ASA5506K	SNTC-8X5XNBD ASA 5506-X with FirePOWER services, 8GE,	12	N/A	163.63	1	163.63	0.00	163.63	
CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m	---	14	0.00	1	0.00	0.00	0.00	
SF-ASA-K-9.6-K8	ASA 9.6 Software image for ASA 5506/5508/5516 series	---	14	0.00	1	0.00	0.00	0.00	
SF-ASA-FP5.4.1-K9	Cisco FirePOWER Software v5.4.1 for ASA 5500-X	---	14	0.00	1	0.00	0.00	0.00	
ASA5506-CTRL-LIC	Cisco ASA5506 Control License	---	14	0.00	1	0.00	0.00	0.00	
AC-VPNO-50	Cisco AnyConnect VPN Only, 50 Simultaneous, ASA Opt (Paper)	---	14	6,995.00	1	6,995.00	0.00	6,995.00	
CON-ECMU-ACVA50	SWSS UPGRADES Cisco AnyConnect VPN Only, 50 Simultaneous, AS	12	N/A	1,608.85	1	1,608.85	0.00	1,608.85	
ASA5506-SSD	ASA 5506-X SSD	---	14	0.00	1	0.00	0.00	0.00	
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	---	14	0.00	1	0.00	0.00	0.00	
ASA5506-PWR-AC	ASA 5506-X Power Adaptor	---	14	0.00	1	0.00	0.00	0.00	
WS-C2960X-48FPD-L	Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base	---	14	7,995.00	5	7,995.00	0.00	39,975.00	5 Switch de 48 puertos POE con uplinks de 10Gb
CON-SNT-WSC296XL	SNTC-8X5XNBD Catalyst 2960-X 48 GigE PoE 740W, 2 x 10	12	N/A	693.00	5	693.00	0.00	3,465.00	
PWR-CLP	Power Retainer Clip For 3560-C, 2960-C and 2960-L Switches	---	14	0.00	5	0.00	0.00	0.00	
CAB-16AWG-AC	AC Power cord, 16AWG	---	28	0.00	5	0.00	0.00	0.00	
C2960X-STACK	Catalyst 2960-X FlexStack Plus Stacking Module	---	21	1,195.00	5	1,195.00	0.00	5,975.00	
CAB-STK-E-0.5M	Cisco FlexStack 50cm stacking cable	---	14	0.00	5	0.00	0.00	0.00	
WS-C2960X-24PD-L	Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base	---	14	4,595.00	4	4,595.00	0.00	18,380.00	4 Switch de 24 puertos POE con uplinks de 10Gb
CON-SNT-WSC604DL	SNTC-8X5XNBD Catalyst 2960-X 24 G	12	N/A	397.38	4	397.38	0.00	1,589.52	
PWR-CLP	Power Retainer Clip For 3560-C, 2960-C and 2960-L Switches	---	14	0.00	4	0.00	0.00	0.00	
CAB-16AWG-AC	AC Power cord, 16AWG	---	28	0.00	4	0.00	0.00	0.00	

Valid through:

FOB Point: None

Notes

Product Total	132,240.00
Service Total :	10,562.23
Subscription Total	0.00
Total Price:	**142,802.23**

Signed:

Fernando Losiza

Figura 4.6 Proforma #1 de equipos de conectividad y seguridad

Se puede apreciar que una solución con equipos reconocidos y garantizados es costosa de implementar. Al menos la inversión inicial es bastante fuerte. Para este caso se tiene una inversión de $142.802,23, que es un valor significativo para cualquier empresa.

Esta proforma cubre el licenciamiento de los equipos por el primer año. La inversión para los años posteriores en seguridad solo será el mantenimiento y licenciamiento

de las características de protección y operación de los equipos.

Proforma 2:

SOLINFRA

PF17- 456 V1
RUC: 1791991591001

Solinfra Cia. Ltda. Quito (Matriz)
(593) 2294 7190/
De los Motivos E15-268 y Julio Arellano Sector Monteserín
info@solinfra.com

Solinfra Cia. Ltda. Guayaquil (Sucursal)
(593) 997 652 698 / (593) 991 304 515
Ciudadela Sauces 8, Mz 454, F6V6

OFERTA COMERCIAL

Empresa: GALLARDO CORP
Contacto: Juan Pablo Gallardo
Dirección: De los Guayacamayos
Proyecto: Seguridad mínima hacia la INTRANET

Fecha: 11/02/2017
Ciudad: QUITO
Teléfono: 998915741
Email: [illegible]

Cant	Unidad	Código	Disponibad	Descripción	Costo unitario	Costo Total
Item 1.1 - Equipos						
1	Unidad		30 DIAS	Detalle General Equipo	$ 57,308.25	$ 57,308.25
1				MARCA: HPE ARUBA Switch de Core 2930F 24G 4SFP+ 24XTX4 Licenciamiento por 3 años		$ 5,371.50
5				Switch de acceso 2540 48G 4SFP+ 24XTX4 Licenciamiento por 3 años		$ 20,783.75
4				Switch de acceso 2540 24G 4SFP+ 24XTX4 Licenciamiento por 3 años		$ 14,815.50
1				Transceivers 10GB		$ 775.00
1				MARCA: MICROTIK ROUTER MICROTIK ROUTER DE FRONTERA		$ 312.50
1				MARCA: FORTINET		$ 15,250.00
Item 2.2 - Servicios profesionales de implementación						
1	Unidad			Alcance de implementación: MONTAJE DE EQUIPOS EN RACK CONFIGURACIÓN Y PRUEBAS DE FUNCIONAMIENTO Horario Normal: L-V 8h30 a 17h30 Horario Extendido: L-V pasadas las 17h30 Horario Fin de Semana: Sábados, Domingos y Feriados	$ 1,500.00	$ 1,500.00

OBSERVACIONES:

TOTAL GENERAL SIN IVA: $ 58,808.25

CONDICIONES COMERCIALES

Figura 4.7 Proforma #2 de equipos de conectividad y seguridad

Esta propuesta de seguridad incluye equipos de conectividad de la marca HP y un firewall Fortinet, se aprecia que, al comparar con la propuesta anterior, los costos bajan considerablemente, además esta propuesta ya contempla el licenciamiento para 3 años, el costo total es de $58.808,25.

Proforma 3.

Esta proforma contempla por separado los equipos de comunicación y seguridad, pero pertenecen a un mismo proveedor, cabe mencionar que al no disponer de conmutadores de 48 puertos nos han cotizado 15 conmutadores de 24 puertos y un enrutador de borde.

