ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

PROPUESTA DE UN SISTEMA DE SEGURIDAD PERIMETRAL MEDIANTE LA PROTECCIÓN FIREWALL DE PRÓXIMA GENERACIÓN NGFW APLICABLE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL CANTÓN RIOBAMBA

ANDRÉS FELIPE BRITO DEL PINO

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

Noviembre 2021

©2021, Andrés Felipe Brito del Pino

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

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN

El **Trabajo de Titulación modalidad Proyecto de Investigación y Desarrollo, titulado PROPUESTA DE UN SISTEMA DE SEGURIDAD PERIMETRAL MEDIANTE LA PROTECCIÓN FIREWALL DE PRÓXIMA GENERACIÓN NGFW APLICABLE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL CANTÓN RIOBAMBA**, de responsabilidad del señor Andrés Felipe Brito del Pino, ha sido minuciosamente revisado y se autoriza su presentación.

Luis Eduardo Hidalgo Almeida

Firmado digitalmente porLuis Eduardo Hidalgo Almeida
DN: cn=Luis Eduardo Hidalgo Almeida gn=Luis Eduardo Hidalgo Almeida c=EC Ecuador l=EC Ecuador o=ESPOCH ou=Instiuto de Posgrado y Educacion continua e=l_hidalgo@espoch.edu.ec
Motivo:Soy el autor de este documento
Ubicaci n:
Fecha:2021-11-18 17:16-05:00

Ing. Luis Eduardo Hidalgo Almeida; PhD.
PRESIDENTE

Firmado electrónicamente por:
OSWALDO GEOVANNY MARTINEZ GUASHIMA

Ing. Oswaldo Geovanny Martínez Guashima; M.Sc.
TUTOR

Firmado electrónicamente por:
CHRISTIAN FERNANDO BARRAGAN QUIZHPE

Ing. Christian Fernando Barragán Quizhpe; M.Sc.
MIEMBRO

ANGEL PATRICIO MENA REINOSO

Firmado digitalmente por ANGEL PATRICIO MENA REINOSO
Fecha: 2021.11.16 10:47:46

Ing. Ángel Patricio Mena Reinoso; M.Sc.
MIEMBRO

Riobamba, noviembre 2021

DERECHOS INTELECTUALES

Yo, Andrés Felipe Brito del Pino, soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyecto de Investigación y Desarrollo, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Firmado electrónicamente por:
ANDRES FELIPE BRITO DEL PINO

Andrés Felipe Brito del Pino

No. Cédula: 0603451089

DECLARACIÓN DE AUTENTICIDAD

Yo, Andrés Felipe Brito del Pino declaro que el presente Trabajo de Titulación, modalidad Proyectos de Investigación y Desarrollo, es de mí autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Firmado electrónicamente por:
ANDRES FELIPE BRITO DEL PINO

Andrés Felipe Brito del Pino

No. Cédula: 0603451089

DEDICATORIA

El presente trabajo de titulación les dedico a mi padre y a mi madre que están en el cielo, por sus enseñanzas de vida, por su guía, por su apoyo en todo momento, merecen mi admiración y respeto.

A mi esposa Sofía y a mi hijo Gabriel, por ser mi felicidad, mi guía, mi inspiración y mi apoyo para seguir adelante.

A mi país Ecuador, que es donde nací y es la tierra que Amo.

Felipe Brito del Pino

AGRADECIMIENTO

Quiero agradecer sobre todo a Dios, por la vida, por el despertar de un nuevo día, por sentirme en su presencia, por estar en su presencia. Por darme la inteligencia y la sabiduría, para no doblegarme a las adversidades, para no rendirme, para luchar por mis sueños, para luchar por un ideal, para luchar por la Verdad.

Felipe Brito del Pino

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo de esta investigación fue realizar una propuesta de un sistema de seguridad perimetral con firewall de próxima generación NGFW para Pymes del cantón Riobamba. La seguridad de la información ha sido un tema fundamental para el sector empresarial, que va a la mano de la seguridad perimetral. La evolución de la tecnología implica problemas de vulnerabilidades que atentan contra la seguridad, disponibilidad e integridad de la información en las redes empresariales. 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 NGFW, además se refiere a un diseño de investigación experimental en el cual los ataques de estudio no están asignados aleatoriamente. La seguridad de la red es una actividad crítica para muchas empresas e incluso puede ser la actividad que define el negocio. Por ello, se debe mantener un equilibrio entre seguridad y acceso a la información. Si la red es muy restrictiva va perjudicar en el funcionamiento de la empresa y si es muy permisiva va a poner en peligro el activo más importante que tiene una empresa que es la información. La alta gerencia y el responsable de tecnologías de la información (TI) son los encargados de implementar la seguridad de la información, por ello se planteó una propuesta de un sistema de seguridad perimetral firewall NGFW para Pymes, que permita asegurar la red empresarial frente a ataques, que disminuya considerablemente las brechas de seguridad, que dicha solución sea económica y de fácil administración para el responsable de tecnologías de la información (TI). Analizando los resultados de la propuesta de un sistema de seguridad perimetral con firewall de próxima generación NGFW se concluye que permite mejorar considerablemente la seguridad en las Pymes.

Palabras Claves: <SEGURIDAD INFORMÁTICA>, <SEGURIDAD PERIMETRAL>, <RED EMPRESARIAL>, <ACCESO A LA INFORMACIÓN>, <FIREWALL NGFW>, <TECNOLOGIAS DE LA INFORMACIÓN (TI)>

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS

Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS

UNIDAD DE PROCESOS TÉCNICOS DBRA DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE ESPOCH

0108-DBRAI-UPT-IPEC-2021

ABSTRACT

The main objective of this study was to propose a perimeter security system with a next-generation firewall NGFW for SMEs of the canton Riobamba. The safety of the Information has been a fundamental issue for the business sector, which goes hand in hand with the security perimeter. The evolution of technology implies vulnerability problems that threaten the security, availability, and integrity of information in business networks. The design of the research is a QUASI-EXPERIMENTAL design since it is experimented with a scenario of T-tests, with NGFW next-generation firewall equipment. It also refers to experimental design research in which the attacks are not randomly assigned. Network security is a critical activity for many companies and may even be the activity that defines the business. Therefore, a balance must be maintained between security and access to information. If the network is very restrictive, it will harm the operations of the company and if it is very permissive it is going to jeopardize the most important asset that a company has, which is the information. The high management and head of information technology (IT) are in charge of implementing information security, which is why a proposal for a security system was proposed a perimeter firewall NGFW for SMEs, that allows securing the business network against attacks and significantly reduce security gaps. This solution needs to be economical and with an easy administration for the person in charge of information technology (IT). Analyzing the results of the proposal for a perimeter security system with a next-generation firewall NGFW it is concluded that it considerably improves the security in SMEs.

Keywords: < NETWORK SECURITY>, <PERIMETER SECURITY>, < BUSINESS NETWORK>, <INFORMATION ACCESS >, <FIREWALL NGFW>, <INFORMATION TECHNOLOGIES (IT)>.

CAPÍTULO I

1. INTRODUCCIÓN

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).

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).

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 lógica hace referencia a la aplicación de mecanismos y barreras para mantener el reguardo 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)

1.1. Problema de la investigación

Hay pequeñas y medianas empresas que piensan que nunca van a tener problemas de seguridad informática. Que eso sólo pasa a las grandes empresas, que son las que tienen más dinero y por tanto los ciberdelincuentes están más interesados en ellas. Lo cierto es que esto no es más que un

mito, ya que son precisamente las pymes quienes muchas veces presentan más problemas de seguridad informática. (Julia, 2017)

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)

1.2. Planteamiento del problema

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)

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 irremediablemente implica a su vez una mayor vulnerabilidad y exposición a los ciberataques. (GESI, 2018)

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 2018, 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. De hecho, 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 avanzo y en cinco días penetró en los ordenadores de 17 empresas privadas e instituciones públicas de Quito, Guayaquil y Cuenca. El programa maligno ingreso en las computadoras y encriptó archivos sensibles de Word, Excel y Autocad, el virus denominado cryptolocker llego 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 Estados Unidos 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).

1.2.1. 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).

1. **Grande**

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

2. **Mediana B**

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

3. **Mediana A**

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

4. **Pequeña**

   V: $ $100.001 a $1´000.000. P: 10 a 49

5. **Microempresa**

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

1.2.2. 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.

Tamaño de Empresa	No. Empresas
Microempresa	816.553
Pequeña empresa	64.117
Mediana empresa "A"	8.529
Mediana empresa "B"	5.749
Grande empresa	4.260
Total	899.208

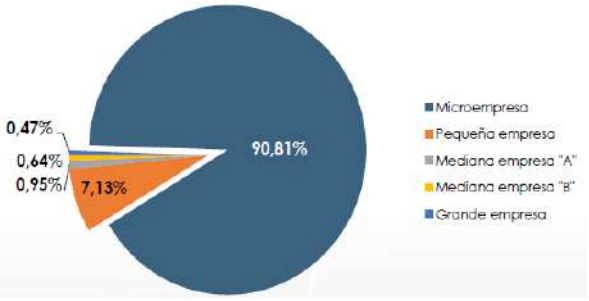


Figura 1-1 Clasificación de tamaño de empresa.

Fuente: INEC, Directorio de Empresas 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).

1. Agricultura, ganadería, silvicultura y pesca.
2. Explotación de minas y canteras.
3. Industrias manufactureras.
4. Comercio.
5. Servicios.

1.2.3. 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.

Sector Económico	No. Empresas
Servicios	383.582
Comercio	314.127
Agricultura, ganadería, silvicultura y pesca	93.336
Industrias Manufactureras	75.364
Construcción	30.826
Explotación de Minas y Canteras	1.973
Total	899.208

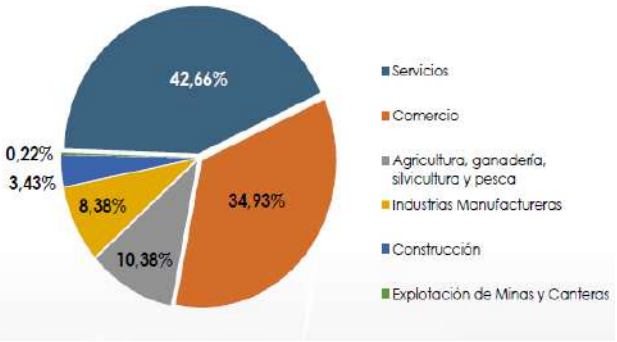


Figura 1-2 Clasificación de empresas según sector económico.

Fuente: INEC, Directorio de Empresas 2018**.**

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

Fuente: INEC, Directorio de Empresas 2018.

En la figura 1-3 se puede observar 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 Riobamba.

1.2.4. Perfil económico del cantón Riobamba

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 en comercios especializados

Servicios

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

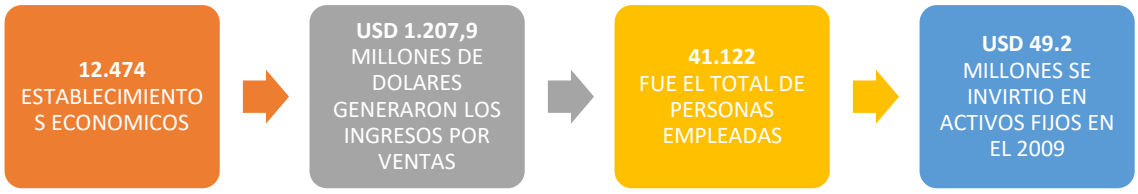


Figura 1-4 Perfil económico del cantón Riobamba.

