DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

TEMA: "IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD INTEGRAL DE SOFTWARE Y HARDWARE PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ"

AUTOR: AGUILAR FEIJOO, JONATHAN ALBERTO

DIRECTOR: ING. AGUILAR SALAZAR, DARWIN LEONIDAS MGS.

SANGOLQUÍ
2020

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

CERTIFICACIÓN

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD INTEGRAL DE SOFTWARE Y HARDWARE PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ***" fue realizado por el señor ***JONATHAN ALBERTO AGUILAR FEIJOO***, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, Enero del 2020.

ING. DARWIN LEONIDAS AGUILAR SALAZAR MGS.

C.C. 1103036826

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORÍA DE RESPONSABILIDAD

AUTORÍA DE RESPONSABILIDAD

Yo, ***JONATHAN ALBERTO AGUILAR FEIJOO,*** con cédula de ciudadanía N° ***0704674332,*** declaro que el contenido, ideas y criterios del trabajo de titulación: **"*IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD INTEGRAL DE SOFTWARE Y HARDWARE PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ*"**, es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, Enero del 2020.

JONATHAN ALBERTO AGUILAR FEIJOO

C.C. 0704674332

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

CARRERA DE INGENIERÍA ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

AUTORIZACIÓN

Yo, ***JONATHAN ALBERTO AGUILAR FEIJOO,*** con cédula de ciudadanía N° ***0704674332,*** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: "***IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD INTEGRAL DE SOFTWARE Y HARDWARE PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE SEDE MATRIZ***", en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, Enero del 2020.

JONATHAN ALBERTO AGUILAR FEIJOO

C.C. 0704674332

DEDICATORIA

El presente trabajo está dedicado a mis padres que han sido los que han confiado en mí y quienes me han apoyado en el largo camino de la vida formándome con sus consejos y enseñanzas para ser una persona de bien.

A todas aquellas personas que han aportado con un grano de arena en sus diversas versiones para poder alcanzar este logro

Y en especial está dedicado para aquellas personas que soñaron con ver esta meta cumplida pero que ya no se encuentran físicamente entre nosotros, aunque siempre nos acompañaran emocional y espiritualmente.

AGRADECIMIENTOS

Quiero agradecer a la vida por el camino entregado que me ha fortalecido, a mis padres por apoyarme y guiarme, a mi familia que siempre ha está presente con un sinnúmero de apoyos, a mis amigos quienes me han alentado a seguir adelante, a mi esposa y a mi hijo que son mi motor y fortaleza, quienes me impulsan a ser cada día mejor y dar mi mejor esfuerzo en cada tarea que realizo.

ÍNDICE DE CONTENIDO

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En el siguiente trabajo se ha recopilado información sobre los sistemas de seguridad de la Universidad de las Fuerzas Armadas ESPE, con la finalidad de detectar vulnerabilidades en sus sistemas de seguridad informático. Estos datos se han logrado recopilar en su mayoría directamente de los equipos de seguridad para poder garantizar una mayor fiabilidad en el análisis de los mismos. Estos datos recopilados se han analizado mediante diversos métodos y basados con diversos criterios para realizar las observaciones necesarias para la optimización del sistema de seguridad. El análisis en su fase final se ha apoyado en un software desarrollado para el caso que nos permite filtra aspectos importantes e identificar factores de posible riesgo en la seguridad de la Universidad. Las observaciones y recomendaciones indicadas son directamente al personal de la Unidad de Tecnología e Información de la ESPE (UTICs) que es el encargado y autorizado a realizar cualquier tipo de modificación, adhesión o borrado de las reglas que rigen las políticas de seguridad informática de la Universidad.

PALABRAS CLAVE:

- **SEGURIDAD INFORMÁTICA**
- **SEGURIDAD DE LA INFORMACIÓN**
- **FORTIGATE DE FORTINET**
- **FIREWALL**

ABSTRACT

In the following work, information has been collected on the security systems of the University of the Armed Forces ESPE, in order to detect vulnerabilities in their computer security systems. These data have been compiled mostly directly from security teams to ensure greater reliability in the analysis of the same. These collected data have been analyzed using various methods and based on various criteria to make the observations necessary for the optimization of the security system. The analysis in its final phase has been based on software developed for the case that allows us to filter important aspects and identify possible risk factors in the University's security. The observations and recommendations indicated are directly to the staff the Technology and Inforrmation Unit of the ESPE (UTICs) who are in charge and authorized to make any type of modification, adhesion or deletion of the rules that govern the University's computer security policies.

KEYWORDS:

- **INFORMATIC SECURITY**
- **SECURITY OF THE INFORMATION.**
- **FORTIGATE OF FORTINET**
- **FIREWALL**

CAPÍTULO I

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

La seguridad informática es un conjunto de normas, procesos y herramientas, que están orientados a la protección de los sistemas y datos informáticos; esta orientación deriva en 2 conceptos válidos para el sector de sistemas, son la seguridad informática y la seguridad de la información.

La seguridad informática es el pilar fundamental sobre el que se levantan las instituciones y más aún aquellas que ofrecen servicios informáticos quienes deben asegurar estos sin interrupciones ni corrupción de la información que entregan.

Son varias las consecuencias de los ataques informático, estas consecuencias van acorde con el peso de los sistemas informáticos y con la importancia de la información que estos sistemas manejan, además de los mecanismos de respaldo que se manejen y la frecuencia con la que se los emplee para tener el respaldo de la información.

Los problemas de los ataques cibernéticos no solo se basan en el daño de sistemas, la corrupción o eliminación de la información, sino el robo de información sensible que puede ser usada con fines ilegales (estafa, extorción, entre otros).

El constante crecimiento de las redes computacionales y los servicios que estas ofrecen nos han llevado a la necesidad de protegernos de estas mismas redes, ya que en su mayoría al ser redes y servicios globalizados muchas personas pueden acceder a estos; en su mayoría son personas que utilizan estas redes y servicios con fines de comunicación y de distracción, pero de igual manera existen personas mal intencionadas que utilizan las mismas redes y servicios para actividades ilegales que perjudican a las demás persona en muchos aspectos.

1.1 Seguridad Informática

La seguridad informática es un área quien es la encargada de las normas, procesos, métodos y técnicas, que busca la forma de proveer condiciones seguras y confiables, para el correcto funcionamiento en los sistemas informáticos.

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. [1]

1.2 Seguridad de la Información:

A diferencia de la seguridad informática que se enfoca en los recursos de red de una institución, la seguridad de la información se enfoca en la información en sí, es decir en la confidencialidad, integridad y disponibilidad de la información en cualquier formato o medio que la institución la pasea.

Figura 01: Seguridad Informática VS Seguridad de la Información.
Fuente: https://www.maestrodelacomputacion.net/seguridad-informatica-seguridad-de-la-informacion/

Una institución no está protegida de forma adecuada si no tiene en cuenta que la seguridad informática debe respaldar de forma óptima la seguridad de la información, ya que la una es complemento de la otra.

1.3 Principios de Seguridad Informática:

La seguridad informática al tener que implemetar varios métodos de acuerdo a las circunstancias de cada sistema que bede proteger, engloba estos diversos procesos en grupos, cuyos sistemas a proteger deben cumplir cabalmente:

Para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informatico: [1]

Confidencialidad: Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios , computadores y datos residen en localidades diferentes , pero están física y lógicamente interconectados.

Integridad: Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén

bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

Disponibilidad: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

1.4 Factores de Riesgo:

Los factores de riesgo son variados y depende del tipo de sistema a proteger, estos factores no solo son externos, también pueden ser internos, ocasionados por el medio ambiente etc., prepararse para disminuir y en lo posible eliminar estos factores es uno de los trabajos más complejos y a la vez importante en el mundo de las redes informática.

Ambientales/Físicos: Factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, humedad, calor entre otros. [1]

Tecnológicos: Fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informático, etc.

Humanos: Hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, alteraciones etc. [2]

1.5 Mecanismos de seguridad

Los mecanismos de seguridad informática son técnicas o herramientas tilizadas para garantizar la fidelidad de un sistema informático.

Hoy en dia existen muchos y variados mecanismos de seguridad informática; su elección depende de diversos puntos como el tipo de sistema a proteger, el nivel de seguridad que requiere de acuerdo a su función y de los factores de riesgo que lo amenazan.

1.5.1 Clasificación según su función:

Como ya se mencionó los sistemas informáticos son diversos y las formas de protegerlos igual, es por eso que tenemos varios tipos.

- Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
- Detectivos: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

- Correctivos: Actúan luego de ocurrido el hecho y su función es corregir las consecuencias.

Según un informe del año 1991 del Congressional Research Service, las computadoras tienen dos características inherentes que las dejan abiertas a ataques o errores operativos. [2]

Una de las grandes vulnerabilidades de una computadora es que se trata de una máquina que realiza las tareas para la cual esta programada, esto incluye revelación de información sensible ya que cualquier persona con la preparación adecuada puede programarlas para el fin que requiera, este este dentro de los limites legales/éticos o no.

1.6 Técnicas de Seguridad.

La seguridad informática es variada según el tipo de sistemas que se desea proteger y según este tipo de sistema se considera las seguridades que pueden ser las siguientes.

1.6.1 Restricciones al acceso Físico

El acceso fisco es una de las barreras más importantes para controlar ataques físicos a los equipos de redes, los cuales se deben asegurar mediante varios métodos.

