



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

**Propuesta para la implementación de un sistema seguridad
perimetral mediante la protección corta fuegos de próxima
generación aplicable para pequeñas y medianas empresas del
cantón Guaranda.**

JORGE FAVIÁN PEÑA ARPI

Trabajo de Titulación modalidad Proyecto de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

Riobamba – Ecuador

Octubre 2023

DECLARACIÓN DE AUTENTICIDAD

Yo, Jorge Favián Peña Arpi, declaro que el presente **Trabajo de Titulación modalidad Proyecto de Investigación y Desarrollo**, es de mi autoría y los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación de Maestría.



Jorge Favián Peña Arpi
C.I. 1400687586

© 2023, **Jorge Favian Peña Arpi**

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DE TRABAJO DE INVESTIGACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyecto de Investigación y Desarrollo, titulado: **Propuesta para la implementación de un sistema seguridad perimetral mediante la protección cortafuegos de próxima generación aplicable para pequeñas y medianas empresas del cantón Guaranda**, de responsabilidad de JORGE FAVIÁN PEÑA ARPI, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal autoriza su presentación.

Dr. Juan Mario Vargas Guambo, Mgtr.
PRESIDENTE



Ing. Oswaldo Geovanny Martínez Guashima, M.Sc.
DIRECTOR



Ing. Joffre Stallin Monar Monar, M.Sc.
MIEMBRO



Ing. Silvia Lorena Morales Noriega, M.Sc.
MIEMBRO

SILVIA LORENA
MORALES
NORIEGA
Firmado digitalmente
por SILVIA LORENA
MORALES NORIEGA
Fecha: 2023.04.26
15:30:20 -05'00'

Riobamba, octubre 2023

DEDICATORIA

Dedico este proyecto de tesis a mi Dios, por brindarme de su infinita bondad y misericordia, permitiéndome experimentar de aquellos retos y pruebas disfrazados de las más grandes bendiciones, a mi padre, quien, sin serlo ante la ley, asumió este rol, dedicando su apoyo y confianza hasta la culminación de mis estudios.

Jorge

AGRADECIMIENTO

Mi agradecimiento a Dios, por ser el pilar fundamental en cada etapa de mi vida, demostrando su eterno amor en tiempos de felicidad y tristeza, guiando mis pasos hacia el cumplimiento de sueños que se vuelven realidad.

A mis padres, Luis y Rafaela, quienes con gran esfuerzo dedicaron todo en cuanto estuvo a su alcance, enseñándome que la perseverancia y entrega tienen su recompensa. A mis amigos, compañeros y hermanos en la fe, que, con sus buenos deseos y oraciones, expresaron su apoyo día a día hasta la culminación de esta tesis.

Jorge

TABLA DE CONTENIDO

RESUMEN..... xvii

SUMMARY xviii

CAPÍTULO I

1. INTRODUCCIÓN..... 1

1.1 PROBLEMA DE LA INVESTIGACIÓN 2

1.1.1 *Planteamiento del problema*..... 2

1.1.2 *Formulación del problema*..... 9

1.1.3 *Sistematización del problema*..... 9

1.2 JUSTIFICACIÓN DE LA INVESTIGACIÓN..... 9

1.3 OBJETIVOS DE LA INVESTIGACIÓN..... 10

1.3.1 *Objetivo General*..... 10

1.3.2 *Objetivos Específicos* 10

1.4 HIPÓTESIS..... 10

CAPÍTULO II

2. MARCO TEÓRICO..... 11

2.1 ANTECEDENTES 11

2.2 METODOLOGÍA..... 12

2.2.1 *Ventajas*..... 13

2.2.2 *Desventajas* 13

2.3 FIREWALL DE PRÓXIMA GENERACIÓN NGFW 14

2.3.1 *Diferencias entre Cortafuego UTM y Cortafuego NGFW*..... 15

2.4 CUADRANTE MÁGICO DE GARTHER..... 15

2.4.1	<i>Novedades en el Cuadrante Gartner 2017 para los Cortafuegos de Redes Empresariales</i>	16
2.4.2	<i>Novedades en el Cuadrante Gartner 2018 para los Firewalls de Redes Empresariales</i>	17
2.4.3	<i>Novedades en el Cuadrante Gartner 2019 para los Firewalls de Redes Empresariales</i>	18
2.5	SELECCIÓN DE UNA MARCA DE FIREWALL PARA LA IMPLEMENTACIÓN DE UN ESCENARIO DE PRUEBAS	19
2.6	NORMAS Y ESTÁNDARES INTERNACIONALES PARA EL ASEGURAMIENTO DE LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS.	20
2.6.1	<i>ISO / IEC 27033</i>	20
2.6.2	<i>ISO / IEC 27033-1: 2015</i>	21
2.6.3	<i>ISO / IEC 27033-2: 2012: Directrices para el diseño e implementación de seguridad de red.</i>	22
2.6.4	<i>ISO / IEC 27033-3: 2010: Escenarios de redes de referencia: amenazas, técnicas de diseño y problemas de control.</i>	22
2.6.5	<i>ISO / IEC 27033-4: 2014</i>	23
2.6.6	<i>ISO / IEC 27033-5: 2013</i>	23
2.6.7	<i>ISO / IEC 27033-6: 2016</i>	24
2.6.8	<i>OEA (Organización de Estados Americanos) y Microsoft</i>	24
2.6.9	<i>Normativas y estándares en el Ecuador de seguridad de la información en las pymes</i>	25
2.7	DESCRIPCIÓN DE PALABRAS	27
2.7.1	<i>Mintel</i>	27
2.7.2	<i>ARCOTEL</i>	27
2.7.3	<i>Firewall</i>	28
2.7.4	<i>Ciberseguridad</i>	28
2.7.5	<i>Interdependencias</i>	28

2.7.6	<i>Seguridad perimetral</i>	28
2.7.7	<i>Resiliencia</i>	28
2.7.8	<i>INCIBE (Instituto Nacional de Ciberseguridad de España)</i>	28
2.7.9	<i>Cuadrante mágico de Garther</i>	29
2.7.10	<i>Criptografía</i>	29
2.8	AMENAZAS A LA SEGURIDAD INFORMÁTICA EMPRESARIAL	29
2.8.1	<i>Amenazas a los activos de la empresa</i>	29
2.8.2	<i>Amenazas a los activos personales</i>	30
2.9	AGENTES DE AMENAZAS	30
2.9.1	<i>Amenazas externas</i>	30
2.9.2	<i>Amenazas internas</i>	31
2.9.3	<i>Amenazas mixtas</i>	31
2.10	ESTRUCTURA DE LA SEGURIDAD INFORMÁTICA PARA PYMES.	31
2.10.1	<i>Pasos fundamentales para asegurar las Pymes</i>	32

CAPÍTULO III

3.	METODOLOGÍA DE INVESTIGACIÓN	34
3.1	DISEÑO DE LA INVESTIGACIÓN	34
3.2	TIPO DE LA INVESTIGACIÓN	34
3.3	MÉTODO DE LA INVESTIGACIÓN	34
3.4	FUENTES DE INFORMACIÓN	35
3.5	TÉCNICAS DE RECOLECCIÓN DE DATOS PRIMARIOS Y SECUNDARIOS	35
3.6	TIPO DE ESTUDIO	36
3.7	DEFINICIÓN DE UN ESCENARIO DE PRUEBAS	36
3.8	DETERMINACIÓN DE VARIABLES	37
3.8.1	<i>Operacionalización de variables</i>	37
3.8.2	<i>Población y muestra</i>	39

3.8.3	<i>Instrumentos de recolección de datos</i>	40
3.8.4	<i>Ambiente de pruebas sin seguridad</i>	41
CAPÍTULO IV		42
4.	RESULTADOS Y DISCUSIÓN	42
4.1	VARIABLE INDEPENDIENTE	42
4.1.1	<i>Indicador 1: Cifrado</i>	43
4.1.2	<i>Indicador 2: Autorización</i>	43
4.1.3	<i>Indicador 3: Aplicabilidad</i>	44
4.1.4	<i>Análisis e interpretación de resultados variable dependiente</i>	45
4.2	VARIABLE DEPENDIENTE	45
4.2.1	<i>Indicador 1: Confidencialidad</i>	46
4.2.2	<i>Indicador 2: Integridad</i>	47
4.2.3	<i>Indicador 3: Autenticación</i>	47
4.3	PRUEBA DE HIPÓTESIS	49
CAPÍTULO V		
5.	PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL MEDIANTE LA PROTECCIÓN CORTAFUEGOS DE PRÓXIMA GENERACIÓN APLICABLE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL CANTÓN GUARANDA	53
5.1	IMPLEMENTACIÓN Y EVALUACIÓN DEL SISTEMA MEDIANTE UNA ESTRUCTURA DE APLICABILIDAD PARA PYMES DEL CANTÓN GUARANDA	54
5.1.1	<i>Inspección de paquetes con estado (SPI)</i>	54
5.1.2	<i>Control de Acceso Web</i>	56
5.1.3	<i>VPN (Red Privada Virtual)</i>	58
5.1.4	<i>Monitoreo automatizado</i>	59
5.1.5	<i>Zona desmilitarizada (DMZ)</i>	60

5.1.6	<i>Control de Aplicaciones</i>	61
5.1.7	<i>Detección de malware</i>	61
5.2	SEGURIDAD SEGÚN LAS CAPAS DEL MODELO OSI	62
	CONCLUSIONES	66
	RECOMENDACIONES	67
	GLOSARIO	
	BIBLIOGRAFÍA	
	ANEXOS	

ÍNDICE DE TABLAS

Tabla 1-1 Ingreso de sectores en dólares.....	8
Tabla 1-2 Ingreso de sectores en dólares.....	19
Tabla 2-2 Elección de la marca de Firewall para Pymes.	20
Tabla 1-3 Operacionalización de variables	37
Tabla 2-3 Operacionalización metodológica de variables.....	38
Tabla 3-3 Algoritmos de cifrado	39
Tabla 4-3 Principales amenazas que afectan la confidencialidad, integridad y autenticación. ..	40
Tabla 5-3 Herramientas y su descripción.....	41
Tabla 1-4 Escala cualitativa de la cuantificación de indicadores de la variable independiente. 42	
Tabla 2-4 Cifrado.....	43
Tabla 3-4 Resultados de Cifrado.....	43
Tabla 4-4 Autorización	43
Tabla 5-4 Resultados de la Autorización	43
Tabla 6-4 Aplicabilidad.....	44
Tabla 7-4 Resultados de Aplicabilidad	44
Tabla 8-4 Resumen del análisis de la variable independiente.....	44
Tabla 9-4 Escala cualitativa de la cuantificación de indicadores de la variable dependiente. 45	
Tabla 10-4 Confidencialidad.....	46
Tabla 11-4 Resultados de Confidencialidad.....	46
Tabla 12-4 Integridad.....	47
Tabla 13-4 Resultados de la Integridad.....	47
Tabla 14-4 Autenticación.....	47
Tabla 15-4 Resultados de la Autenticación.....	48
Tabla 16-4 Resultados totales de la cuantificación de indicadores de la variable dependiente. 48	
Tabla 17-4 Cuantificación de indicadores de la variable dependiente para el acceso seguro	48

Tabla 18-4 Consideraciones de acceso seguro	49
Tabla 19-4 Valorización de la Variable Dependiente	49
Tabla 20-4 Tabla de contingencia de lo observado.....	50
Tabla 21-4 Tabla de frecuencias de lo esperado	50
Tabla 22-4 Tabla del cálculo del Chi-cuadrado	51
Tabla 23-4 Descripción tabla del cálculo del Chi-cuadrado	52
Tabla 1-5 Seguridad según las capas del modelo OSI	62

ÍNDICE DE FIGURAS

Figura 1-1 Clasificación de tamaño de empresa.	6
Figura 2-1 Clasificación de empresas según sector económico.	6
Figura 3-1 Porcentaje de empresas según provincia del Ecuador.	7
Figura 4-1 Perfil económico del cantón Guaranda	7
Figura 5-1 Principales industrias en el Cantón Guaranda.	8
Figura 6-1 Gastos en capacitación e investigación en el Cantón Guaranda.	8
Figura 7-1 Principales industrias en el Cantón Guaranda.	9
Figura 1-2 Cuadrante mágico de Gartner 2017.	17
Figura 2-2 Cuadrante mágico de Gartner 2018.	18
Figura 3-2 Cuadrante mágico de Gartner 2019.	19
Figura 1-3 Intento de ingreso no autorizado a la red empresarial.	36
Figura 2-3 Propuesta de un escenario de Pruebas.	37
Figura 3-3 Escenario de Pruebas sin seguridad.	41
Figura 1-5 Propuesta de un Sistema de Seguridad Perimetral.	54
Figura 2-5 Inspección de paquetes con estado (SPI).	55
Figura 3-5 Estadísticas del tráfico de los puertos del Firewall.	55
Figura 4-5 Tabla de registro del sistema.	55
Figura 5-5 Tabla de procesos Protocolo TCP.	56
Figura 6-5 Tabla de Procesos Protocolo UDP.	56
Figura 7-5 Determino el rango de IP que trabaja la página web.	57
Figura 8-5 Ingreso el rango de IP en la cual se deniega el acceso.	57
Figura 9-5 Ingreso el rango de IP en la cual se deniega el acceso.	57
Figura 10-5 Configuración Cliente-Gateway.	58
Figura 11-5 Cliente VPN.	58
Figura 12-5 Conexión establecida de la VPN para administración del equipo.	59

Figura 13-5 Conexión establecida de la VPN para administración del equipo.....	59
Figura 14-5 Monitoreo Automatizado.	60
Figura 15-5 Tabla de información del sistema.....	60
Figura 16-5 Habilidad de la Zona Desmilitarizada DMZ.	61
Figura 17-5 Estadísticas del tráfico Zona Desmilitarizada DMZ.	61

ÍNDICE DE ANEXOS

Anexo A: Ficha Técnica

Anexo B: implementación del equipo Firewall

Anexo C: implementación del escenario de pruebas tipo laboratorio

Anexo D: Correo real de posible estafa por 850 dólares dentro del correo de la red empresarial (spam)

Anexo E: Bloqueo de correo empresarial no deseado (spam)

Anexo F: Ataques Maliciosos

Anexo G: Funcionamiento Normal de un computador

RESUMEN

El objetivo de realizar una propuesta para la implementación de un sistema de seguridad perimetral mediante la protección de corta fuegos de próxima generación para pequeñas y medianas empresas del cantón Guaranda. Se empezó estudiando los estándares y normativas existentes referentes a la seguridad perimetral para PYMES también se recopiló información con enfoque metodológico cualitativo, investigación de escritorio y campo de varios documentos con respecto al tema. Con la información obtenida se diseñó y posteriormente se definió un escenario de pruebas tipo laboratorio con un equipo que posee funciones de seguridad y firewall de próxima generación (NGFW) utilizando de esta manera una nueva tecnología que es la inspección de paquetes con estado (SPI) que es un mecanismo de seguridad avanzado que inspecciona los paquetes y ejecuta un seguimiento del estado de las conexiones en la red, control de las conexiones activas y decide qué paquetes entrantes o salientes son autorizados de ingresar o salir de la red empresarial con la finalidad de evitar que ingrese tráfico dañino. El siguiente punto fue la evaluación del sistema mediante la estructura de las capas del modelo OSI donde se analizó el tráfico en la capa de transporte, junto con el seguimiento de los estados de las conexiones de la red, como puede ser la comunicación UDP y los flujos TCP que pasan a través del firewall, distinguiendo los paquetes legítimos de los ilegítimos que se dirigen a la red de la empresa. Finalmente se muestra que los firewalls NGFW de última tecnología además de bloquear el tráfico en función de los controles establecidos por las políticas de seguridad realizan un análisis profundo de paquetes y buscan activamente patrones que puedan indicar actividad maliciosa; se recomienda el respaldo periódico de la información crítica de la empresa ya sea en un espacio en la nube o en un disco duro externo.

Palabras Clave: <RED DE SIGUIENTE GENERACIÓN (NGN)>, <FIREWALL>, <MODELO OSI>, <PYMES>, <SEGURIDAD PERIMETRAL>, <GUARANDA (CANTÓN)>



Firmado electrónicamente por:
LUIS ALBERTO
CAMINOS VARGAS



30-01-2023

0006-DBRA-UPT-IPEC-2023

SUMMARY

The aim is to propose implementing a perimeter security system through protecting next-generation firewalls for small and medium-sized companies in the Guaranda canton. It began by studying the current standards and regulations regarding perimeter security for SMEs information was also collected with a qualitative methodological approach, desktop research, and field of various documents on the subject. With the gathered information, a laboratory-type test scenario was expanded and subsequently defined with a team with security functions and a next-generation firewall (NGFW) using a new technology that is stateful packet inspection (SPI). which is an advanced security mechanism that inspects packets and performs connection status monitoring on the network, controls active connections, and decides which incoming or prominent packets are allowed to enter or leave the corporate network to prevent harmful traffic from entering. The next point was the evaluation of the system through the structure of the layers of the OSI model, where the traffic in the transport layer was analyzed, together with the monitoring of the states of the network connections, such as UDP communication and the TCP streams that pass through the firewall, distinguishing legitimate packets from illegitimate packets headed for the company network. Finally, it is shown that state-of-the-art NGFW firewalls, in addition to blocking traffic based on the controls established by security policies, perform deep packet analysis, and actively search for patterns that may indicate malicious activity; Periodic backup of business-critical information is recommended, either to a cloud space or to an external hard drive.

Keywords: < NEXT GENERATION NETWORK (NGN)>, <FIREWALL>, < OSI MODEL>, < SMEs>, < PERIMETER SECURITY >, <GUARANDA (CANTON)>.

CAPÍTULO I

1. INTRODUCCIÓN

Una de las acciones que ayudan a mitigar estos problemas, es establecer una seguridad perimetral lógica afín de poner una barrera o frontera que sea imposible de penetrar entre una red interna y el internet, para restringir y tener un control sobre los datos que entran y salen de la organización, siendo la principal ventaja permitir al administrador concentrarse en los puntos de entrada, sin olvidar la seguridad del resto de servidores internos de la red, para protegerlos frente a una posible intrusión. (Díaz, 2013)

La seguridad de la información ha sido un tema de vital importancia para el sector empresarial y como ende de ella la seguridad perimetral. En los últimos años este concepto ha sufrido algunos cambios y ello ha estado condicionado según al incremento de las brechas en las redes, los sistemas operativos, los equipos de uso cotidiano, la evolución de la tecnología, el uso de mecanismos de comunicaciones móviles y el almacenamiento de información en la nube, siendo necesario integrar a este concepto accesos lógicos y físicos. (Bohórquez_Gutiérrez, 2018).

La seguridad lógica hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático, la seguridad es una herramienta valiosa para cualquier negocio, lo cual conlleva a cuestionarse sobre la manera en que se puede formalizar la intención que tiene la misma en las organizaciones. En el contexto actual cuando se habla de seguridad sobre las tecnologías de la información (TI) se definen o establecen desde diversas áreas, tales como la seguridad informática, la seguridad de la información y la Ciberseguridad. (Pírez, 2018)

La implementación, de la tecnología marca una época de progreso, desarrollo, e innovación, en una serie de aspectos de la sociedad y sobre todo en el campo empresarial. Así mismo (Bohórquez_Gutiérrez, 2018) manifiesta que esta revolución tecnológica implica problemas de vulnerabilidad que atentan contra la disponibilidad, integridad y seguridad de la información, a esta realidad se une el hecho de que muchas empresas crecen en infraestructura (civil, edificios), personal, inversiones, productos, servicios para sus clientes, pero no invierten en mejorar su seguridad ya sea por desconocimiento, costos o falta de personal con preparación en el área de las tecnologías de la información (TI).

1.1 Problema de la investigación

El 17 de marzo del 2020 se da el aislamiento obligatorio en el Ecuador debido a la pandemia del COVID-19, por lo que muchas empresas debieron suspender sus actividades, sin embargo, existieron otras que optaron por el teletrabajo. Esto dio lugar a que las empresas publiquen ciertos servicios en la web o utilicen accesos mediante una red privada virtual (VPN), dependiendo de una tecnología que permita mantener la seguridad perimetral y al mismo tiempo ofrecer una comunicación entre los usuarios desde el internet hacia los servicios de la red local de la Pymes, para no paralizar sus actividades.

La seguridad informática es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o la posibilidad de acceder a ellos por accidente. (Universidad Internacional de Valencia, 2018)

El establecimiento de una cultura de ciberseguridad exige una labor de capacitación de todos los sectores de la sociedad, para la que está llamada a jugar un papel protagonista la universidad; las instituciones universitarias no pueden quedarse ajenas y deben participar en el proceso, contribuyendo a crear un ciberespacio universitario seguro y liderando el arraigo de una cultura de ciberseguridad, cimentada en una cultura de seguridad y defensa, dentro de la Universidad y desde la Universidad a la sociedad. (Fourie, 2014)

En el listado del índice global de ciberseguridad de 194 estados miembros el Ecuador ocupa el puesto 98, entre los países sudamericanos el Ecuador se encuentra en el noveno lugar, el primer lugar es para Uruguay, después México, Brasil, Colombia y Argentina. (ITU, Union Internacional de Telecomunicaciones, 2018)

1.1.1 Planteamiento del problema

La expansión de internet, el uso de las tecnologías de la información y la comunicación (TIC) durante los últimos años permite, como nunca antes, la circulación de ingentes volúmenes de información y el establecimiento de comunicaciones de manera fácil. En mayor medida las actividades sociales, económicas y hasta militares de un Estado, se hacen cada vez más dependientes del uso de las TIC, lo que irremediamente implica a su vez una mayor vulnerabilidad y exposición a los ciberataques. (GESI, 2018)

Invertir en seguridad informática en la PYME es mucho más que un capricho. Al igual que una alarma contra incendios, se espera que en ningún momento se produzca uno, lo cierto es que muchas veces no se da la debida importancia a los riesgos de la informática para la seguridad de los datos. (Julia, 2017)

Según el reporte de la ITU de ciberseguridad global del 2017, casi el uno por ciento de todos los correos electrónicos enviados fueron esencialmente ataques maliciosos, la tasa más alta en los últimos años. Ransomware ataca cada vez más a las empresas y los consumidores, con campañas indiscriminadas que eliminan enormes volúmenes de correos electrónicos maliciosos. Los atacantes demandan cada vez más a las víctimas, con una demanda de rescate promedio que subió a más de 1,000 USD en 2016, en comparación con los 300 USD del año anterior. En mayo de 2017, un ciberataque masivo causó grandes interrupciones en las empresas y hospitales en más de 150 países, lo que provocó un llamado a una mayor cooperación en todo el mundo. Lanzado por primera vez en 2014, el objetivo del Índice Global de Ciberseguridad (GCI) es ayudar a fomentar una cultura global de ciberseguridad y su integración en el núcleo de las tecnologías de la información y comunicación (TIC). (ITU, Global Cybersecurity Index, 2017)

Según la compañía de ciberseguridad Kasperky Lab en un reporte del año 2017 el 60% de las pequeñas y medianas empresas en Europa que fueron víctimas de ciberataque desaparecen a los 6 meses del incidente, además el informe también señala que las Pymes son el blanco de más de un 43% de este tipo de ataques.

La insuficiente atención prestada a la seguridad cibernética es un riesgo importante a nivel internacional, nacional, a las empresas, universidades y a los individuos. La escasez de profesionales de la seguridad cibernética para hacer frente a este riesgo, y la falta de programas de educación para formar a estos profesionales, ha llevado a una “crisis de capital humana en ciberseguridad”. (Anchundia Betancourt, 2017)

Según el estudio Global Corporate Divestment, de EY, las pymes no tienen presupuesto para hacer frente a las ciberamenazas. Estas son demasiado amplias y sus cuentas no son tan flexibles como las de las grandes empresas. Como resultado, son vulnerables a los ataques informáticos. Esto significa que el 87% de las empresas no tiene herramientas para defender sus datos o los de sus clientes. (GlobalCorporateDivestmentStudy, 2018). Según el portal Privacy Rights Clearinghouse, tan solo en 2018 en los Estados Unidos fueron robados 1.371 millones de archivos con datos personales. No es un hecho aislado. Durante los últimos años se ha producido un crecimiento notable de este tipo de robos.

Con foco en el mercado estadounidense, representativo de nuestra forma de operar en negocios virtuales, el 39% de las empresas apenas dedican un 2% de su presupuesto en servicios de tecnología de la información (IT) para defenderse de amenazas externas. Solo el 45% de las organizaciones introduce la seguridad en su estrategia. (PrivacyRightsClearinghouse, 2019).