Fuente: INEC 2011.

Tabla 1-1 Ingreso de sectores en dólares

INGRESOS GENERADOS EN EL CANTÓN RIOBAMBA	
INGRESOS DEL SECTOR	**DOLARES**
Manufactura	**USD 105 millones**

Comercio	**USD 464 millones**
Servicios	**USD 637 millones**
Otros	**USD 1.9 millones**

Fuente: INEC 2011.

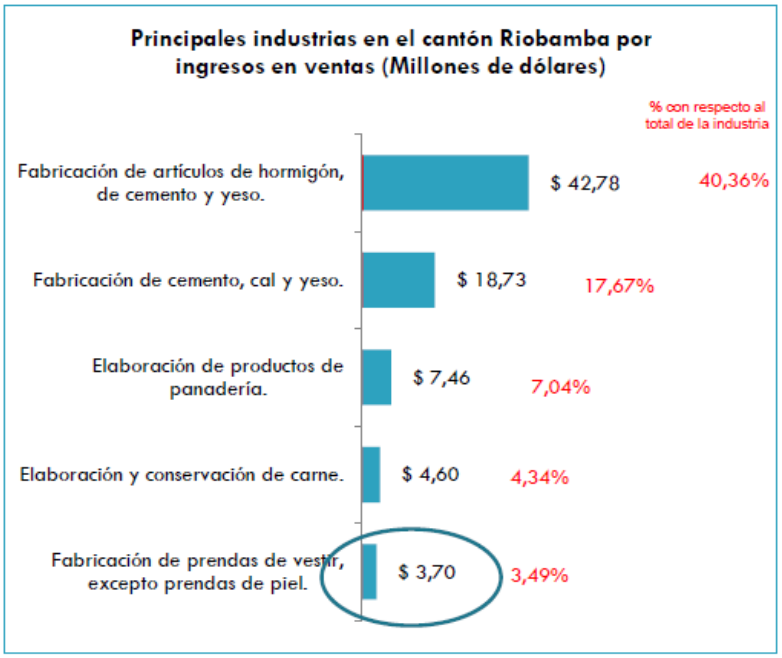


Figura 1-5 Principales industrias en el Cantón Riobamba**.**

Fuente: INEC 2011.

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

Fuente: INEC 2011.

1.3. Formulación del problema

¿Falta de disponibilidad, integridad y seguridad de la información en las Pymes?

1.4. Sistematización del problema

¿Cuál es el estado de las normativas y regulaciones que ha desarrollado el país para fortalecer la seguridad perimetral de las Pymes?

1.5. Justificación de la investigación

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 firewall 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.

Por lo tanto, todas las comunicaciones desde el exterior a las Pymes deben ser minuciosamente analizadas y comprobadas, antes de ser autorizadas, rechazando de forma automática los intentos de ingreso de forma fraudulenta.

Es imprescindible contar con la cooperación de todos los sectores involucrados en la planificación, operación y regulación de las diferentes infraestructuras que proporcionan servicios de internet para las Pymes, como son el estado, la universidad, empresa pública y la empresa privada.

1.6. Objetivos de la investigación

1.6.1. Objetivo General:

- Realizar una propuesta de un sistema de seguridad perimetral con firewall de próxima generación NGFW para Pymes del cantón Riobamba.

1.6.2. Objetivos Específicos:

- Analizar normativas y estándares existentes para el aseguramiento de la información de pymes.
- Diseñar un sistema de seguridad perimetral que permita asegurar la información de las pymes utilizando conceptos de firewall de próxima generación NGFW.
- Definir un escenario de pruebas tipo laboratorio con un equipo que posea funciones de seguridad y firewall para comprobar el diseño y hacer una evaluación del mismo.
- Implementar y evaluar el sistema mediante una estructura de aplicabilidad.

1.7. Hipótesis

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

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes

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)

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)

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)

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 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.

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 de 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).

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)

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.

2.1.1. Metodología

La metodología implementada propone una mejora en la seguridad perimetral en las redes de datos de las pymes, 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.

2.1.2. Ventajas

- Una de las acciones fundamentales que ayudan a mitigar los problemas de seguridad informática en Pymes, es el de establecer una seguridad perimetral de próxima generación NGFW.
- El implementar un firewall NGFW para Pymes es una solución económica y segura, además facilita la administración del responsable de seguridad informática.
- Los firewalls de próxima generación NGFW son aptos para 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.
- El equipo firewall NGFW permite actualizar el firmware, lo cual corrige errores, realiza mejoras a su funcionalidad, aumentando el rendimiento de la red sin tener que comprar ningún hardware nuevo.
- Tanto los firewalls 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.

2.1.3. Desventajas

- En el Ecuador existe escases de profesionales en seguridad telemática, además el desconocimiento de cómo dar seguridad informática por parte de los responsables de la red empresarial de las Pymes, es una vulnerabilidad que los ciberdelincuentes pueden explotar.
- Las Pymes 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 Pymes, 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.

2.2. Firewall de próxima generación NGFW

El Firewall de próxima generación o NGFW fue 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 puertas. 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 o Next Generation o Cortafuegos (NGFW) 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 innensarios, 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 mejor la actividad sospechosa o evasiva con correlación de eventos de terminales y la 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. Diferencias entre Firewall UTM y Firewall 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, sin hacer diferenciación en el mercado que se apliquen.

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. De la cual 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 Firewalls 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 2-1 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 están 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 2-3 Cuadrante mágico de Gartner 2019

Fuente: Gartner (Julio 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 2-1 Estimación selección Firewall.

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

Fuente: Felipe Brito 2019.

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: Felipe Brito 2019.

2.6. Normas y estándares internacionales para el aseguramiento de la información en las pymes.

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)

Alcance y propósito

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 (ISO27033, 2015)

- 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 (como por *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);

2.6.3. ISO / IEC 27033-2: 2012: Directrices para el diseño e implementación de seguridad de red. (ISO27033, 2015)

- Alcance: planificación, diseño, implementación y documentación de la seguridad de la 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 detalladas sobre seguridad de red de extremo a extremo.
- Cubre riesgos, diseño, técnicas y problemas de control.

2.6.4. ISO / IEC 27033-3: 2010: Escenarios de redes de referencia: amenazas, técnicas de diseño y problemas de control. (ISO27033, 2015)

- 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.

2.6.5. ISO / IEC 27033-4: 2014

Asegurar las comunicaciones entre redes utilizando pasarelas de seguridad. (ISO27033, 2015)

- 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 a través de:
    - 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 de una organización.
- Se refiere a varios tipos de firewall como ejemplos de puertas de enlace de seguridad.

2.6.6. ISO / IEC 27033-5: 2013

Asegurando las comunicaciones a través de redes usando Redes Privadas Virtuales (VPN) (ISO27033, 2015)

- Objetivo: proporcionar pautas para la selección, implementación y monitoreo de los controles técnicos necesarios para proporcionar seguridad de red utilizando conexiones de Red Privada Virtual (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 / intercepción 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, aunque estos se mencionan o al menos se insinúan más adelante según los requisitos de seguridad.
- 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.

2.6.7. ISO / IEC 27033-6: 2016

Asegurando el acceso a la red IP inalámbrica (ISO27033, 2015)

- 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 (por ejemplo, arquitectos y diseñadores de redes, administradores de redes y oficiales de seguridad de redes).
- 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.

2.6.8. OEA (Organización de Estados Americanos) y Microsoft

La Organización de los Estados Americanos (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.

Así mismo (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.

2.6.9. Normativas y estándares en el Ecuador para el aseguramiento 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). (EGSI, 2013)

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.

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).

Así mismo (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 todo 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 el Estado Ecuatoriano 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.

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 PYMES, para ser específicos, las 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.

En el artículo primero, literal c) de dicha resolución textualmente se 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*

De acuerdo a la recomendación UIT-T X.1205, sobre 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. 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)

2.7.6. 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)

2.7.7. 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)

2.7.8. 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 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 despechado
- 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 pequeña o mediana empresa 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 firewall NGFW para pequeñas o medianas empresas, 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 constate 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 perdonas 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, en lo posible 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 LA 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 Riobamba.

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 NGFW, 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 NGFW 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 3-1 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.

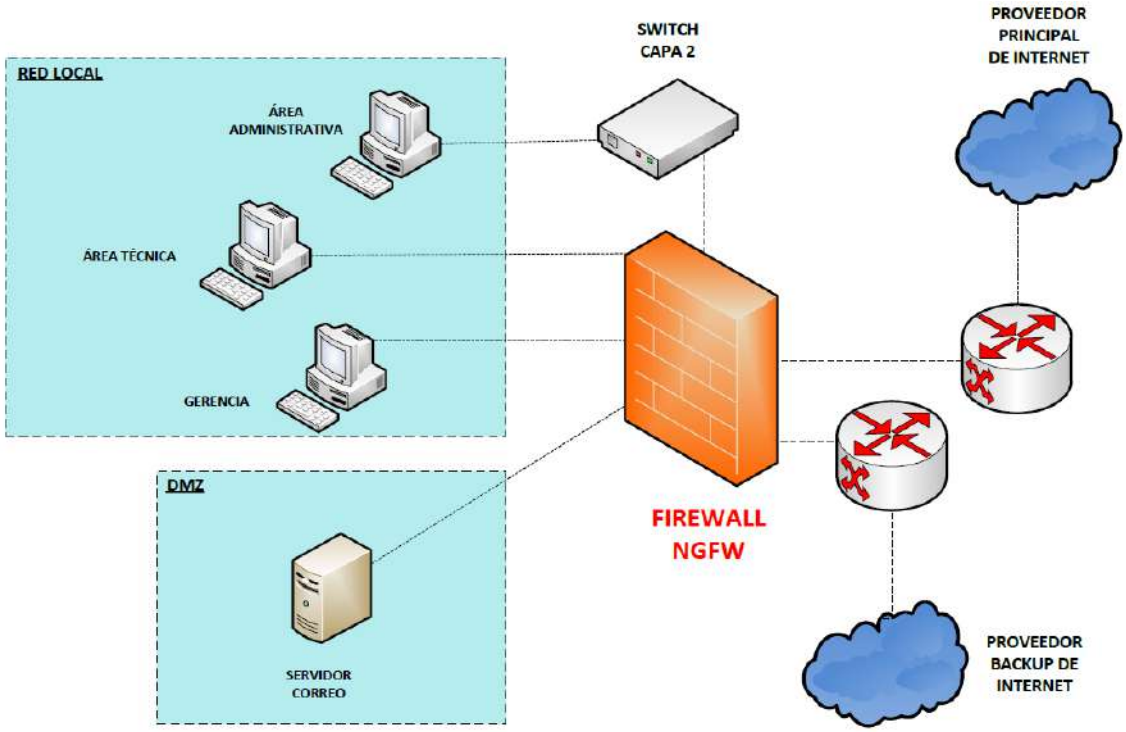


Figura 3-2 Propuesta de un escenario de Pruebas.