Esta consiste en la aplicación de barreas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos de información confidencial. [2]

Figura 02: Ratón de Seguridad (Verifica Usuario Mediante Huella del Pulgar).
Fuente: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del dentro de computo, así como los medios de accesos remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos. Una forma de reducir las brechas de seguridad es asegurarse de que sólo las personas autorizadas pueden acceder a una determinada máquina. Las organizaciones utilizan una gran variedad de herramientas técnicas para identificar a su personal autorizado. Las computadoras pueden llevar a cabo ciertas comprobaciones de seguridad, los guardias de seguridad humanos. En función del sistema de seguridad implementado, podrá acceder a un sistema en función a: [2]

Algo que usted tenga: Una llave, una tarjeta de identificación con una fotografía o una tarjeta inteligente que contenga una identificación digital codificada almacenada en un chip de memoria.

Algo que usted conozca: Una contraseña, un número de identificación, una combinación de bloqueo o algo de su historial personal.

Algo que usted haga: Su firma o su velocidad de escritura y los patrones de error.

Algo suyo: (Sistema Biométrico) La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

Los Beneficios de una Tecnología Biométrica Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración. [2]

Con el uso de equipos biométricos, si bien los costos de inversión pueden ser un poco altos, los de mantenimiento y administración son relativamente bajos, además de contrar con medios confiables de controles de acceso físicos dependiendo, los modelos y marcas pueden pedir 2 o más conbinaciones para dar acceso a la persona que lo esta solcitando.

Huella Digital Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho

minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable. [2]

Verificación de Voz: La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

Verificación de Patrones Oculares: Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

1.6.2 Contraseñas.

Las contraseñas son las herramientas más utilizadas para restringir el acceso a los sistemas informáticos. Sin embargo, sólo son efectivas si se escogen con cuidado, la mayor parte de los usuarios de computadoras escogen contraseñas que son fáciles de adivinar: El nombre de la pareja, el de un hijo o el de una mascota, palabras relacionadas con trabajos o aficiones o caracteres consecutivos del teclado. Un estudio descubrió que las contraseñas favoritas en el Reino Unido son Fred-God, mientras que en América eran, Love- sexy. Los hackers conocen y explotan estos clichés, por lo que un usuario precavido no debe utilizarlos. Muchos sistemas de seguridad no permiten que los usuarios utilicen palabras reales o nombres como contraseñas, evitando así que los hackers puedan usar diccionarios para adivinarlas. Incluso la mejor contraseña sebe cambiarse periódicamente. [2]

Al ser la contraseña uno de los medios mas ampliamente utilizados para los controles de acceso también se convierten en un punto de vulnerabilidad ya que de no contar con un plan adecuado de creación de contraseñas, sistemas de recuperación, mantenimiento y cambios periódicos; son suceptibles de ser decifradas o detectados por los multiples programas creados con este fin, y de ser asi utilizadas a criterio de aquellas personas que no las están robando.

Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves, en tiempos muy breves, hasta encontrar la password correcta. [2]

Los diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta. [2]

1.6.2.1 Normas de Elección de Claves

A continuación, algunos puntos a tomar en cuenta para poder realizar la elección de una contraseña adecuada.

- No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
- No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.).
- No utilizar terminología técnica conocida.
- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
- Deben ser largas, de 8 caracteres o más.
- Tener contraseñas diferentes en máquinas diferentes y sistemas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas. Esto permite que si una password de un sistema cae no caigan todos los demás sistemas por utilizar la misma password.
- Deben ser fáciles de recordar para no verse obligado a escribirlas.
- Realizar reemplazos de letras por signos o números: En seguridad más vale prevenir que curar. [2]

1.6.3 Firewalls

Si bien estos elementos son los más publicitados a la hora de establecer seguridad, nos son ni la única ni la ultima solución a los problemas de seguridad en cuanto a redes se trata, si bien son de gran ayuda cuando están correctamente configurados, tambie hay otras herramientas y método que nos ayudan incluso con información relevante para configyrar estos equipos.

Los Firewalls están diseñados para proteger una red interna contra los accesos no autorizados. En efecto, un firewall es un Gateway con un bloqueo (la puerta bloqueada solo se abre para los paquetes de información que pasan una o varias inspecciones de seguridad), estos aparatos solo lo utilizan las grandes corporaciones. [2]

Un gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. Es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior.

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo, Internet). [2]

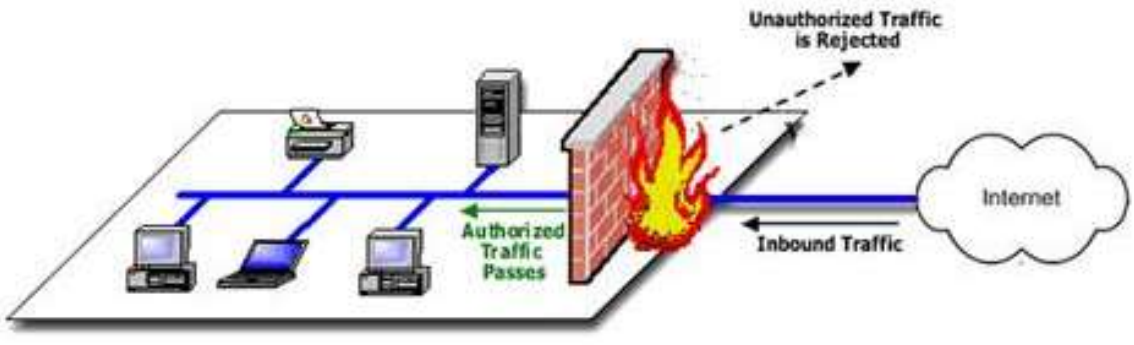

Figura 03: Diagrama de Red con FireWall.
Fuente: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Como puede observarse en la ***Figura 03***, el Muro Cortafuegos básico, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa, es por eso que se debe tomar en cuenta otras formas de seguridad y mecanismos para optimizar las seguridades internas no solo de las amenazas externas, sino de las internas tanbiem.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación. [2]

Tipos de Firewall

- Filtrado de Paquetes
- Proxy-Gateways de Aplicaciones
- Dual-Homed Host
- Screened Host
- Screened Subnet
- Inspección de Paquetes

Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de

Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas. [2]

Firewalls Personales: Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

Filtrado de paquetes: El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la www (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Como su funcionamiento y estructura se basa en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo, presenta debilidades como:

- No protege las capas superiores a nivel OSI.
- Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.

- Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
- No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

Proxy-Gateways de Aplicaciones: Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma. [2]

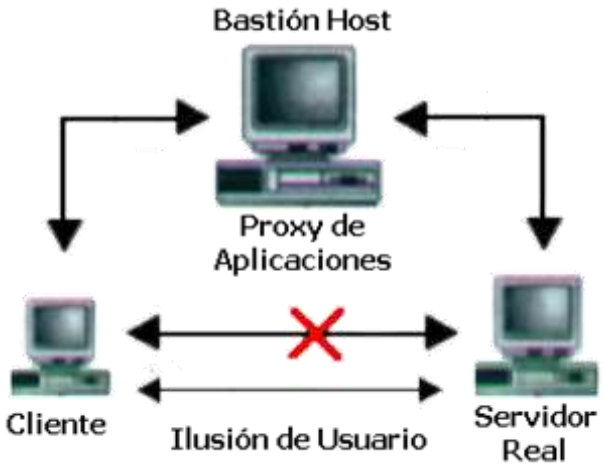

Figura 04: Proxy de Aplicaciones
Fuente: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Dual-Homed Host: Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".

Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior. [2]

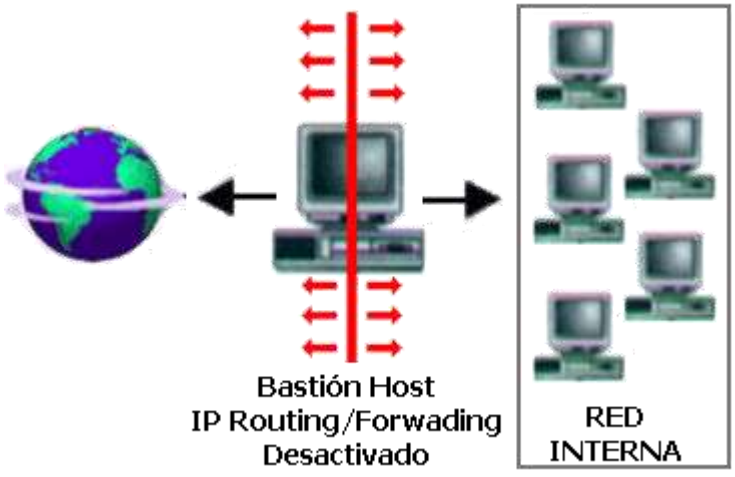

Figura 05: Dual-Homed Host.
Fuente: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Screened Host: En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible

desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios. [2]