Como podemos apreciar en esta propuesta, los costos son mucho más bajos inclusive, con equipos de buenas prestaciones, pero con marcas no tan conocidas en el mercado local, esta solución tiene un costo total de $13.764,8, lo cual está dentro de las posibilidades económicas de una empresa de mediana escala en proceso de crecimiento, ya que registran ingresos anuales entre $1.000.000 y $10.000.000 [67]; pero, si las limitantes no son el dinero se puede escoger cualquiera de las propuestas anteriores. La licencia del firewall está considerada para un año en esta propuesta.

ALTALA®
THE NETWORK COMPANY

Quito, lunes, 4 de diciembre de 2017

ALTALA S.A.

Av. de los Shyris N39-281 y Gaspar de Villarroel Centro de Negocios La Galeria Of. 28
02 2 439 183

Cliente: **USFQ**
Dirección:
Teléfono 0998919741
Contacto JUAN PABLO GALLARDO

Cotización Número: 37

Disponibilidad: Inmediata / Entrega: Inmediata

Forma de Pago: Contado

Aceptamos Todas las Tarjetas de Crédito

Todos Nuestros Productos Cuentan con 1 año de Garantía contra defectos de fábrica

PART NUMBER	DESCRIPTION	Quantity	UNIT NET PRICE	DISC(%)	IVA	EXTEND NET PRICE
CRS326-24G-2S+RM	CLOUD ROUTER SWITCH 326	15,00	249,00	0.00	12%	4183,2
CCR1009-8G-1S-1S+	CLOUD CORE ROUTER 1009	1,00	575,00	0.00	12%	644,00

Figura 4.8 Proforma #3, equipos de comunicación

ESPECIALISTAS EN
SEGURIDADES INFORMÁTICAS

SCProgress

Quito, 24 de noviembre del 2017

Señor:
Ing. Juan Pablo Gallardo
Presente

De mis consideraciones:

Por la presente ponemos a su consideración nuestra oferta para la venta, instalación y configuración de un equipo de seguridad perimetral UTM, marca Cyberoam modelo CR200iNG, para su distinguida empresa.

Vale recalcar, que Servicios Computacionales Progress son representantes en el Ecuador del fabricante desde hace varios años. Tenemos equipos de diferentes modelos, incluido los de 1500iNG y 2500iNG, instalados y funcionando en diferentes instituciones a nivel nacional.

Nuestros técnicos recibieron capacitación directa del fabricante.

Nuestra oferta incluye:

OPCIÓN 1:

Descripción	Cantidad	Valor Unitario	Valor Total
Venta, instalación y configuración de: -Hardware: UTM marca Cyberoam modelo CR200iNG -Software: licencia de Total Value Suscription, valida por **12 meses** contados a partir de la fecha de su instalación. Incluye: Web and Aplication Filter, Intrusion Prevention System, Gateway Antivirus, Gateway Anti-Spam. -Soporte 8x5 para el hardware y software (no incluye las configuraciones) vía e-mail o chat -Instalación y configuración del equipo en las instalaciones de su empresa en la ciudad de Quito -Capacitación para 2 personas de la empresa, durante el proceso de instalación y configuración.	1	7.980,00	7.980,00
		Subtotal	7.980,00
		12% del IVA	957,60
		Total	8.937,60

Figura 4.9 Proforma #3, equipo de seguridad

4.5 GENERALIDADES DEL PLAN DE CONTINGENCIA

¨El plan de contingencia engloba todas las medidas necesarias para recuperar los servicios de un sistema de información tras una emergencia¨ [68]. Principalmente amenazas externas de infección, robo, alteración o daño de archivos esenciales para el giro de negocio de la empresa de mediana escala.

Pero además de virus se tienen otros factores que podrían hacer colapsar la red, tales como:

- Fuego
- Robo de equipos
- Falla en los equipos
- Error de configuración
- Vandalismo

La planificación de un plan de contingencia se agrupa en 4 etapas [68]:

1. Planificación de la contingencia. - identificar cuáles son los servicios indispensables o críticos para que la empresa vuelva a su normal operación una vez superada la interrupción. Esta es una fase de prevención, donde se toman en cuenta las medidas a tomarse antes que ocurra un incidente, entre algunas de las características de esta fase está, prever un sistema de respaldo de energía, respaldo de datos, tener protecciones adicionales para los servicios críticos de la empresa, de ser posible apartados del sitio de operación.

2. Implementación de las medidas de contingencia. - en esta fase se instauran las medidas de contingencia antes que ocurra una emergencia.

3. Ejecución de la preparación de la emergencia. - va conjuntamente con la fase anterior, este es un escenario de prueba donde se realiza un simulacro en el cual se deba seguir las medidas especificadas en el plan de contingencia.

4. Implementación de las medidas planificadas tras una situación de emergencia. – esta es la fase donde sin demora deben implementarse las medidas planificadas ante una emergencia declarada.

Estas cuatro etapas de la planificación de un plan de contingencia están resumidas en la figura 4.10.

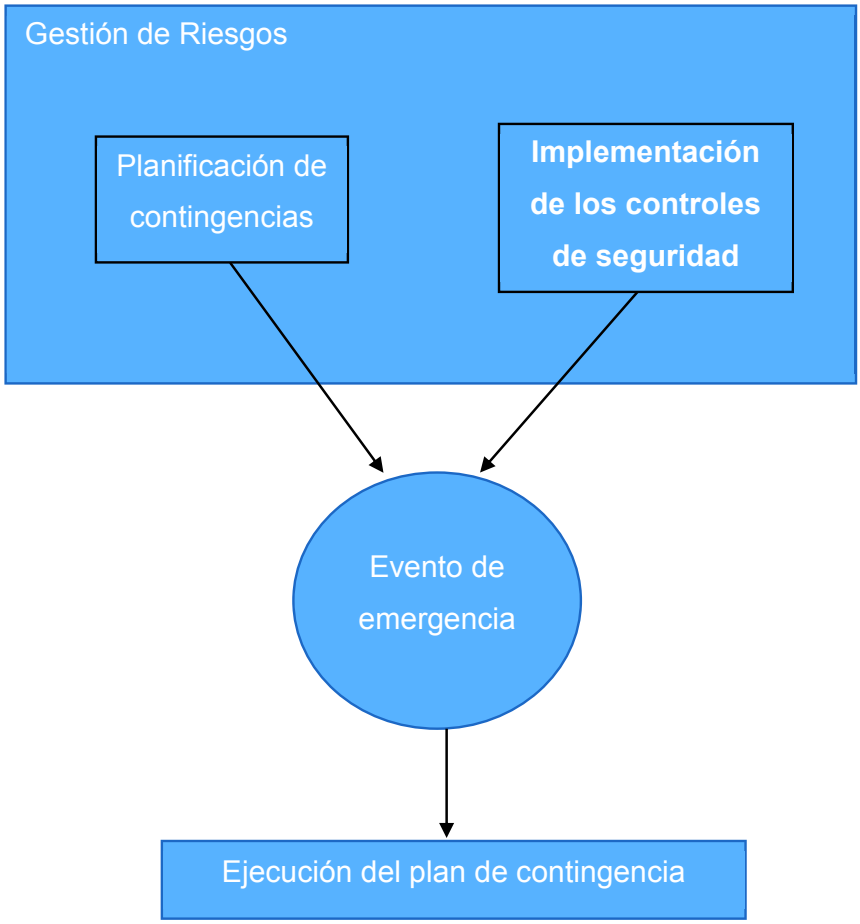


Figura 4.10 Interacción entre las fases de planificación de un plan de contingencia [68]

