
# Análisis comparativo de las nuevas tecnologías de software libre y software propietario para la protección perimetral de la información (firewall) del COMIL 1, con el fin de proponer la mejor tecnología para la protección de la información del área de operaciones de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No. 1 "Eloy Alfaro"

Flores Vaca, Boris Wladimir

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Trabajo de integración curricular previo a la obtención de título de Tecnólogo Superior en Redes y Telecomunicaciones

Msg. Viteri Arias, Santiago Christian

31 de julio del 2023

Latacunga

# Informe de originalidad

NOMBRE DEL CURSO
REVISION TESIS BORIS FLORES

NOMBRE DEL ALUMNO
BORIS WLADIMIR FLORES VACA

NOMBRE DEL ARCHIVO
BORIS WLADIMIR FLORES VACA - Documento sin título

SE HA CREADO EL INFORME
22 feb 2023

## Resumen

| | | |
|---|---|---|
| Fragmentos marcados | 7 | 1 % |
| Fragmentos citados o entrecomillados | 0 | 0 % |

Coincidencias de la Web

| | | |
|---|---|---|
| poexpansion.es | 1 | 0,3 % |
| zaltor.com | 1 | 0,2 % |
| zonalegal.net | 1 | 0,2 % |
| keepcoding.io | 1 | 0,2 % |
| rockcontent.com | 1 | 0,2 % |
| datainnovation.io | 1 | 0,1 % |
| gcfglobal.org | 1 | 0,1 % |

1 de 7 fragmentos

Fragmento del alumno MARCADO

**Características = Registrado, Doble fila, Las ranuras 13 - 24 sólo están disponibles en la configuración de dos procesadores, HPE SmartMemory**

Mejor coincidencia en la Web

**Características: Registrado, Doble Fila, Las Ranuras 13-24 Sólo Están Disponibles En La Configuración De Dos Procesadores, Hpe Smartmemory, Arquitectura De Memoria De 6 Canales**

Servidores Hpe Proliant Dl380 Gen10 Network Choice https://www.poexpansion.es/hpe-proliant-dl380-gen10-network-choice.php

Viteri Arias, Cristian Santiago
C.C: 050247691-4

**Departamento de Eléctrica, Electrónica y Telecomunicaciones**

**Carrera de Tecnología Superior en Redes y Telecomunicaciones**

**Certificación**

Certifico que el trabajo de integración curricular: **Análisis comparativo de las nuevas tecnologías de software libre y software propietario para la protección perimetral de la información (firewall) del COMIL 1, con el fin de proponer la mejor tecnología para la protección de la información del área de operaciones de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 "Eloy Alfaro"**, fue realizado por el señor **Flores Vaca Boris Wladimir** la cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga, 31 de julio del 2023

Viteri Arias, Cristian Santiago
C.C: 050247691-4

**Departamento de Eléctrica, Electrónica y Telecomunicaciones**

**Carrera de Tecnología Superior en Redes y Telecomunicaciones**

**Responsabilidad de Autoría**

Yo, **Flores Vaca Boris Wladimir** con cédula de ciudadanía N° 1754476578, declaro que el contenido, ideas y criterios del trabajo de integración curricular: **Análisis comparativo de las nuevas tecnologías de software libre y software propietario para la protección perimetral de la información (firewall) del COMIL 1, con el fin de proponer la mejor tecnología para la protección de la información del área de operaciones de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 "Eloy Alfaro"**, es de nuestra autoría y responsabilidad, cumpliendo con los requisitoslegales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales deterceros y referenciando las citas bibliográficas.

Latacunga, 31 de julio del 2023

**Flores Vaca Boris Wladimir**

C.C.: 1754476578

**Departamento de Eléctrica, Electrónica y Telecomunicaciones**

**Carrera de Tecnología Superior en Redes y Telecomunicaciones**

**Autorización de Publicación**

Yo, **Flores Vaca Boris Wladimir** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Análisis comparativo de las nuevas tecnologías de software libre y software propietario para la protección perimetral de la información (firewall) del COMIL 1, con el fin de proponer la mejor tecnología para la protección de la información del área de operaciones de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 "Eloy Alfaro"**, en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Latacunga, 31 de julio del 2023

**Flores Vaca Boris Wladimir**

C.C.: 1754476578

## Dedicatoria

Dedico este trabajo en primer lugar a Dios, por haberme dado sabiduría y sobre todo salud en estos tiempos tan complicados. A mis padres Verónica Vaca y Wladimir Flores por ser mi inspiración y ejemplo a seguir y más aún en el campo educativo, a mi querida familia, por su apoyo incondicional dónde el tiempo de pasar junto a ellos, lo dedique al estudio de esta carrera tecnológica.

**FLORES VACA BORIS WLADIMIR**

## Agradecimiento

A Dios por todas las bendiciones, la sabiduría y fortaleza brindas a mi persona durante toda mi vida.

A esta noble y emblemática institución de educación superior que gracias a sus valores y objetivos institucionales logra mantenerse como un ejemplo en la región.

A sus distinguidas autoridades por el empuje y ejemplo de constancia, trabajo e innovación.

A los catedráticos quienes con sus conocimientos supieron guiarme durante mi periodo de formación estudiantil y por quienes he adquirido los conocimientos necesarios para llevar a buen puerto este proyecto de titulación.