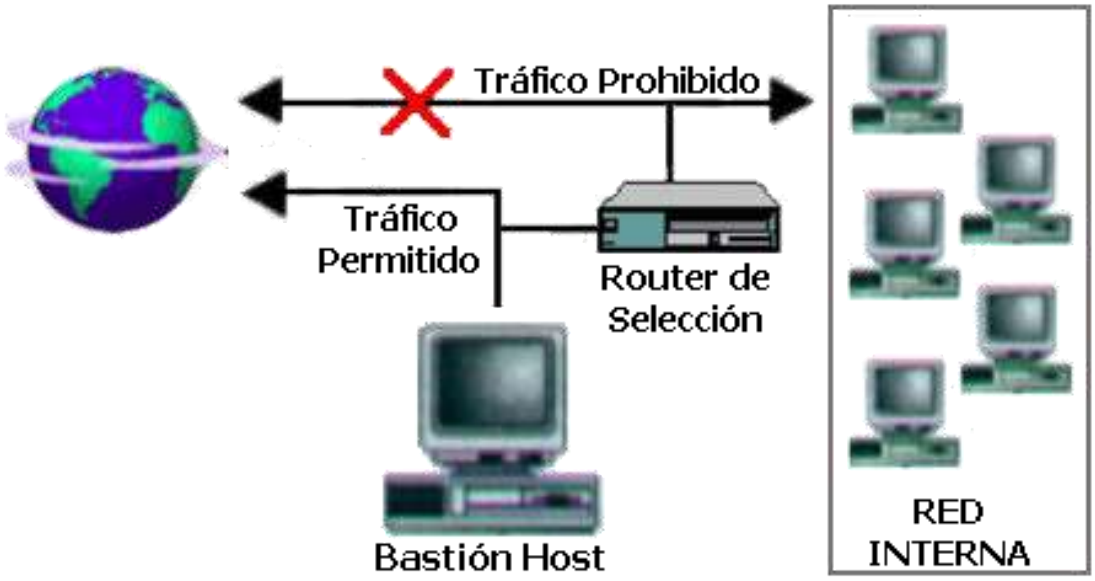

Figura 06: Host Proyectado.
Fuente: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Screened Subnet: En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que si un intruso accede a esta máquina no consiga el acceso total a la subred protegida.

En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varios niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo. [2]

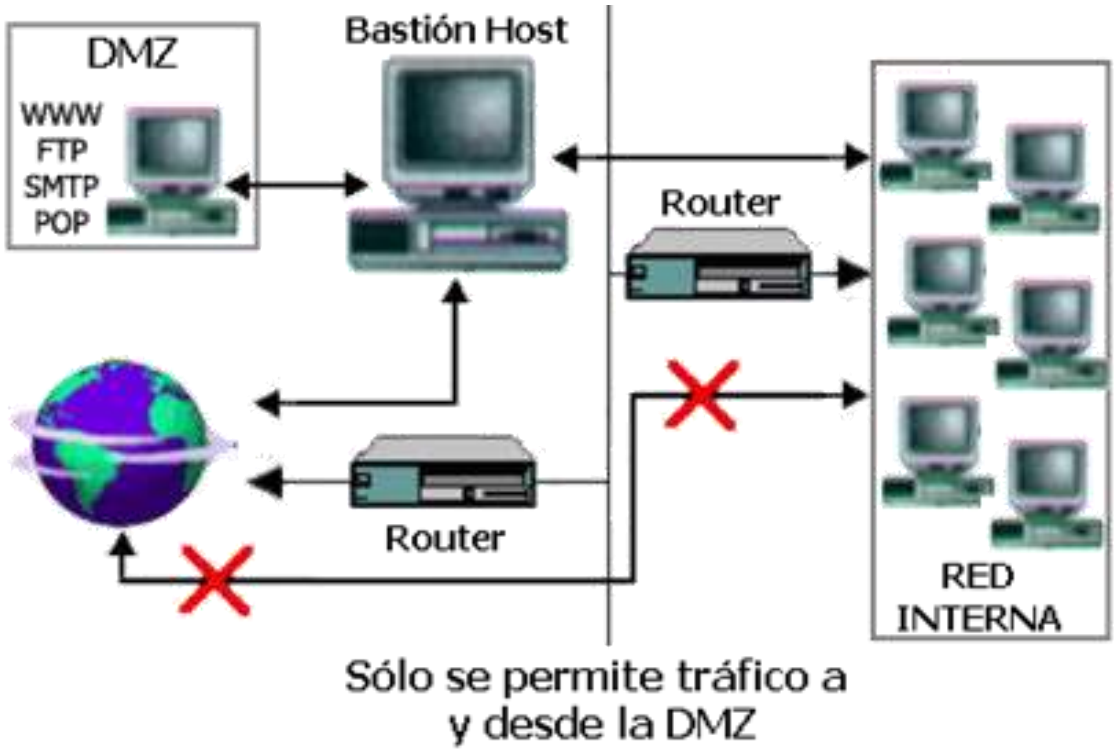

Figura 07: Subred Proyectada.
Fuente: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa. Los sistemas Dual-Homed Host y Screnned pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas: [2]

Los niveles de seguridad pueden ir aumentando y siendo mas complejos cada ves, hay que recordad que mientras se manejen instalaciones mas sofisticadas e información mas delicada, la escala en seguridad de redes va en aumento y no se debe escatimar en esfuerzo o en inversión.

- Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
- Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
- Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red. [2]

Restricciones en el Firewall

La parte más importante de las tareas que realizan los Firewalls, es la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación: [2]

- Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina **Trusted (validados)**. Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
- Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias. [2]

Beneficios de un Firewall

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestos a ataques desde el exterior. Esto significa que la seguridad de

toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho de que en los últimos años en Internet se han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados. [2]

Desde el punto de vista informatico los firewalls tienen un sinnúmero de beneficos, mas aun los de ultima generación los cuales cuentan con herramientas mas avanzadas algunas

de ellas basadas en inteligencia artificial y algoritmos predictivos, sin embargo, estos equipos resultan nulos a la hora de brindar seguridad si no son bien configurados.

Recordemos que sin importar el grado de tegnologia que tengan estos equipos el ser humano es y será siempre el mas importante imbro en el conjunto de seguridad en redes ya que serán las personas encargadas de los sistemas quienen diseñen y configuren los equipos y el ser humanao mismo quien intente violarlar estas normas de seguridad, asi que lo mas imoortante es tener a personal calificado y que se encuentre en constante actualizacion de conocimientos.

Limitaciones de un Firewall

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende, si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que, si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. [2]

Como ya sabemos por mas avanzados que sean estos equipos, los firewalls siguen siendo maquinas disañadas por el ser humano para servir al ser humano, y como seres humanos somo inperfectos, por ende somos susectibles de cometer fallas incluso en sistemas tan importantes como estos, y estas fallas son aprovechadas por otras personas con los conocimientos necesarios como para poder realizar multiples daños a diversos sistemas, o robos de informaciona los mismos ya que estas maquinas hacen aquellas tareas para las que fueron prigramas y no realizan ninguna mas, no son seres inteligente capaces de tomar decisiones fuera de su programación y auto alimentarse de conocimiento o experiencias como lo haría un ser humana para en base a estas experiecias optimizar los sistemas de seguridad.

CAPÍTULO II

SOLUCIONES DE SEGURIDAD INFORMÁTICA - FORTINET

Las empresas, impulsadas por la necesidad de operar más rápido a escala global y al mismo tiempo reducir los costos, experimentan la transformación digital (DX). Esta evolución incluye la adopción de nuevas tecnologías que amplían la superficie de ataque, dejando los perímetros de la red vulnerables frente a amenazas avanzadas, lo que crea un entorno de seguridad complejo. El Security Fabric de Fortinet segmenta toda la red, desde el Internet de las cosas (IoT) hasta la nube, para proveer protección superior contra amenazas sofisticadas. [3]

Figura 08: Subred Proyectada.
Fuente: https://www.fortinet.com/lat/solutions/enterprise-midsize-business/enterprise-security.html

como se puede apreciar en la ***Figura 08***, los equipos Firewalls de nueva generación de FORTINET no solo cumplen las funciones de un firewall normal, sino que se complementan con un sinnúmero de herramientas que apuntan a la concetracion de recursos y optimisacion de los mismos, para el manejo de la información de forma mas organizada, esto logra separa las tareas por categorías o funciones al punto que los análisis y las protecciones se potencializan y se consigen mejores resultados pata la seguridad de las redes.

2.1 FortiGate

A medida que las empresas analizan la forma de proporcionar una visibilidad integral y seguridad avanzada de capa 7 que incluya protección contra amenazas, prevención de intrusiones, Web Filtering y Application Control se enfrentan un obstáculo de gran complejidad al administrar estos productos de punto no integrados y sin visibilidad. Gartner estima que para 2019 el 80 % del tráfico empresarial estará cifrado y el 50 % de los ataques dirigidos a las empresas se ocultará en el tráfico cifrado para infiltrarse en redes o exfiltrar datos, por lo tanto, es necesario emplear la inspección de HTTPS.