Una vez que se ha implementado el plan de contingencia se debe hacer un mantenimiento periódico de la solución, así como simulacros constantes. Esto a fin de asegurarse que la funcionalidad de la empresa se pueda recuperar en el menor tiempo posible con un costo razonable en caso de existir un ataque que afecte al normal funcionamiento de la red empresarial [69].

4.5.1 PLAN DE CONTINGENCIA ANTE ATAQUES DE RED POR UNA AMENAZA EXTERNA PARA UNA EMPRESA DE MEDIANA ESCALA.

La Secretaria Nacional de la Administración Pública del estado ecuatoriano, ha creado directrices para la seguridad de la información [70]; sin embargo, no se tiene un plan en respuesta a incidentes de ataques informáticos.

Las acciones a seguir del plan se mencionan a continuación [71]:

1. Continuidad del negocio. – asegurar las funciones comerciales de la empresa durante y después de la interrupción.
2. Recuperación del negocio. – restauración de los procesos luego de la interrupción.
3. Continuidad de operaciones. – restauración de procesos críticos en un lugar alterno, hasta 30 días antes de retomar las operaciones normales.
4. Comunicaciones ante crisis. – la información hacia el público será llevada por personas autorizadas a comunicar una versión oficial sobre los hechos acontecidos.
5. Respuesta ante ciber incidentes. – el personal de seguridades de la institución debe identificar, mitigar y restablecer los sistemas informáticos frente a intrusos ilegales, caídas de servicios o fallos en la infraestructura tecnológica. Se debe determinar cuántos dispositivos fueron infectados y los que podrían infectarse por estar conectados a un equipo bajo amenaza de seguridad; si más equipos en la red pueden ser afectados se debe incluso desconectar estos dispositivos hasta que la amenaza sea controlada. Identificar la ventana de intrusión y reportar la amenaza al proveedor de seguridad para reportar el ataque, con lo cual ellos pueden generar parches de seguridad en corto plazo.
6. Emergencia ocupacional. – procedimientos que deben seguir los ocupantes frente a una emergencia de amenaza interna o externa.

5 CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

- ✓ Se ha descrito las amenazas más comunes de red que existen, y que se han obtenido mediante una encuesta realizada a administradores de red de diferentes empresas de mediana escala, asimismo se ha investigado la forma de mitigarlas, concluyendo que es necesario la implementación de una solución de seguridad integral, con un antivirus ayudado de un firewall.

- ✓ Mediante la encuesta realizada en el presente trabajo de titulación se concluye que: el 38,5% de las empresas encuestadas tuvieron ataques de red en el último año, el 67,9% de estas empresas pudo recuperarse en un tiempo menor a 24horas, y la infraestructura que se usa en su mayoría es una combinación entre equipos Windows y Linux. Por lo que se concluye que no se puede garantizar la seguridad de una empresa al cien por ciento.

- ✓ De la encuesta realizada y de las referencias bibliográficas se concluye que los equipos que actualmente se usan para proteger la red son firewalls y antivirus. Las marcas más usadas en equipos firewall son CISCO, Fortinet y Checkpoint, mientras que los antivirus empresariales más conocidos son Kaspersky, Eset y McAfee en Ecuador.

- ✓ En base a los requerimientos mínimos de seguridad se propuso dos escenarios, una opción con software libre que podría funcionar bajo ciertos parámetros y una opción con equipos dedicados a brindar seguridad perimetral pero que son licenciados y con un costo representativo para las empresas de mediana escala. Por otro lado, la opción con software libre podría ser muy factible y tener buenas prestaciones para la mediana empresa, siempre que se tenga el personal capacitado que pueda manejar la herramienta de seguridad y que pueda dar soporte cuando el caso lo amerite.

- ✓ Más de la mitad de las empresas de mediana escala no cuentan con un plan de contingencia, y su inversión en seguridad está entre los $10.000 y $50.000 dólares, dependiendo del giro del negocio. Al mismo tiempo muchas de las decisiones en cuanto al plan de respaldo de información para su posterior recuperación en el caso de un ataque, dependen del giro de negocio y de la capacidad económica que se tenga, ya que sí se opta por tener un lugar alejado al sitio de operaciones y disponer ahí de equipos de respaldo de información y servicios, el costo sería bastante elevado, mientras que si se opta por almacenar servicios e información como respaldo en la nube podría ser más conveniente.

- ✓ Es un gran reto planear la protección para lo que se viene: el internet de las cosas, BYOD, todo en la nube. Para lo cual se debe tener una muy buena estrategia y mecanismos de protección para implementar estas tecnologías sin riesgos al usuario final. Esto es lo que se concluye cuando se analizan las nuevas tendencias en seguridad de red enfocadas a amenazas externas a la intranet.

- ✓ Personalmente recomiendo que las empresas inviertan más recursos en capacitar a su personal de TI, al mismo tiempo que se realicen campañas de información en temas de seguridad a los usuarios finales, con esto se crea una cultura de protección ante amenazas en las empresas de mediana escala.

REFERENCIAS BIBLIOGRÁFICAS

[1] Cisco, "Guia de soluciones para la mediana empresa", Marzo 2014. [En línea]. Disponible en: https://www.cisco.com/c/dam/en_us/solutions/midsize/docs/midsize_partner_es.pdf. [Último acceso: 10 Febrero 2017].

[2] R. Correa, "Reglamento a la estructura e institucionalidad de desarrollo productivo, de l ainversión y de los mecanismos e instrumentosde fomento productivo, establecidos en el código orgánico de la producción, comercio e inversiones", Noviembre 2013. [En línea]. Disponible en: http://www.industrias.gob.ec/wp-content/uploads/downloads/2013/10/decreto-757.pdf. [Último acceso: 6 Mayo 2016].

[3] Cisco, "Rethinking the network as a security sensor and enforcer", Octubre 2015.[En línea]. Disponible en: https://www.cisco.com/c/dam/m/en_us/solutions/enterprise-networks/offers/en-01/assets/files/IDC-Security-Whitepaper.pdf?eid=txenNB01_5100013&oid=wpenNB01_5100005. [Último acceso: 11 Junio 2016].