De manera especial a mi familia Flores Vaca por centrar en mis los ideales de trabajo, constancia y compresión para hoy poder culminar finalmente con esta meta propuesta.

**FLORES VACA BORIS WLADIMIR**

**ÍNDICE DE CONTENIDO**

## ÍNDICE DE FIGURAS

## ÍNDICE DE TABLAS

## Resumen

El objetivo de este proyecto es implementar un sistema de video vigilancia con tecnología IP para áreas exteriores y un control de acceso mediante un servidor Radius para el área de docentes en el Colegio Particular “Israel” N°2. El proyecto justifica como se realizó el diseño, el análisis realizado en el establecimiento, los requisitos necesarios para su implementación, y las respectivas pruebas de conectividad y funcionamiento. Esto estableció un sistema inalámbrico sin seguridad. Además, hay espacios donde no hay un sistema de video vigilancia y es necesario implementar el sistema de seguridad. Este proyecto aborda temas relacionados de los elementos que componen un sistema de video vigilancia entre software y hardware por igual en el servidor Radius, centrándose en el análisis de ubicación de cada una de las cámaras de vigilancia para cada uno de los espacios con el objetivo de controlar y supervisar por poder evitar los casos de inseguridad, agresión, etc. De la misma forma, el control de acceso mediante un servidor Radius nos permite un método de autenticación que limita el acceso a usuarios no autorizados en la red inalámbrica del colegio, permitiéndonos fortalecer y mejorar el rendimiento de la red. En definitiva, este plan podrá comprobar un sistema de video vigilancia eficaz y muy fiable que ofrece tranquilidad y seguridad al personal, ya que además podemos acceder a las grabaciones de las cámaras a través de Internet. Además, se pudo brindar una solución para acceder a la red inalámbrica, en la que se imprima el riesgo de perder información importante luego de autenticar al personal.

*Palabras Clave*: Tecnología IP, video vigilancia, conexión segura.

## Abstract

The objective of this project is to implement a video surveillance system with IP technology for outdoor areas and access control through a Radius server for the teachers' area in the Colegio Particular “Israel” N°2. The project justifies how the design was carried out, the analysis made in the establishment, the necessary requirements for its implementation, and the respective connectivity and operation tests. This established a wireless system without security. In addition, there are spaces where there is no video surveillance system and it is necessary to implement the security system. This project addresses related issues of the elements that make up a video surveillance system between software and hardware alike in the Radius server, focusing on the analysis of location of each of the surveillance cameras for each of the spaces in order to control and monitor by being able to prevent cases of insecurity, aggression, etc. In the same way, the access control through a Radius server allows us an authentication method that limits access to unauthorized users in the school's wireless network, allowing us to strengthen and improve the performance of the network. In short, this plan will prove to be an effective and very reliable video surveillance system that offers peace of mind and security to the staff, since we can also access the camera recordings via the Internet. In addition, it was possible to provide a solution to access the wireless network, in which the risk of losing important information after authenticating the staff is printed.


*Keywords:* IP Technology, video surveillance, secure connection.

# Capítulo I

## Planteamiento del problema

### Tema

Análisis comparativo de las nuevas tecnologías de software libre y software propietario para la protección perimetral de la información (firewall) del COMIL 1, con el fin de proponer la mejor tecnología para la protección de la información del área de operaciones de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 “Eloy Alfaro”.

### Introducción

El presente tema ha sido propuesto en base a la realidad que actualmente las empresa de nuestro país están afrontando, el ataque de hackers ha causado grandes pérdidas a nivel mundial así como también a nivel local, se ha recolectado información de diferentes medios como la prensa de pérdidas y secuestros de información a empresas como CNT, BANCO PICHINCHA entre otras, es por esta situación que se ha buscado una institución nacional Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 “Eloy Alfaro”, para elaborar un estudio de factibilidad para la implementación de firewalls basados en software.

Cabe mencionar que los firewalls, son uno de los medios de seguridad implementados en las empresas para evitar ataques de hackers, por lo que luego de realizar el análisis de algunos modelos de software, se procederá a sugerir a la institución el que se ajusta a las necesidades presentadas.

Existe una gran variedad de análisis de software firewall tanto libre como licenciado, por lo que su uso depende de la realidad que se presenta en cada una de las empresas que los utilizan.

La Unidad Educativa de las Fuerzas Armadas Colegio Militar No 1 Eloy Alfaro, al momento utilizan un firewall arrendado marca FORTINET, considerando que no tiene suficiente presupuesto para implementar un Firewall propio.

**Antecedentes**

En un mundo que se encuentra enmarcado por la tecnología informática, que cada día evoluciona con nuevos dispositivos (hardware) y nuevas aplicaciones (software), que facilitan las actividades diarias de los usuarios y que permite a las empresas brindar mejores servicios a sus clientes, es inevitable mencionar que, así como se ha generado mayores posibilidades de negocio, también se crean brechas de seguridad en la información que las empresas guardan en sus servidores.