Los Next-Generation Firewalls de FortiGate utilizan procesadores de seguridad especialmente diseñados y los servicios de seguridad de inteligencia de amenazas de FortiGuard Labs administrados por inteligencia artificial (IA) para brindar la mejor protección e inspección de alto rendimiento del tráfico cifrado y de texto sin formato. FortiGate reduce la complejidad y el costo con una visibilidad completa en las aplicaciones, usuarios y redes, además de proporcionar la mejor seguridad de su clase. Como parte integral del Fortinet

Security Fabric, se pueden comunicar en la cartera de seguridad integral de Fortinet, así como con soluciones de seguridad de terceros en un entorno de múltiples proveedores para compartir inteligencia frente a amenazas y mejorar la postura de seguridad. [4]

Figura 09: Cuadrante Mágico para Firewalls de Red.
Fuente: Gartner (Septiembre 2019)

En la ***Figura 09*** podemos observar que Fortinet es una de las marcas mejor puntuadas dentro del cuadrante de líder de Gartner en el tema de Firewalls para redes. Esto nos da una información muy importante, ya que podedmos saber que estamos contando con una marca que tiene un gran respaldo de experiencia en desarrollo e invistigacion con resultados positivos, por tal motivo la Universidad confía en la solución implementada, ya que cuenta con una marca que se encuentra muy bien posicionada en el mercado mundial.

2.2 Casos de uso del Firewall

La reducción de la complejidad mediante la consolidación de los productos para ahorrar costos es una de las principales preocupaciones de muchas empresas. Es igual de importante garantizar el acceso seguro de recursos de las nubes públicas y privadas sin temor al malware cifrado. Conseguir una visibilidad granular de dispositivos, usuarios, información de amenazas en tiempo real y la automatización son fundamentales para garantizar que los ataques se manejen de manera oportuna. [5]

2.2.1 Reducción de la complejidad

Consolide los productos y servicios para reducir la complejidad. Con la protección contra amenazas líder en la industria y los servicios de FortiGuard Labs, puede reducir los costos y maximizar el retorno de la inversión (ROI). [5]

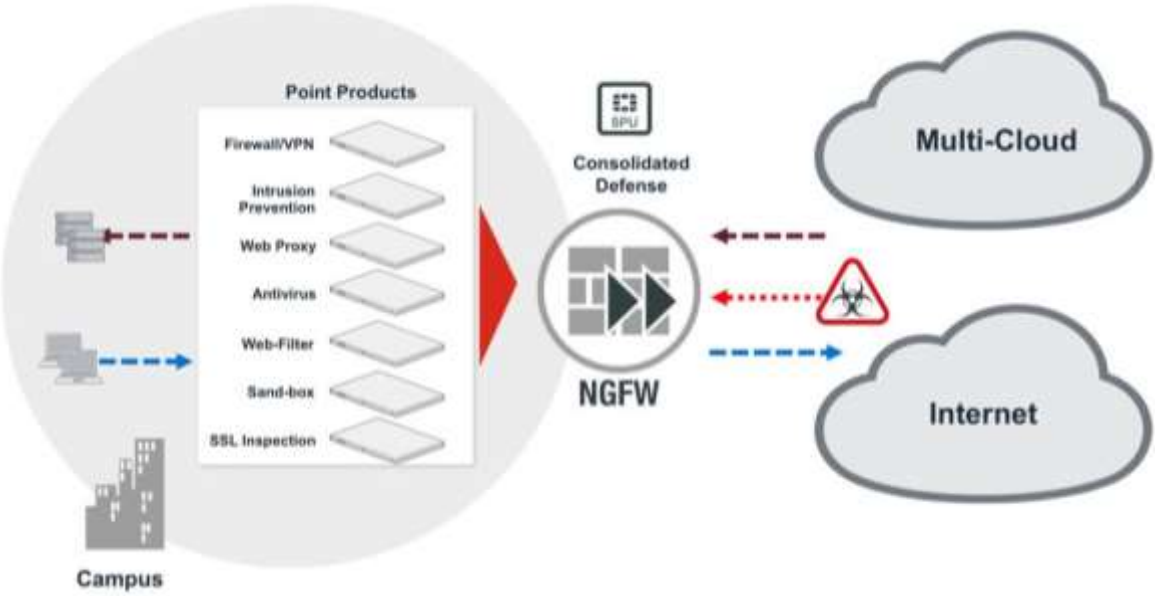

Figura 10: Reducción de la Complejidad.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

Como podemos observar en la ***Figura 10***, la solución de Firewall de próxima generación nos permite consolidar varios servicios en un solo equipo lo cual minimiza los trabajos de interconexión de equipos y ahorrando espacio y dinero a la hora de implementar esa solución.

2.2.2 Acceso cifrado a la nube

Obtenga visibilidad y controles de políticas integrales inspeccionando todo tipo de tráfico, desde texto sin formato hasta cifrado e implemente la protección del sistema de prevención de intrusiones (IPS). [5]

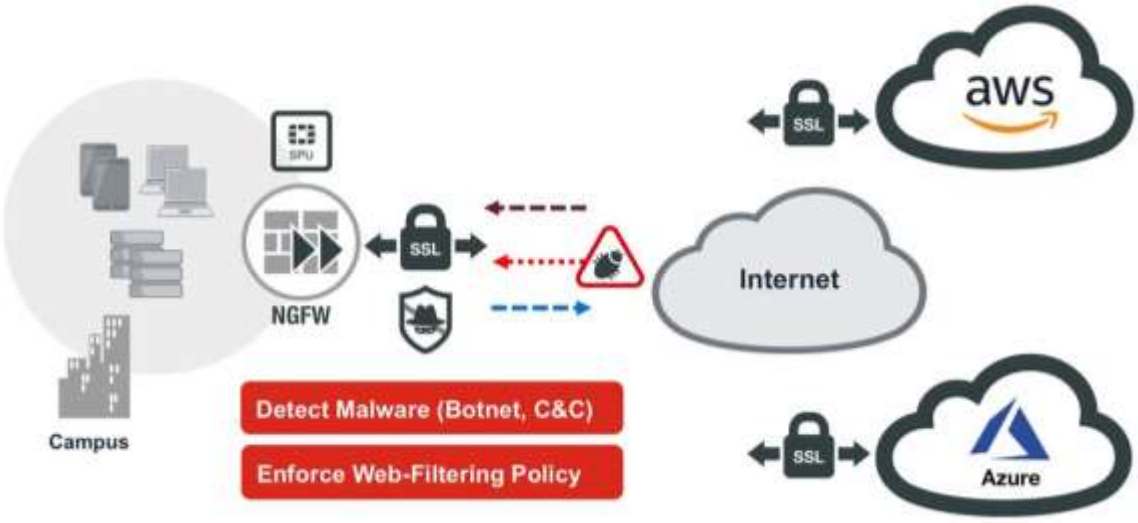

Figura 11: Acceso cifrado a la Nube.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

Los Firewall de Fortinet nos permiten accesos vía web seguro, es decir cómo podemos ver en la ***Figura 11*** la conexión desde nuestra red interna hacia cualquier sitio web o nube privada se realiza de forma cifrada, esto garantizando una mayor seguridad y análisis de esta información para evitar subprogramas espías o cualquiera que pueda comprometer la seguridad de la red interna.

2.2.3 Visibilidad y Automatización

Obtenga acceso a eventos de red y seguridad para obtener visibilidad contextual y simplifique las operaciones con procesos automatizados. [5]

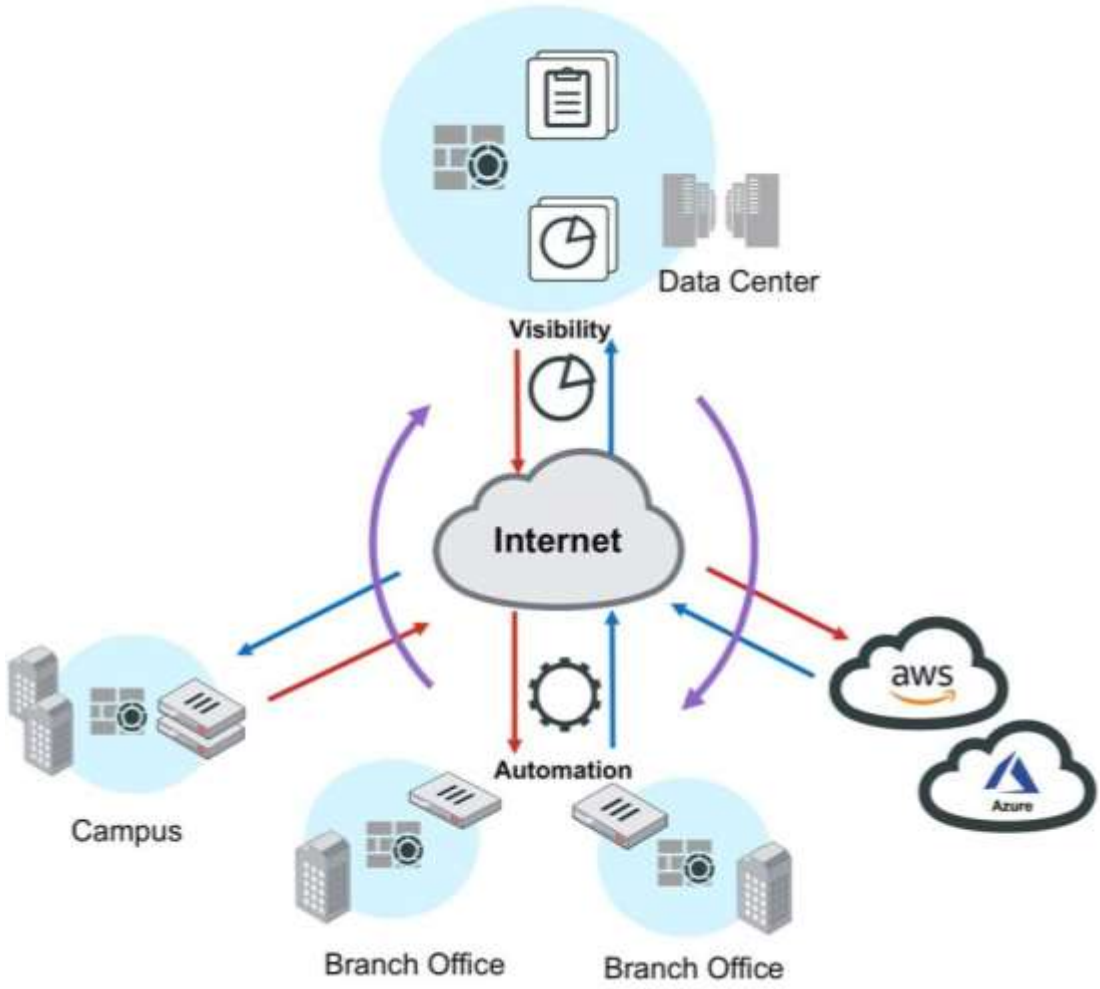

Figura 12: Visibilidad y Automatización.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