Ante esta realidad, aludiendo específicamente a América Latina, la mayor parte de los Estados disponen de capacidad de respuesta ante ciberataques, pero lo cierto es que sólo seis han diseñado una Estrategia de Ciberseguridad. El último en presentar su Estrategia fue México, el 13 de noviembre de 2017, uniéndose al pequeño grupo de países latinoamericanos que, según la OEA (2017), cuenta con este tipo de políticas. El resto son Colombia (2011 y 2016), Panamá (2013), Paraguay (abril de 2017), Chile (abril de 2017) y Costa Rica (abril de 2017). (GESI, 2018)

El Ecuador trabaja en una Estrategia Nacional de Ciberseguridad. Con el fin que Ecuador fortalezca y asegure su entorno digital, Patricio Real, viceministro de Tecnologías de la Información y Comunicación, del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), se reunió con representantes del Banco Interamericano de Desarrollo (BID) y la consultora NRD Cyber Security, para iniciar la consultoría de “Elaboración de la Estrategia Nacional de Ciberseguridad”. (MINTEL, El Ecuador trabaja en la Estrategia Nacional de Ciberseguridad, 2019)

En el año 2015 cibermafias atacaron a 17 empresa ecuatorianas, el malware avanzó y en cinco días penetró en los ordenadores de 17 empresas privadas e instituciones públicas de Quito, Guayaquil y Cuenca. El programa maligno ingresó en las computadoras y encriptó archivos sensibles de Word, Excel y Autocad, el virus denominado cryptolocker llegó a usuarios a través de correos electrónicos con información aparentemente útil, los ciberdelincuentes daban 4 días para que las empresas depositen dinero. (Haro, 2015)

A pesar que las grandes empresas hacen inversiones considerables en seguridad informática y tienen especialistas en tecnologías de la información (TI), no les garantiza que el sistema informático sea 100% seguro, por ejemplo. En el año 2016 el Banco del Austro (BDA) de Ecuador sufrió un robo en el que el sistema SWIFT (Society for Worldwide Interbank Financial Telecommunication) ha sido utilizado como método para transferir el dinero a otros bancos. Al igual que en el caso del robo de 81 millones de dólares del Banco Central de Bangladesh, el modus operandi consiste en comprometer los sistemas informáticos del banco, obtener acceso a la red de mensajería SWIFT y realizar transferencias fraudulentas a otros bancos. En este caso el importe sustraído es de 12 millones de dólares. (incibe-cert, 2016).

En mayo del 2017 el ciberataque global del virus WannaCry (ransomware), que infectó más de 300.000 de ordenadores en 150 países, tuvo un impacto económico de más de 1.000 millones dólares en las empresas afectadas, según reporta la agencia McClathy citando a expertos de la compañía de seguridad informática KnowBe4. La valoración de los daños que sufrieron las organizaciones afectadas contabiliza tanto los directos, los producidos por la pérdida de información o la interrupción de actividades, como los indirectos, relacionados con daños en la reputación. (KnowBe4, 2017)

El virus se propagaba a través de vulnerabilidades existentes en ese sistema operativo, pero que Microsoft, la empresa responsable de Windows, publicó desde marzo un parche para subsanar ese problema. Pese a ello, muchos usuarios no aplicaron esa nueva protección. Según cifras de Avast, 18,4% de las computadoras que usan Windows en Argentina; 17,6% de las de Brasil y 14,71% de las de México no habían aplicado el parche antes de la aparición del WannaCry. En contraste, solo 6,8% de los ordenadores en EEUU permanecían sin actualizar. (ÁngelBermúdez, 2017)

Otros informes señalaron que México pasó del tercer sitio como la nación más infectada por el ataque de ransomware, WannaCry, al país con la mayor cantidad de infecciones registradas por dicho malware en América Latina, seguido por Brasil y en tercer lugar el Ecuador. (Kaspersky, 2017)

1.1.1.1 Tamaño de las empresas en el Ecuador

El tamaño de empresa se define de acuerdo con el volumen de ventas anuales (V) y el número de personas afiliadas (P) sea a nivel de plazas de empleo registrado o empleo registrado en la seguridad social. Para su determinación, prevalece el criterio de volumen de ventas anuales sobre el criterio de personal afiliado (CAN, 2009).

Grande

V: \$5'000.001 o más. P: 200 en adelante.

Mediana B

V: \$2'000.001 a \$5'000.000. P: 100 a 199.

Mediana A

V: \$1'000.001 a \$2'000.000. P: 50 a 99.

Pequeña

V: \$ \$100.001 a \$1'000.000. P: 10 a 49

Microempresa

V: menor o igual a \$100.000. P: 1 a 9

1.1.1.2 Estructura de las empresas según su tamaño (año 2018)

En el Ecuador existen un total de 899.208 empresas según su tamaño como se muestra en la figura 1-1, distribuida por todo el territorio ecuatoriano.

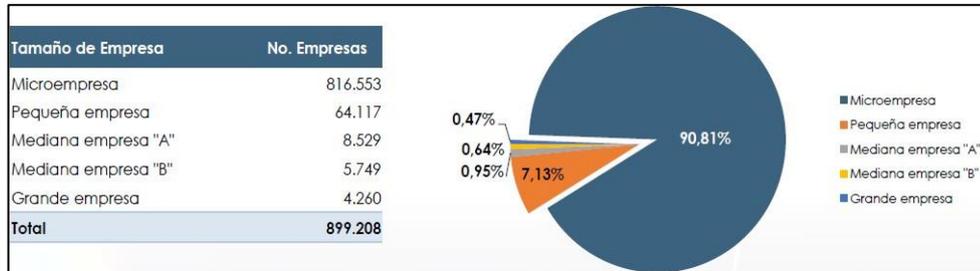


Figura 1-1 Clasificación de tamaño de empresa.

Fuente: INEC, 2018.

Sector Económico

Corresponde a un nivel agrupado de las actividades económicas (sección). La agregación permite simplificar la estructura sectorial de una economía (DIEE, 2019).

- Agricultura, ganadería, silvicultura y pesca.
- Explotación de minas y canteras.
- Industrias manufactureras.
- Comercio.
- Servicios.

1.1.1.3 Estructura de empresas según sector económico en el Ecuador

Las empresas existentes en el país se dedican a diferentes sectores económicos como los nombrados anteriormente, en la figura 1-2 se observa el número de empresas dedicadas a cada sector económico

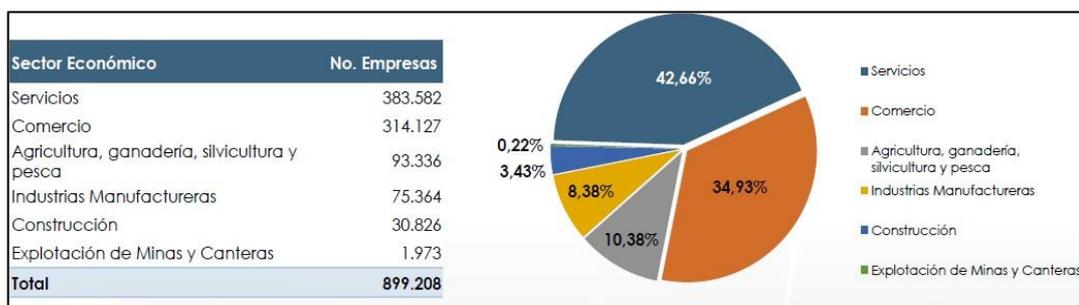


Figura 2-1 Clasificación de empresas según sector económico.

Fuente: INEC, Directorio de Empresas 2018.



Figura 3-1 Porcentaje de empresas según provincia del Ecuador.

Fuente: INEC, Directorio de Empresas 2018.

En la figura 1-3 se observa que la provincia de Chimborazo concentra un porcentaje de 3,18% del total de empresas existentes en todo el país, equivalente a 28594 empresas dedicadas a diferentes sectores económicos, distribuidos en todos los cantones, especialmente en el Cantón Guaranda.

1.1.1.4 Perfil económico del cantón Guaranda

Las principales actividades económicas practicadas en el cantón son:

Actividades productivas

- Fabricación de prendas de vestir
- Elaboración de productos de panadería

Actividades de comercio

- Venta al por menor de alimentos, bebidas y tabaco
- Venta al por menor de prendas de vestir, calzado y artículos de cuero

Servicios

- Actividades de restaurantes y de servicio móvil de comidas
- Otras actividades de telecomunicaciones (INEC, 2011)



Figura 4-1 Perfil económico del cantón Guaranda

Fuente: INEC 2011.

Tabla 1-1 Ingreso de sectores en dólares

INGRESOS GENERADOS EN EL CANTÓN GUARANDA	
INGRESOS DEL SECTOR	DOLARES
Manufactura	USD 105 millones
Comercio	USD 464 millones
Servicios	USD 637 millones
Otros	USD 1.9 millones

Fuente: INEC 2011.

Realizado por: Peña, Jorge, 2023



Figura 5-1 Principales industrias en el Cantón Guaranda.

Fuente: INEC 2011.

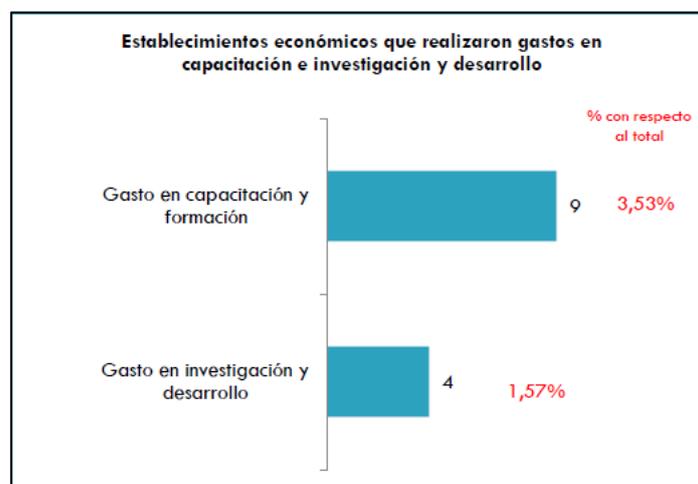


Figura 6-1 Gastos en capacitación e investigación en el Cantón Guaranda.

Fuente: INEC 2011.

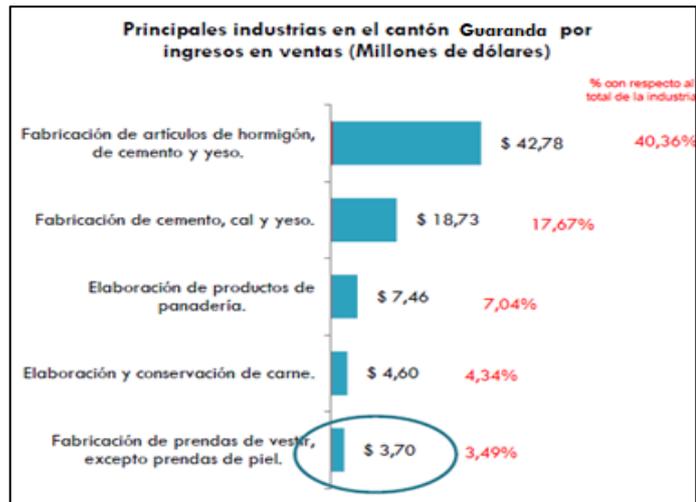


Figura 7-1 Principales industrias en el Cantón Guaranda.

Fuente: INEC 2011.

1.1.2 *Formulación del problema*

¿Cómo se mantendrá la confidencialidad, integridad y autenticación de la información digital de las pequeñas y medianas empresas del cantón Guaranda?

1.1.3 *Sistematización del problema*

¿Los algoritmos de cifrado permiten obtener una mayor seguridad de la información?

¿La aplicación de una VPN permiten a las empresas tener accesos seguros a la información interna de manera segura?

¿Cuál es el estado de las normativas y regulaciones que ha desarrollado el país para fortalecer la seguridad perimetral mediante la protección de corta fuegos de próxima generación en las empresas?

1.2 **Justificación de la investigación**

Los firewalls son una herramienta de seguridad estándar para la mayoría de las compañías, pero en un contexto actual de amenazas en permanente cambio, los firewalls de próxima generación son aquellos que pueden ofrecer una protección segura. La aplicación de una tecnología adecuada para el acceso seguro a la red empresarial, contribuye a obtener una mayor seguridad de la información mediante el análisis de los algoritmos de cifrado que poseen las VPN que generan los firewalls, frente a las vulnerabilidades existentes.

Según un estudio realizado, se desarrolló un análisis ecométrico multifactorial para determinar el impacto a nivel de Ecuador del empleo generado por las pequeñas y medianas empresas, generó un impacto del 66,8 % de incremento en el promedio de empleo en el país. (Rafael Eduardo RON Amores, 2017). Los índices antes señalados muestran el papel fundamental que representan las Pymes en la economía nacional, por lo tanto, es imperioso realizar este tipo de análisis sobre la seguridad perimetral de dicho segmento empresarial, ya que actualmente no existe estadísticas de cómo están protegiendo su información las pequeñas y medianas empresas.

Se realizó un diseño tipo, de seguridad perimetral con equipo corta fuego de próxima generación NGFW que sea aplicable para las pequeñas y medianas empresas, mejorando la seguridad de la información, además se solucionarán brechas de seguridad existentes, posibles robos de datos o información confidencial, además se tendría un mejor control del acceso y manejo de los datos que circula por la red empresarial.

1.3 Objetivos de la investigación

1.3.1 *Objetivo General*

Realizar una propuesta de un sistema de seguridad perimetral con firewall de próxima generación para pequeñas y medianas empresas del cantón Guaranda.

1.3.2 *Objetivos Específicos*

- Analizar los estándares y normativas existentes para el aseguramiento de la información de las pequeñas y medianas empresas en Ecuador.
- Analizar los algoritmos de cifrado DES, Triple DES, AES 128(bits), AES 192(bits) y AES 256(bits), utilizados para el acceso seguro VPN en una red empresarial.
- Definir un escenario de pruebas tipo laboratorio con un equipo que posea funciones de seguridad y corta fuegos para comprobar el diseño y hacer una evaluación del mismo, mediante una estructura de aplicabilidad.

1.4 Hipótesis

El análisis de los algoritmos de cifrado de una VPN generada por un Firewall de próxima generación, permitirá determinar una tecnología adecuada para el acceso seguro a la red de las PYMES.

CAPÍTULO II

2. MARCO TEORICO

2.1 Antecedentes

Durante el año 2017, casi un millón de pymes a nivel mundial fueron víctimas de un ciberataque. Esto no es ninguna sorpresa porque, al igual que las grandes corporaciones, las pymes mantienen datos de clientes, propiedad intelectual y otros activos valiosos. Por lo tanto, son objetivos igualmente válidos y útiles para los delincuentes. (Sepulveda, 2018)

Cuando analizamos fallos de seguridad en las pequeñas empresas, solemos encontrar que hay errores que suelen repetirse en muchos negocios. Estos suelen ser la causa de mayor número de incidencias informáticas en la empresa y consecuencia de una mala previsión en el departamento de informática, si lo hay. (Julia, 2017)

La ciberseguridad es un asunto prioritario para la comisión Europea. No solo aparece como uno de los pilares de los programas marco de I+D de la Unión Europea (UE), sino que ha pasado a la agenda de los políticos comunitarios y de los Estados miembros. Esta estrategia ha sido adoptada conjuntamente por la Comisión y el Alto Representante. Describe la visión de la UE en este ámbito, clarifica roles y responsabilidades y propone actividades específicas en el ámbito europeo. Su objetivo es asegurar una protección fuerte y efectiva y la promoción de los derechos de los ciudadanos, para hacer del entorno online de la UE el más seguro del mundo. (Juan, 2019)

Así mismo (ElevenPaths, 2019) señala que dentro de la amplia gama de ciberdelincuentes que existe, sabemos que abunda una motivación que va más allá del dinero o perjuicio que puedan causar. Se trata de la fama o el reconocimiento que obtienen con el ataque o hackeo. Es decir, algo así como el “enaltecimiento” de su ego.

Las grandes empresas son conscientes de los riesgos existentes en materia de ciberseguridad. Por ello, son muchas las que han incrementado la inversión en la implementación de medidas de protección. Sin embargo, cuando hablamos de PYMEs, nos enfrentamos a una situación diferente, los ataques dirigidos a este segmento empresarial son mayoritarios y van en aumento. Según un estudio de Kaspersky Lab y Ponemon Institut, el 60 % de las pymes que sufren un ataque informático desaparece en los seis meses siguientes. (ElevenPaths, 2019)

Así mismo (ElevenPaths, 2019) señala que el correo electrónico es la principal puerta de ataque con una cifra del 76 %, la navegación web es el segundo canal de ataque preferido por los ciberdelincuentes.

En cifras globales INCIBE gestionó en 2018 más de 111.000 ciberataques contra ciudadanos, empresas y operadores de servicios esenciales. La motivación económica es la que está detrás de más de la mitad de estos ataques. El director general del INCIBE, Alberto Hernández, durante la presentación del estudio de Google, advirtió que “un ataque masivo (que afecte a pymes) puede bloquear gran parte del tejido productivo de un país”, teniendo en cuenta que las pequeñas y medianas empresas, con menos de 250 empleados, suponen el 99,8% del sector empresarial de España. (INCIBE, 2018).

Así mismo (Llumiquinga, 2019) indica que, de todos los sectores de la economía ecuatoriana, la banca es la que mayor capacidad y recursos tiene para responder ante amenazas cibernéticas, sin embargo, es preocupante que sectores como pymes y salud aún sean vulnerables a los ataques de delincuentes informáticos.

En términos generales, las amenazas que más preocupan al sector empresarial son aquellas de origen humano, errores no intencionados y ataques, las cuales pueden llevar a comprometer información estratégica de las organizaciones o incluso poner en riesgo los datos personales y financieros de los clientes. La pérdida de información sensible afecta a las organizaciones y se traduce en la pérdida de ventaja competitiva, asegura Gabriel Llumiquinga, presidente de la AECI, Asociación Ecuatoriana de Ciberseguridad. (Llumiquinga, 2019)

2.2 Metodología

La metodología implementada propone una mejora en la seguridad perimetral en las redes de datos de las pequeñas y medianas empresas, para ello se realizaron pruebas con un equipo que posee funciones de seguridad y firewall, en la cual se aplicaron los conceptos que se están proponiendo en el presente documento.

Primer paso se analizó la normativa existente referente a la seguridad perimetral para pymes o conceptos que puedan estar relacionados.

Segundo paso se recopiló información con enfoque metodológico cualitativo, investigación de escritorio y campo de varios documentos con respecto a la seguridad perimetral para pequeñas y medianas empresas.

Tercer paso se diseñó y posteriormente se definió un escenario de pruebas tipo laboratorio con un equipo que posea funciones de seguridad y firewall.

Cuarto paso se implementó y se evaluó el sistema mediante una estructura de aplicabilidad.

2.2.1 Ventajas

- El implementar un corta fuegos para Pymes es una solución económica y segura, además facilita la administración del responsable de seguridad informática.
- Los firewalls de próxima generación permiten disminuir de forma significativa los riesgos que los firewalls de gestión unificada de amenazas UTM no pueden resolver eficazmente.
- En un entorno tecnológico en constante cambio, al implementar SPI (inspección de paquetes con estado) para Pymes la misma se vuelve flexible, altamente confiable y accesible, adaptándose de forma rentable al crecimiento empresarial.
- Permiten actualizar el firmware, para corregir errores, realiza mejoras a su funcionalidad, aumentando el rendimiento de la red sin tener que comprar ningún hardware nuevo.
- Tanto los corta fuegos NGFW y UTM permiten actualizar el firmware, pero depende de cómo los fabricantes vendan el producto, algunos cobran el soporte de forma anual como el caso de Fortinet, pero el equipo cisco utilizado lo permite gratuitamente.

2.2.2 Desventajas

- En el Ecuador existe escasos de profesionales en seguridad telemática, además el desconocimiento de cómo dar seguridad informática por parte de los responsables de la red empresarial, es una vulnerabilidad que los ciberdelincuentes pueden explotar.
- Las pequeñas y medianas empresas, tienen recursos limitados, el no invertir en seguridad informática empresarial o la insuficiente inversión, pone en riesgo el principal activo de la empresa que es la información.
- Las soluciones de las grandes empresas que ofertan servicio de seguridad informáticas para las Pymes son muy costosas, que pueden ir desde unos 5.000 dólares a más de 20.000 dólares anuales, dependiendo del requerimiento de servicios y de la capacidad de tráfico que circula por la red empresarial.
- El invertir un presupuesto adicional en seguridad informática en las pequeñas y medianas empresas, no necesariamente se refleja en una mayor capacidad de seguridad, también depende de la capacitación y experiencia del personal de tecnologías de la información (TI). Por ello los recursos económicos deben ser manejados y optimizados correctamente.

- Pueden aparecer nuevas herramientas matemáticas más sofisticadas que debiliten sustancialmente los algoritmos de cifrado, previamente considerados inmunes a ataques.
- Al utilizar un algoritmo de cifrado demasiado robusto existe el inconveniente de retrasos al transmitir y recibir información en una red privada virtual (VPN), ya que el equipo firewall está realizando el proceso de cifrado, pero va depender de la cantidad de información que se esté transmitiendo y de la capacidad del equipo.

2.3 Firewall de próxima generación NGFW

Desarrollado con la motivación de resolver la deficiencia de desempeño presentada en los UTM, entregando recursos de control de aplicación e inspección profunda de paquetes en una arquitectura altamente performática y cohesiva. Recursos complementarios como proxy web, protección contra virus, malware y otros, presentes en Firewall UTM, no forman parte de la arquitectura de un NGFW, estas características fueron removidas y tercerizadas, garantizando altas tasas de escalabilidad para grandes ambientes. (OSTEC, 2019)

Así mismo (OSTEC, 2019) indica que la principal contribución del NGFW está en los avances tecnológicos generados a partir de la inspección profunda de paquetes y en la visibilidad de aplicaciones, independientemente de protocolos y puertos. Estos recursos, en conjunto, no sólo permiten evitar ataques, sino que principalmente crean políticas de control de acceso más dinámicas y eficientes para los desafíos actuales de seguridad.

Un Firewall de nueva generación es un dispositivo de red que integra múltiples funcionalidades de seguridad en una única plataforma, de modo que se simplifican la administración de políticas, se eliminan puntos de fallo, latencias y cuellos de botella incensarios, incrementando la seguridad (Secure_it, 2018). Estos cortafuegos integran muchas opciones avanzadas, como son:

- Estar al tanto de cuáles son los activos que corren mayor riesgo con reconocimiento del contexto completo.
- Reaccionar rápidamente ante los ataques con automatización de seguridad inteligente que establece políticas y fortalece las defensas en forma dinámica.
- Detectar actividad sospechosa o evasiva con correlación de eventos de terminales y red.
- Reducir significativamente el tiempo necesario desde la detección hasta la eliminación de la amenaza con seguridad retrospectiva que monitorea continuamente la presencia de actividad y comportamiento sospechosos, incluso después de la inspección inicial.

- Facilitar la administración y reducir la complejidad con políticas unificadas que brindan protección en toda la secuencia del ataque.
- Este tipo de cortafuegos según cisco proporciona de forma exclusiva protección avanzada contra amenazas antes, durante y después de los ataques.

2.3.1 Diferencias entre Cortafuego UTM y Cortafuego NGFW

UTM es el acrónimo de Unified Threat Management o lo que es lo mismo Gestión Centralizada de Amenazas. El término nació en el año 2004 y fue acuñado por la consultora IDC pretendiendo englobar una serie de funcionalidades de seguridad que permitían en un único equipo cubrir la mayoría de necesidades que una red podía presentar. Firewall, VPN, IPS, Antivirus, Web Filtering, Control de Aplicaciones, Email Security y DLP (Data Leak Prevention) en un único equipo. (Martínez, 2017)

Así mismo (Martínez, 2017) dos titanes del mundo de la ciberseguridad crearon un "nuevo" paradigma en el ámbito de soluciones de seguridad de red, los Next Generation Firewall (NGFW). En 2011 Gartner y Palo Alto Networks dieron paso a este término para definir firewalls con capacidad de DPI (Deep Packet Inspection) que les permitía añadir funcionalidades de IPS y control de tráfico en capa 7 a los firewalls tradicionales.

La principal diferencia entre ambas tecnologías es que los firewalls NGFW tienen una orientación de diseño de llevar la seguridad a nivel de aplicación, mientras que los UTM más tradicionales tratan de hacer de todo un poco. Si se espera que los UTM hagan funciones de protección de aplicaciones, se debe utilizar funciones de IPS y tener experiencia en su configuración como, por ejemplo:

- Palo Alto comercialmente los firewalls NGFW son definidos como los de próxima generación, mientras que a los UTM los define como una solución antigua.
- Forcepoint para su firewall también ha adoptado el término NGFW para las soluciones de seguridad de red, dejando de lado las referencias a los firewalls UTM.
- Checkpoint ha eliminado cualquier referencia del término UTM a su catálogo de soluciones. Ahora sus soluciones se definen como Next generation firewall.

2.4 Cuadrante mágico de Garther

El grupo Garther es una empresa consultora y de investigación del mercado de las nuevas tecnologías dedicada exclusivamente a investigar y analizar las tendencias del mercado.

Del cuadrante mágico de Garther se desprenden conclusiones y se elabora un ranking de los fabricantes con mejores soluciones y productos. Los resultados son presentados bajo el nombre de “cuadrante mágico de Garther”. (TIC, 2016)

Así mismo (TIC, 2016) indica que el gráfico está formado por dos ejes, el eje X y el eje Y:

- En el eje X, Garther define la categoría “integridad de visión” y representa el conocimiento de los proveedores sobre cómo se puede aprovechar el momento actual del mercado para generar valor, tanto para sus clientes como para ellos mismos.
- En el eje Y se encuentra la “capacidad de ejecutar”, donde mide la habilidad de los proveedores para ejecutar con éxito su particular visión del mercado.