Con la última emergencia sanitaria presentada durante los años 2020 y 2021 (covid19), se disparó una tendencia que hasta el año 2019 avanzaba lentamente y que por la necesidad provocada por las cuarentenas que restringían la normal ejecución de los negocios , provocó que el comercio y demás actividades labores de las empresas se las realicen desde los hogares mediante el teletrabajo de manera virtual, exponiendo así en gran parte la información de varias empresas, negocios y usuarios del internet.

La tendencia fue aprovechada por los llamados hackers, quienes en la actualidad han puesto sus ojos en empresas ecuatorianas; entre ellas están: CNT, Municipio de Quito, Banco Pichincha, entre otras, mismas que han sido víctimas del robo y secuestro de

información, exponiendo de esta manera los datos confidenciales que estas instituciones guardan en sus bases de datos de los usuarios.

Se conoce que las empresas implementan medidas de seguridad que ayudan a detener en gran parte este tipo de ataques, siendo uno de los principales el contratar o comprar sistemas de seguridad perimetral, que en una primera instancia funciona como barrera para el ingreso a la información de una empresa, en la investigación realizada por (Perdigón Llanes, 2022) donde realiza una evaluación cuantitativa de los rendimientos y funcionalidades de seguridad de los principales cortafuegos basados en software libre, utiliza métricas como ancho de banda, el jitter y la tasa de pérdida de paquetes mediante herramientas IPerf3, así como herramientas htop que para comprobar el consumo de CPU y memoria RAM de las soluciones con lo que identificó que Endian, Zentyal, PfSense, OPNsense, VyOS, IPFire y ClearOs presentan funcionalidades que contribuyen a elevar la seguridad en la red de datos, esto con respecto a soluciones basadas en software libre.

Por otro lado, en el mercado se conoce que también existen soluciones de software propietario como es el caso de la investigación realizada por (Bohórquez & Páez, 2017) en el que menciona los softwares de protección perimetral que actualmente existen en el mercado como son Fortinet, Barracuda Network, Check Point, Palo Alto, que tienen generalidades de protección de detección de amenazas, identificación de usuarios, bloqueo de amenazas en tiempo real, entre otros.

**Planteamiento del Problema**

La nueva era digital trae consigo el desarrollo de los negocios a través del internet, las empresas hoy en día utilizan las herramientas que están disponibles en la nube para generar un impacto positivo en las actividades comerciales, agilizan la comunicación interna entre los

empleados, se realizan trabajos colaborativos y por otra parte es un medio a través del cual mediante aplicaciones orientadas a la web se utilizan para realizar consultas directas a las bases de datos ubicadas en los servidores locales de cada empresa.

Por esta razón los expertos informáticos vieron la necesidad de buscar herramientas basadas en hardware y software que funcione como protección, de lo cual la presente investigación se centra en el software de seguridad perimetral que funciona en un nivel lógico de la red, encontrando en el mercado actual una gran variedad de opciones basadas en software libre y otras con software propietario.

Cabe mencionar que la presente investigación se centra en la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 “Eloy Alfaro”, a fin de definir la tecnología de seguridad con la que se encuentran trabajando y analizar las existentes en el mercado. Para esto se tomará en cuenta 2 herramientas de firewall basado en software libre como (ZoneAlarm y IPfire) y 2 de firewall basado en software propietario como (SonicWall y Fortinet), para determinar la más adecuada y que pueda ser implementada en la unidad de investigación mencionada.

**Justificación e importancia**

En la presente investigación se enfocará a estudiar y analizar los tipos de software libres o propietarios, que sean más favorables en el mercado actual para así dar una comparación reciente y de manera actualizada ya que este ayudara a la para lograr escoger correctamente que tipo de software nos conviene, y para que el firewall trabaje de mejor manera. Este trabajo dará a conocer las nuevas tecnologías que se encuentran en el mercado y lograr dar una propuesta más segura y económica para el área de operaciones del COMIL 1.

En la actualidad a existido una gran variedad de ataques a la seguridad informática a varias empresas del ecuador ya que estas empresas no actualizan o no cambian el sistema de seguridad. Con la presente investigación daremos a conocer al área de operaciones del COMIL 1 el sistema de seguridad que tiene y como se lo puede mejorar, utilizando un análisis comparativo del software libre y propietario que tienen actualmente en el COMIL con el que se encuentra en el mercado actual dando así una propuesta de cómo mejorar el sistema de seguridad en el área de operaciones.

## Objetivos

### *Objetivo General*

- Análisis comparativo de las nuevas tecnologías de software libre y software propietario para la protección perimetral de la información (firewall) del COMIL 1, con el fin de proponer la mejor tecnología para la protección de la información del área de operaciones de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No. 1 “Eloy Alfaro

### *Objetivos Específicos*

- Recabar información sobre los sistemas de protección perimetral existentes, tanto libres como propietarios.
- Definir la mejor herramienta de protección perimetral basada en software.
- Realizar un manual de usuario y un manual técnico para el mejor uso del Firewall seleccionado para el área de operaciones del COMIL 1.

## Alcance

La presente investigación se encuentra orientada a realizar el análisis comparativo de las herramientas de firewall basado en software libre y en software propietario, para esto se tomará en cuenta 2 de cada una de las herramientas que se encuentra en el mercado, a fin de exponer a la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 “Eloy Alfaro” que sistema les conviene conservar y modificar para que así no exista en un futuro fallos en el sistema en el área de operaciones que la tienen en Quito.