Fuente: Felipe Brito 2019.

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: Mejora de la seguridad en las pymes

Variable independiente: Diseño de seguridad perimetral con equipo firewall NGFW

3.8.1. Operacionalización de variables

Tabla 3-1 Operacionalización de variables

VARIABLE	TIPO	DEFINICIÓN
Mejora de la seguridad en las pymes	Dependiente	Selección de la tecnología que permita mejorar la seguridad en las pymes.
Diseño de seguridad perimetral con equipo firewall NGFW	Independiente	Análisis de diferentes protocolos de seguridad existentes utilizados en equipos firewalls.

Fuente: Felipe Brito 2019.

Tabla 3-2 Operacionalización metodológica de variables.

Hipótesis General	Variables	Indicadores	Índices	Técnicas
La implementación de un sistema de seguridad perimetral con firewall de próxima generación NGFW mejorará confidencialidad, integridad y autenticación de la información en las Pymes.	**Variable Dependiente** (Mejora de la seguridad en 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	
		Disponibilidad		

	Variable Independiente (Diseño de seguridad perimetral con equipo firewall NGFW)		Evita desasociación	Observación Recopilación de información Análisis
			Excluye la inserción de tráfico	
		Autorización	Distribución manual de clave	Observación Recopilación de información Análisis
			Inserción de tráfico	
			Autenticación basada en clave	
		Aplicabilidad	Existencia de productos en el Ecuador	Observación Recopilación de información Análisis
			Tecnología permitida y regulada en el país	

Fuente: Felipe Brito 2019.

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 DES, Triple DES, AES 128(bits), AES 192(bits) y AES 256(bits), y protocolo de autenticación IEEE 802.1X.

Tabla 3-3 Algoritmos de cifrado

ALGORITMOS DE CIFRADO					
Confidencialidad	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Autenticación	IEEE 802.1X				

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

PRINCIPIOS	**PRINCIPALES AMENAZAS / VULNERABILIDADES**
Confidencialidad	Phishing (Ingeniería social)
Integridad	Ataque de SQL Injection
Autenticación	Ransomware (malware)

Fuente: Felipe Brito 2019.

Phishing. - Es uno de los métodos más usados por los ciberdelincuentes para obtener información confidencial de forma fraudulenta y estafar, como puede ser información de las tarjetas de crédito o contraseñas valiéndose de técnicas de ingeniería social.

Ataque de SQL Injection. – Es una vulnerabilidad que permite al atacante inyectar instrucciones SQL de forma mal intencionada y maliciosa dentro del código SQL programado para manipula base de datos.

Ransomware. – Es un tipo de malware que no permite a un usuario acceder a sus archivos personales o su sistema, en la cual se exige un rescate para acceder a ellos. El malware puede infectar el ordenador a través de un correo electrónico en la cual se pueden adjuntar archivos maliciosos como PDF o documentos de Word.

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 3-5 Herramientas y su descripción.

HERRAMIENTA	DESCRIPCIÓN
Wireshark	Analizador de red
Kali Linux	Ataque de SQL Injection
Ingeniería Social	Phishing, Ransomware

Fuente: Felipe Brito 2019.

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.

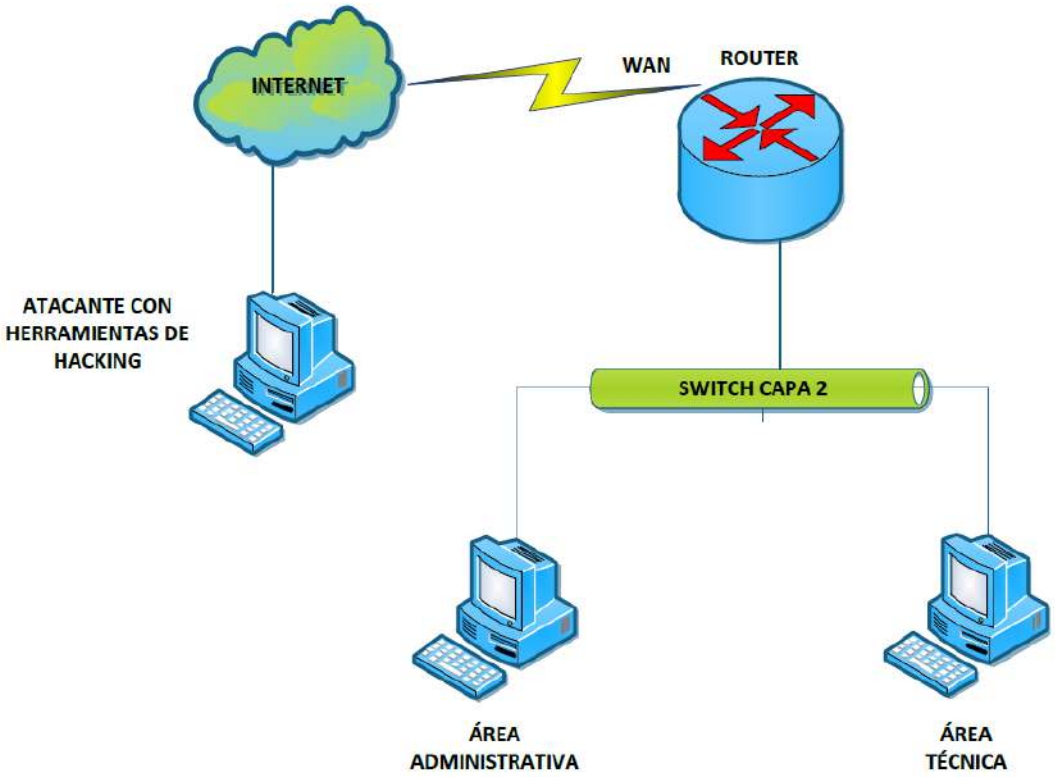


Figura 3-3 Escenario de Pruebas sin seguridad.

Fuente: Felipe Brito 2019.

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 NGFW 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

En el capítulo III se analizan algunos ciberataques que sufren las pequeñas y medianas empresas, más de la mitad están relacionadas con la estafa como el phishing y el ransomware. El phishing consiste en suplantar la identidad de una empresa o persona para poder acceder a información privada de sus víctimas. En el ransomware, los crackers secuestran los sistemas informáticos de empresas o personas, cifrando el contenido y pidiendo un rescate para descifrar la información.

Es una negligencia por parte del responsable de seguridad de una Pyme no conocer las amenazas a las que está expuesta la empresa y las consecuencias que puede tener como una afectación en el normal funcionamiento empresarial hasta su cierre definitivo.

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.

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

CATEGORÍA	ABREVIACIÓN	ESTIMACIÓN

Muy Malo	Mn	0
Malo	M	1
Bueno	B	2
Muy Bueno	Mb	3
Excelente	E	4

Fuente: (Ramos, 2012)

VARIABLE INDEPENDIENTE

Análisis de vulnerabilidades de los algoritmos de cifrado

4.1.1. Indicador 1: Disponibilidad

Tabla 4-2 Disponibilidad

ÍNDICES	**DES**	**Triple DES**	**AES 128(bits)**	**AES 192(bits)**	**AES 256(bits)**
Evita desasociación	Mn	M	B	Mb	E
Excluye la inserción de tráfico	Mn	B	B	Mb	E

Fuente: Felipe Brito 2019.

Tabla 4-3 Resultados de la Disponibilidad

ÍNDICES	**DES**	**Triple DES**	**AES 128(bits)**	**AES 192(bits)**	**AES 256(bits)**
Evita desasociación	0	1	2	3	4

Excluye la inserción de tráfico	0	2	2	3	4

Fuente: Felipe Brito 2019.

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
Inserción de tráfico	SI	SI	NO	NO	NO
Considerado seguro	NO	NO	SI	SI	SI

Fuente: Felipe Brito 2019.

Tabla 4-5 Resultados de la Autorización

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

Fuente: Felipe Brito 2019.

Interpretación:

Actualmente 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 4-6 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
Tecnologia permitida y regulada en el país.	SI	SI	SI	SI	SI

Fuente: Felipe Brito 2019.

Tabla 4-7 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
Tecnología permitida y	1	1	1	1	1

regulada en el país.					

Fuente: Felipe Brito 2019.

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 4-8 Resumen del análisis de la variable independiente

IDENTIFICADOR	INDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
PWI	Disponibilidad	0	3	4	6	8
	Autorización	2	2	1	1	1
	Aplicabilidad	2	2	2	2	2
TOTAL (PT_PW)		4	7	7	9	11

Fuente: Felipe Brito 2019.

4.2. Análisis e interpretación de resultados variable dependiente

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.

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

CATEGORÍA	ABREVIACIÓN	ESTIMACIÓN	PORCENTAJE
Totalmente Incorrecto	TI	0	0%
Incorrecto	I	1	25%
Poco Correcto	PI	2	50%
Correcto	C	3	75%
Muy Correcto	MC	4	100%

Fuente: (Ramos, 2012)

VARIABLE DEPENDIENTE

Tecnología adecuada para el cifrado de la información

4.2.1. *Indicador 1:* Confidencialidad

Tabla 4-10 Confidencialidad

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Algoritmo de cifrado mejorado	TI	I	C	C	MC
Tamaño de algoritmo de cifrado	PI	PI	C	MC	MC
Cifrado generado dinámicamente	I	I	PI	C	MC

Fuente: Felipe Brito 2019.

Tabla 4-11 Resultados de la 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: Felipe Brito 2019.

Interpretación:

La confidencialidad depende el algoritmo de cifrado que se vaya 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 4-12 Integridad.

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Integridad de la cabecera	I	I	PI	C	MC
Integridad cifrada	TI	PI	C	MC	MC

Integridad dependiente de la clave	TI	I	PI	C	MC

Fuente: Felipe Brito 2019.

Tabla 4-13 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: Felipe Brito 2019.

4.2.3. Indicador 3: Autenticación

Tabla 4-14 Autenticación

ÍNDICES	DES	Triple DES	AES 128(bits)	AES 192(bits)	AES 256(bits)
Autenticación de usuario	I	I	PI	C	MC
Uso de protocolo de autenticación	I	I	C	C	MC
Velocidad de ejecución	C	C	PI	I	I

Fuente: Felipe Brito 2019.

Tabla 4-15 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: Felipe Brito 2019.

Tabla 4-16 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	11	12
Integridad	1	4	7	10	12
Autenticación	5	5	7	7	9
SUB TOTAL	**9**	**13**	**22**	**28**	**33**
%	**25,00**	**36,11**	**61,11**	**77,78**	**91,67**

Fuente: Felipe Brito 2019.

Tabla 4-17 Análisis de la 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	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
AUTENTIFICACION	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**	**0**	**5**	**4**	**0**	**0**	**1**	**0**	**6**	**2**	**0**	**1**	**0**	**0**	**8**

Fuente: Felipe Brito 2019.

Tabla 4-18 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: (Ramos, 2012)

Tabla 4-19 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	0,8	0	0	2	1	1	0	0	0	2,5	3	0	0,0	0,25	0,0	4,50	2	0,0	0,25	0,0	0,00	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**	

Fuente: Felipe Brito 2019.

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 del algoritmo de cifrado y autenticación permiten determinar una tecnología adecuada para el acceso seguro a la red empresarial.