Ambas visiones fragmentan el cuadrante de Garther en cuatro sectores. Ahí es donde se plasman las principales compañías de cada competencia en función de su tipología y productos: líderes (leaders), retadores o aspirantes (challengers), visionarios (visionaries) y jugadores de nicho (niche players). En la imagen se muestran más características y representativa del popular cuadrante mágico de Garther. (TIC, 2016).

2.4.1 Novedades en el Cuadrante Gartner 2017 para los Cortafuegos de Redes Empresariales

Líder

Palo Alto y Checkpoint, ésta vez acompañados de Fortinet. Gartner considera que «el Firewall empresarial FortiGate es la única solución que ofrece el escalamiento, automatización y desempeño necesarios para proteger desde el perímetro hasta el centro de datos y desde el IoT hasta la nube». Además, señala que cuando las empresas evalúan productos de seguridad, suele ser uno de los elegidos por su relación precio y rendimiento.

Aspirantes

El gigante asiático Huawei sigue adelante y escala hasta esta nueva posición. Algo que destaca Gartner son los equipos de alto rendimiento para grandes centros de datos. Considera además que debe seguir trabajando para penetrar en el mercado EEUU y Latinoamericano.

Visionarios

Forcepoint pasa de ser un jugador de nicho en 2016 a visionario en 2017, obteniendo además mejor puntuación en capacidad de ejecución que su competidor Sophos.

Sophos también pasa a ocupar la posición de jugador de nicho a visionario. Gartner destaca Security Heartbeat como una ambiciosa estrategia de seguridad que une el firewall y el endpoint.

Sophos es la única empresa de seguridad informática que se posiciona como visionaria en el Enterprise Firewall 2017, líder en la gestión unificada de amenazas (UTM) 2017 y líder en plataformas de Endpoint Protection (EPP) 2017. (Tecnozero, 2017)



Figura 1-2 Cuadrante mágico de Gartner 2017.

Fuente: SIAG Consulting, 2017.

2.4.2 Novedades en el Cuadrante Gartner 2018 para los Firewalls de Redes Empresariales

El Cuadrante Mágico de Gartner evalúa a los proveedores en función de su integridad de la visión y su capacidad de ejecución.

Los productos que aparecen en este cuadrante mágico han sido diseñados para proteger el perímetro de grandes redes empresariales.

Utilizados en despliegues en redes LAN sencillas y múltiples ubicaciones distribuidas. Añaden capacidades de VPN, análisis tráfico cifrado (TLS), integración con los principales servicios en la nube (AWS y Microsoft Azure), etc. (Tecnozero, 2018)

Jugadores de nicho

Aquí se engloban los pequeños proveedores de firewalls. Su mercado principal está más enfocados en las pymes y pretenden hacerse un hueco en el segmento Enterprise.

Los 10 seleccionados son Sophos (que en 2017 fue visionario), Juniper Networks, Barracuda, Sangfor, Hillstone, WatchGuard, SonicWall, AhnLab, Stormshield y New H3C Group.

Líderes

Estos proveedores incluyen funcionalidades avanzadas para proteger a los clientes de amenazas emergentes. Son expertos en su sector y destacan por la seguridad de sus productos. Para 2018, los 4 líderes son Palo Alto Networks, Fortinet, Check Point Software Technologies y Cisco (que el año anterior fue retador).

Cisco

Destaca por su capacidad de ejecución, con su equipo de inteligencia de amenazas centralizado (Cisco Talos) tiene una oferta muy diferenciada de la competencia. Check Point posee una gran capacidad para gestionar la seguridad de múltiples dominios. Fortinet es una apuesta segura por sus funcionalidades avanzadas en el correo electrónico seguro, firewall de aplicaciones web y su mejora continua. Palo Alto recibe una mención por su capacidad para descifrar conexiones TLS concurrentes.



Figura 2-2 Cuadrante mágico de Gartner 2018.

Fuente: SIAG Consulting, 2018.

2.4.3 Novedades en el Cuadrante Gartner 2019 para los Firewalls de Redes Empresariales

Cisco se destaca como uno de los Líderes en el Cuadrante Mágico de Gartner por su inteligencia en amenazas de primer nivel. Firewall de próxima generación (NGFW) marca Cisco, analiza constantemente los datos de amenazas y crea protecciones de seguridad para proteger automáticamente a las organizaciones de las amenazas conocidas, desconocidas y emergentes. Como resultado de la gran capacidad los clientes de Cisco NGFW estuvieron protegidos de los ataques conocidos, como WannaCry, NotPetya y VPNFilter. (CiscoLatinoamerica, 2018).



Figura 3-2 Cuadrante mágico de Gartner 2019.

Fuente: SIAG Consulting, 2019.

Los firewalls Cisco NGFW trascienden la prevención y brinda una mayor visibilidad de la telemetría y posibles actividades de archivo maliciosas entre los usuarios, los hosts, las redes y la infraestructura. Esto permite detectar rápidamente actividad maliciosa y eliminarla antes que pueda causar algún daño. (CiscoLatinoamerica, 2018). El firewall empresarial es uno de los mercados más maduros en el sector de la seguridad, resulta recomendable la actualización de las soluciones cada 4 o 5 años. (Tecnozero, 2018)

2.5 Selección de una marca de Firewall para la implementación de un escenario de pruebas

Para la selección de una marca de firewall se hizo un análisis de los principales fabricantes a nivel mundial, según lo indica el cuadrante mágico de Gartner 2019 para los firewalls de redes empresariales, en la cual se destacan 4 líderes que son Palo Alto Networks, Fortinet, Check Point Software Technologies y Cisco, se ha establecido la siguiente estimación:

Tabla 1-2 Ingreso de sectores en dólares

CATEGORÍA	ESTIMACIÓN (puntos)
Malo	1
Bueno	2
Muy Bueno	3
Excelente	4

Fuente: Jorge Peña, 2023

En la tabla 2-2 Palo Alto Networks al igual que Cisco se destacan por el soporte, la posición en el cuadrante mágico de Gartner 2019, así como también en la facilidad de configuración de sus equipos firewalls empresariales, por ello se ha establecido un puntaje en la que Palo Alto Networks tiene 18 puntos y Cisco 19 puntos (sobre un total de 20 puntos), analizando las características y posicionamiento nivel mundial de los equipos de los fabricantes antes mencionados, por lo tanto se escogió la marca Cisco por el soporte que da a sus clientes, la experiencia de haber manejado equipos de la misma marca y por ser de más fácil acceso en el mercado del Ecuador.

Tabla 2-2 Elección de la marca de Firewall para Pymes.

ELECCIÓN DE LA MARCA DE FIREWALL PARA PYMES						
	Precio	Soporte	Posición Cuadrante mágico de Gartner 2019	Facilidad de Configuración	Facilidad de Acceso en el mercado del Ecuador	Sub Total
Palo Alto Networks	3	4	4	4	3	18
Fortinet	3	4	4	3	3	17
Check Point	3	3	4	3	3	16
Cisco	3	4	4	4	4	19

Fuente: Jorge Peña, 2023

2.6 Normas y estándares internacionales para el aseguramiento de la información en las pequeñas y medianas empresas.

La norma ISO/IEC 27033 proporciona una guía detallada sobre los aspectos de seguridad de la gestión, operación y uso de redes de sistemas de información y sus interconexiones. Esos individuos dentro de una organización responsable de la seguridad de la información en general y de la seguridad de la red en particular, deberían poder adaptar el material de esta norma internacional para cumplir con sus requisitos específicos. (ISO, 2015)

2.6.1 ISO / IEC 27033

ISO / IEC 27033 es un estándar de varias partes derivado del existente ISO / IEC 18028 de cinco partes. El estándar de seguridad de la red se revisó sustancialmente. (ISO27001, 2013).

El propósito de la ISO / IEC 27033 es proporcionar una guía detallada sobre los aspectos de seguridad de la administración, operación y uso de las redes de sistemas de información y sus interconexiones. ISO / IEC 27033 proporciona una guía detallada sobre la implementación de los controles de seguridad de la red que se introducen en la ISO / IEC 27002. Se utiliza para la seguridad de los dispositivos en red y la gestión de su seguridad, aplicaciones y servicios de red, así como también usuarios de red.

2.6.2 ISO / IEC 27033-1: 2015

Visión general y conceptos de seguridad de red.

- Proporciona una hoja de ruta y una visión general de los conceptos y principios que sustentan las partes restantes de ISO / IEC 27033;
- Objetivo: "definir y describir los conceptos asociados con la seguridad de la red y proporcionar orientación de gestión sobre la misma. Esto incluye la provisión de una descripción general de la seguridad de la red y las definiciones relacionadas, y orientación sobre cómo identificar y analizar los riesgos de seguridad de la red y luego definir los requisitos de seguridad de la red. También presenta cómo lograr arquitecturas de seguridad técnica de buena calidad, y los aspectos de riesgo, diseño y control asociados con escenarios de red típicos y áreas de tecnología de red. (ISO27033, 2015)
- Proporciona un glosario de términos de seguridad de la información específicos de las redes.
- Proporciona orientación sobre un proceso estructurado para identificar y analizar los riesgos de seguridad de la red y, por lo tanto, definir los requisitos de control de seguridad de la red, incluidos los exigidos por las políticas de seguridad de la información relevantes.
- Proporciona una descripción general de los controles que soportan las arquitecturas de seguridad técnica de la red y los controles técnicos relacionados, así como los controles no técnicos y otros controles técnicos que no están relacionados únicamente con la seguridad de la red.
- Explica las buenas prácticas con respecto a las arquitecturas técnicas de seguridad de la red, y los aspectos de riesgo, diseño y control asociados con los escenarios típicos de la red y las áreas de tecnología de la red.
- Aborda brevemente los problemas asociados con la implementación y el funcionamiento de los controles de seguridad de la red, y el monitoreo y revisión continuos de su implementación;

- Extiende las directrices de gestión de seguridad previstas en la norma ISO / IEC TR 13335 y ISO / IEC 27002, al detallar las operaciones y mecanismos específicos necesarios para implementar controles de seguridad de red en una gama más amplia de entornos de red, proporcionando un puente entre los problemas generales de gestión de seguridad de la información y los detalles específicos de la implementación de controles de seguridad de red en gran medida técnicos (ejemplo , IDS / IPS, , firewalls, mensajes controles de integridad).
- Menciona requisitos tales como no repudio y confiabilidad, además de la clásica tríada de la CIA (confidencialidad, integridad y disponibilidad); (ISO27033, 2015)

2.6.3 *ISO / IEC 27033-2: 2012: Directrices para el diseño e implementación de seguridad de red.*

- Alcance: planificación, diseño, implementación y documentación de la seguridad de red.
- Objetivo: definir cómo las organizaciones deben lograr arquitecturas, diseños e implementaciones de seguridad técnica de red de calidad que garanticen la seguridad de la red adecuada a sus entornos empresariales, utilizando un enfoque coherente para la planificación, diseño e implementación de la seguridad de la red, según sea relevante con la ayuda del uso de modelos / marcos. (En este contexto, se usa un modelo / marco para delinear una representación o descripción que muestra la estructura y el funcionamiento de alto nivel de un tipo de arquitectura / diseño de seguridad técnica). (ISO27033, 2015)
- Define una arquitectura de seguridad de red para proporcionar seguridad de red de extremo a extremo. La arquitectura se puede aplicar a varios tipos de redes donde la seguridad de extremo a extremo es una preocupación e independientemente de la tecnología subyacente de la red;
- Sirve como base para recomendaciones de seguridad de red de extremo a extremo.
- Cubre riesgos, diseño, técnicas y problemas de control. (ISO27033, 2015)

2.6.4 *ISO / IEC 27033-3: 2010: Escenarios de redes de referencia: amenazas, técnicas de diseño y problemas de control.*

- El objetivo es definir los riesgos específicos, las técnicas de diseño y los problemas de control asociados con los escenarios de red típicos.
- Discute amenazas, específicamente, en lugar de todos los elementos de riesgo.
- Se refiere a otras partes de ISO / IEC 27033 para una orientación más específica. (ISO27033, 2015)

2.6.5 ISO / IEC 27033-4: 2014

Asegurar las comunicaciones entre redes utilizando pasarelas de seguridad.

- Proporciona una descripción general de las puertas de enlace de seguridad a través de una descripción de diferentes arquitecturas.
- Pauta de asegurar las comunicaciones entre las redes a través de pasarelas, cortafuegos, servidores de seguridad de aplicaciones, sistemas de protección contra intrusiones, de acuerdo con una política, que incluye identificar y analizar las amenazas de seguridad de la red, definir los requisitos de control de seguridad y diseñar, implementar, operar, monitorear y revisar los controles.
- Describe cómo las puertas de enlace de seguridad analizan y controlan el tráfico de red mediante:
 - Filtrado de paquetes.
 - Inspección de paquetes con estado.
 - Proxy de aplicación (firewalls de aplicación).
 - Traducción de direcciones de red NAT.
 - Análisis de contenido y filtrado.
 - Guía la selección y configuración de puertas de enlace de seguridad, eligiendo el tipo correcto de arquitectura para una puerta de enlace de seguridad que mejor cumpla con los requisitos de seguridad.
 - Se refiere a varios firewalls como ejemplos de puertas de enlace de seguridad. (ISO27033, 2015).

2.6.6 ISO / IEC 27033-5: 2013

Asegurando las comunicaciones a través de redes usando Redes Privadas Virtuales (VPN)

- Objetivo: proporcionar pautas para la selección, implementación y monitoreo de los controles técnicos necesarios para proporcionar seguridad de red utilizando conexiones de VPN para interconectar redes y conectar usuarios remotos a redes.
- Extiende las pautas de gestión de seguridad de TI de ISO / IEC TR 13335 al detallar las operaciones y mecanismos específicos necesarios para implementar salvaguardas y controles de seguridad de red en una gama más amplia de entornos de red, proporcionando un puente entre los problemas generales de gestión de seguridad de TI y las implementaciones técnicas de seguridad de red.
- Proporciona orientación para asegurar el acceso remoto a través de redes públicas.

- Brinda una evaluación incompleta de alto nivel de las amenazas a las VPN (es decir, menciona las amenazas de intrusión y denegación de servicio, pero no la supervisión / interceptación no autorizada, análisis de tráfico, corrupción de datos, inserción de tráfico falso, varios ataques en puntos finales de VPN, malware, enmascaramiento / robo de identidad, amenazas internas).
- Presenta diferentes tipos de acceso remoto, incluidos protocolos, problemas de autenticación y soporte al configurar el acceso remoto de forma segura.
- Destinado a ayudar a los administradores y técnicos de red que planean hacer uso de este tipo de conexión o que ya lo tienen en uso y necesitan asesoramiento sobre cómo configurarlo y operarlo de manera segura. (ISO27033, 2015)

2.6.7 ISO / IEC 27033-6: 2016

Asegurando el acceso a la red IP inalámbrica.

- Objetivo: definir los riesgos específicos, las técnicas de diseño y los problemas de control para proteger las redes inalámbricas IP. Es relevante para todo el personal involucrado en la planificación detallada, el diseño y la implementación de seguridad para redes inalámbricas.
- Este es un estándar de seguridad de red inalámbrica genérico que ofrece consejos básicos para WiFi, Bluetooth, 3G y otras redes inalámbricas.
- El estándar enumera una serie de "amenazas" que son, de hecho, modos de ataque, escenarios o riesgos. Hubiera sido una lista más útil si la norma abordara sistemáticamente cada uno de ellos.
- El estándar utiliza el término red de cable, comúnmente conocida como red cableada.
- El estándar se refiere repetidamente a "red de acceso", un término curioso que no está definido (aparte de Radio Access Network).
- El estándar indica que el cifrado es un control de integridad, mientras que normalmente otros controles y protocolos criptográficos proporcionan las funciones de confidencialidad. (ISO27033, 2015)

2.6.8 OEA (Organización de Estados Americanos) y Microsoft

La OEA y Microsoft lanzaron el reporte "Protección a infraestructura crítica en Latinoamérica y el Caribe 2018", el cual hace recomendaciones para desarrollar un marco de trabajo o política de infraestructura crítica adecuada en la región. (OAS, 2018).

Algunas de las prácticas recomendadas en el informe incluyen:

- Asegurar una división clara de responsabilidades.
- Establecer referencias de seguridad.
- Desarrollar mecanismos de alerta temprana.
- Invertir en recursos humanos y técnicos.
- Mejorar la resistencia cibernética.
- Participar en redes internacionales para entender el paisaje de amenazas.

De acuerdo con (OAS, 2018) indica que el reporte es el resultado de los esfuerzos entre la OEA y Microsoft para así promover en la región la investigación y respuesta a incidentes cibernéticos, y refleja lo que en la actualidad se lleva a cabo para limitar la vulnerabilidad de infraestructura crítica contra ataques cibernéticos a través de la región. Asimismo, el documento sugiere que, aunque existe una colaboración entre el sector público y privado, y una creciente conciencia referente a los problemas de ciberseguridad, aún se puede hacer más para proteger los recursos vitales. **La infraestructura crítica incluye servicios que son esenciales para el buen funcionamiento de una sociedad, como servicios financieros, energía, comunicaciones y suministro de agua.**

2.6.9 Normativas y estándares en el Ecuador de seguridad de la información en las pymes

En el Ecuador no hay una normativa específica para Pymes referente a la seguridad informática, lo que existen son normativas y regulaciones de manera general que ayudan a mejorar un poco la seguridad de las redes de datos empresariales y son las siguientes:

2.6.9.1 Acuerdo Ministerial 166 - EGSi (Esquema Gubernamental de Seguridad de la Información).

Desarrollado por la Secretaría Nacional de la Administración Pública en el 2013. Este acuerdo fue elaborado en la base a la norma NTE INEN-ISO/IEC 27002 “Código de Práctica para la Gestión de la Seguridad de la Información”. Entre los objetivos de este acuerdo destacamos:

- Mantener la seguridad en la información en diferentes medios y formatos de las entidades de la Administración Pública Central, que dependen de la Función Ejecutiva.
- Minimizar los riesgos a los que está expuesta la información.
- Proteger la infraestructura gubernamental de los ciberataques.

- Se dispuso en todas las entidades públicas el uso obligatorio de este acuerdo, por lo cual se garantiza que se implementen adecuados niveles de seguridad en los sistemas de información utilizados por el sector público. (EGSI, 2013)

2.6.9.2 *Creación del Comando Conjunto de Ciberdefensa*

Se crea con Acuerdo Ministerial 281 en septiembre del 2014, siendo un ente que debe implementar la capacidad de ciberdefensa bajo el Comando Conjunto de las Fuerzas Armadas. Es el responsable de proteger la infraestructura crítica del Estado en el ámbito digital y tecnológico, con prioridad a las Fuerzas Armadas y minimizar o bloquear los sistemas de información del enemigo a fin de contribuir a la defensa de la soberanía nacional. (Aguirre, 2017)

2.6.9.3 *Creación del EcuCERT*

Es el Centro de Respuestas a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador. Su compromiso radica en contribuir a la seguridad de las redes de telecomunicaciones de todo el país y así como del uso de la red de internet. (ecucert, 2018).

Su objetivo principal es la coordinación nacional e internacional de labores técnicas destinadas a lograr usos más seguros de las mencionadas redes, en las que se encuentran incluidos a los prestadores de servicios de telecomunicaciones del país, con esto lograr masificar el uso de internet, las tecnologías de la información y los sistemas de telecomunicaciones en el Ecuador.

Algunos de los propósitos del EcuCERT son:

- Prevenir los delitos mediante reportes de vulnerabilidades encontradas en las redes, para que los prestadores de servicios de internet adopten las medidas necesarias para evitar ser víctimas de los conocidos “hackeos”.
- Gestionar y notificar los reportes a las empresas prestadoras de servicios de telecomunicaciones.
- Ser el punto de contacto entre Ecuador y otros equipos de respuesta internacionales.
- Asesorar en el cumplimiento de la Normativa de Seguridad de la Información de aplicación vigente en el Ecuador.
- Promover la adopción de Políticas de Seguridad de la Información en las Instituciones públicas y el sector de las telecomunicaciones.
- Impulsar la conformación de un Comité de Ciberseguridad. (ecucert, 2018)

2.6.9.4 *Facturación electrónica en el Ecuador*

Según la Resolución NAC-DGERCGC17-00000430 Suplemento de Registro Oficial 59 de 17 de agosto de 2017, emitida por el Servicio de Rentas internas del Ecuador, la cual ya se encuentra vigente a partir del 1 de enero del 2018, existe un grupo de pequeñas y medianas empresas, las cuales se encuentran obligadas a emitir comprobantes de venta, comprobantes de retención y documentos complementarios, de manera electrónica a partir del 1 de enero del 2019.

Artículo primero, literal c) indica: Personas naturales y sociedades cuyos ingresos anuales del ejercicio fiscal anterior sean iguales o superiores al monto contemplado para pequeñas y medianas empresas, en el Reglamento a la Estructura e Institucionalidad de Desarrollo Productivo de la Inversión y de los mecanismos e instrumentos de fomento productivo, establecidos en el Código Orgánico de la Producción, Comercio e Inversiones.

En la única disposición transitoria de esta Resolución, se indica que la obligatoriedad a emitir comprobantes de venta, comprobantes de retención y documentos complementarios, de manera electrónica, será a partir del 1 de enero del 2019.

2.7 **Descripción de palabras**

2.7.1 *Mintel*

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) contribuye a la seguridad de las redes de telecomunicaciones, a través de la coordinación nacional e internacional de labores técnicas destinadas a lograr usos más seguros de estas redes, en las que se incluyen a los prestadores de servicios de telecomunicaciones del país. (MINTEL, 2019).

2.7.2 *ARCOTEL*

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) es un organismo estatal de Ecuador que administra, regula y controla las telecomunicaciones y el espacio radioeléctrico de dicho país.

También gestiona aspectos técnicos asociados al uso de frecuencias del espectro radioeléctrico y la operación de redes. ARCOTEL, dependiente del Ministerio de Telecomunicaciones y de la Sociedad de la Información, fue creado en 2015 y tiene su sede en la ciudad de Quito. (ARCOTEL, 2019).

2.7.3 Firewall

Un firewall es un dispositivo de seguridad que monitorea en tráfico de red entrante y saliente, si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. (Cisco, 2019).

2.7.4 Ciberseguridad

La recomendación UIT-T X.1205, ciberseguridad es la colección de herramientas, regulaciones, conceptos de seguridad, dispositivos de seguridad, guías, manejo de riesgos, acciones, entrenamiento, mejores prácticas, aseguramiento y tecnologías que pueden ser utilizadas para proteger el ciber entorno y los activos de los usuarios y de la organización. (kaspersky, 2019).

2.7.5 Interdependencias

Los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional. (BOE, 2011)

2.7.6 Seguridad perimetral

El perímetro no es más que una línea imaginaria que separa una empresa (computadoras, servidores, etc.) de otras redes (generalmente el internet). Y esta línea es llevada a cabo por un dispositivo que puede ofrecer la comunicación entre las redes, generalmente representada por un router o dispositivo con propósito similar, adjunta o secuencia de un dispositivo de seguridad, llamado firewall. (OSTEC, 2019)

2.7.7 Resiliencia

La resiliencia es una cualidad inherente a un organismo, entidad, empresa o estado que le permite hacer frente a una crisis sin que su actividad se vea afectada. (ENSA, 2018)

2.7.8 INCIBE (Instituto Nacional de Ciberseguridad de España)

Es el Instituto Nacional de Ciberseguridad de España, es una entidad consolidada para el desarrollo de la ciberseguridad y de confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Con una actividad basada en investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional. (INCIBE, 2018)

2.7.9 Cuadrante mágico de Garther

El cuadrante mágico de Garther es una herramienta para saber en qué punto de desarrollo están las empresas dedicadas a la tecnología en el mercado a nivel mundial. Se usa para saber su calidad de desempeño y sirve a las empresas para elegir el proveedor de tecnologías de la información (TI) que más les conviene. (ISC, 2019)

2.7.10 Criptografía

Es la técnica que permite proteger documentos y datos, en la cual se utilizan códigos para el cifrado de mensajes, de tal manera de transformar un mensaje en un texto cifrado mediante la aplicación de un algoritmo determinado.

2.8 Amenazas a la seguridad informática empresarial

El nivel de la complejidad de la amenaza no está relacionado directamente con la complejidad de la tecnología. Hay que esperar que las amenazas se hagan más innovadoras y sofisticadas. Se mejorará en localizar y explotar nuevas vulnerabilidades o antiguas sin corregir, para el robo masivo de datos, a pesar de las medidas existentes y la vigilancia. Además, los métodos de ingeniería social se harán más sutiles, y destinados a los usuarios de una manera más personalizada. (openlearning, 2016).

Para poder aplicar controles es necesario conocer las amenazas a la que está expuesta la red empresarial en las pymes.

2.8.1 Amenazas a los activos de la empresa

Existen amenazas comunes que pueden afectar a la red empresarial:

- Daños a la información personal, confidencial o sensible.
- Falta de disponibilidad por ataques de denegación de servicio.
- Daño a la imagen empresarial, por desinformación o difamación.

En el caso de un ciberataque a la red empresarial, se puede ver afectada la información personal de los empleados, clientes o proveedores, dañando la reputación de la empresa y afectando su normal funcionamiento.