# Capítulo II

# Marco Teórico

## Software

Software según la RAE (Real Academia Española), se lo conoce como un conjunto de programas que permite generar diferentes tipos de acciones informáticas de una computadora con sus distinguidas reglas, como seria los editores de imágenes, el generador de audio y video, los videojuegos entre otras acciones más, en otras todo lo que no podemos hacer físicamente sino digitalmente. (Pérez & Gardey, 2021)

## Sistemas Operativos Libre

Sistema operativo libre, es un software que respeta la libertad de su redistribución, casi siempre el usuario que lo adquiere puede tener acceso al código de fuente de todo el sistema operativo, si por algún motivo no puede acceder al código de fuente no sería posible modificarlo. (Quispe, 2020). Algunos de los sistemas operativos libres más conocidos serian.

- GNU/LINUX
- ANDROID
- FIREFOX OS

## Sistemas Operativos Licenciados

El sistema operativo licenciado, es un programa informático que tiene ciertas limitaciones al momento de ser usado, como modificado o su forma de ser distribuido, ya que da a entender que se contiene con un código cerrado, así también necesita cada cierto tiempo

actualizaciones, brinda con un soporte técnico o brinda con algún manual. (Quispe, 2020). Algunos de los sistemas operativos licenciados más conocidos serian.

- MICROSOFT
- MAC OS
- APPLE

**Software Propietario**

Este tipo de software también se lo conoce como software privado, ya que este tiene propietarios determinados lo que le hace que un ente privado busque la rentabilidad directa en él. Este tipo de software se nos puede presentar en diferentes escenarios como en el que una empresa se desarrolle un software del que no se pueda acceder al código de fuente pero que al usarle sea gratuito, pero no libre. (Llamas, 2021). Existen diferentes tipos de licencias que necesitaremos para que estos tipos de software funcionen correctamente.

- **Licencia de software comercial:** Es un software que se paga por su uso.
- **Licencia de software de OEM:** No está a la venta ya que este forma parte de un nuevo sistema operativo.
- **Licencia de software de Retail:** Es un software pagado y este programa es solo del creador ya que este ve si lo vende o lo regala.
- **Licencia de software de volumen:** Busca empresas grandes y les vende el software, pero en el contrato que solo es para cierta cantidad de equipos en los que se puede implementar el mismo código

**Software Libre**

El software libre es el código fuente en el cual él puede estudiar, modificar y utilizar con cualquier fin, incluso copiar y distribuir el programa con sus respectivos cambios sin ningún tipo

de pago, y este no es necesario que sea gratuito. Cuando el usuario descarga el software sin pagar, pero él no puede modificar la fuente entonces ya no cuenta como software gratuito, esto se conoce como Freeware porque este es un software que él no tiene que pagar, mientras que el software libre.

- **Licencia GPL:** Este tipo de licencia conserva los derechos de autor, pero permite la libre distribución, realización de modificaciones y uso. Sin embargo, cuando este tipo de software es modificado, se debe obligatoriamente conservar la misma licencia del primer autor. Esto se conoce como copyleft y debe estar disponible para realizar copias ilimitadas para cualquier usuario. Lo único que se pagaría serían los gastos de copiado y distribución.
- **Licencia AGPL:** Este tipo de licencia modifica los derechos del autor y obliga a que, al momento de distribuir el software a través de los ordenadores de red, entonces, al momento de crear un nuevo software basándose en el anterior es por ley que este nuevo software debe estar disponible para su libre distribución.
- **Licencia BSD:** Esta es una licencia permisiva ya que no impone condiciones al usuario, al momento de que él cree un nuevo software o aplicación puede venderlo y no tiene la obligación de colocar un código de fuente, mostrando que el software o el aplicativo pueda tener licencias libres como licencias propietarias.
- **Licencia Apache:** Esta licencia permite que él pueda distribuir y modificar siempre y cuando conserve el copyright y el disclaimer, ya que esta no permite que las otras versiones se distribuyan usando su misma licencia, solo podrán distribuirla colocando una carpeta principal con la hoja de licencia y la hoja de distribución.
- **Licencia Creative Commons:** Esta se basa en cuatro condiciones que sería:
    - **Atribución:** esta distribuye, exhibir y representa al autor
    - **No comercial:** esta no permite que comercialicen el software

- **No derivada:** esta no permite modificar el software
- **Compartir igual:** permite que las otras versiones de mantengan siempre y cuando se mantenga la licencia original. (BBVA API_Market, 2014)

**Figura 1**

*Software Libre y Software Propietario*


*Nota.* Ejemplos de Software libre y Software Propietario. Tomado de (Ofimatico Empresarial, 2012)

**Seguridad Informática**

La seguridad de información es una línea estratégica del equipo del usuario, ya que esta se encarga de la implementación técnica de la protección de la información, porque esta establece situaciones de fallas totales o arbitrarias de ciertos riesgos en la información del usuario. (Seguridad de la Información, 2017)

**Tipos de Seguridad Informática**

- **Seguridad de hardware:** Este tipo de seguridad revela el control del tráfico de red, ayuda a encontrar los módulos de seguridad para el mismo hardware, también proporciona ciertos niveles de protección altos y resistentes para la capa de seguridad

del sistema, protegiendo los ordenadores y los equipos informáticos de cualquier tipo de daño que pueda presentarse.