Para instituciones que poseen distintas localidades y un control centralizado, los procesos de registros de actividades y análisis de los mismos pueden ser tediosos y complicados por la cantidad de información recibida en el centro de control; los equipos Fortinet permiten reducir el flujo de esta información mediante filtros y configuraciones que focalizan el esfuerzo del sistema de seguridad en aquellos aspectos que presentan patrones de incidencias siendo un trabajo global del sistema tal como se muestra en la ***Figura 12***.

2.3 Casos de uso de segmentación basada en objetivos

La segmentación basada en objetivos permite a los operadores de la red crear dominios de seguridad o segmentos basados en objetivos de la empresa. La segmentación basada en objetivos es la capacidad de implementar protección contra amenazas donde sea necesario, tanto en entornos locales como en todas las instancias en la nube, para reducir el riesgo, lograr el cumplimiento y proteger las aplicaciones críticas para la empresa. [5]

2.3.1 Reducción de la superficie de ataque

Administre eficazmente los vectores de ataque con microsegmentos, protección contra amenazas líder en la industria y servicios de FortiGuard Labs. [5]

Figura 13: Reducción de la Superficie de Ataque.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

Una de las funcionalidades de los sistemas Fortinet nos permiten segmentar nuestras redes para controles separados y más específicos según las necesidades o características de cada sección, esto permite el desvío y bloqueo de ataques dirigidos, optimizando la seguridad en el sistema ya que como se muestra en la ***Figura 13***, el ataque tiene un solo ingreso, pero internamente es desviado y bloqueado por los diversos segmentos de la red.

2.3.2 Cumplimiento Normativo

Cumpla con los requerimientos normativos y de cumplimiento, como PCI DSS, PII, HIPPA y GDPR. [5]

Figura 14: Cumplimiento Normativo.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

Los equipos Fortinet no solo tienen los algoritmos que detectan amenazas y bloquean ataque y proveen seguridad informática, sino que al ser equipos utilizados globalmente y para redes y servicios globales; estos equipos además cuentan y cumplen con las normativas,

protocolos estándares de la industria que maneja información digital, normalizando sus servicios para el cumplimiento de estas industrias como podemos observar en la ***Figura 14.***

2.3.3 Acceso a aplicaciones confiables

Mejore su postura de seguridad protegiendo las aplicaciones de la empresa e implementando el control de acceso adaptativo. [5]

Figura 15: Acceso a Aplicaciones Confiables.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

Las instituciones que ofrecen servicios y aplicativos tienen que lidiar con el riesgo de accesos masivos y globales a sus redes internas, por lo que como se puede apreciar en la ***Figura 15***, los equipos Fortinet nos permiten accesos cifrados que proveen de la seguridad necesaria para estos servicios y aplicativos sean seguros para los usuarios finales y para las instituciones que los proveen.

CAPITULO III

INSTALACIÓN, CONFIGURACIÓN Y APLICACIÓN DE REGLAS DE SEGURIDAD

La Universidad de las Fuerzas Armadas ESPE, es una Institución de larga trayectoria que a través de los años le ha dado gran importancia a la innovación y mejoramiento de su estructura y tecnología, y al manejar grandes e importantes cantidades de información necesita estar protegida contra ataque informáticos de personas malintencionadas; es por eso que esta institución a realizados varias investigaciones y análisis, apostando a una solución de Hardware y Software con la marca FORTINET.

FORTINET cuanta con equipos con la capacidad de suplir las necesidades de seguridad que la Universidad requiere para bienestar de la entidad en sí y de todas las personas que utilizan sus servicios.

Para esto hay que tener claro que la seguridad implementada es un conjunto de equipos y que mediante las configuraciones realizadas proveen la seguridad esperada.

El departamento de TICs basándose en la seguridad previa que tenía la institución y en otras investigaciones que actualizan estos datos, decidieron que como equipo principal del sistema de seguridad informática actuaria un FortiGate FG-3200D de FORTINET.

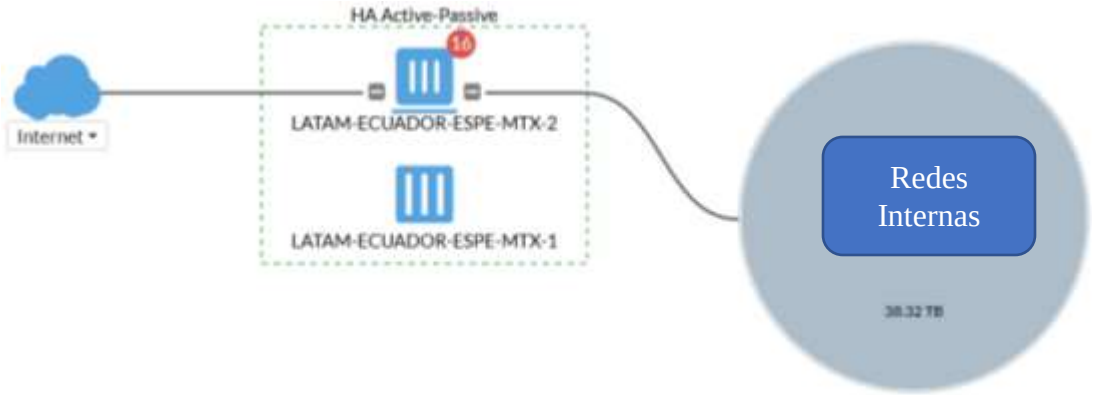

Figura 16: Configuración Lógica del FortiGate.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

En la ***Figura 16*** podemos observar la configuración física de equipo de seguridad informática de la ESPE, podemos observar que el equipo es el enlace entra las redes internas y externas de la Universidad; centralizando en este equipo todos los sistemas y protocolos de servicios que actúan como escudo ante posibles ataques informáticos del exterior.

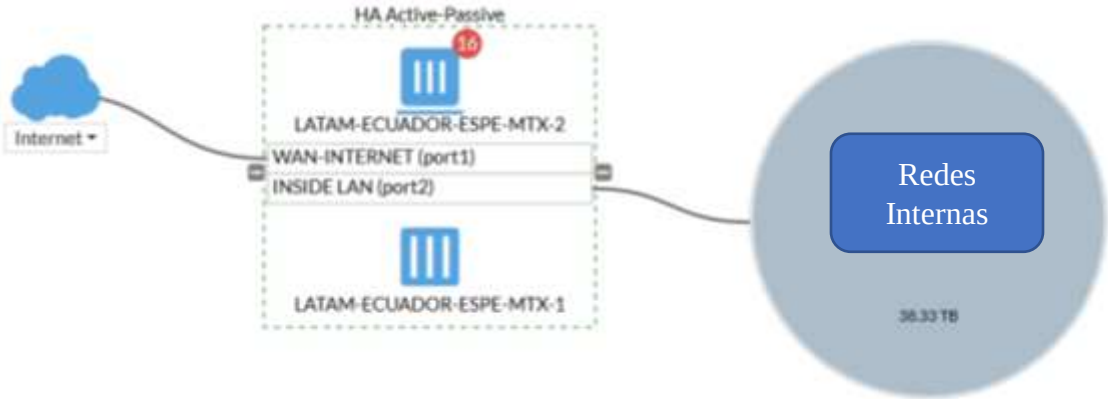

Figura 17: Configuración Física del FortiGate.
Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case

En la ***Figura 17*** podemos observar la configuración lógica de equipo de seguridad informática de la ESPE, podemos observar que el equipo es el enlace entra las redes internas y externas de la Universidad; este equipo al centralizar todos los servicios de seguridad no solo protege a las redes internas de la Universidad de cualquier ataque externo, sino que también protege a las diversas redes internas de cualquier amenaza que se pueda generar dentro de la institución, ya que estas redes son utilizadas por una gran variedad de personas y la institución debe estar preparada para cualquier posible escenario de riesgo.

La Universidad maneja variados mecanismos de seguridad informática lo cual hace más óptimo el mecanismo de seguridad, actualización y crecimiento del mismo; esto hace que el sistema se divida en varios niveles de seguridad o en segmentos escalonados donde dependen unos de otros.