2.8.2 Amenazas a los activos personales

Los activos personales se relacionan con la identidad y la información personal, de las cuáles se desprende posibles amenazas a activos de la información personal:

- Robo de datos personales para su uso fraudulento
- Chantaje para la no revelación de información comprometedora
- Robo de identidad digital
- Robo de datos financieros y de proveedores
- Robo de secretos industriales
- Localización geográfica
- Invasión a la privacidad

2.9 Agentes de amenazas

Un agente de amenaza es un individuo o grupo de individuos que tiene algún papel en la ejecución o apoyo de un ataque, ya sea por motivos políticos, religiosos o económicos. Las capacidades, conocimientos, financiación, etc. y las intenciones como diversión, crimen o espionaje, son fundamentales en el momento de evaluar las vulnerabilidades y riesgos, así como para el desarrollo e implementación de controles. Además, se debe tener en cuenta que pueden producirse pérdidas debido a fallos, funcionamiento incorrecto, negligencia o errores humanos. (openlearning, 2016)

Los agentes de amenazas se pueden clasificar en tres tipos:

- Amenazas externas
- Amenazas internas
- Amenazas mixtas

2.9.1 Amenazas externas

- Incidencias relacionadas con socios y agentes
- Capacitación de los empleados referente a las nuevas tecnologías

- Sistema de la red empresarial con fácil acceso a datos personales y empresariales.
- Ciberdelincuencia organizada internacionalmente

2.9.2 Amenazas internas

- Empleado despedido y despedido
- Deterioro del clima laboral interno
- Falta de controles en el perfil de usuario de los empleados y negligencia
- Falta de capacitación al responsable de las tecnologías de la información (TI) y del personal en general.
- Dificultad de llevar a cabo amenazas externas debido al incremento de los niveles de seguridad de la red empresarial.

2.9.3 Amenazas mixtas

- El uso de ingeniería social
- La dificultad de realizar ataques a la red de las pymes sin ningún consentimiento desde el exterior.
- Con la finalidad de obtener ganancias económicas facilitando información confidencial de la empresa a posibles atacantes.

2.10 Estructura de la seguridad informática para pymes.

En el siguiente análisis se establece una estructura integral de seguridad informática para que una PYME pueda aplicarla siguiendo determinadas directrices, cabe señalar que se introduce este apartado en la propuesta de tesis ya que es algo complementario que no necesariamente está directamente vinculado con la seguridad perimetral con NGFW para las PYMES, sino se lo hace para comprender de mejor manera los aspectos que abarca la seguridad informática para pymes.

El correcto funcionamiento o incluso la supervivencia de las Pymes depende en gran medida de la adaptación al medio ya que las empresas se encuentran en un entorno tecnológico en constante cambio y la seguridad informática debería ser una prioridad.

Para comprender realmente lo que es la seguridad se debe tener una visión integral del entorno interno y externo, no solo analizando los aspectos técnicos, sino también los físicos, organizacionales y legales. Con esta perspectiva será más fácil adaptarse al riesgo identificando los riesgos a los que se expone la empresa y localizando los puntos débiles. (INCIBE, 2018)

Así también (INCIBE, 2018) indica que hoy en día los sistemas de información están presentes de alguna forma en todos los procesos de cualquier empresa: comunicación interna, relación con proveedores, logística, producción, marketing, atención al cliente, selección y formación de personal, internacionalización, innovación etc. Las pymes no están al margen de este entorno tecnológico. Las que no han nacido digitales se ven obligadas a evolucionar, por sus clientes o por la competencia, arrolladas por la necesidad de supervivencia. Por lo tanto, se debe garantizar la seguridad de la red informática empresarial, cumpliendo todas las leyes y normativas que establece el estado ecuatoriano.

2.10.1 Pasos fundamentales para asegurar las Pymes

2.10.1.1 La pyme tiene que analizar su estado de seguridad y definir a dónde quiere llegar.

- Para este caso se mejorará su sistema de control de accesos lógicos.
- Realizar copias de seguridad para recuperarse de la mayor parte de incidentes que se puedan presentar.
- Actualizar todo el software de la red empresarial
- Controlar los soportes de información durante toda su vida útil.

2.10.1.2 Política y Normativa de la Seguridad para las Pymes

El compromiso de la seguridad se demuestra definiendo, documentando y difundiendo una política de seguridad que defina cómo se va abordar la seguridad. También se concreta con el desarrollo de normativas y procedimientos que recojan las obligaciones a las que están sujetos los usuarios en lo que respecta al tratamiento y seguridad de la información. (INCIBE, 2018)

2.10.1.3 Control de Acceso

Al igual que se controla el acceso físico de las personas a dependencias, edificios, cuarto de equipos etc., se debe realizar un control de acceso de los recursos de la información de la pyme para que sean protegidos aplicando los siguientes controles:

- Permisos y privilegios de los usuarios
- Credenciales de los empleados en la cual se les asigne un nombre de usuario y contraseña.
- Control de personal con la ayuda de un lector biométrico.
- Horarios establecidos para el uso de las instalaciones.

2.10.1.4 Copias de seguridad de la información empresarial

El activo más importante que tiene una empresa es la información de los procesos productivos a esto se llama seguridad de la información. Por lo tanto, se debe garantizar la disponibilidad, integridad y confidencialidad de la información empresarial, tanto la digital cómo la física.

Independientemente de la actividad que realice la empresa, se deben tomar una serie de medidas generales para la protección de la información empresarial:

- Cifrar la información
- Copias de seguridad
- Control de acceso a la información de las pymes
- Destrucción de la información sensible

2.10.1.5 Protección contra malware

De la misma manera que avanzado la tecnología para mejorar los procesos industriales, también lo han hecho los ciberdelincuentes ahora con muchos casos de motivación económica.

La seguridad contra malware debe aplicarse a todos los dispositivos y equipos de las pymes, así como también los teléfonos móviles, discos duros externos y flash memory. Las pymes deben contar con medidas de detección, prevención y contención de amenazas que puede estar expuesta una empresa y la pueden hacer de la siguiente manera:

- Mejorar la seguridad perimetral con la ayuda de equipo firewall NGFW para pymes.
- Instalar un antivirus y mantenerle actualizado en todos los dispositivos empresariales, debería incluir funcionalidades para el análisis de correo electrónico y páginas web.
- Dividir la red empresarial de tal manera que el posible atacante tenga restringido el acceso a otros segmentos de red.
- Solo el responsable de tecnologías de la información (TI) tiene la autorización para instalar y modificar programas, en los dispositivos de la red empresarial.
- Tener activo un plan para respuesta de incidentes con roles, responsabilidades y procedimientos bien documentados.
- Realizar un monitoreo de los equipos de red de forma centralizada, analizando los logs de los diferentes equipos.

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

El desarrollo de la propuesta de un sistema de seguridad perimetral con Firewall de próxima generación NGFW para Pequeñas y Medianas empresas, será el resultado de la integración de todas las fases de investigación, desde su planteamiento, diseño, definición de un escenario de pruebas tipo, implementación y evaluación mediante una estructura de aplicabilidad. Todo ello dentro del área de seguridad telemática y orientado específicamente en la protección firewall de las Pymes del Cantón Guaranda.

3.1 Diseño de la investigación

El diseño de la investigación es de tipo CUASI-EXPERIMENTAL, ya que se experimenta con un escenario de pruebas tipo, con equipo firewall de próxima generación, además se refiere a un diseño de investigación experimental en el cual los ataques de estudio no están asignados aleatoriamente.

3.2 Tipo de la investigación

El tipo de investigación es descriptiva y aplicada, ya que se basa en conocimientos existentes, emanados de investigaciones previas, dirigida a la mejora de la seguridad perimetral de las redes de datos de las pequeñas y medianas empresas.

3.3 Método de la investigación

Para la investigación el método seleccionado es el científico, se refiere a una serie de etapas que hay que recorrer para obtener un conocimiento válido, además es exploratorio, descriptivo y documental, ya que se realiza una observación sistemática dando lugar a la formulación del problema de la falta de disponibilidad, integridad y seguridad de la información en las Pymes.

Se formula la hipótesis basada en el razonamiento deductivo, mediante la experimentación de un escenario de pruebas tipo, analizando los resultados obtenidos, con la finalidad de obtener soluciones apropiadas que cumplan con la hipótesis de la investigación, ya sea confirmando o rechazando la hipótesis propuesta.

3.4 Fuentes de información

Se basa en la lectura de fuentes de información bibliográficas primarias como pruebas y observación de resultados y secundarias como:

- Trabajos de investigación nacionales e internacionales
- Tesis de cuarto nivel nacionales e internacionales
- Artículos científicos
- Publicaciones realizadas en revistas de prestigio
- Información de internet de fuentes reconocidas nacionalmente e internacionalmente.
- Estándares internacionales:
 - ISO / IEC 27033-2: 2012: Directrices para el diseño e implementación de seguridad de red. Objetivo: definir cómo las organizaciones deben lograr arquitecturas, diseños e implementaciones de seguridad técnica de red de calidad que garanticen la seguridad de la red adecuada a sus entornos empresariales, utilizando un enfoque coherente para la planificación, diseño e implementación de la seguridad de la red, según sea relevante con la ayuda del uso de modelos / marcos. (En este contexto, se usa un modelo / marco para delinear una representación o descripción que muestra la estructura y el funcionamiento de alto nivel de un tipo de arquitectura / diseño de seguridad técnica).
 - ISO / IEC 27033-4: 2014: Asegurar las comunicaciones entre redes utilizando pasarelas de seguridad. Pauta de asegurar las comunicaciones entre las redes a través de pasarelas, cortafuegos, servidores de seguridad de aplicaciones, sistemas de protección contra intrusiones, de acuerdo con una política, que incluye identificar y analizar las amenazas de seguridad de la red, definir los requisitos de control de seguridad y diseñar, implementar, operar, monitorear y revisar los controles.

3.5 Técnicas de recolección de datos primarios y secundarios

Revisión Documental: para recopilar archivos de datos primarios y secundarios con el objetivo de obtener información relacionada al tema de estudio.

Lectura: para la comprensión de información o ideas primarias y secundarias en textos y artículos científicos referentes al tema de estudio.

Observación: para las fuentes primarias y secundarias verificando los controles y datos, permitiendo analizar los resultados de las pruebas ejecutadas en el equipo firewall que ayuda a mejorar la seguridad en pymes.

3.6 Tipo de estudio

El tipo de estudio es científico, ya que es de tipo aplicada, en la cual se basa en conocimientos existentes de nivel exploratorio y descriptivo, además permite describir las vulnerabilidades que se pueden presentar por la falta de un equipo firewall de próxima generación NGFW, para mejorar la seguridad perimetral de una Pyme a nivel de la capa de transporte y capa de aplicación del modelo OSI en la red LAN.

3.7 Definición de un escenario de pruebas

Para la propuesta de un escenario de pruebas con equipo firewall se han tomado ciertas directrices señaladas en la ISO / IEC 27033-4: 2014 en la cual incluye identificar y analizar las amenazas de seguridad de la red, definir los requisitos de control de seguridad y diseñar, implementar, operar, monitorear y revisar los controles. Así como también en las recomendaciones hechas por Microsoft referente a la ciberseguridad en Ecuador y América del Sur haciendo hincapié a la prevención, detección y respuesta, adaptada a nuestra realidad.

- La prevención dificulta el acceso a la red empresarial por parte de los ciberdelincuentes, aumentando el costo de los ataques, además previene de irrupciones eficaces y baratas.
- La detección y respuesta, aprovecha de la tecnología del firewall para aplicar controles adicionales en el caso de detectar un tipo de ataque o un intento de ingreso no autorizado a la red empresarial.

2019-12-07, 21:34:12	User Log	User login failed.
2019-12-07, 21:34:27	User Log	User firewall login failed.
2019-12-07, 21:34:42	User Log	User firewall login failed.

Figura 1-3 Intento de ingreso no autorizado a la red empresarial.

Fuente: Equipo Firewall.

Cisco señala que las Pymes se enfrentan a los mismos retos en seguridad que las grandes empresas, pero con presupuestos inferiores, por ello ha desarrollado dispositivos económicos y altamente eficientes para pequeñas y medianas empresas, como el equipo Cisco RV320 que dispone de funcionalidades de seguridad y firewall incluidos, además permite al administrador de la red conectarse al equipo de una forma segura ya sea desde su lugar de trabajo o desde su hogar.

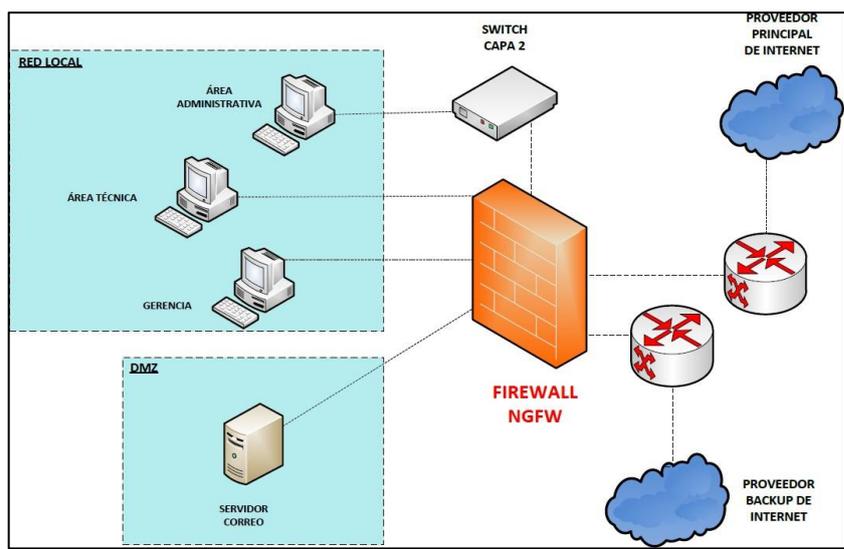


Figura 2-3 Propuesta de un escenario de Pruebas.

Fuente: Jorge Peña, 2023.

Para la propuesta de un escenario de pruebas se ha previsto utilizar un equipo Cisco RV320, ya que posee funciones de seguridad y firewall que utiliza un mecanismo avanzado de seguridad llamado SPI (inspección de paquetes con estado), ya que realiza una inspección activa de paquetes y un seguimiento del estado de las conexiones de red.

3.8 Determinación de variables

Variable dependiente: Tecnología adecuada para el acceso seguro a la red de las Pymes

Variable independiente: Análisis de vulnerabilidades de Algoritmos de Cifrado

3.8.1 Operacionalización de variables

Tabla 1-3 Operacionalización de variables

VARIABLE	TIPO	DEFINICIÓN
Tecnología adecuada para el acceso seguro a la red de las Pymes	Dependiente	Selección de la tecnología que permita mejorar la seguridad en las pymes.
Análisis de vulnerabilidades de Algoritmos de Cifrado	Independiente	Análisis de diferentes protocolos de seguridad existentes utilizados en equipos firewalls.

Fuente: Jorge Peña, 2023.

Tabla 2-3 Operacionalización metodológica de variables.

Hipótesis General	Variables	Indicadores	Índices	Técnicas
El análisis de los algoritmos de cifrado de una VPN generada por un Firewall de próxima generación, permitirá determinar una tecnología adecuada para el acceso seguro a la red de las PYMES.	Variable Dependiente (Tecnología adecuada para el acceso seguro a la red de las Pymes)	Confidencialidad	Algoritmo de cifrado mejorado	Observación Análisis Pruebas
			Tamaño de algoritmo de cifrado	
			Cifrado generado dinámicamente	
		Integridad	Integridad de la cabecera	Observación Análisis Pruebas
			Integridad cifrada	
			Integridad dependiente de la clave	
		Autenticación	Autenticación de usuario	Observación Análisis Pruebas
			Uso de protocolos de autenticación	
			Velocidad de ejecución	
	Variable Independiente (Análisis de vulnerabilidades de Algoritmos de Cifrado)	Cifrado	Tamaño de Clave	Observación Recopilación de información Análisis
			Tamaño de Bloque	
			Número de Rondas	
		Autorización	Clave Simétrica	Observación Recopilación de información Análisis
			Bloquea inserción de Tráfico	
			Considerado Seguro	
Aplicabilidad		Existencia de productos en el Ecuador	Observación Recopilación de información Análisis	
		El uso de la tecnología está permitido y regulado en el Ecuador		

Fuente: Jorge Peña, 2023.

3.8.2 Población y muestra

La población se refiere al conjunto o totalidad de elementos sobre los que se investiga. Mientras que la muestra es una parte de los elementos seleccionados de una población para la ejecución del estudio.

En la presente propuesta se analizan las falencias del protocolo independiente de la tecnología o de la marca, por lo tanto, se definirán dos aspectos para su desarrollo:

- Algoritmos de cifrado
- Vulnerabilidades existentes

En la propuesta de un sistema de seguridad perimetral con firewall de próxima generación se evalúan los algoritmos de cifrado:

Tabla 3-3 Algoritmos de cifrado

Algoritmos de Cifrado				
DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)

Fuente: Equipo Cisco

En el modo túnel se encapsula todo el paquete IP con la misma dirección IP, el último paquete tiene su propia cabecera IP que va dirigido desde el elemento que inicia el túnel hasta el elemento que lo termina y desencapsula. Además, permite escoger el algoritmo de cifrado y su autenticación para transmitir la información.

La información que viaja a través de un túnel VPN se puede escoger el método de cifrado, se puede comprobar su integridad, la información se cifra utilizando un algoritmo de cifrado y una llave simétrica. Al llegar el paquete a su destino, el receptor comprueba su integridad, si la misma es correcta, procede a descifrar la información, o a su vez el receptor desecha el paquete sin descifrarlo.

Una vez comprobada la integridad de la información se puede asegurar de que no ha sido modificada durante el trayecto a su destino.

Tabla 4-3 Principales amenazas que afectan la confidencialidad, integridad y autenticación.

PRINCIPIOS	PRINCIPALES AMENAZAS / VULNERABILIDADES
Confidencialidad	Fuerza bruta/ diccionario
Integridad	Man-in-the-Middle
Autenticación	Fuerza Bruta o exhaustivo

Fuente: Jorge Peña, 2023.

Fuerza Bruta. - Los ataques de fuerza bruta se producen cuando los hackers intentan descifrar una contraseña mediante ensayos de prueba y error masivos con la ayuda de un equipo informático. El alcance y la definición de fuerza bruta se han ampliado a medida que se ha ido desarrollando la tecnología informática. Los ataques simples de fuerza bruta no requieren mucha capacidad informática ni ingenio. Combinan sistemáticamente palabras, letras y caracteres hasta alcanzar su objetivo. Las contraseñas largas y complejas no están al alcance de los ataques simples, que generalmente se limitan a variaciones de las contraseñas más comunes o probables.

Man-in-the-Middle. –No se limita únicamente al ámbito de la seguridad informática o el mundo online. Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas. Por ejemplo, en el mundo offline, se crearían facturas falsas, enviándolas al correo de la víctima e interceptando los cheques de pago de dichos recibos.

En el mundo online, un ataque MiTM es mucho más complejo, pero la idea es la misma. El atacante se sitúa entre el objetivo y la fuente; pasando totalmente desapercibido para poder alcanzar con éxito la meta.

3.8.3 Instrumentos de recolección de datos

En referencia a la propuesta de un sistema de seguridad perimetral, los instrumentos más idóneos para la recolección de la información de los datos fueron los estándares, guía de observación, documentos técnicos IEEE, INCIBE, CISCO etc. Con los cuáles se pudieron establecer los parámetros de comparación para la ejecución del análisis los algoritmos de cifrado y la autenticación en la red alámbrica empresarial.

Una vez analizadas las vulnerabilidades que se pueden encontrar en las pymes se medirá las contramedidas adecuadas frente a ataques asociadas a dichas inseguridades, con la ayuda del equipo firewall y herramientas de monitoreo, escaneo y vulneración.

Tabla 5-3 Herramientas y su descripción.

HERRAMIENTA	DESCRIPCIÓN
Wireshark	Analizador de red
Kali Linux	Man-in-the-Middle
Kali Linux	Ataque de fuerza Bruta

Fuente: Jorge Peña, 2023.

3.8.4 Ambiente de pruebas sin seguridad

En este ambiente de pruebas con una seguridad básica en la cual la red empresarial únicamente tiene instalado un antivirus básico de uso libre, se analizan las vulnerabilidades de la red y el daño que puede sufrir cuando un ciberdelincuente ataca la red.

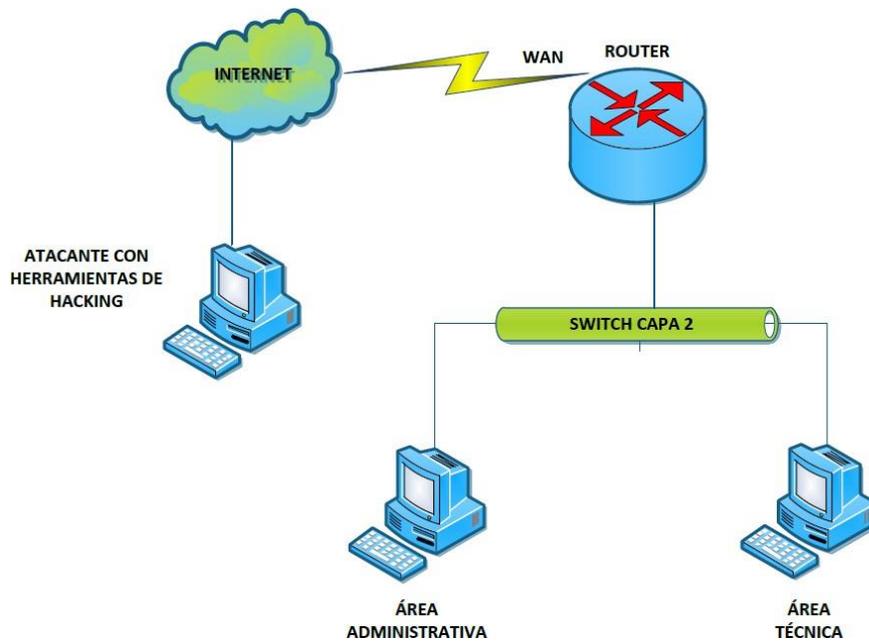


Figura 3-3 Escenario de Pruebas sin seguridad.

Fuente: Jorge Peña, 2023.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

En la propuesta planteada referente a la seguridad perimetral de una red empresarial tipo, todo el tráfico de internet pasa por el equipo firewall para ser inspeccionada, de esa manera el diseño se vuelve efectivo.

Además en el equipo firewall se habilitan controles con la finalidad de proteger la red empresarial, en la cual se autoriza o se niega el paso del tráfico, además el firewall permite al administrador de la red monitorear y tener su control, prohibiendo la entrada o salida de información que puedan vulnerar los servicios de red, el equipo utilizado también permite realizar conexiones seguras por medio de una red privada virtual (VPN), se puede escoger el tipo de cifrado y autenticación, en la cual se necesite un nivel de seguridad más alto dependiendo del tipo de información que se esté transmitiendo.

Se está utilizando VPN sobre IPsec que es configuración de una VPN entre dos redes distintas a través de internet, IPsec es un protocolo que está sobre la capa de internet (IP), permitiendo a dos equipos conectarse de manera segura, por lo tanto, la concientización a los directivos de la empresa es fundamental, comprender los riesgos que existen, ya que ello permitiría tomar las medidas adecuadas tanto para el personal como a los equipos informáticos, con la finalidad de mejorar la seguridad y minimizar las consecuencias de un potencial ataque.

4.1 VARIABLE INDEPENDIENTE

Análisis de vulnerabilidades de los algoritmos de cifrado

Para el análisis de la variable independiente, se hizo referencia a los datos existentes en las especificaciones técnicas de cada algoritmo de cifrado, asignándoles un valor cuantitativo, para ello, lo primero es definir una escala cualitativa de cuantificación de indicadores de la variable.

Tabla 1-4 Escala cualitativa de la cuantificación de indicadores de la variable independiente.

CATEGORÍA	ABREVIACIÓN	ESTIMACIÓN
Malo	M	1
Bueno	B	2
Muy Bueno	Mb	3
Excelente	E	4

Fuente: Jorge Peña, 2023

4.1.1 *Indicador 1: Cifrado*

Tabla 2-4 Cifrado.

Cifrado	Peso			
	1	2	3	4
Tamaño de Clave	<=64	>64 y <=128	>128 y <=192	>192 y <=256
Tamaño de Bloque	<=32	>32 y <=64	>64 y <=128	>128 y <=192
Número de Rondas	<=8	>8 y <=16	>16 y <=32	>32

Fuente: Jorge Peña, 2023.

Tabla 3-4 Resultados de Cifrado

Cifrado	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Tamaño de Clave	1	2	2	3	4
Tamaño de Bloque	2	2	3	3	3
Número de Rondas	2	4	2	2	2

Fuente: Jorge Peña, 2023.

Interpretación:

El cifrado de la información y el uso de algoritmos de encriptación son indispensables para la seguridad de un sistema de control de accesos, ya que garantiza su invulnerabilidad entre los dispositivos que se encuentran interconectados.