- **Seguridad de software:** Este tipo de seguridad sirve para la protección de aplicaciones o programas de los ciberdelincuentes u otros tipos de riesgos, pueden presentar programas que puedan afectar su funcionamiento sin ningún riesgo. Los problemas que pueden surgir en el software pueden ser errores de buffer, defectos de diseño específicos. Cualquier aplicación que tenga conexión a internet puede enfrentar riesgos de seguridad en algún momento. Cuando se detecta este software, se aprovecha para aplicar medidas de protección para las aplicaciones o programas.
- **Seguridad de red:** Aquí se busca aumentar la integridad y la seguridad de la transmisión de datos de la red asignada, ya que esta red debe enfrentar una serie de amenazas como los gusanos, el caballo de Troya, los hackers, los programas espías, entre otros, y como todavía no existen soluciones para todas las amenazas que pueden presentarse, ciertos niveles de seguridad pueden seguir deteniendo la amenaza informática que se encuentra en el equipo. (APD, 2019)

**Figura 2**

*Seguridad Informática*


*Nota.* Tipos de Seguridad Informática. Tomado de (Soporte en Computo, 2018)

**Componentes de Seguridad Informática**

- El primero es ver los programas de antivirus y los antispyware.
- El segundo es que el firewall, deben de bloquear los accesos que no tienen información a una red.
- El tercero son los modelos de ISP, ya que estos identifican la amenazas que tienen una alta propagación, como los ataques de día cero.
- El cuarto sería los VPN, ya que a este se le presenta un sistema de acceso remoto y seguro de los sistemas locales. ( (APD, 2019)

**Tipos de Vulnerabilidades en la Seguridad Informática**

- **Buffer overflow o desbordamiento de buffer**: Este se presenta cuando las aplicaciones que se descargan no controlan la cantidad de información que mandan al buffer, es ahí cuando sobrepasa el tamaño de la memoria continua y empieza a dañar la información de datos.
- **Condición de carrera:** Este al momento de descargar aplicaciones no tienen el acceso a recursos compartidos, ya que estos procesos logran acceder al mismo tiempo obteniendo así valores no esperados.
- **Error de formato en cadena:** Al momento de descargar aplicaciones y que no soliciten el usuario o contraseña, hay la posibilidad de que se ejecute comandos sin saberlo y es ahí cuando el atacante tiene la oportunidad de obtener datos informáticos o dañar el PC.
- **Cross Site Scripting:** Aquí los atacantes mandan códigos de hackeo a páginas oficiales que tienen problemas de vulnerabilidad, cuando el usuario entra a estas páginas pide el usuario y contraseña, pero en realidad esos datos van al sistema del atacante, robando así la información.

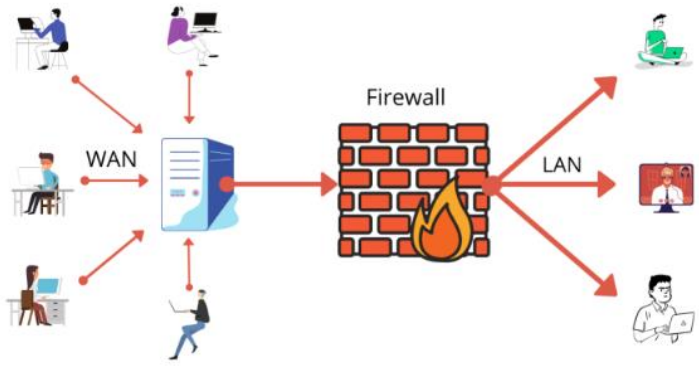
- **Inyección de SQL:** Este se presenta cuando no validan los datos de entrada en ciertos formularios que trabajan con base de datos, se puede ingresar lo que seria los códigos SQL maliciosos y es ahí cuando pueden robar información confidencial hasta pueden conseguir la tabla oficial de datos de varios usuarios. (Santander, 2020)

**Firewall**

El Firewall es un dispositivo que trata de no admitir el acceso a una red privada que se encuentra conectada a internet, los usuarios que pueden estar autorizados como no pueden estar. Cuando no están autorizados el firewall mismo establecerá una barrera entre las redes internas seguras como las redes externas no confiables, como la web. El Firewall se encuentra en el Hardware como el Software. (Cisco, 2020)

**Figura 3**

*Diagrama de un Firewall*




*Nota.* Ejemplo de un diagrama del funcionamiento de un Firewall. Tomado de (GEEKFLARE, 2020)

**Tipos de firewall**

- **Firewalls en hardware:** Este tipo de firewall es un dispositivo físico que se instala al momento de que una red de información deba de ser monitoreada por ciertos paquetes de datos que entran y salen del perímetro.
- **Firewalls en software:** Este tipo de firewall ayuda a que los equipos se mantengan protegidos en lugares externos o públicos, ya que este se ejecuta como un programa y nos ayuda a observar el tráfico de red, para así poder interferir cuando algún programa malicioso intente ingresar a nuestro equipo. (Pathak, 2022)