[4] W. Stalling, "Cryptography and network security: principles ans practices", Boston: Prentice Hall, 2011.

[5] W. Stallings, "Comunicaciones y Redes de Computación", Septima Edición, Madrid: Prentice Hall, 2014, pp. 508-509.

[6] CONATEL, "LISTADO DE EQUIPOS HOMOLOGADOS EN LA CONATEL", 05 Octubre 2017. [En línea]. Disponible en: https://www.conatel.gov.py/images/iprincipal/RNST%202017/Lista%20de%20Equipos%20Homologados_05102017.pdf. [Último acceso: 25 Febrero 2018].

[7] "Microsoft Word - 6. Capítulo 2 - Familia IEEE 802.11.doc - f.+Capítulo+2+-+Familia+IEEE+802.11.pdf", [En línea]. Disponible en: http://bibing.us.es/proyectos/abreproy/11579/fichero/f.+Cap%C3%ADtulo+2+-+Familia+IEEE+802.11.pdf+. [Último acceso: 3 Mayo 2017].

[8] P. Rodríguez, "Los nuevos tipos de WiFi (AC, AD y HaLow): así conseguiremos 100 Gbps", [En línea]. Disponible en: https://www.xataka.com/ordenadores/los-nuevos-tipos-de-wifi-ac-ad-y-halow-asi-conseguiremos-100-gbps. [Último acceso: 4 Mayo 2017].

[9] CISCO, "Campus, Resumen de diseño", Abril 2014. [En línea]. Disponible en: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf. [Último acceso: 07 Marzo 2018].

[10] El Taller del BIT , "Redes Jerárquicas" [En línea]. Disponible en: http://eltallerdelbit.com/redes-jerarquicas. [Último acceso: 5 Mayo 2017].

[11] "Router Cisco 1861, Integrated Services, Licencia SRST 8 Usuarios, 4 FXS, 4 FXO, 8 POE, SP, SVCS, 1 HWIC slot para WAN | intercompras", [En línea]. Disponible en: https://intercompras.com/p/router-cisco-servicios-integrados-usuarios-srst-4fxs-4fxo-8poe-sp-svcs-47484. [Último acceso: 5 Mayo 2017].

[12] Cisco Systems, Inc, "Lo que usted necesita saber de routers y switches. Conceptos generales", 2012. [En línea]. Disponible en: https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf. [Último acceso: 3 Enero 2017].

[13] “Switch DGS-1500 SmartPro Administrable, 48 puertos Gigabit y 4 puertos 100 / 1000Base-X SFP DGS-1500-52”, [En línea]. Disponible en: http://www.ds3comunicaciones.com/dlink/DGS-1500-52.html. [Último acceso: 6 Mayo 2017].

[14] Cisco, “Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet”, 17 Mayo 2018. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html.

[15] M. Naranjo y D. Silva, “Propuesta para el rediseño de la red de datos corporativa del gobierno autónomo descentralizado de la Provincia de Bolívar-Prefectura, ubicado en la ciudad de Guaranda”, Universidad Politécnica Salesiana Sede Quito, Quito, 2017.

[16] Cisco, “Cisco Nexus 7000 Series Switches Data Sheet”, 6 Marzo 2018. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/Data_Sheet_C78-437762.html.

[17] Infortelecom, “Qué es un servidor y para qué sirve”, 29 Septiembre 2016. [En línea]. Disponible en: https://infortelecom.es/blog/que-es-un-servidor-y-para-que-sirve/. [Último acceso: 23 Octubre 2017].

[18] NFON, cloud telephone system, “Teléfono IP”, 2017. [En línea]. Disponible en: https://www.nfon.com/es/soluciones/recursos/glosario/telefono-ip/. [Último acceso: 3 Mayo 2017].

[19] Zerovoz, “Instalación de terminales IP-Zerovoz”, [En línea]. Disponible en: http://zerovoz.com/instalacion-de-terminales-ip/. [Último acceso: 8 Mayo 2017].

[20] Cisco, “Cisco Aironet 1700 Series Access Points - Cisco”, [En línea]. Disponible en: http://www.cisco.com/c/es_mx/products/wireless/aironet-1700-series-access-points/index.html. [Último acceso: 9 Mayo 2017].

[21] Gartner, “Magic Quadrant for Enterprise Network Firewalls.”, 10 Junio 2016. [En línea]. Disponible en: https://www.gartner.com/doc/reprints?id=1-3805JH8&ct=160525&st=sb. [Último acceso: 14 Julio 2016].

[22] “¿Qué es el Cuadrante Mágico de Gartner? - Big Data Social”, [En línea]. Disponible en: http://www.bigdata-social.com/informe-cuadrante-magico-gartner/. [Último acceso: 9 Mayo 2017].

[23] R. Castaño, “Cuadrante Mágico de Gartner”, 10 Octubre 2015. [En línea]. Disponible en: http://revista.helpdesktic.com/cuadrante-magico-de-gartner/.

[24] J. García, Y. Fernández, R. Martínez, Á. Ochoa y A. Ramos, "Hacking y seguridad en internet", Bogotá: Ediciones de la U, 2013, pp. 371-373.

[25] osiseguridad, “Comprueba si el cortafuegos está activado en tu equipo | Oficina de Seguridad del Internauta”, [En línea]. Disponible en: https://www.osi.es/es/actualidad/blog/2014/04/04/comprueba-si-el-cortafuegos-esta-activado-en-tu-equipo. [Último acceso: 11 Mayo 2016].

[26] Palo Alto Networks, Inc, “WHAT IS AN INTRUSION PREVENTION SYSTEM?”, 2017. [En línea]. Disponible en: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips. [Último acceso: 5 Febrero 2017].

[27] TP-Link, “¿Qué es DMZ?”, 29 11 2011. [En línea]. Disponible en: http://www.tp-link.es/FAQ-28.html. [Último acceso: 1 Marzo 2017].

[28] H. Mancheno y I. Robles, "Vulnerabilidades y seguridad en redes TCP/IP", Guayaquil, 2013.

[29] L. Andersson y T. Madsen, “Provider Provisioned Virtual Private Network (VPN) Terminology,” The Internet Society, 2005.

[30] 3 digits, “Antimalware-Antivirus”, 2017. [En línea]. Disponible en: http://www.3digits.es/sistemas/Antimalware_-_Antivirus_-_Antispyware_-_Antispam_-_Seguridad.html. [Último acceso: 6 Abril 2017].