H_0 = El análisis del algoritmo de cifrado y la autenticación de la red no permiten determinar una tecnología adecuada para el acceso seguro a la red empresarial.

Nivel de significación:

$$\propto = 0{,}05$$

Criterio

$$\text{Rechace la } H_0 \text{ si } \boldsymbol{X_c^2 \geq X_t^2}$$

$\boldsymbol{X_c^2}$ = chi cuadrado calculado.

$\boldsymbol{X_t^2}$ = chi cuadrado de tabla

Tabla 4-20 Tabla de contingencia de lo observado

Dependiente	Índices	DES	Triple DES	AES 128 (bits)	AES 192 (bits)	AES 256 (bits)	TOTAL
Mejora de la seguridad en 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: Felipe Brito 2019.

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

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

Dónde N es el número total de frecuencias observadas

Tabla 4-21 Tabla de frecuencias de lo esperado

Dependiente	Índices	DES	Triple DES	AES 128 (bits)	AES 192 (bits)	AES 256 (bits)	TOTAL
Mejora de la seguridad en 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: Felipe Brito 2019.

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

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

DÓNDE:

O = EL NÚMERO OBSERVADO

E = EL NÚMERO ESPERADO

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

Tabla 4-22 Tabla del cálculo del Chi-cuadrado

	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: Felipe Brito 2019.

PROBABILIDAD	0,05		
CHI CUADRADO	**16,11**		
GRADOS DE LIBERTAD	8	GL=(M-1)*(N-1)	M=NUMERO DE FILAS
VALOR DE REFERENCIA	**15,5**		N=NUMERO DE COLUMNAS

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 4-23 Descripción tabla del cálculo del Chi-cuadrado

HIPÓTESIS	PROTOCOLO		O	E	O-E	(O-E)^2	(O-E)^2/E
La implementación de un sistema de seguridad perimetral con firewall de próxima generación NGFW mejorará disponibilidad, integridad y seguridad de la información en 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: Felipe Brito 2019.

5. PROPUESTA DE UN SISTEMA DE SEGURIDAD PERIMETRAL MEDIANTE LA PROTECCIÓN FIREWALL DE PRÓXIMA GENERACIÓN NGFW APLICABLE PARA PEQUEÑAS Y MEDIANAS EMPRESAS DEL CANTÓN RIOBAMBA

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.

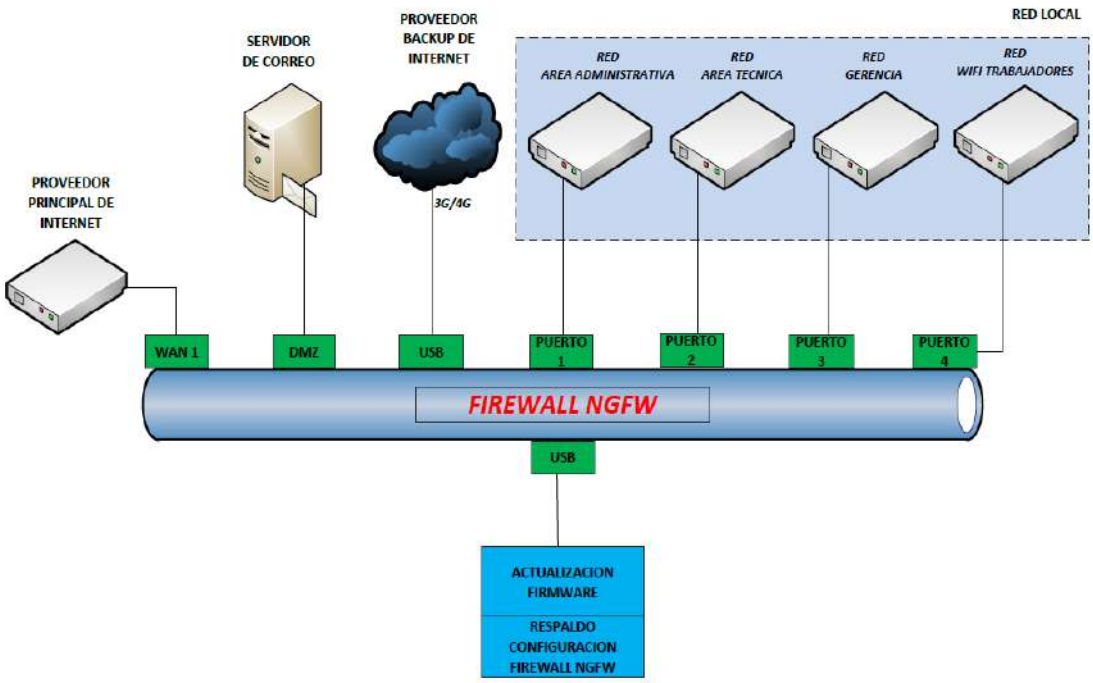


Figura 5-1 Propuesta de un Sistema de Seguridad Perimetral.

Fuente: Felipe Brito 2019.

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

Para la implementación de la propuesta de un sistema de seguridad perimetral con equipo Firewall de Próxima Generación NGFW para Pymes del cantón Riobamba, 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.

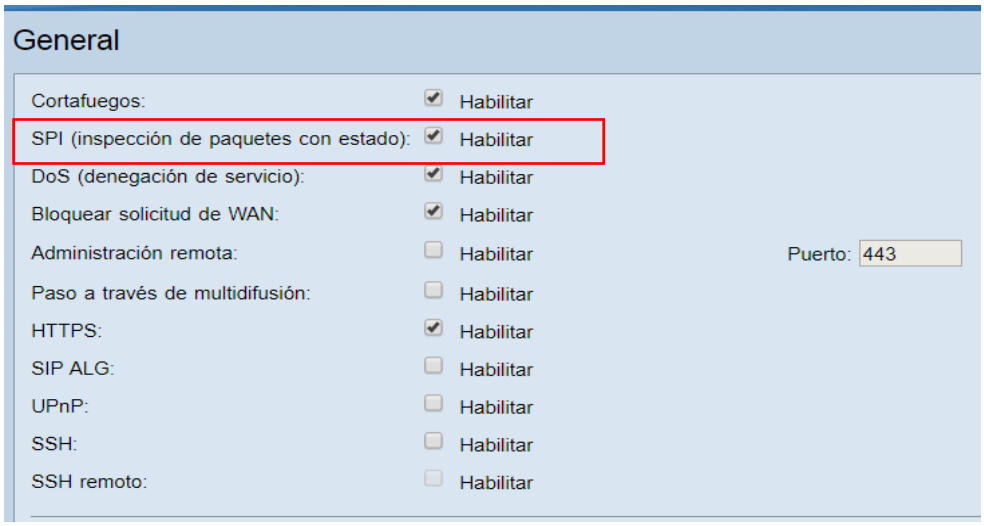


Figura 5-2 Inspección de paquetes con estado (SPI).

Fuente: Equipo Firewall 2019.

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

Fuente: Equipo Firewall 2019.

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 5-4 Tabla de registro del sistema.

Fuente: Equipo Firewall 2019.

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 2019.

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	Cliente 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 5-6 Tabla de Procesos Protocolo UDP.

Fuente: Equipo Firewall 2019.

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.

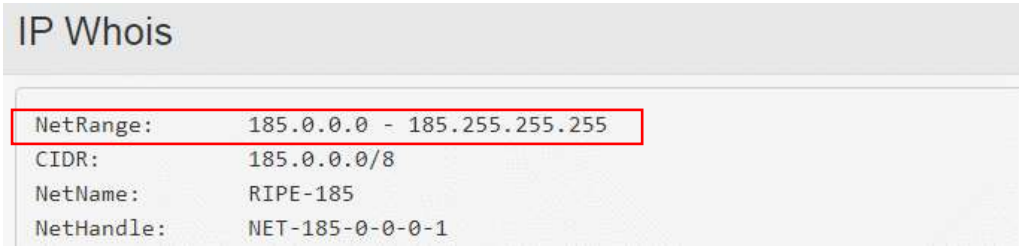


Figura 5-7 Determino el rango de IP que trabaja la página web.

Fuente: IP Whois 2019.

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

Fuente: Equipo Firewall 2019.

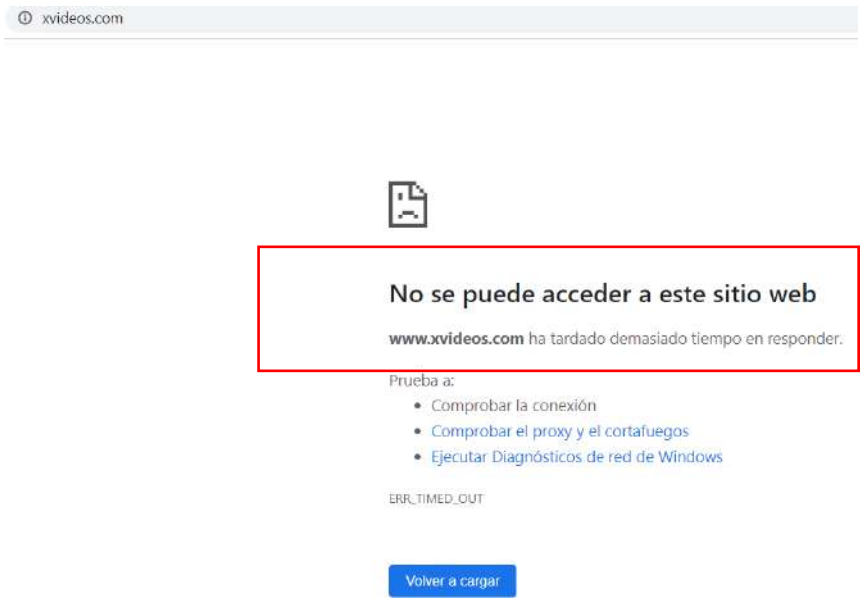


Figura 5-9 Bloqueo de página Web.

Fuente: Ingreso a sitio para adultos 2019.

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.

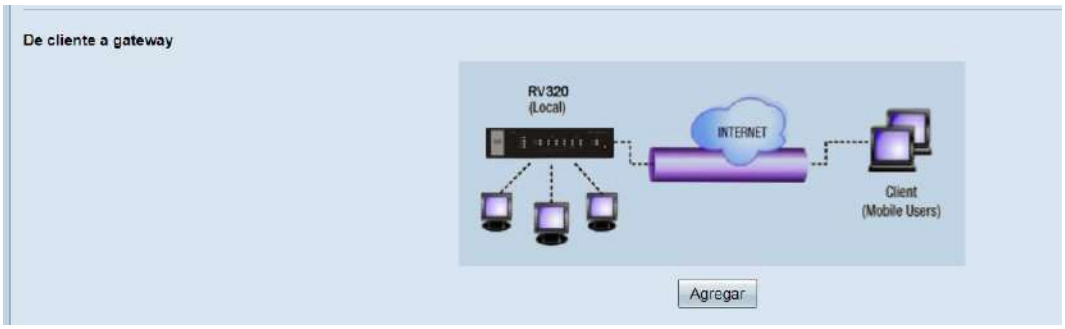


Figura 5-10 Configuración Cliente-Gateway.

Fuente: Equipo Firewall 2019.