**Tipos de Ataques Informáticos**

- **Gusanos Informáticos:** El gusano informático es más conocido como una subclase de virus, ya que este realiza copias de sí mismos y se distribuya en diferentes partes del ordenador, hasta llegar al mayor número de dispositivos que se puedan infectar, este tipo de subvirus se distribuye por medio de correos electrónicos, mensajes, archivos a diferentes equipos y se los descargan sin saber (Panda Security, 2020), en la mayoría de ordenadores que llega a analizar se encuentran los gusanos informáticos más conocidos que seria.
    - **Gusano Morris:** Robert Morris en 1988 libero un código que estaba completamente llenos de bugs y este causo una gran variedad de problemas a los anfitriones, ya que este sobrecargo a miles de ordenadores que funcionaban con UNIX.
    - **Gusano Storm:** Este tipo de gusano surgió de un mensaje falso de un correo electrónico y este se envió por más de 10 años infectando a más de 1200 millones de usuarios por el Gusano Storm, según estudios en la actualidad existen todavía un millón de ordenadores infectados.

  - **Gusano SQL:** Este tipo de gusano es el único con su método de propagación ya que este genera direcciones IP aleatorias, al momento de ser lanzadas solo infectan a los equipos que no están equipados por antivirus. (HORNETSECURITY, 2022)

- **Malware:** El malware es más conocido como el software malicioso que infecta y daña al sistema del usuario, este tipo de software malicioso suele presentarse de diferentes formas, como seria a menudo el robo de datos del ordenador, encriptar la información o fácilmente elimina la información, también tiene la posibilidad de controlar el ordenador por completo. (SoftwareLab.org, 2021). Los daños que llegan a causar es el robo de la información, lentitud de programas, anuncios grandes sin autorización, mayor consumo de memoria RAM, envió de mensajes raros al equipo del usuario, actividades no realizadas por el usuario en el correo electrónico, aparición de publicidad engañosa para descargas de “antivirus”. (Briceño V., 2022)
- **Troyanos Informáticos:** Los Troyanos o conocidos como caballo de Troya, proviene este de un software malicioso, al momento de descargar el malware troyano se activa y este código viene disfrazado para ayudar al usuario, pero realiza lo contrario, al momento de dar acceso, este mismo ingresa a la seguridad del dispositivo y los ciberdelincuentes tiene la oportunidad de tomar el control en su totalidad, así bloqueando al usuario y dañando el equipo. (ayudaley, 2021). Cuando un equipo ya está infectado por este tipo de virus troyano presenta estas características.
  - Si el sistema se encuentra infectado con este virus troyano el autor podría ingresar y tomar el control de todo el sistema, así enviando, recibiendo, elimina archivos, mostrando datos del usuario.

  - Los troyanos pueden utilizar los exploits, estos son programas que utilizan ciertos códigos para generar aplicaciones que se encuentran vulnerables en nuestro sistema informático.
  - Puede ser rootkits, ya que estos son creados para ocultar actividades que se realizan en nuestro sistema, este también evita que no se detecten los programas maliciosos y ayuda a que ese programa malicioso infecte con más rapidez que equipo. (ayudaley, 2021)

- **Cracker:** Los Cracker, Proviene del idioma inglés que significa "romper" o "romper" un sistema de seguridad informática. Un cracker es una comunidad que irrumpe en los sistemas, descifra claves y contraseñas de programas, roba datos y comete otras actividades ilegales. (Significados, 2020). Existen diferentes tipos de cracker que se pueden llegar a presentar.
  - **Cracker de sistema:** Estos son programadores que alteran el contenido de aplicaciones, herramientas que se instalan en nuestro equipo.
  - **Cracker de Criptografía:** Estas son personas que se dedican a quebrar la criptografía.
  - **Cyberpunk:** Estos se presentan por medio de páginas webs o sistemas informatizados y destruyen el trabajo ajeno.
  - **Pirata:** Se realiza la copia ilegal de programas, rompiendo así el sistema de protección de nuestro equipo para que después lo distribuya por medio del internet o CD´s.
  - **Lammer:** Esto se realiza por personas que intercambian herramientas que no son creadas por ellas, sino que solo lo realizan el intercambio para atacar a los ordenadores.

  - **Pheakers:** Estos realizan crakeos por medio de líneas telefónicas, ya que se encargan de quebrar el sistema telefónico para dañarlos o solo para llamar de forma gratuita.
  - **Trasher:** Traducidos como basureros ya que son personas que buscan papeleras de retiros de cajeros, números de cuentas o información de ciertos usuarios para así poder realizar estafas por medio de internet.
  - **Insiders:** Estos son crackers corporativos, ya que ciertos empleados atacan al sistema desde adentro. (Anónimo, 2019)

- **Phishing Informático:** El phishing es un método de hackeo por medio de un correo electrónico ya que se hace pasar por empresas de confianza como seria los bancos, seguros, servicios básicos y estos les envían un mensaje o un documento que, al momento de descargarlo, lo único que hacen es descargar el acceso o el virus al equipo y los que están atrás de este correo lograran manipular en su totalidad el equipo, accediendo así a información confidencial. (Panda Security, 2019). La forma por la que se puede realizar un hackeo a nuestros equipos es por.
  - Correo electrónico no esperado
  - Cuenta de correo sospechoso
  - Saludos genéricos
  - Redacción extraña con faltas ortográficas
  - Envía enlaces que guían a otra página web
  - Envían archivos para descargar no esperados
  - Solicita información personal del usuario
  - Diseño extraño de la página que no cumple con el diseño oficial de la página mismo. (Universidad Nacional de Lujan, 2020)