4.1.2 *Indicador 2: Autorización*

Tabla 4-4 Autorización

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Clave simétrica	SI	SI	SI	SI	SI
Bloquea Inserción de Tráfico	NO	NO	SI	SI	SI
Considerado seguro	NO	NO	SI	SI	SI

Fuente: Jorge Peña, 2023.

Tabla 5-4 Resultados de la Autorización

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Clave simétrica	1	1	1	1	1
Bloquea Inserción de Tráfico	0	0	1	1	1
Considerado seguro	0	0	1	1	1

Fuente: Jorge Peña, 2023.

Interpretación:

Los cifrados más utilizados son el TripleDES y AES, se utilizan comúnmente en cifrados de bloque, además el algoritmo más seguro es AES (Advanced Encryption Standard), está clasificado por la Agencia de Seguridad Nacional (NSA) de EEUU y es seis veces más rápido que el TripleDES.

4.1.3 *Indicador 3: Aplicabilidad*

Tabla 6-4 Aplicabilidad

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Existencia de productos en el Ecuador	SI	SI	SI	SI	SI
El uso de la tecnología está permitido y regulado en el Ecuador	SI	SI	SI	SI	SI

Fuente: Jorge Peña, 2023.

Tabla 7-4 Resultados de Aplicabilidad

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Existencia de productos en el Ecuador	1	1	1	1	1
El uso de la tecnología está permitido y regulado en el Ecuador	1	1	1	1	1

Fuente: Jorge Peña, 2023.

Interpretación:

De manera general en el Ecuador sí existen equipos firewall que permiten ejecutar los algoritmos de cifrados antes señalados, además dicha tecnología es permitida y regulada en el país, pero los equipos más sofisticados con la tecnología más actualizada deben hacer una importación dependiendo de las necesidades de seguridad de las Pymes.

Tabla 8-4 Resumen del análisis de la variable independiente

IDENTIFICADOR	INDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Análisis de vulnerabilidades de Algoritmos de Cifrado	Cifrado	5	8	7	8	9
	Autorización	1	1	3	3	3
	Aplicabilidad	2	2	2	2	2
TOTAL		8	11	12	13	14

Fuente: Jorge Peña, 2023.

Al finalizar el análisis comparativo de los indicadores de la variable independiente se ha determinado que el algoritmo criptográfico AES 256 (bits) es el más óptimo para hacer frente a vulnerabilidades de cifrado, autorización y aplicación.

4.1.4 *Análisis e interpretación de resultados variable independiente*

Para el respectivo análisis de la variable independiente, se hizo referencia a las características técnicas del equipo firewall NGFW, específicamente en los cifrados que utiliza en una comunicación VPN, los mismos que están detallados en los capítulos II y III de la presente propuesta de un sistema de seguridad perimetral con equipo firewall para pequeñas y medianas empresas.

Además, se debe señalar que el equipo firewall NGFW tiene una nueva tecnología de inspección de paquetes con estado (SPI), añaden servicios adicionales, estos sistemas reemplazan en la memoria de las sesiones de la capa de transporte y realizan inspección de protocolos en la capa de aplicación, para permitir el filtrado de contenidos y protocolos.

Por lo tanto, al aplicar la propuesta de un sistema de seguridad perimetral con firewall de próxima generación NGFW para pequeñas y medianas empresas, la red empresarial se asegura de manera eficaz, permitiendo o denegando el tráfico que entra o sale de la red, además se controlan las aplicaciones o contenidos permitidos para un eficiente funcionamiento de la empresa, también facilita la administración al administrador de la red empresarial.

4.2 VARIABLE DEPENDIENTE

Tecnología adecuada para mejorar la seguridad de la información

Tabla 9-4 Escala cualitativa de la cuantificación de indicadores de la variable dependiente.

CATEGORÍA	ABREVIACIÓN	ESTIMACIÓN	PORCENTAJE
Totalmente Inadecuado	TI	0	0%
Inadecuado	I	1	25%
Poco Adecuado	PA	2	50%
Adecuado	A	3	75%
Muy Adecuado	MA	4	100%

Fuente: Jorge Peña, 2023.

Al sufrir un ataque, cuan efectiva es la contramedida de los algoritmos DES, Triple DES, AES 128(bits), AES 192(bits) y AES 256(bits) para dar seguridad a la Confidencialidad integridad y Autenticación de la información que se transmite mediante una VPN.

4.2.1 *Indicador 1: Confidencialidad*

Tabla 10-4 Confidencialidad

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Algoritmo de cifrado mejorado	TI	I	A	A	MA
Tamaño de algoritmo de cifrado	PA	PA	A	MA	MA
Cifrado generado dinámicamente	I	I	PA	A	MA

Fuente: Jorge Peña, 2023.

Tabla 11-4 Resultados de Confidencialidad

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Algoritmo de cifrado mejorado	0	1	3	3	4
Tamaño de algoritmo de cifrado	2	2	3	4	4
Cifrado generado dinámicamente	1	1	2	3	4

Fuente: Jorge Peña, 2023.

Interpretación:

La confidencialidad depende del algoritmo de cifrado que se va a usar y el mismo va depender del nivel de seguridad que se desee.

Por lo resultados mostrados anteriormente el algoritmo DES se considera inseguro ya que tiene una longitud de clave relativamente corta de 56 bits por lo que su confidencialidad puede ser vulnerada.

En cuanto al algoritmo Triple DES se lo puede considerar más seguro que el algoritmo DES ya que se agranda la longitud de la clave sin la necesidad de cambiar el algoritmo de cifrado con una longitud de 3X56 bits en total 168 bits, pero en la actualidad no es un algoritmo muy seguro, por lo tanto, se acostumbra usar el algoritmo AES con sus variantes de claves de cifrado de 128 bits, 192 bits y 256 bits, ya que son los más usados en criptografía simétrica.

4.2.2 *Indicador 2: Integridad*

Tabla 12-4 Integridad

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Integridad de la cabecera	I	I	PA	A	MA
Integridad cifrada	TI	PA	A	MA	MA
Integridad dependiente de la clave	TI	I	PA	A	MA

Fuente: Jorge Peña, 2023.

Tabla 13-4 Resultados de la Integridad

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Integridad de la cabecera	1	1	2	3	4
Integridad cifrada	0	2	3	4	4
Integridad dependiente de la clave	0	1	2	3	4

Fuente: Jorge Peña, 2023.

4.2.3 *Indicador 3: Autenticación*

Tabla 14-4 Autenticación

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Autenticación de usuario	I	I	PA	A	MA
Uso de protocolo de autenticación	I	I	A	A	MA
Velocidad de ejecución	A	A	PA	I	I

Fuente: Jorge Peña, 2023.

Tabla 15-4 Resultados de la Autenticación

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Autenticación de usuario	1	1	2	3	4
Uso de protocolo de autenticación	1	1	3	3	4
Velocidad de ejecución	3	3	2	1	1

Fuente: Jorge Peña, 2023.

Tabla 16-4 Resultados totales de la cuantificación de indicadores de la variable dependiente.

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Confidencialidad	3	4	8	10	12
Integridad	1	4	7	10	12
Autenticación	5	5	7	7	9
SUB TOTAL	9	13	22	27	33
%	25,00	36,11	61,11	75,00	91,67

Fuente: Jorge Peña, 2023.

Tabla 17-4 Cuantificación de indicadores de la variable dependiente para el acceso seguro

IDENTIFICADOR	INDICES	DES				Triple DES				AES 128(bits)				AES 192(bits)				AES 256(bits)							
		0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4				
CONFIDENCIALIDAD	Algoritmo de cifrado Mejorado	X					X						X				X					X			
	Tamaño de algoritmo de Cifrado			X				X					X					X				X			
	Cifrado generado Dinámicamente		X					X					X					X				X			
INTEGRIDAD	Integridad de la Cabecera		X					X					X					X				X			
	Integridad Cifrada	X						X					X					X				X			
	Integridad dependiente de la Clave	X						X					X					X				X			
AUTENTICACION	Autenticación de Usuario		X					X					X					X				X			
	Uso de protocolos de Autenticación		X					X					X					X				X			
	Velocidad de Ejecución				X				X				X				X				X				
TOTAL		3	4	1	1	0	0	6	2	1	0	0	5	4	0	0	1	0	6	2	0	1	0	0	8

Fuente: Jorge Peña, 2023.

Tabla 18-4 Consideraciones de acceso seguro

Categoría	Valorización	Descripción	Abreviatura
Totalmente inadecuado	0	Acceso seguro bajo	ASB
Inadecuado	1		
Poco adecuado	2	Acceso seguro moderado	ASM
Adecuado	3	Acceso seguro alto	ASA
Muy adecuado	4		

Fuente: Jorge Peña, 2023.

Se realizó los respectivos cálculos de la valorización de la variable dependiente aplicando las consideraciones de Acceso Seguro.

Tabla 19-4 Valorización de la Variable Dependiente

DES					Triple DES					AES 128(bits)					AES 192(bits)					AES 256(bits)				
0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
3	4	1	1	0	0	6	2	1	0	0	0	5	4	0	0	1	0	6	2	0	1	0	0	8
0	1	0,5	0,75	0	0	1,5	1	0,75	0	0	0	2,5	3	0	0	0,25	0	4,5	2	0	0,25	0	0	8
1	0,5	0,75	1,5	1	0,75	0	2,5	3	0,25	0,0	6,50	0,25	0,0	8,00										
ASB	ASM	ASA	ASB	ASM	ASA	ASB	ASM	ASA	ASB	ASM	ASA	ASB	ASM	ASA	ASB	ASM	ASA	ASB	ASM	ASA	ASB	ASM	ASA	ASB

Fuente: Jorge Peña, 2023.

4.3 Prueba de hipótesis

La implementación de un sistema de seguridad perimetral con firewall de próxima generación NGFW mejora la confidencialidad, integridad y autenticación de la información en las Pymes.

La hipótesis es sometida a prueba para establecer si es apoyada o refutada en referencia a lo observado, es decir, para determinar la existencia o no de independencia entre las dos variables; que dos variables sean independientes significa que no tienen relación, eso quiere decir que la una no depende de la otra.

Hay una prueba estadística que permite algunos límites de confianza, una de ellas es la prueba del chi-cuadrado (X^2), consiste en calcular la probabilidad de obtener que únicamente por efecto del azar se desvíen de las expectativas de la magnitud observada si una solución al problema es correcta.

La prueba de hipótesis estadística es una regla con base a la hipótesis nula H_0 que determina si la hipótesis es aceptada o rechazada.

H_1 = El análisis de los algoritmos de cifrado de una VPN generada por un Firewall de próxima generación, permiten determinar una tecnología adecuada para el acceso seguro a la red de las PYMES.

H_0 = El análisis de los algoritmos de cifrado de una VPN generada por un Firewall de próxima generación, no permiten determinar una tecnología adecuada para el acceso seguro a la red de las PYMES.

Nivel de significación: $\alpha = 0,05$

Criterio: Rechace la H_0 si $X_c^2 \geq X_t^2$

X_c^2 = chi cuadrado calculado

X_t^2 = chi cuadrado de la tabla

Tabla 20-4 Tabla de contingencia de lo observado

Dependiente	Índices	DES	Triple DES	AES 128 (bits)	AES 192 (bits)	AES 256 (bits)	TOTAL
Tecnología adecuada para el acceso seguro a la red de las Pymes	Acceso seguro Alto	0,75	0,75	3	6,50	8,00	19
	Acceso Seguro Moderado	0,5	1	2,5	0,0	0,0	4
	Acceso Seguro Bajo	1	1,5	0	0,25	0,25	3
TOTAL		2,25	3,25	5,5	6,75	8,25	26

Fuente: Jorge Peña, 2023.

La frecuencia esperada de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas.

$$f_e = \frac{(\text{total fila})(\text{total columna})}{N}$$

Donde N es el número total de frecuencias observadas

Tabla 21-4 Tabla de frecuencias de lo esperado

Dependiente	Índices	DES	Triple DES	AES 128 (bits)	AES 192 (bits)	AES 256 (bits)	TOTAL
Tecnología adecuada para el acceso seguro a la red de las Pymes	Acceso seguro Alto	1,64	2,38	4,02	4,93	6,03	19
	Acceso Seguro Moderado	0,35	0,50	0,85	1,04	1,27	4
	Acceso Seguro Bajo	0,26	0,38	0,63	0,78	0,95	3
TOTAL		2,25	3,25	5,5	6,75	8,25	26

Fuente: Jorge Peña, 2023.

En base a la tabla de lo esperado y de lo observado obtenemos la tabla de Chi-cuadrado con la siguiente formula:

$$X_c^2 = \sum \frac{(O - E)^2}{E}$$

DONDE:

O = EL NUMERO OBSERVADO

E = EL NUMERO ESPERADO

\sum = ES LA SUMATORIA DE TODOS LOS VALORES POSIBLES DE (O-E)²/E

Tabla 22-4 Tabla del cálculo del Chi-cuadrado

INDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Acceso seguro Alto	0,49	1,11	0,26	0,50	0,64
Acceso Seguro Moderado	0,07	0,50	3,23	1,04	1,27
Acceso Seguro Bajo	2,11	3,38	0,63	0,36	0,52

Fuente: Jorge Peña, 2023.

PROBABILIDAD 0,05

CHI CUADRADO 16,11

GRADOS DE

LIBERTAD

8

GL=(M-1)*(N-1)

M=NUMERO DE FILAS

N=NUMERO DE

VALOR DE

COLUMNAS

REFERENCIA

15,5

Como $X^2 = 16,11$ cae en el área de rechazo H_0 , se rechaza la hipótesis nula y se acepta H_1 , es decir, se acepta la hipótesis de la investigación.

Tabla 23-4 Descripción tabla del cálculo del Chi-cuadrado

HIPÓTESIS	ALGORITMO	INDICE	O	E	O-E	(O- E)^2	(O-E)^2/E
El análisis de los algoritmos de cifrado de una VPN generada por un Firewall de próxima generación, permitirá determinar una tecnología adecuada para el acceso seguro a la red de las PYMES.	DES	Acceso seguro alto	0,75	1,64	-0,89	0,80	0,49
		Acceso seguro moderado	0,5	0,35	0,15	0,02	0,07
		Acceso seguro bajo	1,00	0,26	0,74	0,55	2,11
	Triple DES	Acceso seguro alto	0,75	2,38	-1,63	2,64	1,11
		Acceso seguro moderado	1,00	0,50	0,50	0,25	0,50
		Acceso seguro bajo	1,50	0,38	1,13	1,27	3,38
	AES 128(bits)	Acceso seguro alto	3	4,02	-1,02	1,04	0,26
		Acceso seguro moderado	2,5	0,85	1,65	2,74	3,23
		Acceso seguro bajo	0	0,63	-0,63	0,40	0,63
	AES 192(bits)	Acceso seguro alto	6,5	4,93	1,57	2,46	0,50
		Acceso seguro moderado	0	1,04	-1,04	1,08	1,04
		Acceso seguro bajo	0,25	0,78	-0,53	0,28	0,36
	AES 256(bits)	Acceso seguro alto	8	6,03	1,97	3,89	0,64
		Acceso seguro moderado	0	1,27	-1,27	1,61	1,27
		Acceso seguro bajo	0,25	0,95	-0,70	0,49	0,52
CHI CUADRADO							16,11

Fuente: Jorge Peña, 2023.

CAPÍTULO V

5. PROPUESTA DE IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL MEDIANTE LA PROTECCIÓN CORTAFUEGOS DE PRÓXIMA GENERACIÓN APLICABLE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL CANTÓN GUARANDA

Los firewalls antiguos evitan que cierto tráfico ingrese a la red y accedan a los recursos, bloqueando direcciones IP específicas y números de puerto, en la actualidad los ciberataques se lanzan en su mayor parte en la capa de aplicación, pudiendo escabullirse de los firewalls antiguos que no pueden analizar dentro de los paquetes de datos para ser analizados y determinar si son maliciosos.

En las Pymes la falta de presupuesto y el desconocimiento de las TI (Tecnologías de la información), ponen en riesgo la seguridad informática de las empresas, por ello los Firewall de próxima generación NGFW ofrecen una funcionalidad avanzada que protege de mejor manera a la red empresarial, creando una seguridad perimetral reforzada para evitar que ingrese tráfico dañino a la red.

Se va utilizar un firewall integrado con hardware, ya que este dispositivo está listo para conectarse y configurarse permitiéndome optimizar el tiempo, a diferencia de un firewall basado en software que requiere instalar un sistema operativo, drivers del dispositivo de hardware y software para el firewall antes de su configuración.

Para la propuesta de un sistema de seguridad perimetral con firewall de próxima generación NGFW para Pymes, se va a utilizar una nueva tecnología que es la inspección de paquetes con estado (SPI) que es un mecanismo de seguridad avanzado que inspecciona los paquetes y ejecuta un seguimiento del estado de las conexiones en la red, control de las conexiones activas y decide qué paquetes entrantes o salientes son autorizados de ingresar o salir de la red empresarial.

Según la estructura de las capas del modelo OSI, se analiza el tráfico en la capa de transporte (capa 4), además se hace un seguimiento de los estados de las conexiones de la red, como puede ser la comunicación UDP y los flujos TCP que pasan a través del firewall, distinguiendo los paquetes legítimos de los ilegítimos que se dirigen a la red de la empresa.

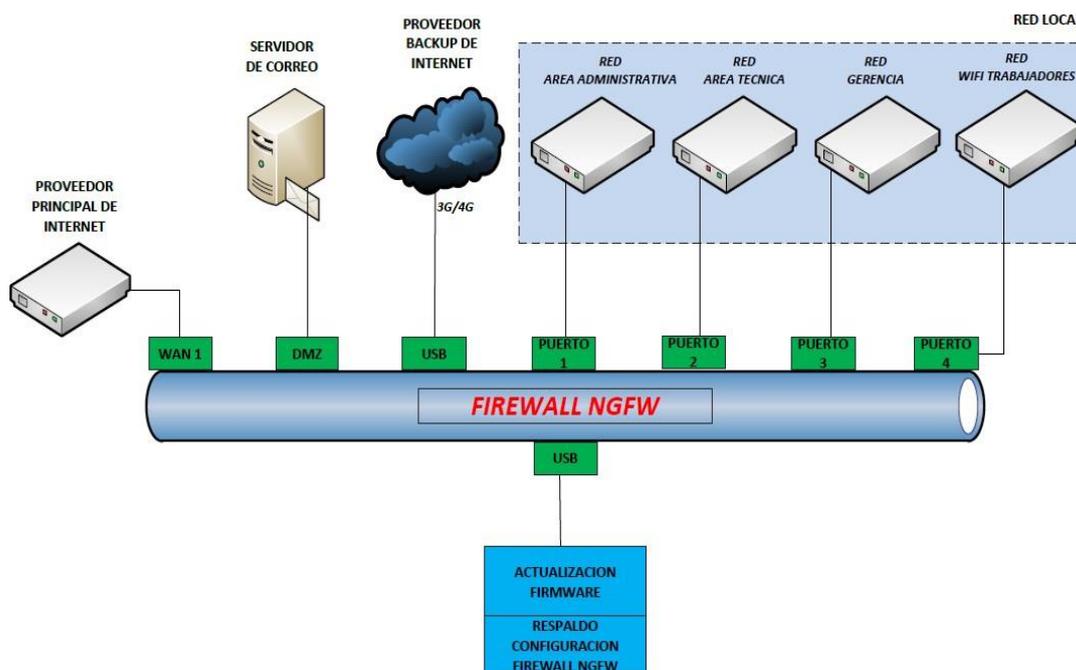


Figura 1-5 Propuesta de un Sistema de Seguridad Perimetral.

Fuente: Jorge Peña, 2023.

5.1 Implementación y evaluación del Sistema mediante una estructura de aplicabilidad para Pymes del cantón Guaranda

Para la implementación de la propuesta de un sistema de seguridad perimetral con equipo Firewall de Próxima Generación NGFW para Pymes del cantón Guaranda, se va a controlar el tráfico de entrada y de salida de la red empresarial por medio de un análisis de paquetes, administrando las funciones de los navegadores y aplicaciones, para permitir o denegar el acceso, por ello se va seguir el siguiente procedimiento:

5.1.1 Inspección de paquetes con estado (SPI)

Utiliza un mecanismo avanzado de seguridad llamado SPI, con inspección de paquetes y seguimiento del estado de las conexiones de red, hace un seguimiento de los estados de las conexiones de los protocolos de transporte TCP y UDP, dicho tráfico analizado corresponde a la capa de transporte (capa 4 del modelo OSI). Mantiene el registro de información de las solicitudes que se originan en la red empresarial. Analiza y decide qué paquetes entrantes y salientes son autorizados para ingresar o salir de la red, esto va depender de los controles implementados por el administrador de la red.

General

Cortafuegos: Habilitar

SPI (inspección de paquetes con estado): Habilitar

DoS (denegación de servicio): Habilitar

Bloquear solicitud de WAN: Habilitar

Administración remota: Habilitar Puerto:

Paso a través de multidifusión: Habilitar

HTTPS: Habilitar

SIP ALG: Habilitar

UPnP: Habilitar

SSH: Habilitar

SSH remoto: Habilitar

Figura 2-5 Inspección de paquetes con estado (SPI).

Fuente: Equipo Firewall, 2023.

Estadísticas de tráfico

Tabla de Ethernet

Id. de puerto	Estado de enlace	Paquetes Rx	Bytes Rx	Paquetes Tx	Bytes Tx	Error de paquete
LAN1	Inactivo	36100	3286857	61824	85232477	0
LAN2	Activo	5867	442004	24496	3533306	0
LAN3	Activo	1452469	317858939	2664453	18446744073021321288	0
LAN4	Activo	54536	4017142	16471	2378157	0
WAN1	Activo	2689609	3543231823	1453631	317901916	0
DMZ	Activo	696	57676	3356	401574	0

Actualizar Restablecer

Figura 3-5 Estadísticas del tráfico de los puertos del Firewall.

Fuente: Equipo Firewall, 2023.

Tabla de registro del sistema

Hora	Tipo de evento	
2019-11-27, 00:29:55	Kernel	TCP 192.168.1.103:57696 -> 185.88.181.6:80 on eth0
2019-11-27, 00:29:55	Kernel	TCP 192.168.1.103:57697 -> 185.88.181.6:80 on eth0
2019-11-27, 00:29:55	Kernel	TCP 192.168.1.103:57698 -> 185.88.181.6:80 on eth0
2019-11-27, 00:32:33	Kernel	TCP 192.168.1.103:57874 -> 185.88.181.6:80 on eth0
2019-11-27, 00:32:45	Kernel	TCP 192.168.1.103:57882 -> 185.88.181.6:80 on eth0
2019-11-27, 00:35:06	Kernel	TCP 192.168.1.103:57992 -> 185.88.181.4:80 on eth0
2019-12-01, 21:49:13	Kernel	TCP 192.168.1.100:50072 -> 107.154.155.5:80 on eth0
2019-12-01, 21:51:38	Kernel	TCP 192.168.1.100:50081 -> 107.154.155.5:80 on eth0
2019-12-01, 21:58:57	Kernel	TCP 192.168.1.100:50662 -> 107.154.155.5:80 on eth0
2019-12-01, 21:59:28	Kernel	TCP 192.168.1.100:50677 -> 107.154.155.5:80 on eth0

Actualizar Cerrar

Figura 4-5 Tabla de registro del sistema.

Fuente: Equipo Firewall, 2023.

Procesos					
Tabla de procesos					
Nombre	Descripción	Protocolo	Puerto	Dirección local	Dirección externa
confd	N/A	tcp	8008	0.0.0.0	0.0.0.0
nginx:	N/A	tcp	80	0.0.0.0	0.0.0.0
dnsmasq	Retransmisor DNS	tcp	53	0.0.0.0	0.0.0.0
confd	N/A	tcp	4565	127.0.0.1	0.0.0.0
dropbear	N/A	tcp	22	0.0.0.0	0.0.0.0
pptpd	Servidor PPTP	tcp	1723	0.0.0.0	0.0.0.0
nginx:	N/A	tcp	443	0.0.0.0	0.0.0.0
confd	N/A	tcp	4565	127.0.0.1	127.0.0.1
nginx:	N/A	tcp	59829	192.168.1.10	192.168.1.10
nkconfd	N/A	tcp	59514	127.0.0.1	127.0.0.1
confd	N/A	tcp	4565	127.0.0.1	127.0.0.1
nginx:	N/A	tcp	443	192.168.1.10	192.168.1.100
nginx:	N/A	tcp	443	192.168.1.10	192.168.1.100
nkconfd	N/A	tcp	59515	127.0.0.1	127.0.0.1
nginx:	N/A	tcp	443	192.168.1.10	192.168.1.100

Figura 5-5 Tabla de procesos Protocolo TCP.