3.1 Configuración del Equipo FortiGate.

La configuración básica como conexiones físicas, nombre de equipo, accesos, claves, red y demás no lo toparemos en este trabajo por motivos de seguridad, en cuanto a la configuración de reglas y políticas de seguridad se indicará de forma que no se incurrirá en detalles que puedan comprometer la seguridad informática de la institución.

La aplicación de reglas o de políticas de seguridad con el equipo FortiGate es un proceso escalonado esto quiere decir que los niveles superiores dependen de los niveles inferiores.

3.1.1 Tabas de Registros en la Plataforma.

El equipo FortiGate cuenta con una plataforma de administración la cual nuestra todos los aspectos físicos y lógicos del equipo.

Esta plataforma no solo nos permite ver el estado físico del equipo en tiempo real sino también mediante archivos de registro y estadísticas lo cual se convierte en una herramienta adicional para la toma de decisiones basado en comportamientos de la red.

Esta plataforma permite realizar el registro de datos en las diferentes tablas, tales como Address, Address Group entre otras; mismas tablas que nos permiten configurar las reglas de seguridad, estas tablas ya vienen creadas en el equipo y están relacionadas entre sí ya que como lo mencionamos unas dependen de otras.

3.1.1.1 Tabla Address.

La tabla Address es una de las tablas base del sistema, es donde se registra e identifica a cada usuario (entendiéndose como usuario a un Host o conjuntos de Host) que estará dentro de las diferentes redes que maneja la ESPE; esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

TYPE: Es el tipo de registro ya que este puede ser una SubRed, Rango IP o FQDN.

DETAILS: El detalle del registro, este variará según el tipo de registro, es decir puede ser la dirección de una red IP, un rango de direcciones IP o FQDN (dirección web específica).

3.1.1.2 Tabla Address Group.

La tabla AddressGroup es una de las tablas de siguiente nivel basándose en la Tabla Address, es donde se registra e identifica los diferentes grupos usuarios que estará dentro de las diferentes redes que maneja la ESPE; esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS GROUP: El detalle es donde se especifica los integrantes de este grupo que ya se han registrado en la tabla Address, cabe recalcar que hay grupos integrados por otros grupos previamente creados.

3.1.1.3 Tabla Wildcard FQDN.

La tabla Wildcard FQDN es una de las tablas base del sistema, es donde se registra e identifica sitios web importantes para la ESPE como sitios de actualización de software entre otros; esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: En este campo se asigna el detalle del registro, es decir del sitio web que normalmente está dado por el dominio o subdominio del mismo.

3.1.1.4 Tabla Schedules.

La tabla Schedules es una de las tablas base del sistema, es donde se registra los periodos de tiempos que se asignaran posteriormente a las reglas de la ESPE; esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DAYS: Son los días de operación asignados.

START: Es la hora de inicio del registro.

END: Es la hora de fin del registro.

3.1.1.5 Tabla Schedules Group.

La tabla Schedules Group es una de las tablas de siguiente nivel ya que hace grupos con los registros de la tabla Schedules, esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DAYS: Son los días de operación asignados.

START: Es la hora de inicio del registro.

END: Es la hora de fin del registro.

3.1.1.6 Tabla Virtual IPs.

La tabla Virtual IPs es una de las tablas base del sistema, es donde se registra el intercambio de ips físicas por virtuales, lo cual es parte del proceso de seguridad informática de la ESPE; esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: En este campo se registra el cambio de dirección IP de físicas a virtuales y de una red a otra.

3.1.1.7 Tabla Virtual IPs Group.

La tabla Virtual IPs Group es una de las tablas de siguiente nivel ya que hace grupos con los registros de la tabla Virtual IPs, esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre del grupo a registrar.

DETAILS: En el detalle van los nombres de los registros que pertenecen al grupo, ya que son los registros de la tabla Virtual IPs.

3.1.1.8 Tabla IP PoolS.

La tabla IP Pools es una de las tablas base del sistema, es donde se registra los Pool o grupos de direcciones Ip que serán utilizados por las reglas del firewall; esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: El detalle del Pool o grupo de direcciones ip pertenecientes al registro.

3.1.1.9 Tabla User.

La tabla User es una de las tablas base del sistema, es donde se registra las personas u organizaciones que tendrán acceso al equipo (estas personas u organizaciones son acreditadas por la Universidad para el acceso al equipo y tienen distintos niveles de acceso que restringen sus acciones, todo esto por motivos de seguridad); esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: El detalle según el tipo de registro, ya que pude tener distintos niveles de acceso o de seguridad.

3.1.1.10 Tabla User Group.

La tabla User Group es una de las tablas de siguiente nivel ya que hace grupos de personas u organizaciones que tendrán acceso al equipo (estas personas u organizaciones son acreditadas por la Universidad para el acceso al equipo y tienen distintos niveles de acceso que restringen sus acciones, todo esto por motivos de seguridad); esta tabla cuenta con varios campos entre ellos los más importantes son:

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: En este campo va el tipo de registro.

VISIBILITY: En este campo se coloca el grupo o persona para el cual es visible este registro, eventualmente para os demás quedara oculto.

3.1.1.11 Tabla Service.

La tabla Service es una de las tablas base del sistema, es donde se registra los servicios que implementaran las deferentes reglas del firewall, restringiendo o dando acceso a los servicios de la ESPE; esta tabla cuenta con varios campos entre ellos los más importantes son:

CATEGORIA: Es el grupo al que pertenece el servicio (interno o externo a la ESPE).

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: En este campo se detalla el servicio que ofrece este registro siendo puertos TCP, UDP, o combinaciones.

3.1.1.12 Tabla Service Group.

La tabla Service Group es una de las tablas de siguiente nivel ya que hace grupos de servicios basado en la tabla Service; esta tabla cuenta con varios campos entre ellos los más importantes son:

CATEGORIA: Es el grupo al que pertenece el servicio (interno o externo a la ESPE).

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: En este campo se detalla el servicio que ofrece este registro siendo puertos TCP, UDP, o combinaciones.

3.1.1.13 Tabla IPv4 Policy.

La tabla IPv4Policy es la tabla de más alto nivel ya que engloba a todas las anteriores, se basa en todos los registros de todas las tablas existentes para poder orientar reglas generales para grupos o sectores y también reglas específicas para grupos o personas basadas en horarios, servicios, direccionamiento ip, etc.; esta tabla cuenta con varios campos entre ellos los más importantes son:

CATEGORIA: Es el grupo al que pertenece el servicio (interno o externo a la ESPE).

NAME: Es el campo donde se le asignara el nombre al registro.

DETAILS: El detalle de los servicios que pertenecen a este registro.

Cabe recalcar que esta es la tabla donde están todas las reglas existentes basadas en todos los registros existentes en las tablas y que es donde se maximiza las propiedades y potencias del equipo, ya que aquí es donde se niega o concede los accesos a sectores, equipos, servicios etc., basado en los diversos grupos y necesidades de cada uno de ellos que ocupan los servicios de la ESPE.

CAPÍTULO IV

EVALUACIÓN DE LA SOLUCIÓN DE SEGURIDAD INFORMÁTICA

El sistema de seguridad informática operante en la Universidad de las Fuerzas Armadas "ESPE", tiene reglas configuradas basadas y las reglas anteriormente operantes y a los análisis de seguridad realizados por parte del personal de UTICs, estas reglas se han optimizado para cubrir todos los aspectos y necesidades de las diferentes áreas y personal que utiliza los servicios de las redes de la Universidad.

La evaluación del sistema de seguridad informático se ha efectuado basado en las reglas y los registros de todas las tablas de la plataforma antes mencionado, se ha desarrollado un software de análisis que nos permite ver factores como duplicidad de registros, de puertos, de servicios, incoherencias, y posibles riesgos para la seguridad informática.

El programa trabaja creando una base de datos con los registros completos para posteriormente ser analizados tabla por tabla.

Para una mejor comprensión del trabajo que realiza el software realizaremos un pequeño ejemplo con registros similares.

Tabla 01:
Estructura Original de la Tabla Address

NAME	*TYPE*	*DETAILS*	*VISIBILITY*	*REF.*
Registro 001	Subnet	2.3.69.209/32	Visible	0
Registro 002	Subnet	10.0.0.0/8	Visible	0
Registro 003	Subnet	10.1.0.0/16	Visible	0
Registro 004	Subnet	10.1.0.25/32	Visible	0
Registro 005	Subnet	10.1.0.41/32	Visible	0
Registro 006	Subnet	10.1.0.83/32	Visible	0
Registro 007	Subnet	10.1.0.25/32	Visible	0
Registro 008	Subnet	188.112.147.234/32	Visible	0
Registro 009	Subnet	10.9.24.11/32	Visible	0
Registro 010	Subnet	10.1.0.41/32	Visible	0
Registro 011	Subnet	10.1.0.112/32	Visible	0

En la ***Tabla 01*** podemos observar una tabla con la estructura original de la Taba Address, en la cual hemos colocado registros similares para proceder con un ejemplo del procedimiento.

En el programa se crea la base de datos con las diferentes tablas, las cuales se crean con la misma estructura de las originales añadiendo una columna al final que será donde se colocará el resultado del análisis.