[31] P. Fernández, "Estudio de un sistema centralizado de Autenticación, Autorización y accounting (AAA) que facilite la previsión de políticas de calidad para los servicios de banda ancha de la corporación nacional de telecomunicaciones E.P", Quito, 2014, pp. 20-25.

[32] F. Flores y D. Jiménez, "Diseño de un sistema de gestión de seguridad de la información para la empresa Megadatos S.A en la ciudad de quito, aplicando las normas ISO 27001 e ISO", Quito, 2010, pp. 4-8.

[33] J. Areito, "Seguridad de la información. Redes, informática y sistemas de información", Madrid: Paraninfo, 2008.

[34] G. Álvarez, "Cómo protegernos de los peligros de Internet", Madrid: CSIC, 2009.

[35] EcuRed, “Caballo de Troya (Informática)”, EcuRed, [En línea]. Disponible en: https://www.ecured.cu/Caballo_de_Troya_(Inform%C3%A1tica). [Último acceso: 26 Octubre 2017].

[36] M. Pallo, "Diseño de un sistema de seguridad operacional para mejorar la protección en las redes Lan y Wan de Petroindustrial", 8 Noviembre 2016. [En línea]. Disponible en: http://bibdigital.epn.edu.ec/handle/15000/16793. [Último acceso: 04 08 2018].

[37] O. Ortega y L. Fuentes, “Códigos Maliciosos”, 1 Junio 2008. [En línea]. Disponible en: http://www.ru.tic.unam.mx:8080/bitstream/handle/123456789/1790/9.pdf?sequence=1&isAllowed=y. [Último acceso: 4 Agosto 2018].

[38] J. Bhardwaj, “Naked Security”, 2012. [En línea]. Disponible en: https://nakedsecurity.sophos.com/2012/09/14/new-techniquein-ransomware-explained/. [Último acceso: 4 Agosto 2018].

[39] J. Ruiz, “UAM. Departamento de Ingeniería Informática”, Junio 2017. [En línea]. Disponible en: https://repositorio.uam.es/handle/10486/679544. [Último acceso: 5 Agosto 2018].

[40] Y. Rodríguez, “Propuesta de Herramientas de Seguridad para la Intranet de la Empresa Geominera del Centro"Universidad Central Marta Abreu de Las Villas, 20 Junio 2007. [En línea]. Disponible en: http://dspace.uclv.edu.cu/bitstream/handle/123456789/6041/Yossel%20Rodr%C3%ADguez%20Cruz.pdf?sequence=1&isAllowed=y. [Último acceso: 6 Agosto 2018].

[41] E. López, Repositorio Universitario de la DGTIC, 5 Enero 2010. [En línea]. Disponible en: http://www.ru.tic.unam.mx:8080/handle/123456789/1721. [Último acceso: 6 Agosto 2018].

[42] ECUCERT, “Recomendaciones para evitar el Phishing”, 2017. [En línea]. Disponible en: https://www.ecucert.gob.ec/gu%C3%ADas-y-consejos.html.

[43] M. González, “Fraudes en Internet y Estafa Informática",Universidad de Oviedo, Mayo 2014. [En línea]. Disponible en: http://digibuo.uniovi.es/dspace/bitstream/10651/27824/3/TFM_Gonzalez%20Suarez,%20Marcos.pdf. [Último acceso: 6 Agosto 2018].

[44] H. Paredes, "Implementación de un sistema de gestión central y unificada sobre seguridad en ambientes Microsoft en el Laboratorio de Tecnologías de Información y Comunicación (LTIC) de la Facultad de Ingeniería" ,Repositorio Pontificia Universidad Católica el Ecuador, 2010. [En línea]. Disponible en: http://repositorio.puce.edu.ec/handle/22000/3424. [Último acceso: 6 Agosto 2018].

[45] C. Krieg, A. Dabrowski, H. Hobel, K. Krombholz y E. Weippl, "Hardware Malware", Viena: Morgan&Claypool Publisher, 2013.

[46] Cisco, “Reporte Anual de Ciberseguridad 2018”, 2018.

[47] Investigación Ekos Negocios y la Unidad de Investigación Económica y de Mercado, UIEM, Corporación Ekos, “PYMES: CONTRIBUCIÓN CLAVE EN LA ECONOMÍA,” 2013. [En línea]. Disponible en: http://www.ekosnegocios.com/revista/pdfTemas/770.pdf. [Último acceso: 12 Abril 2017].

[48] Ekos, “Especial Pymes 2016,” *Ekos,* nº Sep 2016, p. 62, 2016.

[49] F. Velásquez, “La estrategia, la estructura y las formas de asociación: fuentes de ventaja competitiva para las pymes colombianas,” Estudios Gerenciales*,* vol. 20, nº 93, pp. 73-93, 19 10 2004.

[50] M. Altamirano, “La Responsabilidad Social y su Relación con las PyMES en el Perú y su Entorno Económico ",Escuela de PostGrado de la UPC, 16 10 2011. [En línea]. Disponible en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/333466/32-82-1-PB.pdf?sequence=1&isAllowed=y. [Último acceso: 31 07 2018].

[51] M. Orozco y G. Quiroz, “El 82% de pymes de Ecuador accede a Internet, pero su uso se limita a enviar correos y tareas,” *EL COMERCIO,* 19 Julio 2015.

[52] Mundo Ejecutivo, “49% de los usuarios temen realizar transacciones financieras en línea,” 25 Junio 2015. [En línea]. Disponible en: http://mundoejecutivo.com.mx/tecnologia/2015/06/25/49-usuarios-temen-realizar-transacciones-financieras-linea. [Último acceso: 11 Enero 2017].

[53] M. Beroes, “40% de empresas regionales sufrieron ataques malware,” 7 Junio 2016. [En línea]. Disponible en: http://www.cioal.com/2016/06/07/40-de-empresas-regionales-sufrieron-ataques-malware/. [Último acceso: 12 Agosto 2017].

[54] Netlife, “Netlife - Clud Pyme,” Netlife, [En línea]. Disponible en: https://www.netlife.ec/form-cloud-pyme/. [Último acceso: 31 07 2018].

[55] CNT, “CNT - Plan Corporativo Pymes,” [En línea]. Disponible en: https://www.cnt.gob.ec/internet/plan-corporativo/internet-pymes/. [Último acceso: 31 07 2018].

[56] S.Conver y B.Trudel “Cisco SAFE: Un modelo de seguridad para las redes de las empresas”. Cisco Systems, [En Linea]. Disponible en: https://www.cisco.com/c/dam/global/es_es/assets/docs/safe_wp1.pdf

[57] B. Verdezoto, "Diseño de una red LAN para el trasporte de voz, datos y video para el municipio del Cantón Valencia Provincia de los Rios", Quito, 2015.