Fuente: Equipo Firewall, 2023.

pluto	N/A	udp	4500	127.0.0.1	0.0.0.0
pluto	N/A	udp	4500	192.168.1.10	0.0.0.0
pluto	N/A	udp	4500	192.168.2.1	0.0.0.0
pluto	N/A	udp	4500	192.168.3.1	0.0.0.0
pluto	N/A	udp	4500	192.168.100.70	0.0.0.0
charon	N/A	udp	4500	0.0.0.0	0.0.0.0
dnsmasq	Retransmisor DNS	udp	53	0.0.0.0	0.0.0.0
dhcpd	Servidor DHCP	udp	67	0.0.0.0	0.0.0.0
webBoot	N/A	udp	22088	127.0.0.1	0.0.0.0
mdnsd	Servicio Discovery	udp	34507	0.0.0.0	0.0.0.0
ntpclient	Ciente NTP	udp	17374	192.168.100.70	132.163.96.1
mdnsd	Servicio Discovery	udp	5353	0.0.0.0	0.0.0.0
pluto	N/A	udp	500	127.0.0.1	0.0.0.0
pluto	N/A	udp	500	192.168.1.10	0.0.0.0
pluto	N/A	udp	500	192.168.2.1	0.0.0.0
pluto	N/A	udp	500	192.168.3.1	0.0.0.0
pluto	N/A	udp	500	192.168.100.70	0.0.0.0
charon	N/A	udp	500	0.0.0.0	0.0.0.0
charon	N/A	udp	4500	::	::
dnsmasq	Retransmisor DNS	udp	53	::	::
mdnsd	Servicio Discovery	udp	52433	::	::
mdnsd	Servicio Discovery	udp	5353	::	::
charon	N/A	udp	500	::	::

Figura 6-5 Tabla de Procesos Protocolo UDP.

Fuente: Equipo Firewall, 2023.

5.1.2 Control de Acceso Web

Los proveedores del firewall NGFW han analizado y categorizado sitios de acuerdo al tipo de contenido. Las empresas pueden limitar o bloquear el acceso a cierto tipo de sitios como: redes sociales, juegos de azar, pornografía, compras, citas entre otras. Esto ayuda a que se optimice el tiempo y se logre un mejor desempeño empresarial, además evita que ciertos usuarios accedan a sitios que podrían tener código malicioso que afecte a la red interna empresarial.

IP Whois

NetRange:	185.0.0.0 - 185.255.255.255
CIDR:	185.0.0.0/8
NetName:	RIPE-185
NetHandle:	NET-185-0-0-0-1

Figura 7-5 Determino el rango de IP que trabaja la página web.

Fuente: IP Whois 2023.

Reglas de acceso

IPv4 IPv6

Tabla de reglas de acceso							
	Prioridad	Habilitar	Acción	Servicio	Interfaz de origen	Origen	Destino
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	Denegar	Todo el tráfico [1]	LAN	Cualquiera	185.0.0.0 ~ 185.255.255.255
<input type="radio"/>		<input checked="" type="checkbox"/>	Permitir	Todo el tráfico [1]	LAN	192.168.1.10/255.255.255.0	Cualquiera
<input type="radio"/>		<input checked="" type="checkbox"/>	Permitir	Todo el tráfico [1]	LAN	192.168.2.1/255.255.255.0	Cualquiera
<input type="radio"/>		<input checked="" type="checkbox"/>	Permitir	Todo el tráfico [1]	LAN	192.168.3.1/255.255.255.0	Cualquiera
<input type="radio"/>		<input checked="" type="checkbox"/>	Denegar	Todo el tráfico [1]	USB1	Cualquiera	Cualquiera

Agregar Editar Eliminar Restaurar a reglas predeterminadas Administración de servicios...

Figura 8-5 Ingreso el rango de IP en la cual se deniega el acceso.

Fuente: Equipo Firewall 2023.

xvideos.com



No se puede acceder a este sitio web

www.xvideos.com ha tardado demasiado tiempo en responder.

Prueba a:

- Comprobar la conexión
- Comprobar el proxy y el cortafuegos
- Ejecutar Diagnósticos de red de Windows

ERR_TIMED_OUT

Volver a cargar

Figura 9-5 Ingreso el rango de IP en la cual se deniega el acceso.

Fuente: Ingreso a sitio para adultos 2023.

5.1.3 VPN (Red Privada Virtual)

Para mejorar los tiempos de respuesta y mantener la operatividad del negocio, algunas empresas necesitan que sus trabajadores accedan a los recursos de la red de forma remota para realizar actividades adicionales desde su casa o desde alguna parte del mundo. Por ello la VPN crea una conexión privada y segura a través de la red de internet, cifrando y protegiendo los datos entre un usuario remoto y la red empresarial. El firewall NGFW simplifica y asegura el acceso remoto por medio de conexiones VPN que puede ser en IPV4 o IPV6. Además, aumenta la productividad de la empresa proporcionando acceso LAN a los usuarios remotos con diversas aplicaciones empresariales.

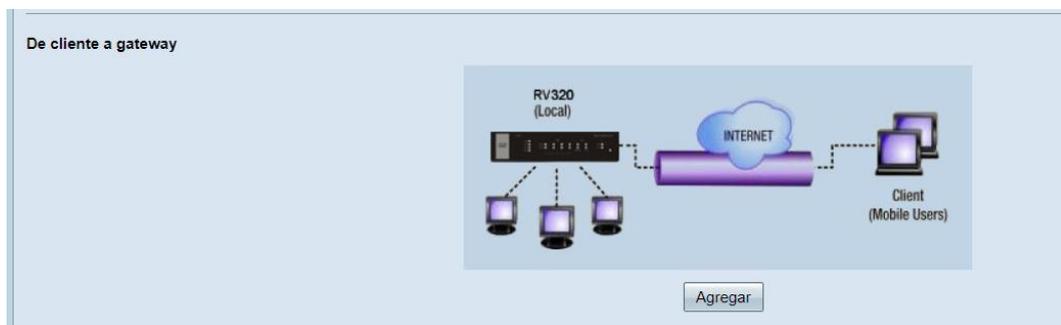


Figura 10-5 Configuración Cliente-Gateway.

Fuente: Equipo Firewall 2023.



Figura 11-5 Cliente VPN.

Fuente: TheGreenBow VPN Client.

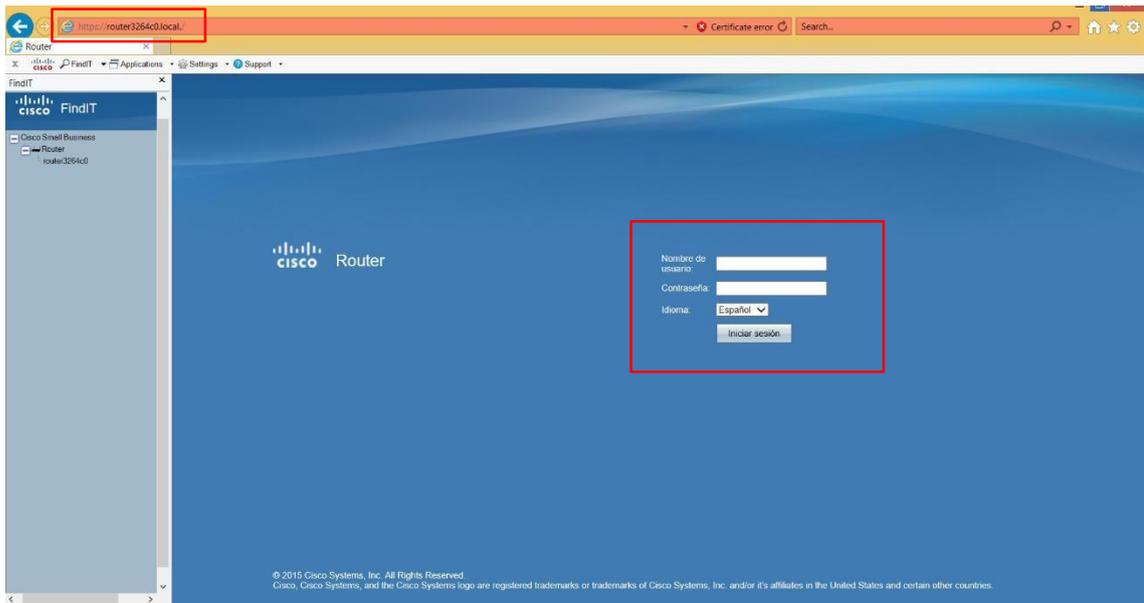


Figura 12-5 Conexión establecida de la VPN para administración del equipo.

Fuente: Equipo Firewall 2023.

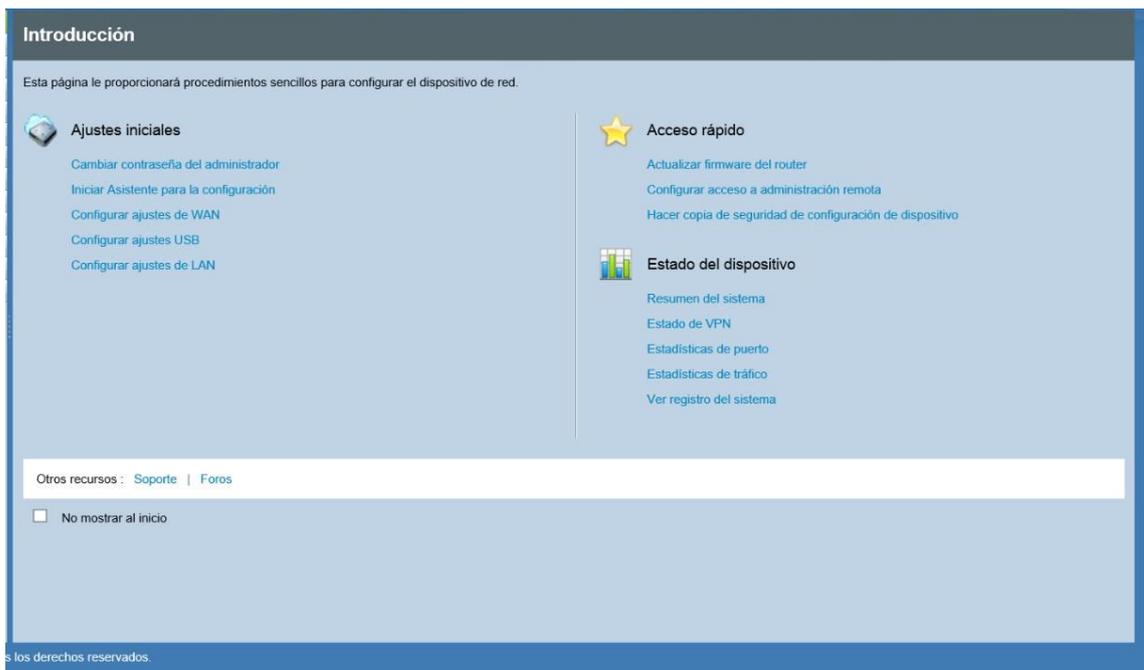


Figura 13-5 Conexión establecida de la VPN para administración del equipo.

Fuente: Equipo Firewall 2023.

5.1.4 *Monitoreo automatizado*

Los firewalls NGFW de última tecnología además de bloquear el tráfico en función de los controles establecidos por las políticas de seguridad, realizan un análisis profundo de paquetes y buscan activamente patrones que puedan indicar actividad maliciosa.

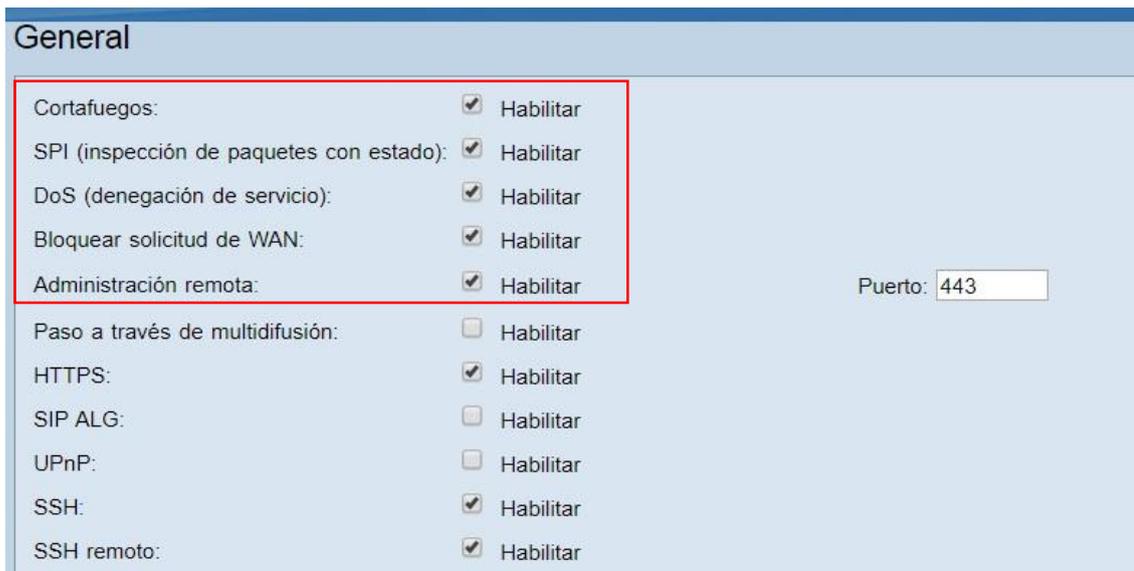


Figura 14-5 Monitoreo Automatizado.

Fuente: Equipo Firewall 2023.

Tabla de información del sistema		
Interfaz	WAN1	DMZ
Nombre del dispositivo	eth1	eth2
Estado	Conectado	Conectado
Dirección IP del dispositivo	192.168.100.70	192.168.2.15
Dirección MAC	28-AC-9E-32-64-C1	28-AC-9E-32-64-C2
Máscara de subred	255.255.255.128	255.255.255.0
Gateway predeterminada	192.168.100.1	0.0.0.0
DNS	8.8.8.8	0.0.0.0
Paquetes recibidos	2712118	1192
Paquetes transmitidos	1468001	3488
Paquetes totales	4180119	4680
Bytes recibidos	3562834778	111220
Bytes de paquetes transmitidos	320585840	418992
Bytes de paquetes totales	3883420618	530212
Bytes/seg. recibidos	2288	0
Bytes/seg. transmitidos	491	0

Figura 15-5 Tabla de información del sistema.

Fuente: Equipo Firewall 2023.

5.1.5 Zona desmilitarizada (DMZ)

Es una solución de seguridad efectiva para las Pymes, ya que ofrece la posibilidad de conectarse a la red empresarial desde un medio externo como puede ser al Servidor Web o Servidor de Correo, sin afectar la seguridad de la red interna, ya que se ingresa a un área protegida y aislada del resto de la red.



Figura 16-5 Habilitación de la Zona Desmilitarizada DMZ.

Fuente: Equipo Firewall 2023.

Estadísticas de tráfico

Tabla de Ethernet						
Id. de puerto	Estado de enlace	Paquetes Rx	Bytes Rx	Paquetes Tx	Bytes Tx	Error de paquete
LAN1	Inactivo	36100	3286857	61824	85232477	0
LAN2	Activo	5867	442004	24496	3533306	0
LAN3	Activo	1452469	317858939	2664453	18446744073021321288	0
LAN4	Activo	54536	4017142	16471	2378157	0
WAN1	Activo	2689609	3543231823	1453631	317901916	0
DMZ	Activo	696	57676	3356	401574	0

Actualizar Restablecer

Figura 17-5 Estadísticas del tráfico Zona Desmilitarizada DMZ.

Fuente: Equipo Firewall 2023.

5.1.6 Control de Aplicaciones

Los firewalls NGFW permite que las aplicaciones legítimas circulen por la red y bloquea otras aplicaciones que las políticas empresariales no lo permiten.

5.1.7 Detección de malware

Los firewalls NGFW reconocen que algunos sitios web legítimos pueden alojar malware sin saberlo, algunas organizaciones pueden dar acceso a ciertos usuarios a las plataformas de redes sociales, que en algunos casos tienen enlaces o archivos maliciosos. Los firewalls NGFW analizan el tráfico de la red de forma profunda para detectar malware y prevenir que se entregue a los usuarios.

5.2 Seguridad según las capas del modelo OSI

Tabla 1-5 Seguridad según las capas del modelo OSI

<p>CAPA FISICA</p>	<p>Se encarga de las conexiones físicas desde la PC hacia la red, tanto en lo referente al medio físico como a la forma en que se transmite la información.</p> <p>Medio físico:</p> <p>Medios guiados: como el cable coaxial, par trenzado, fibra óptica.</p> <p>Medios no guiados: microondas, radio, infrarrojos, láser y demás redes inalámbricas.</p> <p>Desde una perspectiva de seguridad informática, a este nivel debemos preocuparnos por:</p> <ul style="list-style-type: none"> • Impedir que personas no autorizados ingresen a las instalaciones. • Control de acceso a las instalaciones donde se encuentra desplegada la red. • Amenaza interna, un trabajador despedido realizando acciones no autorizadas con el fin de dañar o deteriorar la red. • La disposición del cableado no debe permitir escuchas indebidas, por ello se vuelve necesario restringir el acceso al cuarto de equipos • Proteger el cableado y equipamiento para que no pueda ser intencionalmente dañado con algún objeto corto punzante que pueda provocar un ataque a la disponibilidad del servicio.
<p>CAPA DE ENLACE</p>	<p>Es responsable de la transferencia confiable de la información a través de un circuito de transmisión de datos. Recibe peticiones del nivel de red y utiliza los servicios de la capa física.</p> <p>Protocolos utilizados:</p> <p>Ethernet o IEEE 802.3, IEEE 802.11 o</p> <p>Wi-Fi, IEEE 802.16 o WiMAX.</p> <p>PPP (Point to point protocol o protocolo punto a punto)</p> <ul style="list-style-type: none"> • Se basa en la correcta configuración de los switches • Debe existir bloqueo de acceso físico con la inutilización lógica de aquellos puertos sin utilizar, con el fin de impedir conexiones fraudulentas que puedan llevar a escuchas indebidas, ataques de saturación de las tablas o envenenamiento ARP. • Se debe elegir de forma correcta los protocolos que dan seguridad para la comunicación. • Configuración correcta de las redes virtuales. • VLANs guardan un punto crítico en la seguridad del sistema, contribuye a la segmentación de la red y la separación del tráfico, con una mejor organización y favoreciendo un rápido análisis.

CAPA DE RED	<p>Proporciona la conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas, con la finalidad que los datos lleguen desde el origen al destino.</p> <p>Orientación de conexión:</p> <ul style="list-style-type: none"> • Datagramas: Cada paquete se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo. • Circuitos virtuales: los dos equipos que quieran comunicarse tienen que empezar por establecer una conexión. • Protocolos de la capa de red: IP (IPv4, IPv6, IPsec), ARP, OSPF, DHCP, IS-IS, BGP, RIP, ICMP, ICMPv6, IGMP, RARP. <p>La configuración correcta con características de seguridad que se encuentran embebidas en estos aparatos resulta importante para impedir el control no autorizado del equipo. Se debe utilizar contraseñas fuertes y una configuración adecuada de los protocolos de administración a través de conexiones cifradas.</p> <p>Se debe tener en cuenta las vulnerabilidades que puedan existir en los protocolos de encaminamiento, como RIP u OSPF, puede darse el caso que terminan con la inyección de routers falsos.</p> <p>El protocolo IPv4 no incluye mecanismos de seguridad para proteger las comunicaciones, y es por esto que el administrador de la red debe considerar otras medidas extras al momento de proteger sus datos. Por ejemplo, puede elegirse cifrar todos los paquetes de la red, o intercambiar una clave de sesión que proteja la conexión.</p> <p>Por lo anteriormente manifestado se debe considerar la implementación de IPSec: la suite de protocolos encargada de proveer funcionalidades de seguridad al protocolo IP, sirviendo a la utilización de Redes Virtuales Privadas, o VPNs.</p> <p>Existen otros problemas que atañen a esta capa, como la posibilidad de un atacante pretenda enviar datos desde un equipo con una determinada dirección IP cuando en realidad lo hace desde otro, se denomina IP spoofing. Una manera de las maneras de disminuir estos ataques es la inclusión de procesos de autenticación en la capa de la aplicación, seguidos de mecanismos de cifrado de los datos.</p> <p>Otro de los elementos clave para la seguridad informática dentro de la capa de red es la Lista de Control de Acceso ACL, del inglés Access Control List. Éstas permiten o denegación conexiones entre equipos pertenecientes a redes diferentes, según el protocolo, los puertos, o las direcciones IP involucradas en la comunicación.</p> <p>La configuración correcta de las ACLs resulta una tarea de magnitud considerable, ya que implica el conocimiento de los protocolos que funcionarán en la red, y del diseño de ésta. Cualquier configuración incorrecta puede conducir a la autorización de tráfico fraudulento, o la denegación de conexiones legítimas.</p>
--------------------	---

<p>CAPA DE TRANSPORTE</p>	<p>En la capa de transporte se recomienda instalar un equipo firewall, para poder analizar todo el tráfico que entra o sale de la red con una inspección minuciosa de paquetes.</p> <p>Protocolos de transporte de internet:</p> <p>Protocolo de Datagramas de Usuario (UDP): Es un protocolo mínimo de nivel de transporte con orientación a mensajes. Este protocolo proporciona una sencilla interfaz entre la capa de red y de aplicación.</p> <p>Protocolo de Control de Transmisión (TCP): Se define como una de los principales protocolos de la capa de transporte. En el nivel de aplicación facilita la administración de datos, siendo el nivel más bajo de este modelo.</p> <p>Las preocupaciones de seguridad a este nivel se especifican sobre el cifrado de los datos al transmitir información, la autenticación entre el transmisor y el emisor, el prevenir las manipulaciones que afecten a la integridad de los datos, y el control de ataques de reinyección.</p> <p>Se debe utilizar protocolos de capa 4 para una comunicación segura, como pueden ser SSL, TLS o SSH, ya que protegen los datos mediante el cifrado, se debería considerar al momento de establecer conexiones de administración remota de los dispositivos.</p>
<p>CAPA DE SESIÓN</p>	<p>Esta capa proporciona el control de sesiones del diálogo entre aplicaciones de los sistemas finales. Además, proporciona mecanismos para controlar el diálogo entre las aplicaciones de los sistemas terminales.</p> <p>También realiza funciones que permite a los procesos, comunicarse a través de la red, ejecutando seguridad, como el reconocimiento de nombres, registro.</p>
<p>CAPA DE PRESENTACION</p>	<p>Esta capa se encarga de la representación de la información, de manera que, aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.</p> <p>La Capa de presentación, cumple tres funciones principales. Estas funciones son las siguientes:</p> <ul style="list-style-type: none"> ● Formateo de datos ● Cifrado de datos ● Compresión de datos

<p>CAPA DE APLICACION</p>	<p>La capa de aplicación brinda a las aplicaciones de un usuario la posibilidad de acceder a los servicios del resto de capas y establece los protocolos que utilizan las aplicaciones para el intercambio de datos.</p> <p>En esta capa se realiza la implantación de un firewall, para un mayor control del tráfico de red, en la cual se filtran paquetes y se incluyen una variedad de protocolos.</p> <p>El interesado normalmente no interactúa directamente con el nivel de capa de aplicación, sino interactúa con programas que a su vez se comunican con el nivel de aplicación, pero escondiendo la complejidad subyacente.</p> <p>Servicios:</p> <ul style="list-style-type: none"> • Aplicaciones de Red • www (World Wide Web). • Enlace a capas inferiores <p>La capa de aplicación contiene las aplicaciones visibles para el usuario, como: cifrado y seguridad, nombre de origen de datos (DNS) y también una de las aplicaciones más usadas a nivel mundial es el internet World Wide Web (www).</p>
----------------------------------	---

Fuente: Jorge Peña 2023.

CONCLUSIONES

- En el Ecuador no hay una normativa específica para Pymes referente a la seguridad informática, lo que existen son normativas y regulaciones de manera general que ayudan a mejorar un poco la seguridad de las redes de datos empresariales
- Las Pymes se enfrentan a los mismos retos en seguridad que las grandes empresas, pero con presupuestos inferiores, por ello ha desarrollado dispositivos económicos y altamente eficientes para pequeñas y medianas empresas, como el equipo Cisco RV320 que dispone de funcionalidades de seguridad y firewall incluidos.
- Para garantizar la seguridad informática en las Pymes, únicamente no se puede tomar en cuenta la capacidad técnica del departamento de tecnologías de la información (TI) y de los equipos del sistema de seguridad perimetral, sino de la concientización a todo el personal de la empresa, desde sus directivos hasta el personal de menor rango, ya que la falla humana suele ser la principal puerta de entrada para los ataques.
- El algoritmo de Cifrado AES 256(bits), es el más adecuado para el acceso seguro en una VPN generada por los firewall de próxima generación, permitiendo obtener una mayor seguridad en la confidencialidad, integridad y autenticación de la información.
- El cifrado de la información y el uso de algoritmos de encriptación son indispensables para la seguridad de un sistema de control de accesos, ya que garantiza su invulnerabilidad entre los dispositivos que se encuentran interconectados.
- Las Pymes tienen recursos limitados y presentan necesidades de defensa contra amenazas que puedan afectar su normal funcionamiento, por ello la capacidad del firewall NGFW para pymes buscan dar una protección avanzada contra amenazas, administración flexible y dar soluciones de seguridad de forma económica.
- En el firewall NGFW permite un análisis profundo de paquetes con tecnología SPI (inspección de paquetes con estado); en el modelo OSI corresponde a la capa de transporte (capa 4), además realiza inspección de protocolos en la capa de aplicación (capa 7) para permitir el filtrado de protocolos y contenidos.