Tabla 02:
Estructura Modificada de la Tabla Address

REGISTRO	*NAME*	*TYPE*	*DETAILS*	*VISIBILITY*	*REF.*	*OBSERVACION*
1	Registro 001	Subnet	2.3.69.209/32	Visible	0	
2	Registro 002	Subnet	10.0.0.0/8	Visible	0	
3	Registro 003	Subnet	10.1.0.0/16	Visible	0	
4	Registro 004	Subnet	10.1.0.25/32	Visible	0	
5	Registro 005	Subnet	10.1.0.41/32	Visible	0	
6	Registro 006	Subnet	10.1.0.83/32	Visible	0	
7	Registro 007	Subnet	10.1.0.25/32	Visible	0	
8	Registro 008	Subnet	188.112.147.234/32	Visible	0	
9	Registro 009	Subnet	10.9.24.11/32	Visible	0	
10	Registro 010	Subnet	10.1.0.41/32	Visible	0	
11	Registro 011	Subnet	10.1.0.112/32	Visible	0	

Con las tablas creadas se insertan los registros de las tablas con el ultimo campo vacío mediante el código sql que se ve a continuación.

INSERT INTO ADDRESS VALUES ('Registro 001', 'Subnet', '2.3.69.209/32', 'Visible', '0', ')";

Estos códigos nos permiten insertar los registros en las tablas las cuales quedan como se muestra en la ***Tabla 02***. Una vez creadas las tablas e insertados los respectivos registros procedemos a mediante una rutina de código leer por completo la columna "***DETAILS***" y guardando los valores en variables que se comparan una a una y detentan registros duplicados; cuando se detectan registros duplicados se modifica la fila a la que pertenecen estos registros colocando la respectiva observación.

Tabla 03:
Estructura Final de la Tabla Address

REGISTRO	*NAME*	*TYPE*	*DETAILS*	*VISIBILITY*	*REF.*	*OBSERVACION*
1	Registro 001	Subnet	2.3.69.209/32	Visible	0	Ok
2	Registro 002	Subnet	10.0.0.0/8	Visible	0	Ok
3	Registro 003	Subnet	10.1.0.0/16	Visible	0	Ok
4	Registro 004	Subnet	10.1.0.25/32	Visible	0	Duplicado01
5	Registro 005	Subnet	10.1.0.41/32	Visible	0	Duplicado02
6	Registro 006	Subnet	10.1.0.83/32	Visible	0	Ok
7	Registro 007	Subnet	10.1.0.25/32	Visible	0	Duplicado01
8	Registro 008	Subnet	188.112.147.234/32	Visible	0	Ok
9	Registro 009	Subnet	10.9.24.11/32	Visible	0	Ok
10	Registro 010	Subnet	10.1.0.41/32	Visible	0	Duplicado02
11	Registro 011	Subnet	10.1.0.112/32	Visible	0	Ok

Una vez realizado el análisis en la tabla y modificados los registros en la columna "***OBSERVACION***" queda como se muestra en la ***Tabla 03***, la misma que en base a los datos en la columna "***OBSERVACION***" de cada registro podrá ser filtrada por los mismos.

4.2 Ingreso al sistema.

El software desarrollado nos presenta una interface de ingreso al mismo mediante acceso restringido por usuario y contraseña.

Figura 18: Interface de Ingreso al Software.

El acceso está restringido por una combinación de usuario y clave fijos, los cuales de ser necesario podrían ser cambiado desde el código fuente del programa.

Figura 19: Ventana Principal sin Base de Datos.

Esta ventana muestra las opciones, pero al ser ejecutada por primera vez el programa verifica en el sistema si existe la base de datos y si tiene cargados los registros de no ser así se muestra con la ***Figura 19***, dándonos pocas opciones; al presionar el botón de "Generar Base de Datos" de la ***Figura 20***, el programa primero revisa las condiciones del sistema y de ser adecuadas prosigue con la generación de la base de datos, de no ser las condiciones adecuadas adecua el sistema dentro de lo que su programación lo permite, caso contrario nos mostrara una alerta indicando las novedades y los obstáculos encontrado.

El programa genera la base de datos y posteriormente ingresa todos los registros de cada una de las tablas para ser analizados; cabe recalcar que el software no trabaja en tiempo real con la plataforma ni los equipos, ya que incurriría en una nueva vulnerabilidad para la seguridad informática de la Universidad.

Figura 20: Ventana Principal Generando Base de Datos.

Cuando se ha presionado el botón de "***Generar Base de Datos***", el programa primero boquea este botón para evitar que sea presionado en más de una ocasión y puedan duplicarse los registros en la base de datos tal como se muestra en la ***Figura 20***.

Figura 21: Ventana Principal con Base de Datos.

En la figura anterior podemos observar la ventana del software una vez a terminado de generar la base de datos y de integrar todos los registros en la misma, esta misma ventana es la que se abrirá de ahora en adelante ya que el sistema verificará la existencia e integridad de la base de datos y según eso nos da la primera o segunda ventana.

En esta ventana podemos acceder a todas las tablas base y de alto nivel que se han analizado para ver sus registros y las observaciones dadas en base al análisis realizado.

4.3 Análisis de los Registros de las Tablas.

Todas y cada una de las tablas aquí mostradas han sido analizadas, en busca de información en sus registros que puedan resultar perjudiciales para la seguridad del sistema informático de la Universidad de las Fuerzas Armadas ESPE.

Se han tomado en cuenta parámetros como duplicidad de registros, de puertos, de servicios, además de políticas de seguridad riesgosas, como entrega de servicios a programas especifico con todos los puertos abiertos o disponibles cuando se debería restringir estos puertos.

Estas observaciones el software las entrega en un informe generado para el análisis del personal de UTICs, ya que ellos son los únicos autorizados a modificar reglas en el sistema.

4.3.1 Análisis de Tabla Address.

En la tabla Address al ser una tabla base se analizó los registros repetidos, la duplicidad se analizó en la columna de "***Detalles***" ya que es en esa columna donde está la información principal del registro, tal como se muestra en la ***Figura 22***.

Figura 22: Tabla Address Completa.

El software tiene la posibilidad de filtrar los registros por observación, es decir que los registros donde se encuentra alguna observación serán filtrados para poder ser observados con más atención y localizar posibles conflictos existentes en los registros como se puede observar en la ***Figura 23***, además de este filtro existe un filtro adicional, es un filtro dedicado donde se puede separar registros con observaciones específicas como se puede observar en la ***Figura 24***, esto para poder analizar y realizar las acciones que crean pertinentes el personal de UTICs

Figura 23: Tabla Address Filtrada.

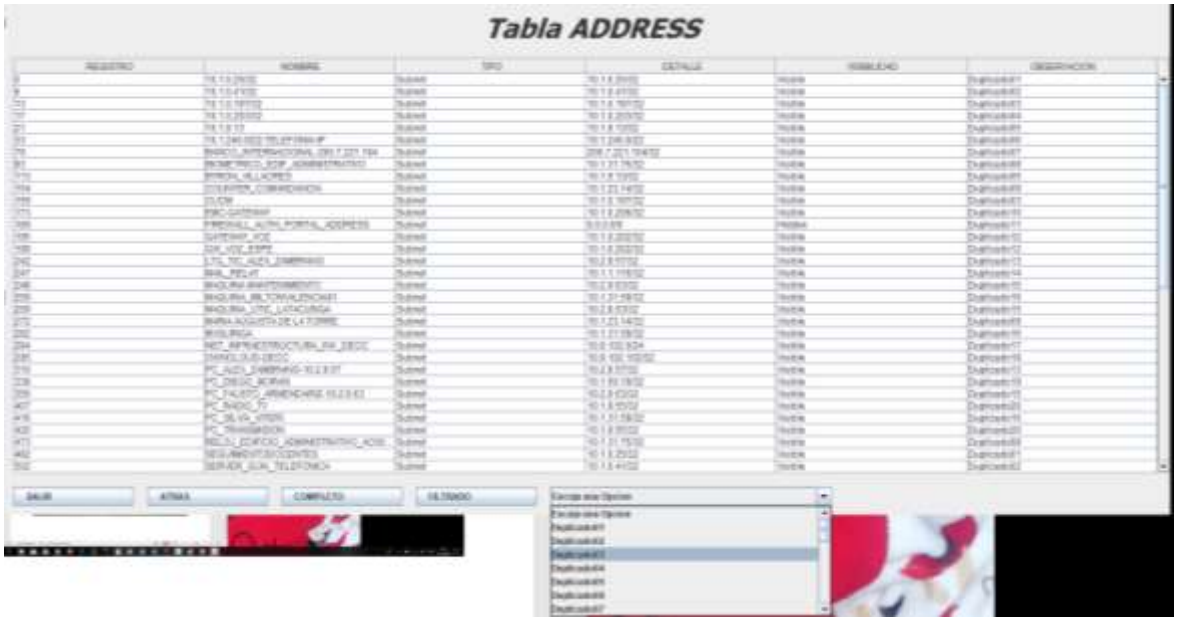

Figura 24: Tabla Address con Filtro Dedicado.

Figura 25: Tabla Address con Filtro Especifico.

Una vez escogido el filtro dedicado en la lista desplegable como se puede observar en la ***Figura 24***, el programa limpia la tabla y muestra solo los registros que cumplen con el criterio de la lista desplegable tal como se muestra en la ***Figura 25***.