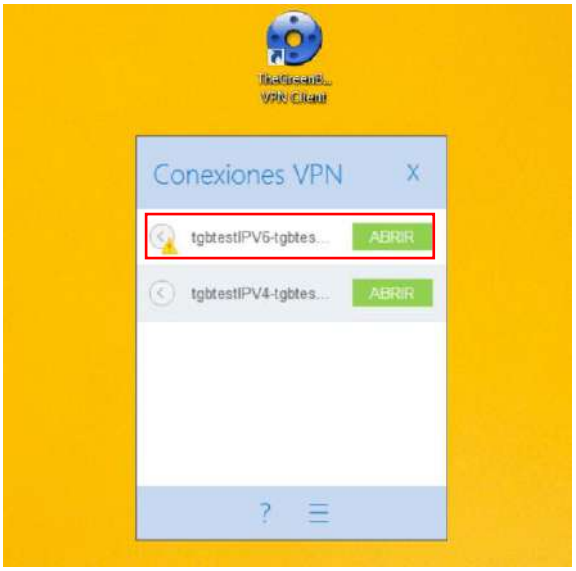


Figura 5-11 Cliente VPN.

Fuente: TheGreenBow VPN Client.

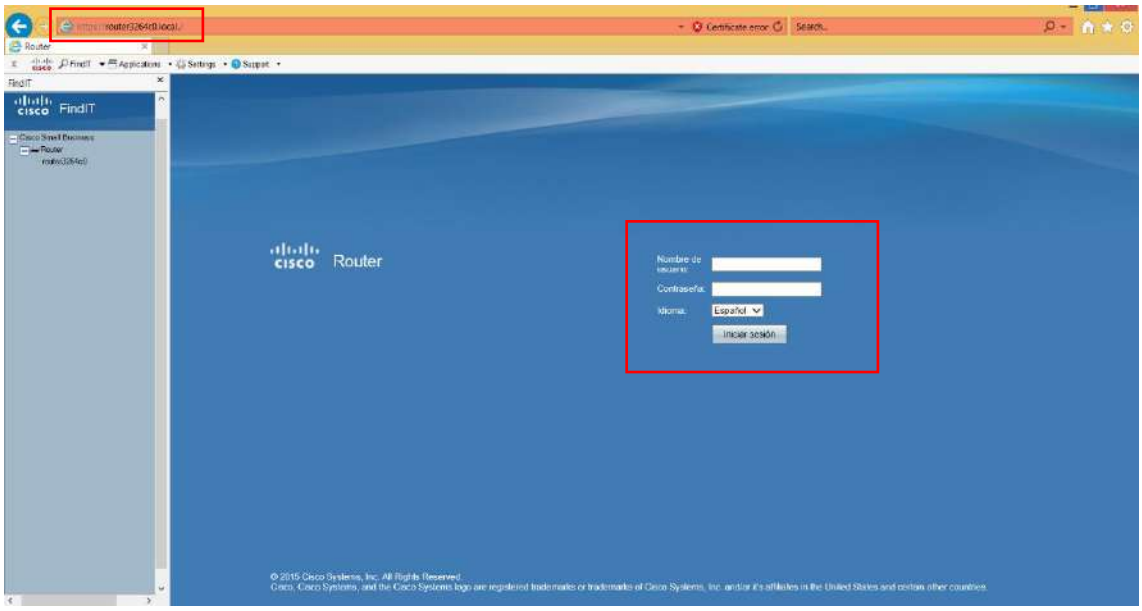


Figura 5-12 Conexión establecida de la VPN para administración del equipo.

Fuente: Equipo Firewall 2019.

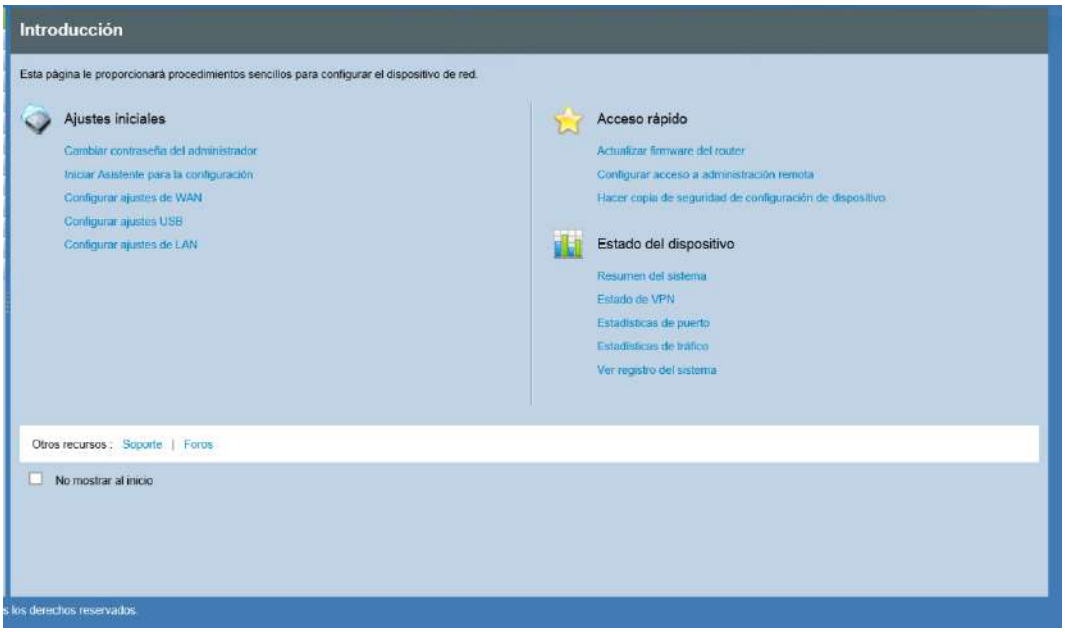


Figura 5-13 Conexión establecida de la VPN para la administración del equipo.

Fuente: Equipo Firewall 2019.

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.

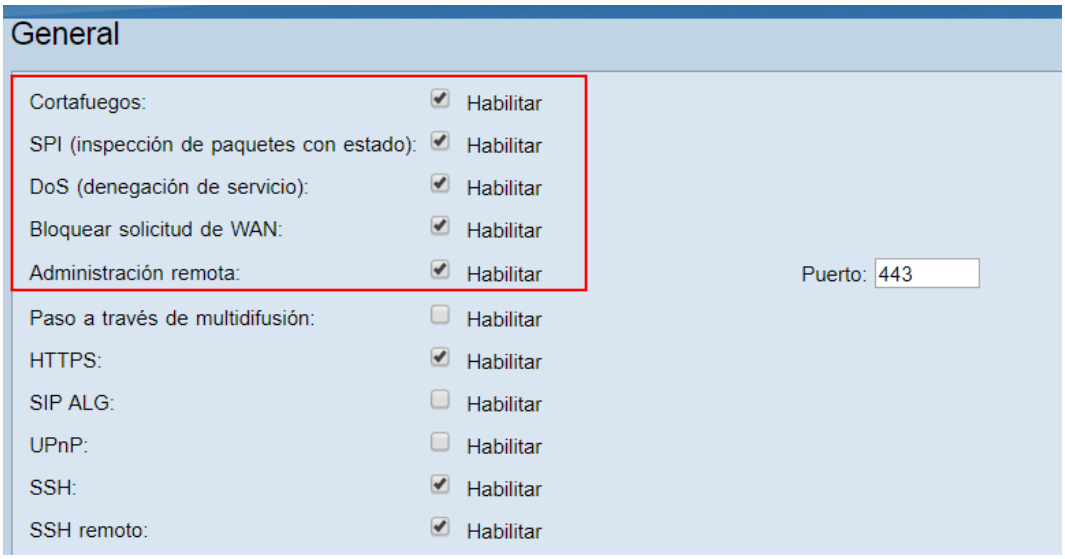


Figura 5-14 Monitoreo Automatizado.

Fuente: Equipo Firewall 2019.

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 5-15 Tabla de información del sistema.

Fuente: Equipo Firewall 2019.

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 5-16 Habilitación de la Zona Desmilitarizada DMZ.

Fuente: Equipo Firewall 2019.

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 5-17 Estadísticas del tráfico Zona Desmilitarizada DMZ.

Fuente: Equipo Firewall 2019.

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 5-1 Seguridad según las capas del modelo OSI

CAPA FÍSICA	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. Medio físico: Medios guiados: como el cable coaxial, par trenzado, fibra óptica. Medios no guiados: microondas, radio, infrarrojos, láser y demás redes inalámbricas. Desde una perspectiva de seguridad informática, a este nivel debemos preocuparnos por: • 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 despechado 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.
CAPA DE ENLACE	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. Protocolos utilizados: Ethernet o IEEE 802.3, IEEE 802.11 o Wi-Fi, IEEE 802.16 o WiMAX. PPP (Point to point protocol o protocolo punto a punto)

	• 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	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. Orientación de conexión: • 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. 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.

	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. 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. 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. 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. 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 denegan conexiones entre equipos pertenecientes a redes diferentes, según el protocolo, los puertos, o las direcciones IP involucradas en la comunicación. 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.

CAPA DE TRANSPORTE	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. Protocolos de transporte de internet: **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. **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. 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. 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.
CAPA DE SESIÓN	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. También realiza funciones que permite a los procesos, comunicarse a través de la red, ejecutando seguridad, como el reconocimiento de nombres, registro.
PRESENTACIÓN	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. La Capa de presentación, cumple tres funciones principales. Estas funciones son las siguientes: • Formateo de datos • Cifrado de datos • Compresión de datos
APLICACIÓN	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. 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. 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. **Servicios:** • Aplicaciones de Red • www (World Wide Web). • Enlace a capas inferiores 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).

Fuente: Felipe Brito 2019.

6. CONCLUSIONES

- La propuesta de un sistema de seguridad perimetral con firewall de próxima generación NGFW permite mejorar considerablemente la seguridad en las Pymes.
- En el escenario de pruebas tipo laboratorio se pudo comprobar que la mayoría de ataques y vulnerabilidades se reducen notoriamente.
- Al implementar y evaluar el sistema mediante una estructura de aplicabilidad, en el cual la red no sea muy permisiva ni muy restrictiva, se concluyó que la misma permite el normal funcionamiento de la red empresarial sin descuidar el activo más importante que es la información.
- 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.
- 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.

7. 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:

- Se recomienda implementar la presente propuesta de un sistema de seguridad perimetral de próxima generación NGFW para Pymes en las distintas empresas del Ecuador y Sudamérica con la finalidad de mejorar su seguridad informática.
- El Ecuador debería actualizar su legislación referente a normativas y estándares que permitan el aseguramiento de mejor manera de las redes de datos empresariales.
- El Ecuador debería crear un organismo público – privado y alianzas estratégicas a nivel internacional que le permita estar al día en conocimientos técnicos, para hacer frente a las amenazas y vulnerabilidades que pueda presentar en un determinado segmento empresarial.
- La empresa pública y privada deberían tomar en serio la seguridad de las redes informáticas, contratando especialistas en seguridad telemática o carreras afines, con la finalidad de proteger el funcionamiento empresarial y por ende el empleo.
- Al hablar de seguridad informática no es solamente instalar un antivirus o actualizar un sistema operativo, sino es un sistema en el cual se integra la red informática empresarial con el personal, desde la alta gerencia hasta el último trabajador de la nómina.