RECOMENDACIONES

Una vez implementada la propuesta de un sistema de seguridad perimetral con equipo firewall de próxima generación NGFW aplicable para Pymes se establecieron las siguientes recomendaciones:

- Por motivos de seguridad es importante cambiar el nombre de usuario y contraseña que viene por defecto en el equipo Firewall, por regla general la longitud mínima de una contraseña debe ser de 8 dígitos, en la cual se utilicen números, letras mayúsculas, minúsculas y caracteres especiales.
- Es fundamental actualizar el firmware, ya que permite corregir errores, realiza mejoras a la funcionalidad de firewall, aumentando el rendimiento de la red sin tener que comprar ningún hardware nuevo. Esta actualización, es la combinación de actualizaciones entre los controladores del software y hardware de un determinado dispositivo.
- La copia de seguridad se la realiza respaldando todo el archivo de configuración del equipo firewall, si el archivo de configuración se daña por una determinada razón se carga el respaldo desde una PC o desde una memoria flash, de esa manera se restablecen las configuraciones en un menor tiempo posible para un funcionamiento continuo de la empresa.
- La IP y la MAC del equipo se vinculan por seguridad, cuando al dispositivo se le configura como servidor DHCP, además se pueden bloquear direcciones MAC de la lista con direcciones IP incorrectas, o a su vez direcciones MAC no incluidas en la lista.
- Se debe tener cuidado con los enlaces que se visitan, ya que son una de las entradas más comunes de malware, se debe verificar que la página sea https, eso indica que la conexión es segura, por lo tanto, el certificado es válido.
- A pesar que no tiene mucha relación con el tema analizado, es muy importante desde el punto de vista de la seguridad, por lo tanto, las redes Wifi no son tan seguras como las cableadas, ya que transmiten información en todas las direcciones y pueden ser escuchadas por cualquier dispositivo, por ello, se recomienda desactivar el WPS y utilizar un nivel de cifrado alto en la comunicación como el WPA2 + AES.
- Se debe respaldar la información crítica de la empresa en forma periódica ya sea en un espacio en la nube o en un disco duro externo.

GLOSARIO

NGN: (Next Generation Network) Modelo de arquitectura de redes de referencia que debe permitir desarrollar toda la gama de servicios IP multimedia de nueva generación (comunicaciones de VoIP, videocomunicación, mensajerías integradas multimedia, integración con servicios IPTV, domótica, sistemas de seguridad, etc.).

Firewall: Un firewall es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada.

Modelo OSI: El Modelo OSI (de las siglas en inglés: Open Systems Interconnection, o sea, “Interconexión de Sistemas Abiertos”), es un modelo de referencia para los protocolos de comunicación de las redes informáticas o redes de computadores.

Entorno Virtual: Un entorno virtual de aprendizaje es una plataforma web utilizada para administrar, distribuir, realizar las tareas de seguimiento y evaluación de todas aquellas actividades involucradas en los procesos de enseñanza y de aprendizaje.

PYMES: Empresa pequeña o mediana en cuanto a volumen de ingresos, valor del patrimonio y número e trabajadores.

Seguridad Perimetral: La seguridad perimetral corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

UDP: Es un protocolo de comunicación que se utiliza en Internet para transmisiones sujetas a limitaciones temporales, como la reproducción de vídeo o las búsquedas en DNS. Acelera las comunicaciones al no establecer formalmente una conexión antes de transferir los datos.

TCP: Protocolo de Control de Transmisión, por sus siglas en inglés Transmission Control Protocol, es un protocolo de red importante que permite que dos anfitriones (hosts) se conecten e intercambien flujos de datos. TCP garantiza la entrega de datos y paquetes (en-US) en el mismo orden en que se enviaron.

BIBLIOGRAFÍA

- Tecnozero*. (2017). Obtenido de Gartner 2017 para los Firewalls de Redes Empresariales:
<https://www.tecnozero.com/firewall/gartner-2017-para-los-firewalls-de-redes-empresariales/>
- Tecnozero*. (2018). Obtenido de Gartner 2018 para los Firewalls de Redes Empresariales:
<https://www.tecnozero.com/firewall/gartner-2018-para-los-firewalls-de-redes-empresariales/>
- ISC. (11 de 2019). Obtenido de Ingeniería, Servicios y Comunicaciones S.A.:
<https://www.isc.cl/que-es-el-cuadrante-magico-de-gartner-transformacion-digital/>
- Aguirre, P. (2017). *Ciberseguridad en Infraestructuras Críticas de la Información*. Buenos Aires: Universidad de Buenos Aires.
- Anchundia Betancourt, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias*, 200-217.
- ÁngelBermúdez. (16 de Mayo de 2017). *Cuáles son los países de América Latina más afectados por WannaCry, el virus protagonista del ciberataque de alcance global*. Obtenido de <https://www.bbc.com/mundo/noticias-america-latina-39931455>
- ARCOTEL. (2019). Obtenido de <http://www.arcotel.gob.ec/>
- BOE. (28 de Abril de 2011). *Medidas para la protección de infraestructuras críticas*. Recuperado el 24 de Marzo de 2019, de <https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf>
- Bohórquez_Gutiérrez. (25 de Agosto de 2018). *Diseño de un sistema de seguridad perimetral en las instalaciones del consorcio PTAR Salitre, Sede Bogota DC*. Obtenido de <https://repository.ucatolica.edu.co/handle/10983/15322>
- CAN. (21 de 08 de 2009). *Resolucion 1260*. Obtenido de Resolucion 1260: <http://www.comunidadandina.org/StaticFiles/DocOf/RESO1260.pdf>
- Cisco. (2019). Qué es un Firewall. <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>.
- CiscoLatinoamerica. (2018). *Cisco, líder en firewalls de redes empresariales*. Recuperado el 15 de Octubre de 2019, de <https://gblogs.cisco.com/la/sc-geeritt-cisco-lider-en-firewalls-de-redes-empresariales-segun-el-cuadrante-magico-de-gartner-2018-para-firewalls-de-redes-empresariales/>
- Díaz, C. (2013). *Implantación de un sistema de seguridad perimetral*. Obtenido de http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf
- DIEE. (09 de 2019). *Directorio de Empresas y Establecimientos 2018*. Obtenido de Directorio de Empresas y Establecimientos 2018: <https://www.ecuadorencifras.gob.ec/documentos/web->

- inec/Estadisticas_Economicas/DirectorioEmpresas/Directorio_Empresas_2018/Principales_Resultados_DIEE_2018.pdf
- ecucert. (2018). *Centro de respuesta a incidentes informáticos en el Ecuador*. Recuperado el 21 de Marzo de 2019, de <https://www.ecucert.gob.ec/>
- EGSI. (25 de Septiembre de 2013). *Normativa del Esquema Gubernamental de Seguridad de la Información*. Recuperado el 21 de Febrero de 2019, de <http://www.planificacion.gob.ec/wp-content/uploads/downloads/2015/04/Acuerdo-No.-166-EGSI.pdf>
- ElevenPaths. (18 de Julio de 2019). *Pymes y ciberseguridad*. Obtenido de <https://empresas.blogthinkbig.com/pymes-y-ciberseguridad-por-donde-empiezo/>
- ENSA. (19 de Septiembre de 2018). *Apunte Empresarial "Cómo marcha la ciberseguridad en América Latina"*. Recuperado el 17 de Mayo de 2019, de <https://www.esan.edu.pe/apuntes-empresariales/2018/09/como-marcha-la-ciberseguridad-en-america-latina>
- Fourie, L. S. (2014). *The Global Cyber Security Workforce – An Ongoing Human Capital Crisis*. Recuperado el 12 de Mayo de 2019, de <http://unitec.researchbank.ac.nz/bitstream/handle/10652/2457/Cyber2.pdf?sequence=1&isAllowed=y>
- GESI. (27 de Febrero de 2018). *Grupo de Estudios en Seguridad Internacional*. Recuperado el 13 de Mayo de 2019, de <http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina>
- GlobalCorporateDivestmentStudy, 2. (2018). *Global Corporate Divestment Study 2018*. Obtenido de [https://www.ey.com/Publication/vwLUAssets/ey-global-corporate-divestment-study-2018/\\$FILE/ey-global-divestment-study-2018.pdf](https://www.ey.com/Publication/vwLUAssets/ey-global-corporate-divestment-study-2018/$FILE/ey-global-divestment-study-2018.pdf)
- Haro. (27 de Febrero de 2015). *Cibermafias atacaron 17 a empresas ecuatorianas*. Obtenido de <https://prezi.com/nnfhkzrme8zs/cibermafias-atacaron-a-17-empresas-ecuatorianas/>
- INCIBE. (2018). *Instituto Nacional de Ciberseguridad*. Obtenido de <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
- incibe-cert. (19 de Mayo de 2016). *Banco ecuatoriano sufre el robo de \$12M a través del sistema SWIFT*. Obtenido de <https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/banco-ecuatoriano-sufre-el-robo-12m-traves-del-sistema-swift>
- INEC. (07 de 2011). *INEC*. Obtenido de INEC: https://www.ecuadorencifras.gob.ec/documentos/web-inec/CENEC/Presentaciones_por_ciudades/Presentacion_Guaranda.pdf
- ISO. (08 de 2015). *ISO/IEC 27033*. Obtenido de <https://www.iso.org/standard/63461.html>
- ISO27001. (2013). *ISO/IEC 27002*. Obtenido de <https://www.iso27001security.com/html/27002.html>

- ISO27033. (2015). *ISO/IEC 27033-2015*. Obtenido de <https://www.iso.org/standard/51581.html?browse=tc>
- ITU. (2017). *Global Cybersecurity Index*. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- ITU. (27 de Marzo de 2018). *Union Internacional de Telecomunicaciones*. Recuperado el 09 de 04 de 2019, de https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf
- Juan, M. A. (28 de Julio de 2019). *La ciberseguridad en Europa*. Obtenido de <https://www.theeconomyjournal.com/texto-diario/mostrar/939545/ciberseguridad-europa>
- Julia, S. (2017). *Importancia de la seguridad informática en las pymes*. Obtenido de <http://www.gadae.com/blog/seguridad-informatica-en-las-pymes/>
- Kaspersky. (15 de Mayo de 2017). *Kaspersky Lab en América Latina*. Obtenido de <https://cnnespanol.cnn.com/2017/05/15/este-es-el-pais-de-latinoamerica-mas-afectado-por-el-ciberataque-wannacry/>
- kaspersky. (2019). *what-is-cyber-security*. Recuperado el 17 de Abril de 2019, de <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- KnowBe4. (25 de Mayo de 2017). *El ataque del WannaCry costó más de 1.000 millones de dólares a las empresas afectadas*. Obtenido de <https://actualidad.rt.com/actualidad/239380-wannacry-costar-mil-millones-dolares>
- Llumiquinga, G. (24 de Marzo de 2019). *Seguridad: temas pendientes para las empresas ecuatorianas*. Obtenido de <https://www.itahora.com/actualidad/seguridad/seguridad-temas-pendientes-para-las-empresas-ecuatorianas/>
- Martínez, T. (2017). *Diferencias entre UTM y NGFW*. 06: <https://www.telequismo.com/2017/07/utm-ngfw.html/>.
- MINTEL. (2019). Obtenido de <https://www.telecomunicaciones.gob.ec/>
- MINTEL. (28 de Marzo de 2019). *El Ecuador trabaja en la Estrategia Nacional de Ciberseguridad*. Obtenido de <https://www.telecomunicaciones.gob.ec/ecuador-trabaja-en-la-estrategia-nacional-de-ciberseguridad/>
- OAS. (5 de Marzo de 2018). *Lanzamiento del Informe OEA - Microsoft*. Recuperado el 22 de Febrero de 2019, de https://www.oas.org/es/acerca/discurso_secretario_general.asp?sCodigo=18-0015
- openlearning. (Octubre de 2016). *penlearning*. Obtenido de http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/
- OSTEC. (03 de Enero de 2019). *Firewall UTM y NGFW, conozca las principales diferencias*. Obtenido de <https://ostec.blog/es/seguridad-perimetral/firewall-utm-ngfw-diferencia>

- Paloalto. (2019). *8-TIME GARTNER MAGIC QUADRANT LEADER*. Obtenido de 8- TIME GARTNER MAGIC QUADRANT LEADER: <https://start.paloaltonetworks.com/2019-gartner-mq-for-firewalls.html>
- Pírez, M. R. (2018). SISTEMA DE SEGURIDAD PERIMETRAL EN UN ENTORNO UNIVERSITARIO. pág. mramirez@ecotec.edu.ec.
- PrivacyRightsClearinghouse. (1 de Octubre de 2019). *Check on data breaches at the Privacy Rights Clearinghouse*. Obtenido de <https://www.journalofaccountancy.com/issues/2019/sep/data-breaches-privacy-rights-clearinghouse.html>
- Rafael Eduardo RON Amores, V. A. (28 de Julio de 2017). *Las PYMES ecuatorianas*. Obtenido de <https://www.revistaespacios.com/a17v38n53/a17v38n53p15.pdf>
- Ramos, M. (2012). Análisis de vulnerabilidades de protocolos de protección y autenticación inalámbrico. *Tesis Maestría Seguridad en Redes*, 82.
- Secure_it. (20 de Agosto de 2018). *Seguridad perimetral lógica*. Obtenido de [https://www.secureit.es/sistemas-de-seguridad-it/seguridad-perimetral-logica/Sepulveda, W. \(14 de Noviembre de 2018\). Necesitan las pymes tanta protección de ciberseguridad. Obtenido de https://www.enserio.cl/2018/11/14/pymes-necesitan-proteccion-de-ciberseguridad/](https://www.secureit.es/sistemas-de-seguridad-it/seguridad-perimetral-logica/Sepulveda, W. (14 de Noviembre de 2018). Necesitan las pymes tanta protección de ciberseguridad. Obtenido de https://www.enserio.cl/2018/11/14/pymes-necesitan-proteccion-de-ciberseguridad/)
- TIC, S. p. (7 de 11 de 2016). *SIAG Consulting* . Obtenido de <http://www.solopiensoentic.com/cuadrante-magico-de-gartner/>
- Universidad Internacional de Valencia, E. d. (21 de Marzo de 2018). *Universidad Internacional de Valencia*. Obtenido de Universidad Internacional de Valencia: <https://www.universidadviu.com/>

ANEXOS

Anexo A: Ficha Técnica

FICHA TECNICA

- Los puertos WAN Gigabit Ethernet dobles facilitan el equilibrio de carga y la continuidad comercial
- Los puertos Gigabit Ethernet asequibles y de alto rendimiento permiten la transferencia rápida de archivos grandes y admiten varios usuarios
- Los puertos USB dobles admiten un módem 3G/4G o una unidad flash; la red WAN también tiene conmutación por falla con el módem 3G/4G conectado a un puerto USB
- Las plataformas VPN con SSL y VPN de sitio a sitio permiten una conectividad altamente segura, por lo que el router Cisco RV320 es perfecto para empleados remotos y diversas oficinas
- El firewall con inspección activa de estado de paquetes (SPI) y el cifrado de hardware ofrecen una sólida seguridad
- Las herramientas de configuración fáciles de utilizar, de acuerdo con asistentes, pueden utilizarse para establecer la conectividad de red y administrar la seguridad

General

Tipo de dispositivo	<u>Router</u> - conmutador de 4 puertos (integrado)
Tipo de caja	Sobremesa
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Rendimiento	Tasa de transferencia: 900 Mbps Capacidad VPN (<u>IPSec</u>): 100 Mbps Capacidad VPN (SSL): 20 Mbps

Capacidad	<p>Interfaces virtuales (VLAN): 16</p> <p>Túneles PPTP VPN: 10</p> <p>Túneles VPN SSL: 10</p> <p>Túneles VPN (de sitio a sitio): 25</p> <p>Túneles VPN <u>IPSec</u>: 25</p> <p>Conexiones concurrentes: 20000</p>
Red / Protocolo de transporte	<p>PPTP, L2TP, <u>IPSec</u>, <u>PPPoE</u>, DHCP, Bonjour, DDNS</p>
Protocolo de direccionamiento	<p>RIP-1, RIP-2, direccionamiento IP estático, <u>RIPng</u></p>
Protocolo de gestión remota	<p>SNMP 1, SNMP 3, SNMP 2c, HTTP, HTTPS</p>
Algoritmo de cifrado	<p>DES, Triple DES, MD5, SHA-1, AES de 128 bits, AES de 192 bits, AES de 256 bits</p>

Características	<p>Puerto DMZ, soporte de NAT, cifrado del hardware, asistencia técnica VPN, soporte para PAT, equilibrio de carga, soporte para <u>Syslog</u>, <u>Stateful Packet Inspection (SPI)</u>, prevención contra ataque de <u>DoS</u> (denegación de servicio), filtrado de contenido, Alerta de correo electrónico, soporte IPv6, actualizable por firmware, <u>Quality of Service (QoS)</u>, <u>IPSec NAT-Traversal (NAT-T)</u>, Servidor DHCP, botón de reinicio, control de ancho de banda, relé DHCP, relé DNS, cliente DHCP</p>
-----------------	---

Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1Q, certificado FCC Clase B, UL, BSMI, CUL , CB, CCC, ANATEL, KC
Indicadores de estado	Velocidad de transmisión del puerto, alimentación, WAN, DMZ, enlace/actividad, DMZ/Internet, diagnóstico, USB, VPN

Expansión / Conectividad

Interfaces	LAN: 4 x 10Base-T/100Base-TX/1000Base-T - RJ-45 WAN: 1 x 10Base-T/100Base-TX/1000Base-T - RJ-45 WAN / DMZ: 1 x 10Base-T/100Base-TX/1000Base-T - RJ-45 USB 2.0: 2 x USB de 4 clavijas Tipo A
------------	--

Alimentación

Dispositivo de alimentación	Transformador eléctrico externo
-----------------------------	---------------------------------

Diverso

Cables incluidos	1 x cable de red
------------------	------------------

Software / Requisitos del sistema

Software incluido	Controladores y utilidades
-------------------	----------------------------

Dimensiones y peso

Anchura	20.6 cm
Profundidad	13.2 cm

Altura	4.4 cm
--------	--------

Garantía del fabricante

Servicio y mantenimiento	Garantía limitada - de por vida
--------------------------	---------------------------------

Parámetros de entorno

Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	10 - 85% (sin condensación)

web: CISCO Small Business RV320 - RV320-K9-G5

Características y Beneficios

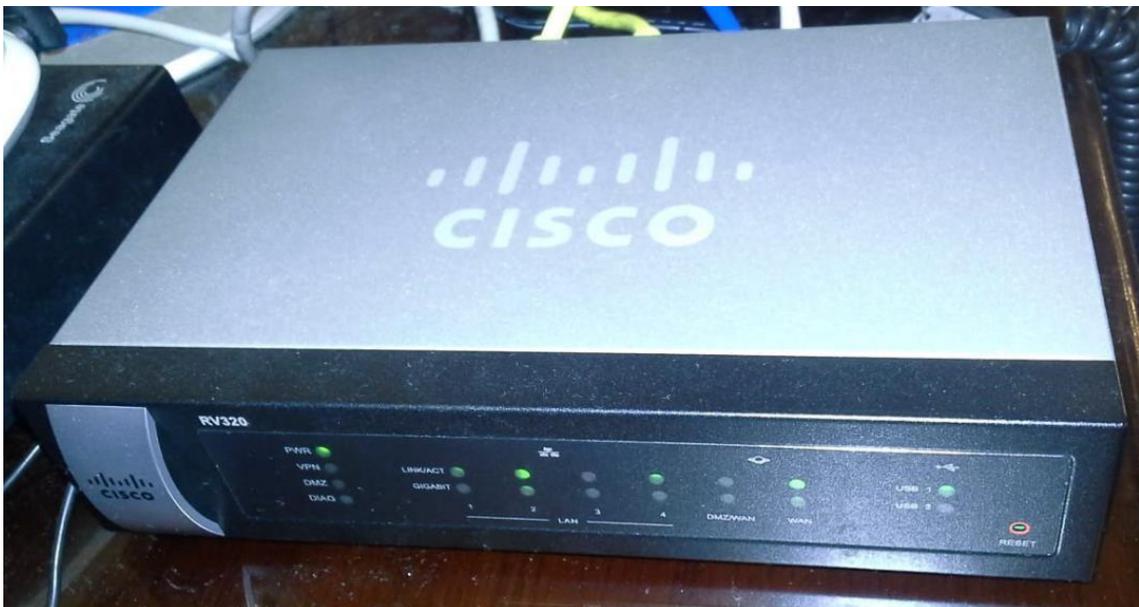
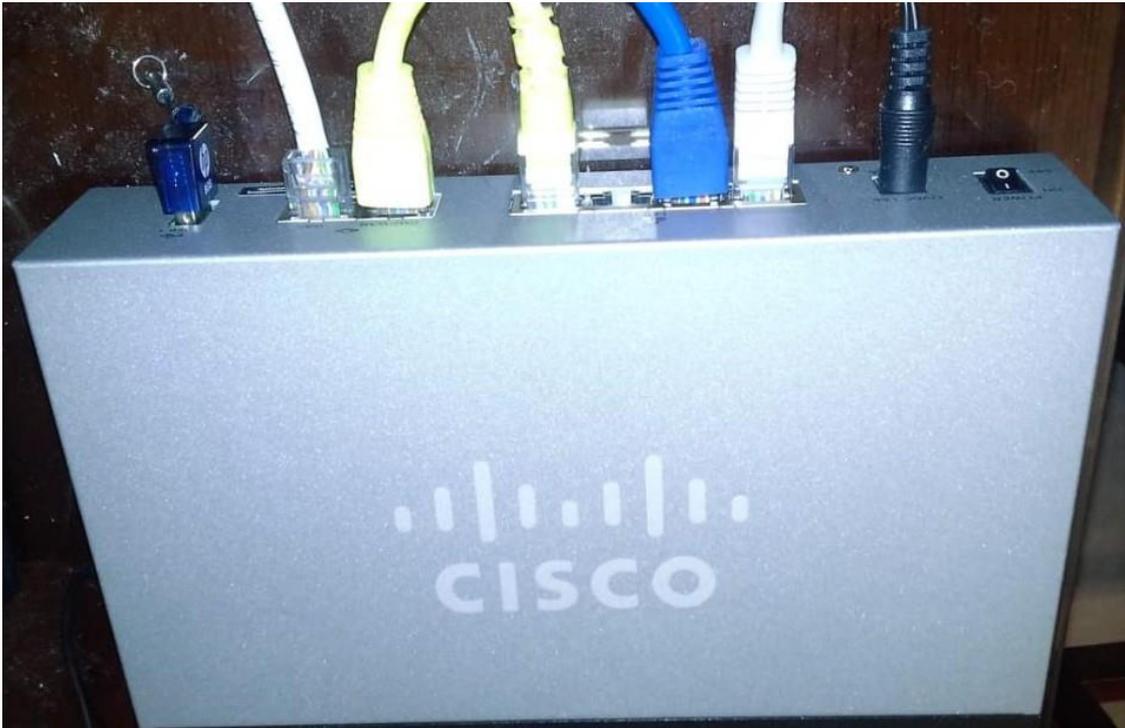
- Los puertos WAN Gigabit Ethernet dobles permiten el equilibrio de carga y la continuidad del negocio.
- Los puertos Gigabit Ethernet asequibles y de alto rendimiento permiten la transferencia rápida de archivos de gran tamaño y admiten múltiples usuarios.
- Los puertos USB dobles admiten un módem 3G / 4G o una unidad flash. La WAN también puede conmutar por error al módem 3G / 4G conectado al puerto USB.
- SSL VPN y VPN de sitio a sitio permiten una conectividad altamente segura, lo que hace que el Cisco RV320 sea perfecto para empleados remotos y múltiples oficinas.

- El firewall de inspección de paquetes (SPI) y el cifrado de hardware proporcionan una seguridad sólida.

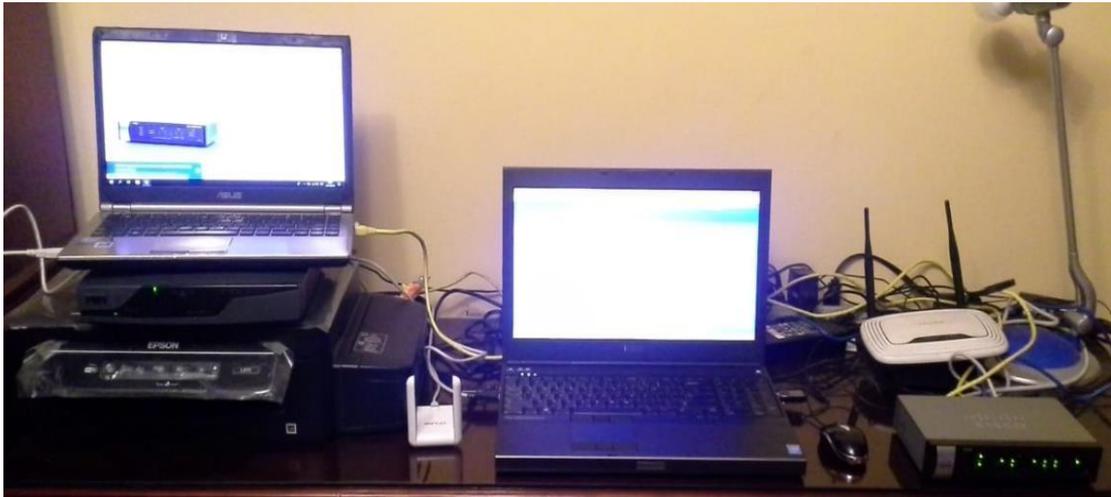
- Las herramientas de configuración basadas en asistente fáciles de usar se pueden usar para establecer la conectividad de la red y administrar la seguridad.