4.3.2 Análisis de Tabla Address Group.

La tabla Address Group está compuesta por los registros de la tabla Addres y la analizamos en 2 grupos ya que hay grupos formados por otros grupos, al igual que en la tabla Address se analiza la columna Observaciones donde se indican lo encontrado en cada registro.

Figura 26: Tabla Address Group 1 Completa.

En la tabla Address Group 1 no se encuentran registro con observaciones como se observa en la ***Figura 26***.

Figura 27: Tabla Address Group 2 Completa.

La tabla Address Group 2 está constituida en cascada ya que se compone de los registros de la tabla Address Group 1 y está de los registros de la tabla Address, además de los registros de la tabla Address directamente como se muestra en la ***Figura 27***.

Figura 28: Tabla Address Group 2 Filtrada.

En la tabla Address Group 2 está disponible la opción de filtrado general presionando el botón "***FILTRADO***" para poder observar todos los registros con alguna observación tal como se muestra en la ***Figura 28***.

Figura 29: Tabla Address Group 2 con Filtro Especifico.

Además, una vez filtrados los registros de la tabla Address Group 2 se puede escoger una opción de la lista desplegable para un filtro dedicado y ver una los registros correspondientes a una observación en específico, tal como se muestra en la ***Figura 29***.

4.3.3 Análisis de Tabla WildCard.

La Tabla WildCard es una de las tablas base del sistema la cual sirve para alimentar con sus registros a tablas de mayor nivel, en esta tabla no se encontraron novedades de duplicidad ni inconsistencias.

Figura 30: Tabla WildCard Completa.

4.3.4 Análisis de Tabla Schedule.

Esta es una de las tablas bases del sistema la cual tiene algunas observaciones que pueden ser filtradas ya sea por filtro general presionando el botón "***FILTRADO***" o posterior a esto

escogiendo mediante la lista desplegable un filtro dedicado como se observa en la ***Figura 31***.

Figura 31: Tabla Schedules Completa.

La tabla Schedules Group es una tabla de alto nivel cuyos registros están compuestos pos los registros de la tabla Schedules, es esta tabla no se han encontrado problemas de duplicación o inconsistencias, pero sirven los registros para las tablas de mas alo nivel, esto se puede observar en la ***Figura 32***.

Figura 32: Tabla Schedules Group.

4.3.5 Análisis de Virtual IPs.

La tabla de Virtual IPs es una tabla base para las reglas en la tabla superior, esta tabla no tiene observaciones a considerar en sus registros como se observa en la ***Figura 33***.

Figura 33: Tabla Virtual IPs.

La Tabla Virtual IPs es una base para la tabla Virtual IPs Group, estas 2 tablas sirven para poder ingresar sus registros en las tablas superiores o en las reglas de las políticas de seguridad; como se puede observar en la ***Figura 34***, esta tabla no tiene observaciones en sus registros.

Figura 34: Tabla Virtual Ips Group.

4.3.6 Análisis de IP Pools.

La tabla Ip Pools es de las bases del sistema y no tiene observaciones de duplicaciones ni de inconsistencias, sirve para las tablas de más alto nivel y para las reglas de seguridad.

Figura 35: Tabla IP Pools.

4.3.7 Análisis de Tabla User.

La tabla USER es la más importante en cuanto a administración ya que se trata de las personas autorizadas para el uso del sistema y los niveles de acceso que ellas tienen.

De esta tabla se deriva o construye la tabla USER Group que engloba a los registros de la tabla User, el análisis de estas 2 tablas nos muestra que no hay duplicidad ni tampoco inconsistencias, aunque su existencia es indispensable ya que nos provee de los datos para los accesos al sistema y control del mismo.

Figura 36: Tabla USER.

Figura 37: Tabla USER Group.

4.3.8 Análisis de Tabla Service.

La tabla Service es de suma importancia pues es donde se configuran los servicios que se darán o negarán, los rangos de puertos los tipos de servicios, etc.

En esta tabla el análisis para encontrar falencia ha sido minucioso ya que depende de otras tablas y de los servicios a los cuales está orientado cada registro en esta tabla.

Figura 38: Tabla Service Completa.

Al igual que las otras tablas analizadas se ha añadido una columna llamada Observaciones que es donde se indica las falencias encontradas tales como servicios repetidos, puertos repetidos entre otros; en la ***Figura 38*** se puede observar la tabla completa pero estas observaciones pueden observarse de mejor manera usando un filtro.

Figura 39: Tabla Service Filtrada.

Presionando el botón de “FILTRO” el programa nos muestra solo los registros que tienen alguna observación como se puede apreciar en la ***Figura 39***.

Figura 40: Tabla Service Filtrado Especifico 1.

Además, en software permite hacer un filtrado por tipo de observación como se muestra en la ***Figura 40***, lo cual hace más efectivo la búsqueda de falencias.

Figura 41: Tabla Service Filtrado Especifico 2.

Al escoger de la lista desplegable una observación en específico se muestran solo los registros que coinciden con este criterio como se muestra en la ***Figura 41***.

Al existir muchos grupos y muchos servicios todos estos registros de esta tabla Service se agrupan en registros de mayor nivel en la Tabla Service Group (***Figura 42***).

Figura 42: Tabla Service Group Completa.

La consecuencia de estar basada en registros de tablas de niveles inferiores es que, si estas tablas origen tiene falencias, estas se pasarán a la nueva, por tal motivo se analizó y encontró falencias en los registros.

Figura 43: Tabla Service Group Filtrada.

4.3.9 Análisis de Tabla IPv4 Policy.

Esta es la tabla de más alto rango ya que engloba todas las tablas anteriormente revisadas, es un complejo sistema funcional que arrastra todas las falencias ya observadas.

Al estar compuesta por otra tabla la seguridad de que no presenta falla se da modificando los registros de las tablas base, el programa nos permite el análisis de regla a regla viendo estas falencias para darnos la orientación necesaria y corregirlas.

Figura 44: Tabla IPv4 Policy Completa.

El programa en esta ocasión nos permite filtrar regla por regla con todas sus características para poder observar cada aspecto de la misma, y poder tomar las decisiones del caso, se si tuviese que modificar, borrar o crear una nueva regla.

Figura 45: Tabla IPv4 Policy Filtrada por Regla.

4.3.10 Análisis de Tabla Verificación de Datos.

La tabla verificación de datos nos permite ver la integridad de la base de datos, las tablas que incluye, los registros que posee y su respectivo estado. Además, genera un informe con datos relevantes sobre las observaciones echa en cada tabla.

Figura 46: Tabla de Verificación de la Base de Datos.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Los sistemas de seguridad informática pueden optimizarse de forma continua y la Universidad de las Fuerzas Armadas ESPE no es la ecxepción.
- Con el crecimiento de las redes y los servicios que estas ofrecen, aumenta el riesgo de ataque en las redes y de igual manera debe aumentar el control y esfurzo por la mejor de las seguridades de las mismas.
- La aplicación desarrollada nos da información sobre posibles falencias en los registros del sistema de seguridad de la ESPE.
- La información obtenida en el presente trabajo, nos da un punto de vista que nos ayuda para modificar los registros detectados, con el fin de optimizar la seguridad informática.
- Entre la información detectada en el presente trabajo lo más riesgoso son los servicios no optimizados, donde los puertos libres que se asignan son vulnerabilidades de alto riesgo.
- El resultado del presente trabajo es una guía a considerar con alto grado de fidelidad para la optimización de los sistemas por parte del personal de UTICs.

- Los resultados encontrados están sujetos a implementación según criterios del personal de UTICs.

5.2 Recomendaciones

- Realizar un análisis periódico de las redes en busca de vulnerabilidades en los sistemas.
- Implementar procesos y procedimientos para la modificación de registros base para disminuir el impacto en los registros de nivel superior.
- Analizar y obtener registros e historiales de actividades para optimizar las seguridades.
- Realizar análisis y capacitaciones constantes sobre nuevas tecnologías y el impacto que estas puedan generar en los sistemas existentes.
- Obtimizar la herramienta de software desarrollada y otras que puedan implimentarse a futuro para mejorar el análisis y/o la presentación de resultados, con el fin de hacer mas rápido y presiso el análisis de seguridad

5.3 Bibliografía

[1] J. Rojas, «Monografias.com,» 17 Agosto 2010. [En línea]. Available: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml. [Último acceso: 15 Noviembre 2019].

[2] J. Rojas, «Monografias.com,» 17 Agosto 2010. [En línea]. Available: https://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml. [Último acceso: 16 Noviembre 2019].

[3] «FORTINET,» [En línea]. Available: https://www.fortinet.com/lat/solutions/enterprise-midsize-business/enterprise-security.html. [Último acceso: 25 Noviembre 2019].

[4] «FORTINET,» [En línea]. Available: https://www.fortinet.com/lat/products/next-generation-firewall.html. [Último acceso: 26 Noviembre 2019].

[5] «FORTINET,» [En línea]. Available: https://www.fortinet.com/lat/products/next-generation-firewall.html#use-case. [Último acceso: 26 Noviembre 2019].

[6] «www.fortinet.com,» 11 Abril 2019. [En línea]. Available: https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security.html.

ANEXOS