[58] J. Jiménez, “La Seguridad informática y el usuario final,” Revista Digital Universitaria, vol. 9, nº 4, pp. 7-11, 2008.

[59] M. Soriano, "Seguridad en redes y seguridad de la información", Czech Republic : Improvet, 2011.

[60] Á. Gómez, "Enciclopedia de la Seguridad Informática", Madrid: RA - MA, 2014.

[61] CSIRT UTPL, “CSIRT-SEGURIDAD DE LA INFORMACIÓN”, 11 Noviembre 2015. [En línea]. Disponible en: https://csirt.utpl.edu.ec/consejos?page=1. [Último acceso: 20 11 2017].

[62] Organización para la Cooperación y el Desarrollo Económicos, “OCDE Pequeñas y Medianas Empresas,” 2002. [En línea]. Disponible en: https://www.oecd.org/centrodemexico/laocde/. [Último acceso: 31 07 2018].

[63] CISCO, “Hoja de datos del servidor de seguridad de red de Cisco RV220W,” 18 08 2014. [En línea]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/routers/rv220w-wireless-network-security-firewall/data_sheet_c78-630461.html. [Último acceso: 1 Agosto 2018].

[64] E. Mira, "Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia", Valencia, 2015, pp. 13-16.

[65] F. Almeida, “Estudio y Diseño de un Sistema de Comunicaciones Bajo Esquema Compartido para el Chequeo de Pasajeros en el Aeropuerto Mariscal Sucre de Quito”, Quito, 2001.

[66] CISCO, “IP MultiLayer Switching Sample Configuration”, 17 Noviembre 2007. [En línea]. Disponible en: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/12022-39.html. [Último acceso: 1 Agosto 2018].

[67] Ekos, “Pymes en el Ecuador: No paran de evolucionar,” *Ekos,* nº Nov 2017, pp. 100-112, 2017.

[68] J. Areitio, "Seguridad de la información", Madrid: Paraninfo, pp. 256-262.

[69] R. Martínez, "Diseño de un esquema de seguridad para la red de datos de una institución educativa", Quito: EPN, 2010.

[70] Secretaria Nacional de la Administración Pública, “Esquema Gubernamental de Seguridad de la Infomración EGSI,” de *Acuerdo Ministerial 166*, Quito, 2016.

[71] F. Freire, “PLAN DE CONTINGENCIA ANTE CIBERATAQUES ", Repositorio Escuela Superior Politécnica del Litoral, 2017. [En línea]. Disponible en: https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf. [Último acceso: 7 Agosto 2018].

[72] PC World, “10 buenas prácticas de seguridad necesarias para las PYME,” 22 Noviembre 2013. [En línea]. Disponible en: http://www.pcworld.es/seguridad/10-buenas-practicas-de-seguridad-necesarias-para-las-pyme. [Último acceso: 20 Enero 2017].

[73] A. Prokofiev, Y. Smirnova y V. Surov, “A method to detect Internet of Things botnets,” Moscu, 2018.

[74] J.F. Carpentier, "La seguridad informática en la PYME: Situación actual y mejores prácticas", Barcelona: ENI, 2016.

[75] F. H. S. M. T. V. L. R. K. Advait Dixit, “Towards an Elastic Distributed SDN Controller,” de *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, Hong Kong, 2013.

[76] S. Ortiz, “Software-Defined Networking: On the Verge of a Breakthrough”, vol. 46, nº 7, pp. 10-12, 2013.

[77] C. M. R. V. C. A. C. F. C. C. B. Alejandro García Centeno, “Controladores SDN, elementos para su selección y evaluación”, *Telematica,* vol. 13, nº 3, pp. 10-20, 2014.

[78] M,Ashton & Asociados, “Ten Things to Look for in an SDN Controller”, Necam, 2013. [En línea]. Disponible en: https://www.necam.com/docs/?id=23865bd4-f10a-49f7-b6be-a17c61ad6fff. [Último acceso: 30 07 2018].

ANEXOS

ANEXO A.- ENCUESTA DE SEGURIDAD DE REDES

Encuesta de Seguridad de Redes

Encuesta con finalidad de descubrir los ataques de red, a los que han sido expuestas las empresas de mediana escala, con el fin de proponer un método para prevenir una interrupción en la línea de negocio de estas empresas.

*Obligatorio

1. ¿En el último año, su empresa ha sido víctima de algún ataque cibernético? * Marca solo un óvalo.
   - SI
   - NO

2. Si su respuesta anterior fue afirmativa, describa como afectó al normal funcionamiento de su empresa.

   _____
   _____
   _____
   _____
   _____

3. Si su empresa fue víctima de algún ataque cibernético. ¿Qué tiempo pasó antes que se vuelva a su normal funcionamiento? * Marca solo un óvalo.
   - Menor a 24 horas
   - Menor a 48 horas
   - Mayor a 48 horas

4. Los servicios de red que presta su empresa están montados sobre una plataforma: * Marca solo un óvalo.

   - Linux
   - Windows
   - Combinación de las anteriores
   - Otro: _____

5. ¿Qué servicios propios que están conectados a la red dispone en la empresa? * Selecciona todos los que correspondan.

   - [ ] Telefonía IP
   - [ ] Bases de Datos
   - [ ] DNS
   - [ ] Circuito cerrado de televisión
   - [ ] Correo Electrónico
   - [ ] DHCP
   - [ ] Almacenamiento de Información
   - [ ] Bases de datos
   - [ ] Impresión _____

   Otro:

6. ¿Qué tipo de amenazas son las más comunes en su red? * Selecciona todos los que correspondan.

   - [ ] Virus
   - [ ] Troyanos
   - [ ] Gusanos
   - [ ] Spyware
   - [ ] Malware
   - [ ] Phishing
   - [ ] _____
   - [ ] DoS
   - [ ] Spoofing
   - [ ] _____ Defacement

   Otro:

7. ¿Qué herramienta de seguridad dispone en su empresa? * Selecciona todos los que correspondan.

- [ ] Firewall
- [ ] Sistemas de Detección de Intrusos (IDS)
- [ ] Zonas Deslimitarizadas (DMZ)
- [ ] Antivirus, Antispyware, Antimalware
- [ ] Sistema de Prevención de Intrusos (IPS)
- [ ] Redes Privadas Virtuales (VPNs)

Otro:

8. ¿Cuál de los siguientes firewalls es utilizado para proteger su red? * Selecciona todos los que correspondan.

- [ ] CISCO
- [ ] Palo Alto
- [ ] Check Point
- [ ] Sophos
- [ ] Fortinet
- [ ] Huawei
- [ ] JUNIPER

Otro:

9. ¿Existe en su empresa un plan de contingencia si la seguridad de red falla? * Marca solo un óvalo.