- **Spam:** El spam se presenta sin ser solicitado, casi siempre muestra publicidad de todo tipo hasta llega a enviarte mensajes que no son solicitados, en algunos casos no son maliciosos, pero pueden serlo. (Belcic, 2021) Existen diferentes tipos de spam que se nos pueden presentar de diferente manera.
    - **Spam por correo electrónico:** Este tipo de spam es el más conocido ya que invade tu bandeja de entrada, de paso distrae al usuario de mensajes que son importantes para el usuario y este los ignora completamente.
    - **Spam SEO:** Este tipo se lo conoce como spamdexing, ya que abusa de los métodos de optimización de búsqueda SEO de los sitios webs. Existen dos tipos de spam SEO.
        - **Spam de contenido:** Este tipo llena las páginas con palabras claves que no son relacionadas con los sitios webs y reescriben con otras palabras el mismo contenido para que sus páginas aparenten que son exclusivas
        - **Spam de enlaces:** Este tipo se presenta en comentarios de blogs o publicaciones, ya que aquí el spammer publica enlaces que no tienen nada que ver con el contenido del blog y al momento de ingresar a este enlace hay la posibilidad de que traiga tráfico hacia la página, esto proviene de la mecánica de SEO llamada “backlinking”.
    - **Spam de redes sociales:** En este tipo los spammers intentan propagar su spam por medio de cuentas falsas en las redes sociales más usadas por el público en general.
    - **Spam móvil:** Este tipo se presenta por medio de SMS, ya que estos utilizan las publicaciones push para llamar la atención del usuario por medio de ofertas.

    - **Spam de mensajería:** Este tipo es más o menos similar al correo electrónico, pero este es más rápido, ya que este envía el spam por mensajes de WhatsApp, Skype, Instagram o Snapchat. (Belcic, 2021)

- **Adware:** El adware se trata de un software que le muestra al usuario, diferentes tipos de anuncios mientras ocupa la aplicación o cuando recién lo está instalando, puede ser inofensivo o puede llegar a obtener información demasiada sensible del usuario como la ubicación, contraseñas, direcciones IP y esto le llegara a afectar el usuario. (Porto & Merino, 2017) El adware tiene ciertas características que se presentan de las siguientes formas.
    - Este puede consumir todo el procesamiento del equipo.
    - También produce que al descargar y al ejecutar se presenten anuncios y haga que el equipo se vuelva lento.
    - Gasta más datos, también este es un tipo de software publicitario.
    - Este no necesita que el usuario lo manipule al momento de ser instalado.
    - Se presenta en la interfaz una gran serie de anuncios de forma seguida.
    - Este también sigue el patrón de navegación. (Briceno, 2022)
- **Ingeniería Social:** La ingeniería social en informática da a conocer que los ciberdelincuentes ocupan para el robo de información de diferentes usuarios, uno de los métodos seria por llamadas telefónicas, visitas personales haciéndose pasar por una agencia, aplicaciones, correos electrónicos y redes sociales. Estos tipos de ciberdelincuentes se hacen pasar por familia o trabajo para así poder sacar información muy detallada al usuario. (Argentina.gob.ar, 2020). La mayoría de métodos que utilizan para llegar a conocer la información de los usuarios es por.
    - Llamadas telefónicas
    - Visitas personales

  - Aplicaciones de mensajes
  - Correo electrónico
  - Redes sociales
  - Hacerse pasar por un familiar o compañero.
  - Ofrecen premio o promociones ilimitadas con tal de que muestre sus datos.
  - Hacerse pasar por una empresa como bancos, operadoras entre otros
  - Generar un formulario para que el usuario crea que va a ganar un premio y que solicite los datos personales.
  - A través de páginas falsas ofrecen actualizaciones del sistema del equipo o de aplicaciones. (Argentina.gob.ar, 2020)

- **Spyware:** El spyware más conocido como programa para espiar no-autorizado que va al sistema operativo sin advertir al usuario, al momento de instalar el programa y que el ordenador este encendido, ahí es cuando empieza a recolectar la información sensible del usuario, como contraseñas, usuarios de bancos entre otros, también crea problemas de estabilidad del sistema, llega a controlar el sistema inscribiéndole al usuario en páginas costosas sin su aprobación. (Significados, 2020). El spyware logra tener ciertas características de la cual se la puede llegar a identificar como.
  - Al momento de que ingreso e infecto a nuestro sistema puede auto instalarse sin ningún problema.
  - Al momento de que se prende el equipo y se lo utiliza de forma continua el spyware se sigue ejecutando.
  - Utiliza la memoria RAM y empieza a reducir la capacidad y estabilidad.
  - Este no puede pasar de equipo a equipo
  - Su función en general es considerada como un parasito, pero más se lo conoce como software espía. (Briceño, 2022)

**Figura 4**

*Tipos de Ataque Informáticos*


*Nota.* Porcentaje de Ataques Informáticos. Tomado de (Revista Gerencia, 2018)

# Capítulo III

# Desarrollo

## Unidad de Análisis

La presente investigación se va a realizar en la Unidad Educativa de Fuerzas Armadas Colegio Militar No. 1 Eloy Alfaro ubicada en Quito Ecuador Av. Orellana 1506 y Amazonas, en el departamento de Tecnologías Informáticas, el cual se encuentra conformado por tres Ing. En Sistemas, la infraestructura con la que trabajan se encuentra conformada por 500 equipos que son utilizados por el personal de la institución, 4 servidores (datos, sistemas, redes e internet, antivirus) con una infraestructura de red basada en el estándar de categoría 6.