BIBLIOGRAFÍA

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 Informacion.* 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

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_Riobamba.pdf

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/

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). Análsis de vulerabiliades de protocolos de protección y autenticación inalámbrico. *Tesis Maestria 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/

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/

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

El enrutador VPN VPN WAN dual Gigabit RV320 es una opción ideal para cualquier oficina pequeña o pequeña empresa que busque rendimiento, seguridad y confiabilidad en su red. La conectividad de red es el corazón de todas las pequeñas empresas, y el acceso seguro, la protección de firewall y el alto rendimiento son los pilares de cada enrutador de la serie RV de Cisco Small Business. El enrutador VPN VPN WAN dual Gigabit RV320 no es una excepción. Con una interfaz de usuario intuitiva, el Cisco RV320 le permite estar en funcionamiento en minutos. El Cisco RV320 proporciona conectividad de acceso confiable y altamente segura para usted y sus empleados que es tan transparente que no sabrá que está allí.

Características y capacidades

El enrutador VPN WAN dual Gigabit Cisco RV320 ofrece:

- Puertos WAN Ethernet Gigabit dual para equilibrio de carga y continuidad comercial < / li>
- Conmutador Gigabit Ethernet de 4 puertos incorporado
- Seguridad sólida con firewall de inspección de paquetes con estado comprobado (SPI) y cifrado de hardware
- Alta capacidad, alto rendimiento, SSL, IP Security (IPsec) Capacidades de VPN
- Administrador de dispositivos intuitivo basado en navegador y asistentes de configuración

Rendimiento

Admite velocidades Gigabit Ethernet para conexiones cableadas internas y externas; gestiona fácilmente archivos grandes y usuarios concurrentes para mantener a los empleados productivos

Acceso simple y altamente seguro.

Conecte múltiples ubicaciones y trabajadores remotos usando VPN, o configure redes virtuales y reglas de acceso separadas para ayudar a proteger los datos confidenciales

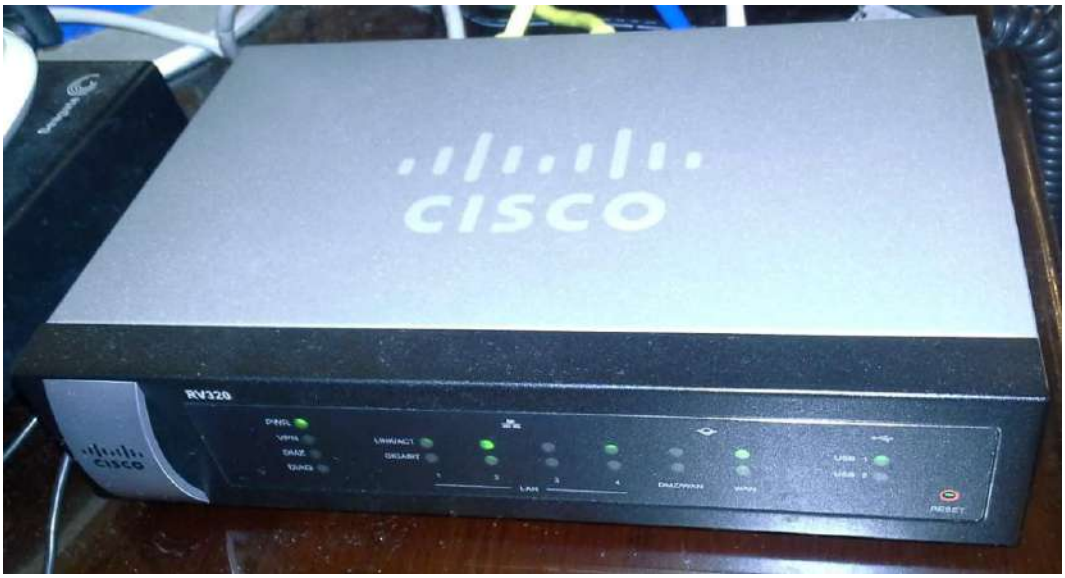
Facilidad de uso.

Se puede implementar directamente desde el primer momento; los asistentes de configuración reducen el tiempo de configuración a minutos

Flexible

Los puertos USB ofrecen la capacidad de utilizar módems 3G y 4G para la conmutación por error de banda ancha

ANEXO B: IMPLEMENTACION CON EQUIPO FIREWALL



ANEXO C: TIPOS DE ATAQUES INFORMÁTICOS

CORREO REAL DE POSIBLE ESTAFA POR 850 DÓLARES DENTRO DEL CORREO DE LA RED EMPRESARIAL (SPAM)

Yøuř åccøuňt ís běíňg usěd by åňøthěř pěřsøň!

acnn@biologie.uni-oldenburg.de

Enviado: lunes 0:24

Para:

Hěllø!

Í åm å håcker whø hås åccess tø yøür øpěråtíng systěm.
Í ålsø håvě full åccěss tø yøür åccøüňt.

Í'vě běěn wåtchíng yøü før å fěw mønths nøw.
Thě fåct ís thåt yøü wěrě ínfěctěd wíth målwårě thrøügh ån ådült sítě thåt yøü vísítěd.

Íf yøü årě nøt fåmílíår wíth thís, Í wíll ěxplåín.
Trøjån Vírüs gívěs mě füll åccěss ånd cøntrøl øvěr å cømpütěr ør øthěr děvícě.
Thís měåns thåt Í cån sěě ěvěrythíng øn yøür scrěěn, türn øn thě cåměrå ånd mícrøphøně, büt yøü dø nøt knøw åbøüt ít.

Í ålsø håvě åccěss tø åll yøür cøntåcts ånd åll yøür cørrěspønděncě.

If yoou want to prevent this, transfer the amount of $850(USD) to my bitcoin address (if you do not know how to do this, write to Google: 'Buy Bitcoin').

My bitcoin address (BŤC Wallet) is: 1KVX9hCnQ9MfSoEFyxqAXGFXdTFNyzD22n

After receiving the payment, I will delete the video and you will never hear me again.
I give you 48 hours to pay.
I have a notice reading this letter, and the timer will work when you see this letter.
Filing a complaint somewhere does not make sense because this email cannot be tracked like my bitcoin address.
I do not make any mistakes.

If I find that you have shared this message with someone else, the video will be immediately distributed.

Best regards!

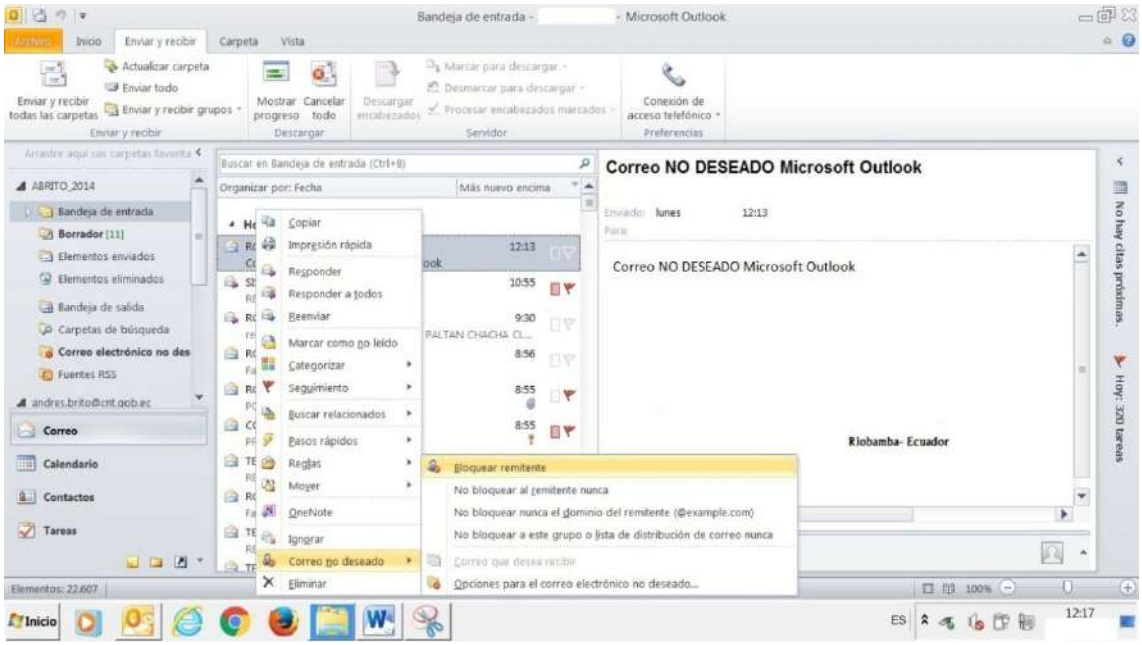
BLOQUEO DE CORREO EMPRESARIAL NO DESEADO (SPAM)

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 clic 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.

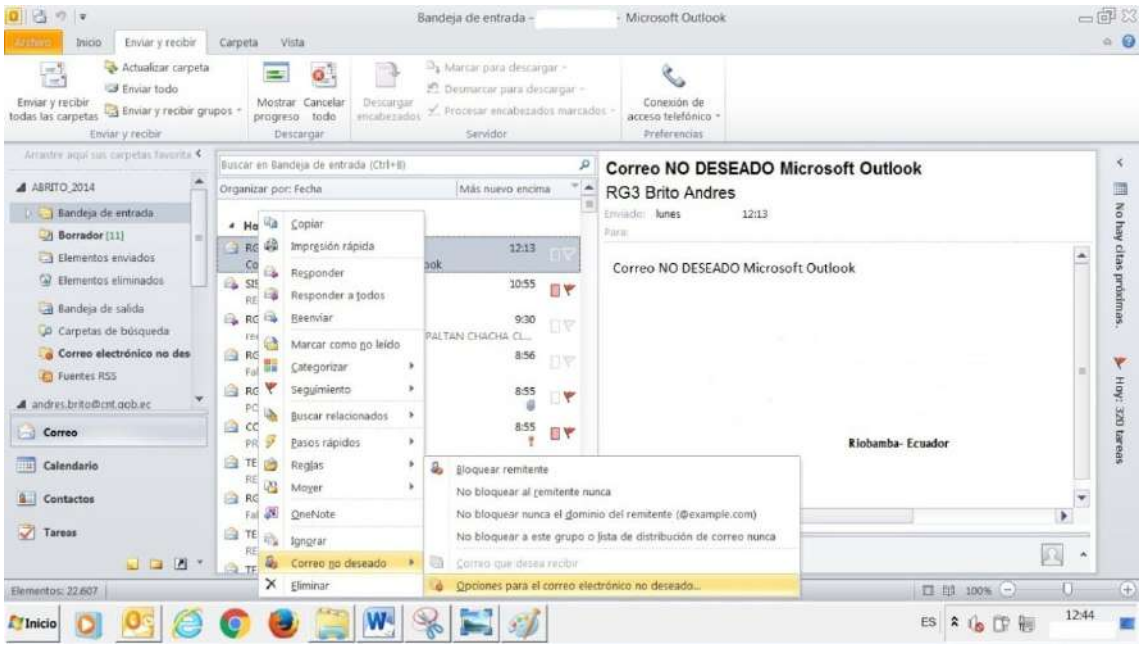
Para mayor seguridad se debe eliminar de forma permanente el correo spam siguiendo el siguiente procedimiento:

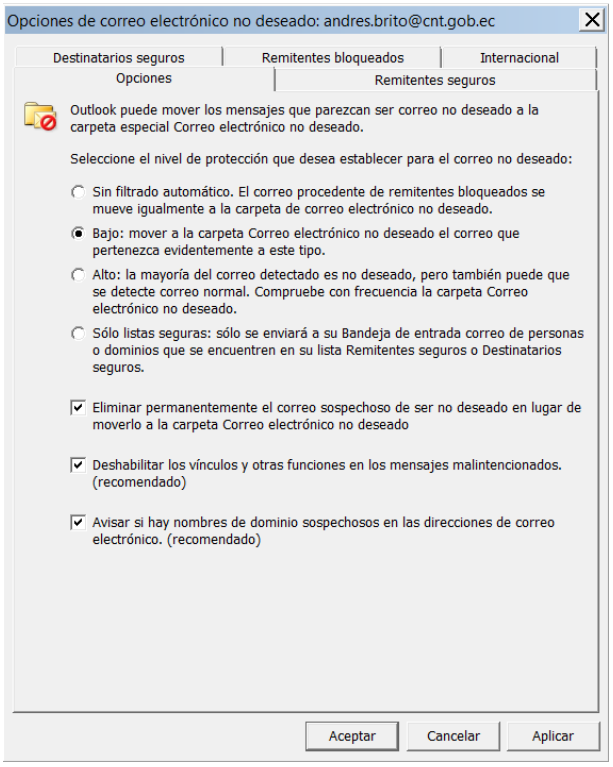
1.- Hacer clic derecho en el **correo Spam**

2.- Se escoge la opción de **Correo no deseado**

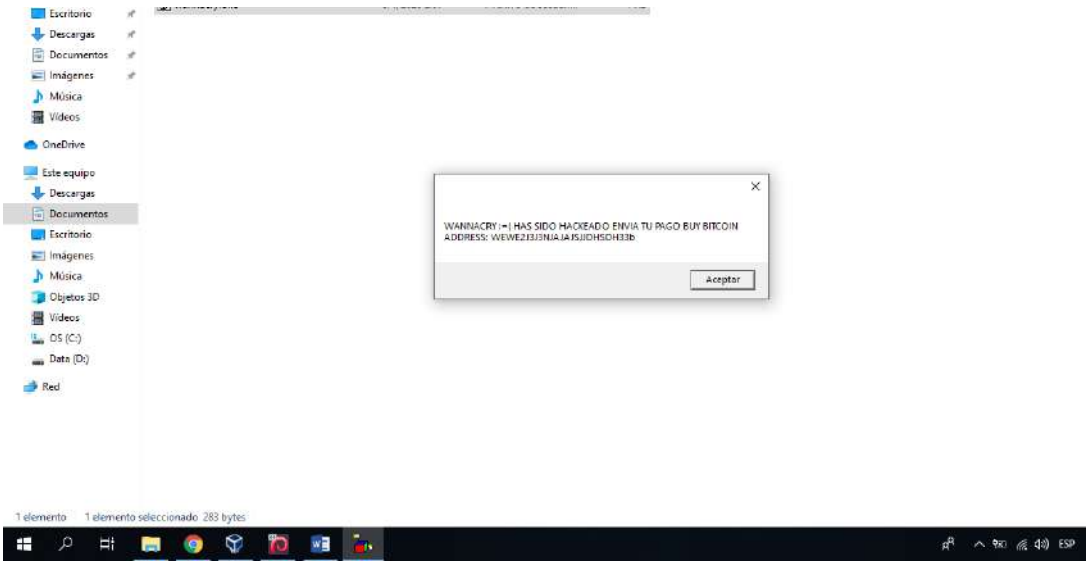
3.- Después se escogemos **Opciones para el correo electrónico no deseado**

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**

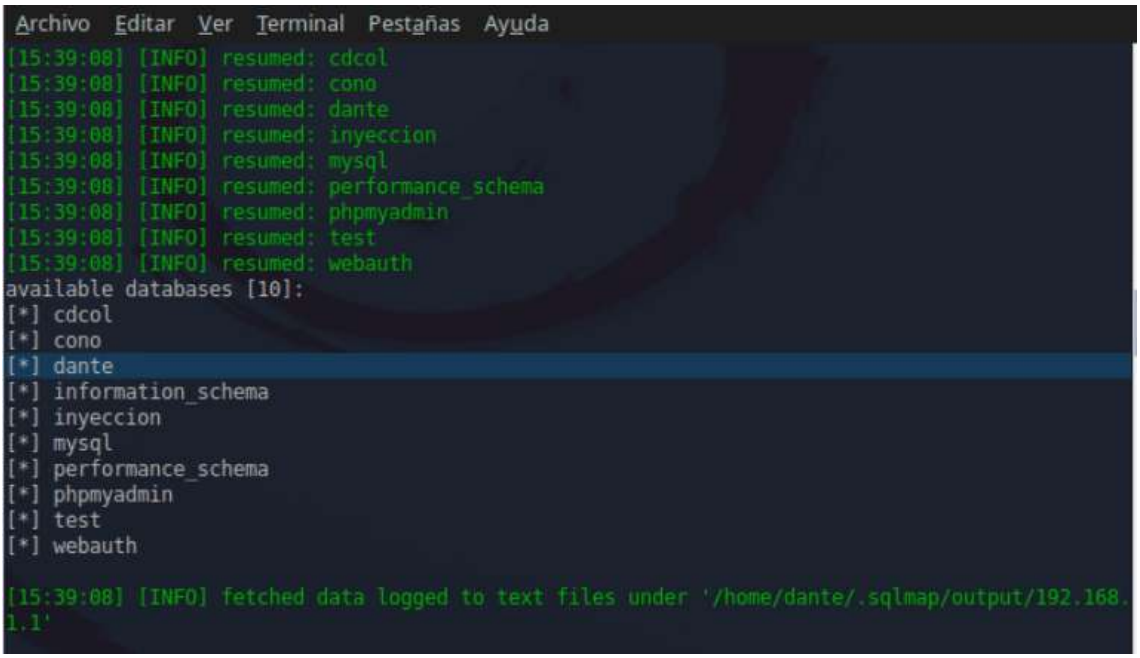




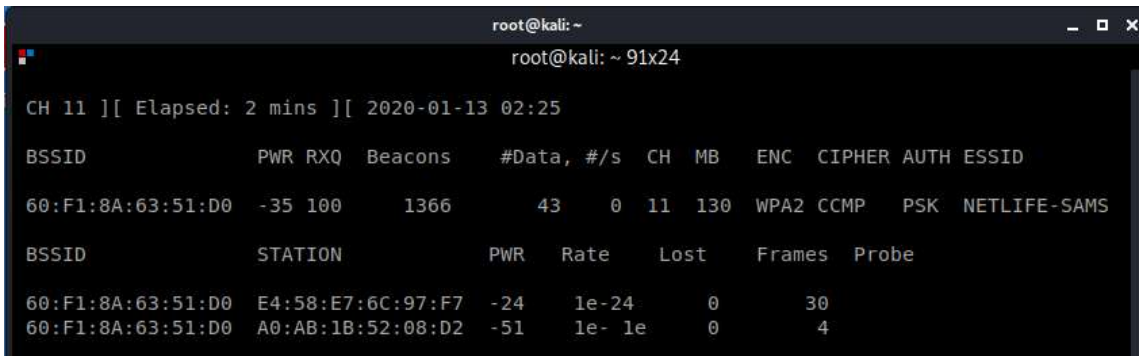
ATAQUE DE RANSOMWARE UTILIZANDO INGENIERIA SOCIAL