- ( ) si
- ( ) no

10. El valor monetario de su solución de seguridad aproximadamente es: * Marca solo un óvalo.

- ( ) $0 - $10000
- ( ) $10000 - $50000
- ( ) $50000 - $100000
- ( ) Mayor a $100000

11. ¿Tiene total conocimiento de los equipos actuales de seguridad que existen en el mercado? * Marca solo un óvalo.

	1	2	3	4	5	
Nada	◯	◯	◯	◯	◯	Totalmente

Con la tecnología de
Google Forms

ANEXO B.- FICHA DE DATOS DE EQUIPOS DE SEGURIDAD.

Router de Frontera Cisco C2911

Enabling Borderless Networks at the Branch

The Cisco 2911 Integrated Services Router (ISR) delivers highly secure data, voice, video, and application service. Key features include:

3 integrated 10/100/1000 Ethernet ports (RJ-45 only)

1 service module slot

4 enhanced high-speed WAN interface card slots

2 onboard digital signal processor (DSP) slots

1 Internal Service Module slot for application services

Fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE

Security

Embedded hardware-accelerated VPN encryption for secure connectivity and collaborative communications Integrated threat control using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, and Cisco IOS Content Filtering

Identity management using authentication, authorization, and accounting (AAA) and public key infrastructure

Voice

High-density-packet voice DSP module, optimized for voice and video support

Standards-certified VoiceXML browser services

Cisco Unified Border Element capabilities

Cisco Unity Express voicemail support

Support for Cisco Communications Manager Express and Survivable Remote Site Telephony

Más información:

http://www.cisco.com/c/dam/en/us/products/collateral/routers/2800-series-integrated-services-routers-isr/product_data_sheet0900aecd8057f2e0.pdf

ROUTER DE FRONTERA ALCATEL LUCENT 7750

Features and benefits

Quality of service (QoS)

- Hierarchical QoS (HQoS)

Provides a built-in QoS engine that supports hierarchical QoS (HQoS) and can implement a hierarchical scheduling mechanism based on ports, user groups, users, and user services; also cooperates with MPLS Traffic Engineering (TE) to implement bandwidth reservation and scheduling based on tunnels and services

- Weighted random early detection (WRED)/random early detection (RED)

Delivers congestion avoidance capabilities through the use of queue management algorithms

- Advanced classifier-based QoS Classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information; applies QoS policies such as setting priority level and rate limit to selected traffic on a per-port or per-VLAN basis
- Bandwidth shaping

– Port-based rate limiting Provides per-port ingress-/egress-enforced increased bandwidth

– Classifier-based rate limiting

Uses an access control list (ACL) to enforce increased bandwidth for ingress traffic on each port

– Reduced bandwidth

Provides per-port, per-queue egress-based reduced bandwidth

- Traffic policing Supports Committed Access Rate (CAR) and line rate

Virtual private network (VPN)

- Layer 2 Tunneling Protocol (L2TP) An industry standard-based traffic encapsulation mechanism supported by many common operating systems; will tunnel the Point-to-Point Protocol (PPP) traffic over the IP and non-IP networks; may use the IP/UDP transport mechanism in IP networks
- Generic Routing Encapsulation (GRE)

Transports Layer 2 connectivity over a Layer 3 path in a secured way; enables the segregation of traffic from site to site Management

- Command authorization Leverages RADIUS to link a custom list of CLI commands to an individual network administrator's login; an audit trail documents activity
- Command-line interface (CLI)

Provides a secure, easy-to-use CLI for configuring the module via SSH or a switch console; provides direct real-time session visibility

- FTP, TFTP, and SFTP support

Offers different mechanisms for configuration updates; FTP allows bidirectional transfers overa TCP/IP network; trivial FTP (TFTP) is a simpler method using User Datagram Protocol (UDP); Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security Data sheet | Alcatel-Lucent 7750 Service Router Series3

- Network management

SNMP v2c/v3 MIB-II with traps

- Remote Monitoring (RMON) Uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group
- SNMP v1, v2, and v3

Provide complete support of SNMP; provide full support of industry-standard Management Information Base (MIB) plus private extensions; SNMP v3 supports increased security using encryption Layer 3 routing

- Layer 3 IPv4 routing

Provides routing of IPv4 at media speed; supports static routes, RIP and RIPv2, OSPF, IS-IS, and BGP

- Layer 3 IPv6 routing Provides routing of IPv6 at media speed; supports static routes, RIPng, OSPFv3, IS-ISv6, and MP-BGP

- Dual IP stack Maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design
- Equal-Cost Multipath (ECMP)

Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth

- IPv6 tunnels over IPv4 Allows IPv6 infrastructure to be connected over legacy IPv4 networks
- MPLS support Provides extended support of MPLS, including MPLS VPNs and MPLS Traffic Engineering (MPLS TE)
- Multiprotocol Label Switching (MPLS) Layer 3 VPN

Allows Layer 3 VPNs across a provider network; uses MP-BGP to establish private routes for increased security; supports RFC 2547bis multiple autonomous system VPNs for added flexibility

- Multicast VPN

Supports multicast domain (MD) multicast VPN, which can be distributed on separate service cards, providing high performance and flexible configuration

- Multiprotocol Label Switching (MPLS) Layer 2 VPN

Establishes simple Layer 2 point-to-point VPNs across a provider network using only MPLS Label Distribution Protocol (LDP); requires no routing and therefore decreases complexity, increases performance, and allows VPNs of non-routable protocols; uses no routing information for increased security; supports Circuit Cross Connect (CCC), Static Virtual Circuits (SVCs), Martini draft, and Kompella-draft technologies

- Virtual Private LAN Service (VPLS) Establishes point-to-multipoint Layer 2 VPNs across a provider network Data sheet | Alcatel-Lucent 7750 Service Router Series 4
- Multiprotocol Label Switching Traffic Engineering (MPLS TE)

Traffic Engineering (TE) is used to enhance traffic over large MPLS networks based on type of traffic and Disponible en resources; TE dynamically tunes traffic management attributes and enables true load balancing; MPLS TE supports route backup using fast reroute (FRR)

- VPLS support

Provides extended support of VPLS for data center to data center communication at Layer 2; provides support of hierarchical VPLS for scalability Security

- Access control lists (ACLs) Provide IPv4 and IPv6 filtering based on source and destination IP address/subnet and source/destination TCP/UDP port number
- Network Address Translation (NAT) Provides a method for translating private IP addresses to public IP addresses, reducing the number of IP addresses used, and isolates the enterprise addressing environment
- Secure management access Delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2 and SNMPv3
- Unicast Reverse Path Forwarding (URPF)

Allows normal packets to be forwarded correctly, but discards the attaching packet due to lack of reverse path route or incorrect inbound interface; prevents source spoofing and distributed attacks; supports distributed UFPF Resiliency and high availability

- Non-Stop Routing provides instant recovery from a control plane failure without relying on an adjacent router. It uses a hot-standby control card with the latest router image, configuration and network state and is able to maintain existing protocol sessions with adjacent routers while continuing to learn new route updates during the fail over
- Non-Stop Services Extends non-stop routing to ensure uninterrupted availability of network services during a control plane fail over. The hot-standby control card maintains the state of services and sessions so that VPLS, VLL, IP VPN, and enhanced Internet services are not affected during a control plane fail over
- Graceful restart Supports graceful restart for OSPF, IS-IS, BGP, LDP, and RSVP; the network remains stable during the active-standby switchover; after the switchover, the device quickly learns the network routes by communicating with adjacent routers; forwarding remains uninterrupted during the switchover to achieve nonstop forwarding (NSF)
- Hot-swappable modules Permits modules and mini-GBICs to be added or swapped without interrupting the network.