El Cisco RV320 Dual Gigabit WAN VPN Router es la opción para cualquier red en la que el rendimiento, la seguridad, la confiabilidad y la adaptabilidad sean los más importantes. Cisco RV320 admite dos conexiones a un proveedor de servicios, lo que proporciona un alto rendimiento mediante el equilibrio de carga, o dos proveedores diferentes para ofrecer continuidad empresarial. Las redes privadas virtuales (VPN) de alta capacidad conectan varias oficinas y permiten que docenas de empleados tengan acceso a la información que necesitan desde cualquier ubicación geográfica con la misma seguridad que si estuvieran trabajando en su oficina principal.

Anexo B: implementación del equipo Firewall



Anexo C: implementación del escenario de pruebas tipo laboratorio



Anexo D: Correo real de posible estafa por 850 dólares dentro del correo de la red empresarial (spam)

Yøur åccøũnt is bëing usëd by åñøthër përsøn!

acnn@biologie.uni-oldenburg.de

Enviado: lunes 0:24

Para:

Hëllø!

Í åm å håcker whø hås åccess tø yøur øpëráting systëm.
Í ålsø håvë full åccëss tø yøur åccøũnt.

Í've bëën wåtching yøu før å fëw mønths nøw.
Thë fáct is thåt yøu wërë ínfëctëd with målwårë thrøugh ån ådũlt síte thåt yøu vísítëd.

If yøu årë nøt fåmíliår with thís, Í wíll ëplåín.
Trøjån Vírus gívës më full åccëss ånd cøntrol øvër å cømpütër ør øthër dëvícë.
Thís mëåns thåt Í cån sëë ëvërything øn yøur scrëën, türn øn thë cåmërá ånd mícrøphønë, büt yøu dø nøt knøw åbøut ít.

Í ålsø håvë åccëss tø åll yøur cøntåcts ånd åll yøur cørrëspøndëncë.
If yøu want tø prevent thís, transfer the amount of \$850(USD) tø my bitcoin address (if yøu dø nøt knøw høw tø dø thís, wríte tø Google: 'Buy Bitcoin').

My bitcoin address (BTC Wallet) is: 1KVX9hCnQ9MfSoEFyxqAXGFxdTFNyzD22n

After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours tø pay.
I have a notice reading this letter, and the timer will work when yøu sëe thís lëttër.
Filing a complaint somewhere døes nøt make sënsë becåusë thís email cånnøt bë tråckëd líkë my bitcoin address.
I dø nøt make any mistakes.

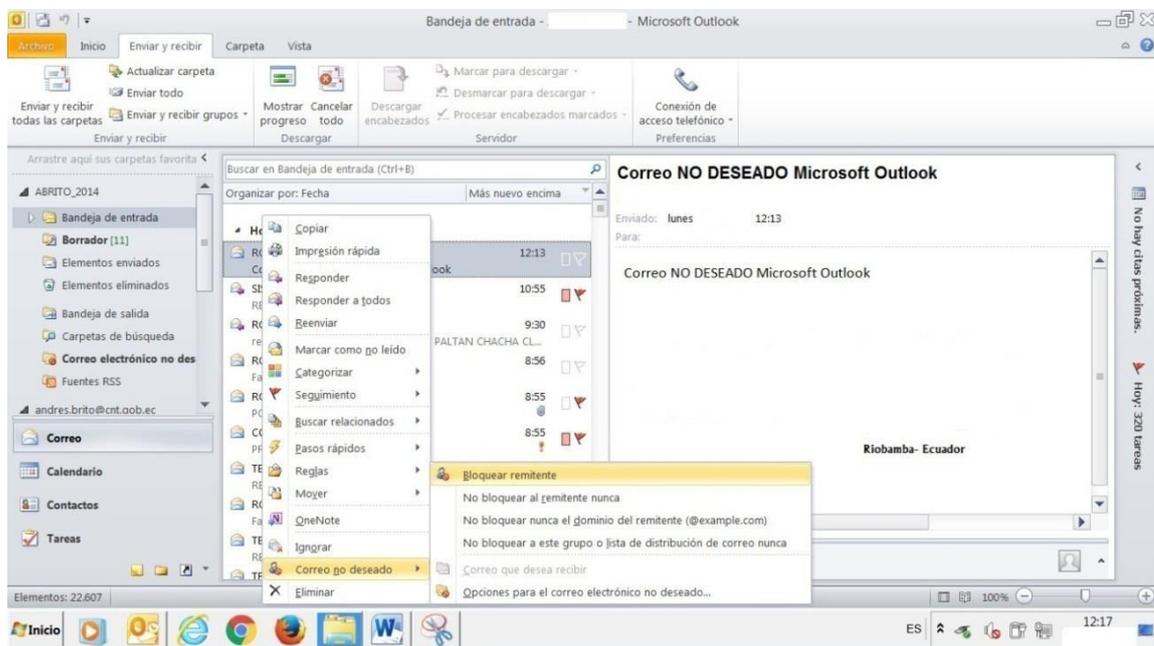
If I find thåt yøu håvë shårëd thís mëssågë with sòmëønë ëlsë, thë vídëø wíll bë ímmedíåttëly dístribúted.

Best regards!

Anexo E: Bloqueo de correo empresarial no deseado (spam)

Procedimiento a seguir en el caso que el correo electrónico empresarial de Microsoft Outlook se vea afectado por un correo de Fraude o spam, ya que la cuenta corporativa puede estar registrada en portales web o páginas de proveedores que se encuentran configurados en el servidor de correo Exchange es la siguiente:

- 1.- Hacer click derecho en el **correo Spam**
- 2.- Se escoge la opción de **Correo no deseado**
- 3.- Después se escogemos la opción **Bloquear remitente**

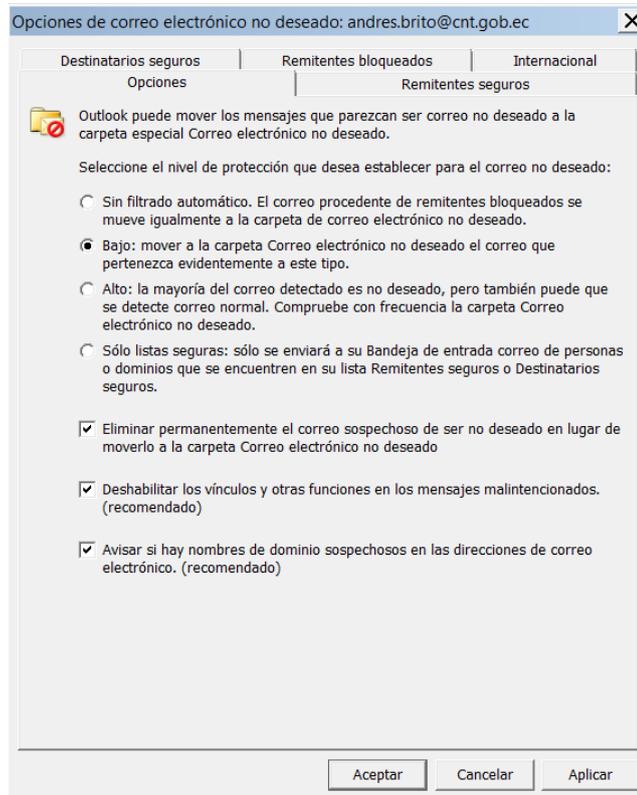
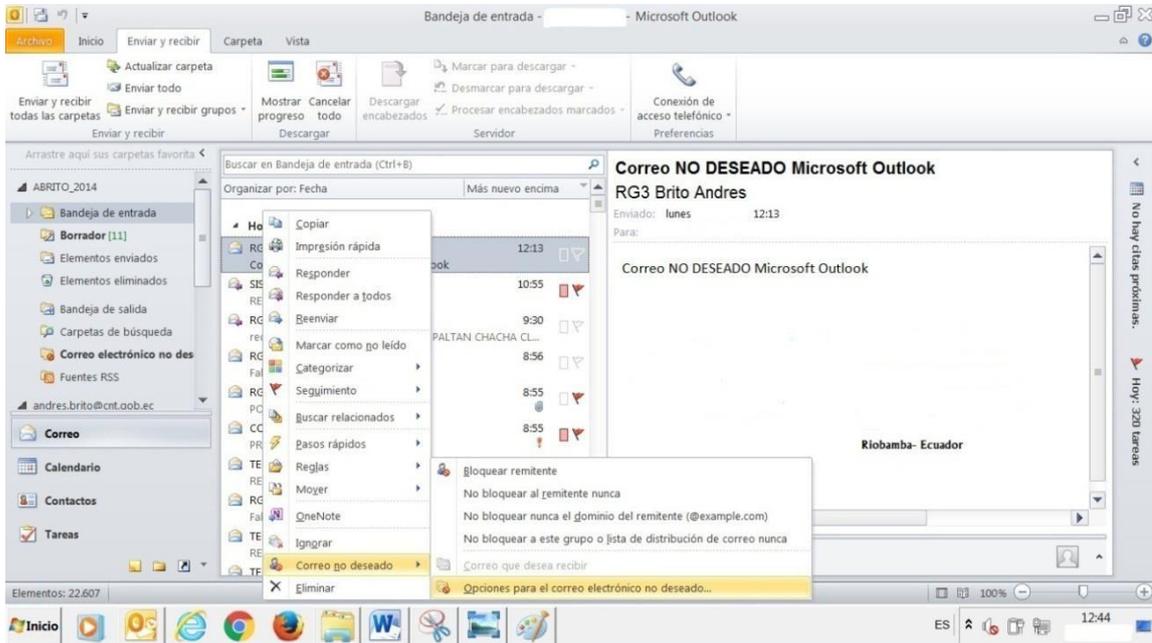


De esta manera queda configurado para se bloqueen los correos de este remitente y no ingresen a su bandeja de entrada de correo.

Para mayor seguridad se debe eliminar de forma permanente el correo spam siguiendo el siguiente procedimiento:

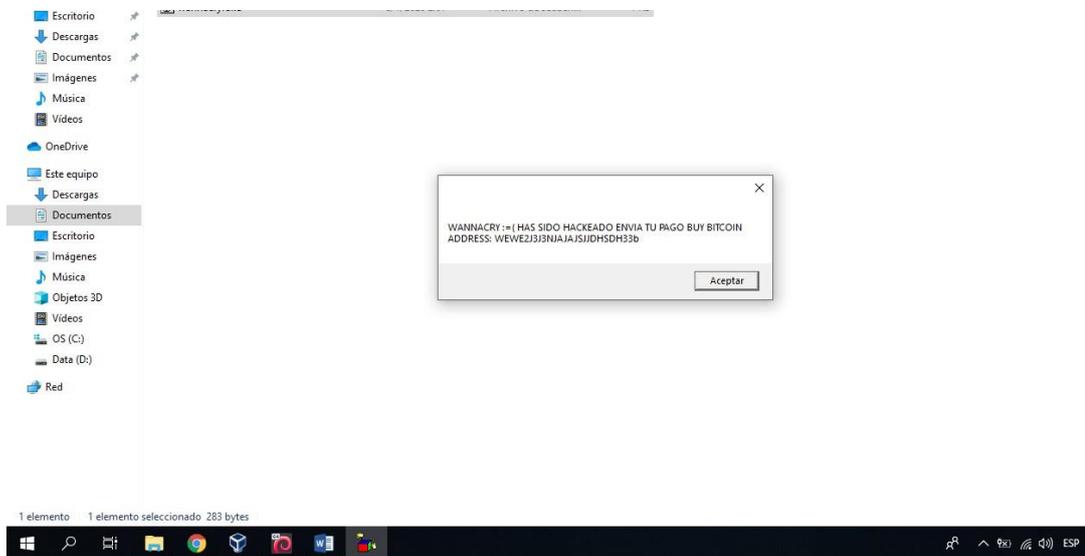
- 1.- Hacer click derecho en el **correo Spam**
- 2.- Se escoge la opción de **Correo no deseado**
- 3.- Después se escogemos **Opciones para el correo electrónico no deseado**

4.- Después ir a opciones y poner aplicar en **Eliminar permanentemente el correo sospechoso de ser no deseado en lugar de moverlo a la carpeta Correo electrónico no deseado**



Anexo F: Ataques Maliciosos

ATAQUE DE RANSOMWARE UTILIZANDO INGENIERIA SOCIAL



ATAQUE DE SQL INJECTION

```
Archivo Editar Ver Terminal Pestañas Ayuda
[15:39:08] [INFO] resumed: cdcol
[15:39:08] [INFO] resumed: cono
[15:39:08] [INFO] resumed: dante
[15:39:08] [INFO] resumed: inyeccion
[15:39:08] [INFO] resumed: mysql
[15:39:08] [INFO] resumed: performance_schema
[15:39:08] [INFO] resumed: phpmyadmin
[15:39:08] [INFO] resumed: test
[15:39:08] [INFO] resumed: webauth
available databases [10]:
[*] cdcol
[*] cono
[*] dante
[*] information_schema
[*] inyeccion
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
[*] webauth

[15:39:08] [INFO] fetched data logged to text files under '/home/dante/.sqlmap/output/192.168.1.1'
```

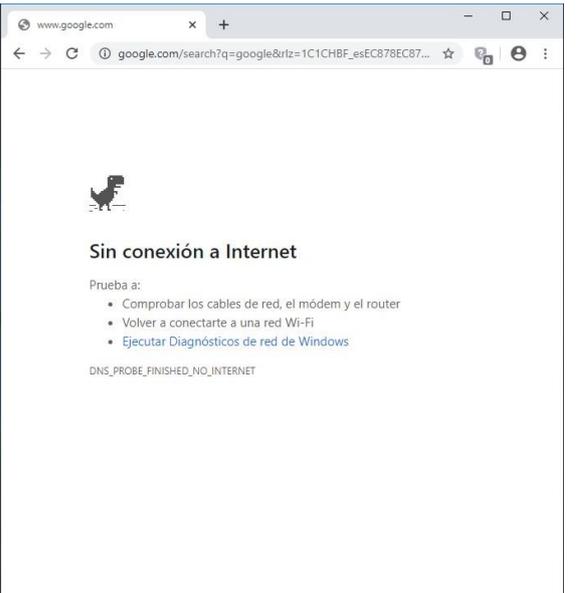
ATAQUE DENEGACION DE SERVICIO

```
root@kali: ~  
root@kali: ~ 91x24  
CH 11 ][ Elapsed: 2 mins ][ 2020-01-13 02:25  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
60:F1:8A:63:51:D0 -35 100 1366 43 0 11 130 WPA2 CCMP PSK NETLIFE-SAMS  
BSSID STATION PWR Rate Lost Frames Probe  
60:F1:8A:63:51:D0 E4:58:E7:6C:97:F7 -24 1e-24 0 30  
60:F1:8A:63:51:D0 A0:AB:1B:52:08:D2 -51 1e- 1e 0 4
```

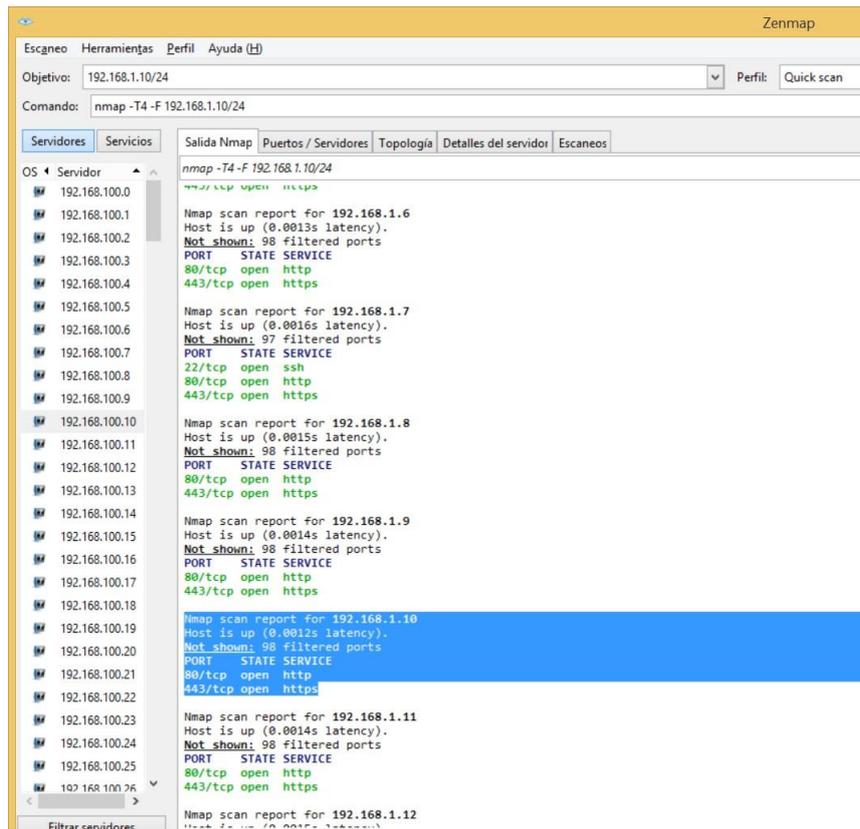
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# airodump-ng --bssid 78:32:1B:BC:BC:88 --channel 6 --write test wlan0
```

```
00:38:26 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|63 ACKs]  
00:38:27 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:27 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:28 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:29 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|65 ACKs]  
00:38:30 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|63 ACKs]  
00:38:30 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:31 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:32 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:32 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:33 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:34 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:34 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|64 ACKs]  
00:38:34 Sending 64 directed DeAuth (code 7). STMAC: [40:25:C2:A6:32:0C] [ 0|46 ACKs]  
root@kali:~# aireplay-ng --deauth 1000 -a 60:F1:8A:63:51:D0 -c 40:25:C2:A6:32:0C wlan0
```

```
Simbolo del sistema - ping 8.8.8.8 -  
Respuesta desde 8.8.8.8: bytes=32 tiempo=98ms TTL=55  
Respuesta desde 8.8.8.8: bytes=32 tiempo=99ms TTL=55  
Respuesta desde 8.8.8.8: bytes=32 tiempo=101ms TTL=55  
Respuesta desde 8.8.8.8: bytes=32 tiempo=98ms TTL=55  
Tiempo de espera agotado para esta solicitud.  
Tiempo de espera agotado para esta solicitud.  
Error general.  
Error general.  
Error general.  
Tiempo de espera agotado para esta solicitud.  
Tiempo de espera agotado para esta solicitud.  
Tiempo de espera agotado para esta solicitud.  
Respuesta desde 192.168.100.72: Host de destino inaccesible.  
Tiempo de espera agotado para esta solicitud.  
Tiempo de espera agotado para esta solicitud.  
Respuesta desde 192.168.100.72: Host de destino inaccesible.  
Respuesta desde 192.168.100.72: Host de destino inaccesible.  
Respuesta desde 192.168.100.72: Host de destino inaccesible.  
Respuesta desde 192.168.100.72: Host de destino inaccesible.
```



ESCANEOS DE PUERTOS



ATAQUE DE DENEGACION DE SERVICIO CON METASPLOIT FRAMEWORK

```
.100000001.
.dod,
.

=[ metasploit v5.0.60-dev ]
-- ==[ 1947 exploits - 1089 auxiliary - 333 post ]
-- ==[ 556 payloads - 45 encoders - 10 nops ]
-- ==[ 7 evasion ]

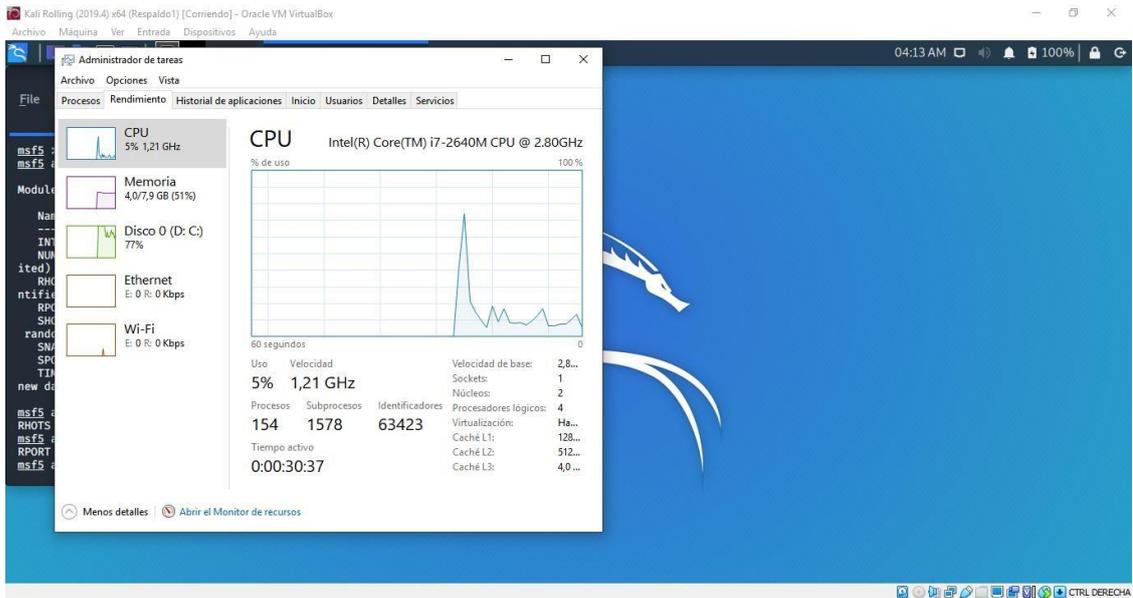
msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

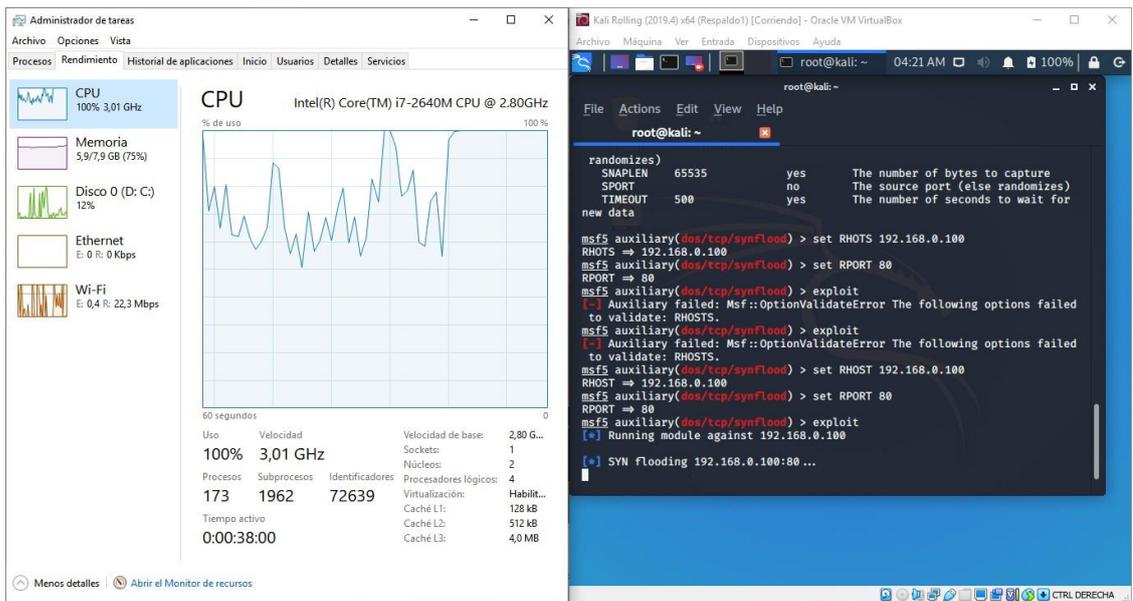
Name      Current Setting  Required  Description
-----
INTERFACE  no               no        The name of the interface
NUM        no               no        Number of SYNs to send (else unlimited)
RHOSTS    yes              yes       The target host(s), range CIDR identifier, or hosts file with
syntax 'file:<path>'
RPORT     80               yes       The target port
SHOST     no               no        The spoofable source address (else randomizes)
SNAPLEN   65535            yes       The number of bytes to capture
SPORT     no               no        The source port (else randomizes)
TIMEOUT   500              yes       The number of seconds to wait for new data

msf5 auxiliary(dos/tcp/synflood) >
```

Anexo G: Funcionamiento Normal de un computador



Funcionamiento de un computador bajo ataque





epoch

Dirección de Bibliotecas y
Recursos del Aprendizaje 0

UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y
DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 26 / 06 / 2023

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: <i>Jorge Favián Peña Arpi</i>
INFORMACIÓN INSTITUCIONAL
<i>Instituto de Posgrado y Educación Continua</i>
Título a optar: <i>Magíster en Seguridad Telemática</i>
f. Analista de Biblioteca responsable: Lic. Luis Caminos Vargas Mgs.



LUIS ALBERTO
CAMINOS VARGAS



0006-DBRA-UTP-IPEC-2023