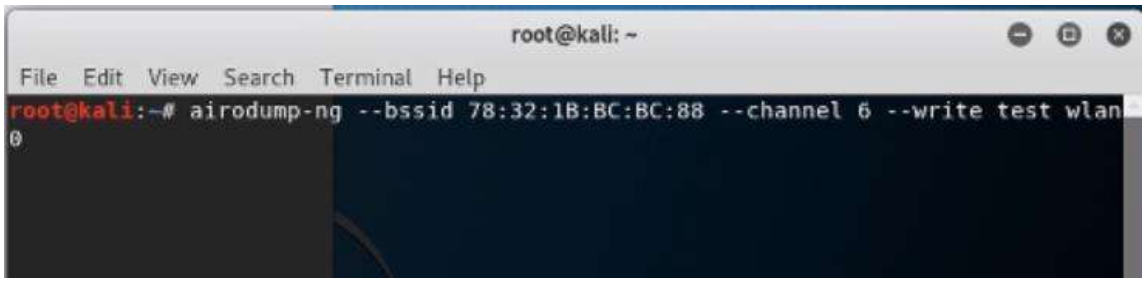


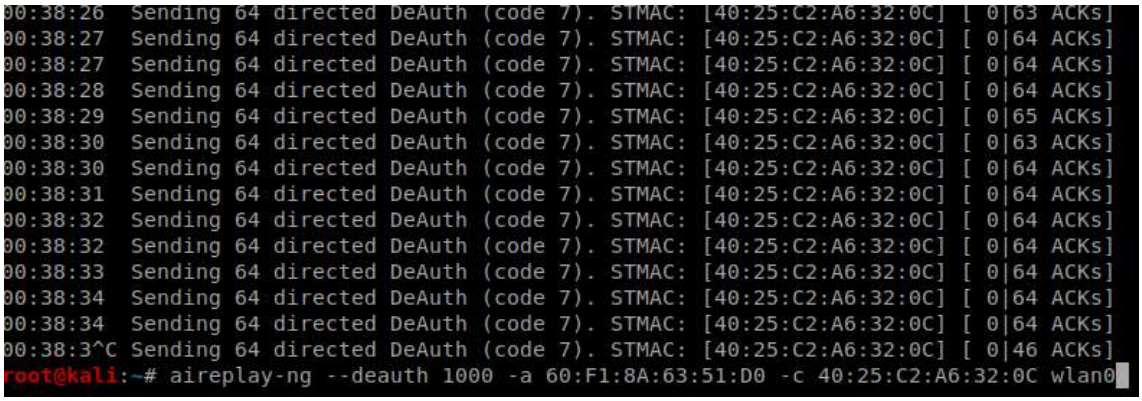
ATAQUE DE SQL INJECTION

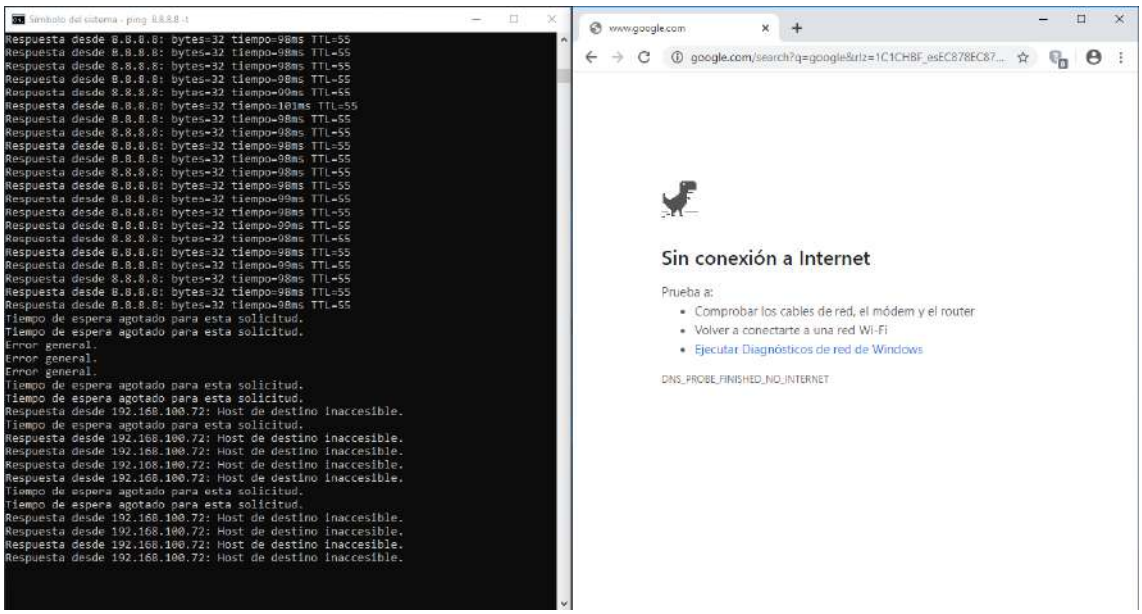


ATAQUE DENEGACION DE SERVICIO

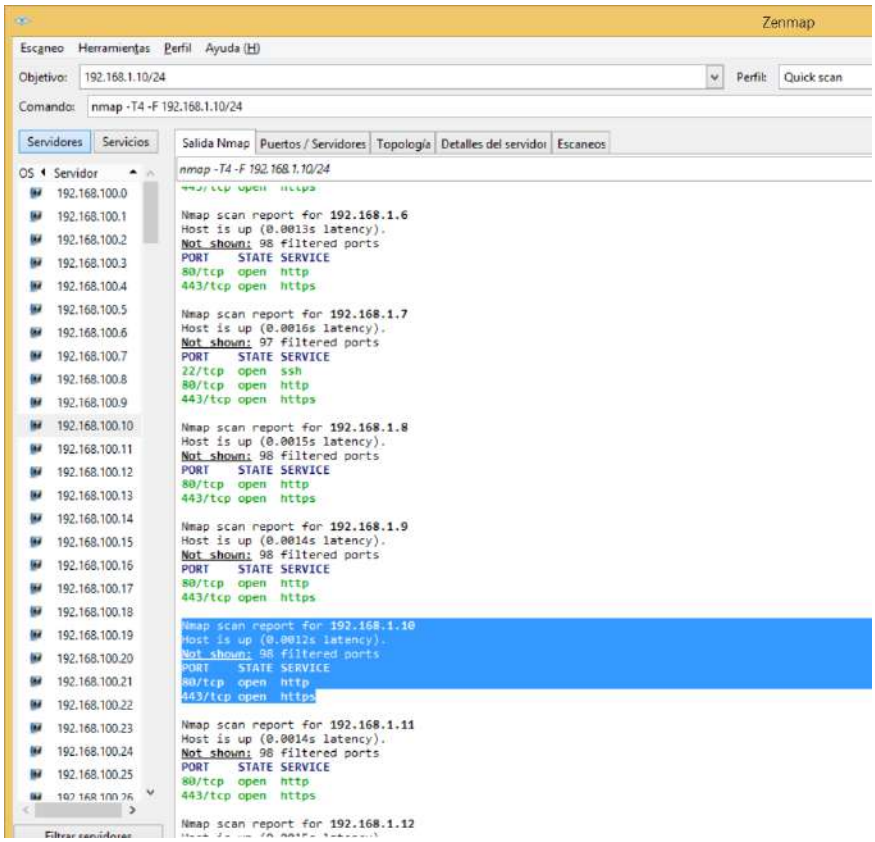




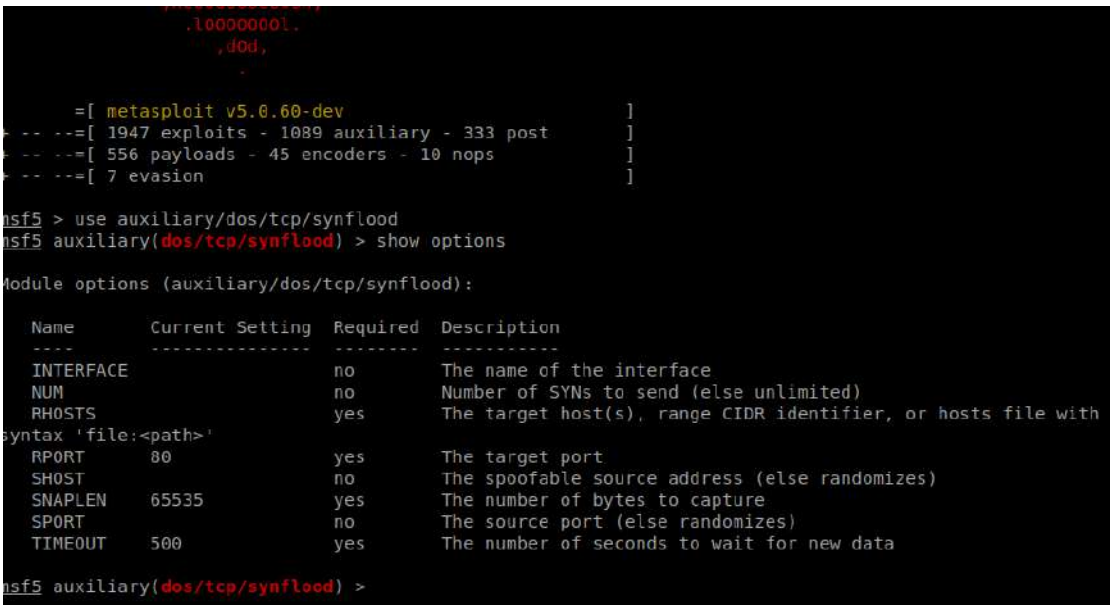




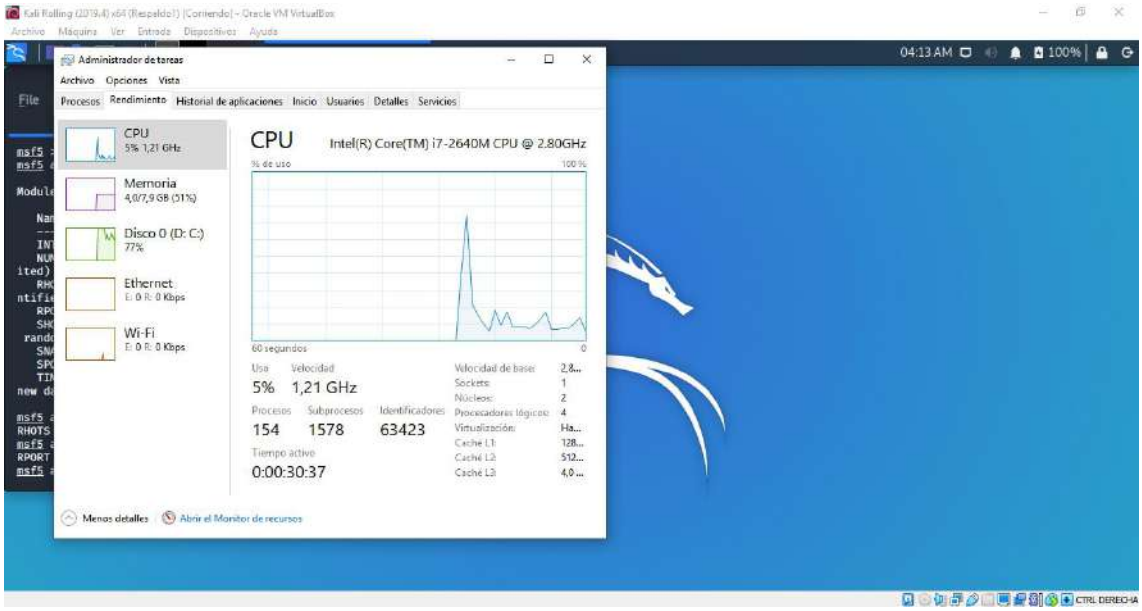
ESCANEO DE PUERTOS



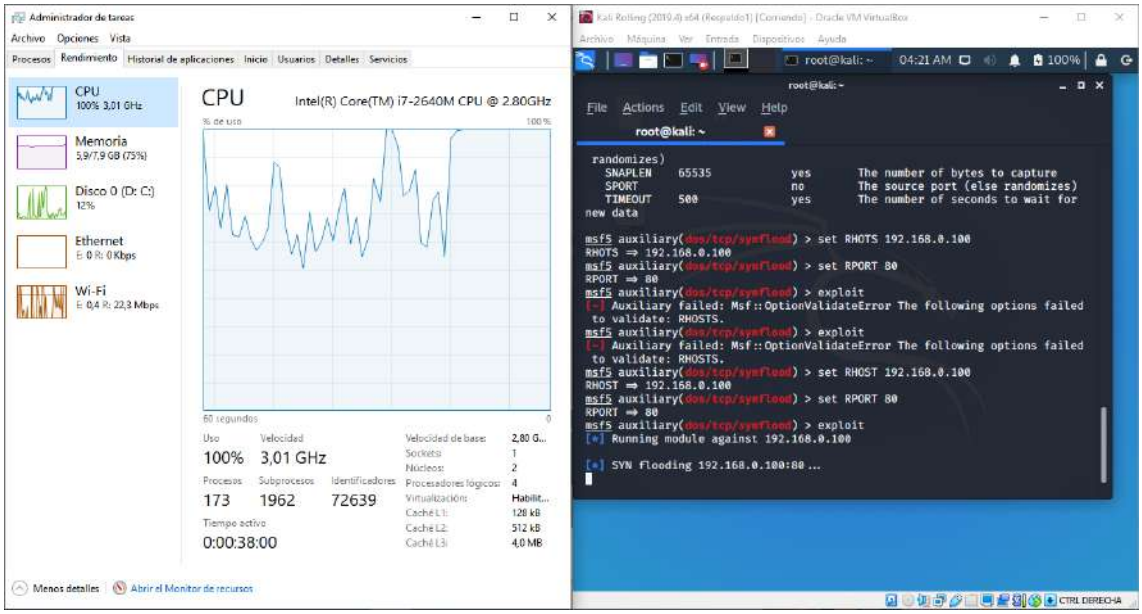
ATAQUE DE DENEGACION DE SERVICIO CON METASPLOIT FRAMEWORK



Funcionamiento Normal de un computador



Funcionamiento de un computador bajo ataque



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

DBRAI

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: *19 / 11 / 2021*

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: *Andrés Felipe Brito del Pino*
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: *Magíster en Seguridad Telemática*
f. Analista de Biblioteca responsable: *Lic. Luis Caminos Vargas Mgs.*

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
DN: cn=LUIS ALBERTO CAMINOS VARGAS c=EC l=RIOBAMBA
Motivo:Soy el autor de este documento
Ubicación:
Fecha:2021-11-19 18:13-05:00

UNIDAD DE PROCESOS TÉCNICOS DBRAI ESPOCH