- IP Fast Reroute (FRR) Nodes are configured with backup ports and routes; local implementation requires no cooperation of adjacent devices, simplifying the deployment; solves the traditional convergence faults in IP forwarding; achieves restoration within 50 ms, with the restoration time independent of the number of routes and fast link switchovers without route convergence Data sheet

Alcatel-Lucent 7750 Service Router Series 5

- Redundant design of main processing unit and power supply Increases the overall system availability
- Separate data and control planes Provide greater flexibility and enable continual services
- Virtual Router Redundancy Protocol (VRRP)

Allows groups of two routers to back each other up dynamically to create highly Disponible en routed environments in IPv4 and IPv6 networks

- Assured high availability

– Resilient switch fabric Protection from a single failed fabric module, supporting total capacity by the remaining fabric module

– Optional redundant management Automatic failover for active and standby management modules

– Modular and distributed software Increase capability/capacity by using distributed hardware and software

– Optional redundant power supply Uninterrupted power

– No single point of failure architecture Separate control and management planes

- In-service software upgrades Leveraging non-stop routing and non-stop services, allows major and minor upgrades to be installed without restarting the device, increasing network uptime and simplifying maintenance Software-defined networking
- OpenFlow

Supports OpenFlow 1.0 and 1.3 specifications to enable SDN by allowing separation of the data (packet forwarding) and control (routing decision) paths

Multicast support

- Internet Group Management Protocol (IGMP)

Utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage

IPv4 multicast networks; supports IGMPv1, v2, and v3

- Protocol Independent Multicast (PIM)

Defines modes of Internet IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; PIM Dense Mode (DM), Sparse Mode (SM), and Source-Specific Mode (SSM) are supported

- Multicast Source Discovery Protocol (MSDP)

Allows multiple PIM-SM domains to interoperate; is used for inter-domain multicast applications

- Multicast Border Gateway Protocol (MBGP)

Allows multicast traffic to be forwarded across BGP networks separately from unicast traffic

Más información:
http://www.curvesales.com/datasheets/routers/Data-Center/Alcatel-Lucent-7750-Service-Router-Series-DataSheet.pdf

FIREWALL ASA NGFW 5506

Features and Benefits of Cisco ASA with FirePOWER Services

Feature	Benefits
Next-generation firewall	Industry's first threat-focused NGFW; provides ASA firewall functionality, advanced threat protection, and advanced breach detection and remediation combined in a single device
Proven ASA firewall	Rich routing, stateful firewall, Network Address Translation, and dynamic clustering for high-performance, highly secure, and reliable access with Cisco AnyConnect® VPN
Market-leading NGIPS	Superior threat prevention and mitigation for both known and unknown threats
Advanced malware protection	Detection, blocking, tracking, analysis, and remediation to protect the enterprise against targeted and persistent malware attacks
Full contextual awareness	Policy enforcement based on complete visibility of users, mobile devices, client-side applications, communication between virtual machines, vulnerabilities, threats, and URLs
Application control and URL filtering	Application-layer control (over applications, geolocations, users, websites) and ability to enforce usage and tailor detection policies based on custom applications and URLs

Enterprise-class management	Dashboards and drill-down reports of discovered hosts, applications, threats, and indications of compromise for comprehensive visibility
Streamlined operations automation	Lower operating cost and administrative complexity with threat correlation, impact assessment, automated security policy tuning, and user identification
Purpose-built, scalable	Highly scalable security appliance architecture that performs at up to multigigabit speeds; consistent and robust security across small office, branch offices, Internet edge, and data centers in either physical and virtual environments
On-device management	Simplifies advanced threat defense management for small and medium sized business with small scale deployments
Remote Access VPN	Extends secure corporate network access beyond corporate laptops to personal mobile devices, regardless of physical location; support for Cisco AnyConnect Secure Mobility Solution, with granular, application-level VPN capability, as well as native Apple iOS and Android VPN clients
Site-to-site VPN	Protect traffic, including VoIP and client-server application data, across the distributed enterprise and branch offices
Integrated wireless access	Integrated Wi-Fi is Disponible en in the desktop form factor (ASA 5506W-X) for compact and simplified small office deployments
Ruggedized form factor	A ruggedized model (ASA 5506H-X), designed specifically for extreme environmental conditions, is Disponible en for critical infrastructure and control network applications
Third-party technology ecosystem	Open API that enables the third-party technology ecosystem to integrate with existing customer work streams
Integration with Snort and OpenAppID	Open source security integration with Snort and OpenAppID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
Collective Security intelligence (CSI)	Unmatched security and web reputation intelligence provides real-time threat intelligence and security protection

Más información:

http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-x-series-next-generation-firewalls/data-sheet-c78-729807.html

ANEXO C.- INCIDENTES Y VULNERABILIDADES REPORTADOS EN EL 2016 SEGÚN ECUCERT.

Juan Pablo Gallardo

De:	.Edwin Narvaez via RT <incidente@ecucert.gob.ec>
Enviado el:	Monday, July 17, 2017 1:14 PM
Para:	Juan Pablo Gallardo
Asunto:	[ECUCERT-ARCOTEL #44271] Informe de los ataques reportados en el 2016 Ecuador
Marca de seguimiento:	Seguimiento
Estado de marca:	Marcado

Estimados Señores:

En el siguiente cuadro se presentan Vulnerabilidades e incidentes que se presentan en las redes de nuestro país

Incidente

Drones_Botnet

Sinkhole_HTTP_IPv6

Sinkhole_HTTP

Microsoft_Sinkhole

bruteforce

Compromised_website

phishing

CC_Server

Vulnerabilidad

Open_TFTP

CWMP

DNS_Open_Resolver

Open_SSDP

Blacklisted

Open_Netbios

Open_Telnet