**Figura 5**

*Departamento de Tecnologías Informáticas del COMIL 1*

*Nota.* Área de las Tic´s del COMIL 1

## Tipo de Investigación

Para recabar la información requerida sobre el presente proyecto, se optó por utilizar uno de los tipos de investigación aplicada que es la investigación tecnológica, “misma que se utiliza en el sector productivo con el fin de impulsar un impacto positivo en la vida cotidiana“

https://www.significados.com/tipos-de-investigacion/, esto permitirá conocer y analizar las mejores herramientas de firewall basadas en software existentes en el mercado actual.

**Método de Investigación**

Al aplicar el método deductivo se trata de realizar una investigación a fondo de cómo se encuentra conformado actualmente el área de tecnologías en la Unidad Educativa, respecto a seguridad y su infraestructura física como lógica.

Por otro lado, al aplicar el método inductivo se realiza un análisis del sistema de protección de información que se maneja actualmente en el área Tic´s de la UEFFA COLEGIO MILITAR No.1 ELOY ALFARO, a fin de utilizar dicha, información y complementarla con la presente investigación para determinar si existe alguna herramienta en el mercado que pueda ser implementado en la Unidad Educativa mencionada.

**Técnicas a Aplicar**

Para poder realizar correctamente la investigación, se procedió a aplicar la recolección de información como seria entrevistas y la observación al personal del área de las Tic´s.

**Procedimiento de la Investigación**

Luego de realizar una entrevista al analista de tecnologías de la información 2 y jefe del área de Tic´s, se pudo determinar que : tienen la necesidad de contar con dispositivos de seguridad integral para toda la infraestructura de la red institucional, no cuentan con personal especializado en seguridad, están interesados en implementar medidas de seguridad basadas prioritariamente en software libre, no se han presentado problemas de seguridad en la información hasta el momento, el único medio de seguridad que utilizan se encuentra basado en Iptables.

Se acudió al lugar de investigación donde se observó, que efectivamente cuentan con el área de servidores, misma que no ha sido estructurada en su totalidad como debe de estar equipada una área de sistemas, esto se debe a la falta de asignación de recursos

presupuestarios pese a que anualmente se realiza el requerimiento no se ha podido conseguir que este recurso se atendido, no obstante se observa que tiene equipos servidores de potentes características mediante los cuales se controla el acceso a la información y se brindan todos los servicios que se requieren para el funcionamiento del establecimiento educativo.

**Figura 6**

*Área de los Servidores del COMIL 1*

*Nota.* Servidores que se encuentran dentro del área de las Tic´s del COMIL 1

**Características de los servidores del COMIL 1**

**Tabla 1**

*Características del Servidor del COMIL 1*

| CARACTERÍSTICAS | SERVIDOR |
|---|---|
| Marca y modelo | HPE / DL380 Gen10 Performance |
| Almacenamiento óptico | Tipo = Ninguno Tipo de unidad = Sin unidad óptica |

| CARACTERÍSTICAS | SERVIDOR |
|---|---|
| Conexión de redes por protocolos de interconexión de datos | Ethernet / Fast Ethernet / Gigabit Ethernet |
| Controlador de almacenamiento de Nivel RAID | RAID 0, RAID 1; RAID 5, RAID 6, RAID 10, RAID 50; RAID 60, RAID 1 ADM, RAID 10 ADM |
| Controlador de almacenamiento 2 | Serial ATA |
| Dimensiones y peso | Altura = 8.74 cm; Anchura = 44.55 cm Peso = 14.76 kg; Profundidad = 73.07 cm |
| Disco duro | Sin disco duro |
| Estándares medioambientales | Certificado por Energy Star |
| Memoria caché | Procesador = 13.75MB Tamaño instalado = 13.75MB |
| Memoria de video | Tamaño instalado = 16MB |

| CARACTERÍSTICAS | SERVIDOR |
|---|---|
| Memoria RAM | Características = Registrado, Doble fila.<br>Las ranuras 13 - 24 sólo están disponibles en la configuración de dos procesadores, HPE SmartMemory<br>Tiene 23 ranuras vacías<br>Tamaño de instalado 32GB<br>Tamaño máximo admitido 1.5TB<br>Velocidad de memoria 2400MHz |
| Placa Principal | Socket del procesador = FCLGA3647<br>Tipo de conjunto de chips= Intel C621 |
| Procesador | Fabricante = Intel<br>Número de núcleos = 10 núcleos<br>Número de procesador = 4114<br>Tipo = Xeon Silver; Velocidad reloj = 2.2 GHz |
| Servicio y mantenimiento | Garantía in situ = In situ; Tipo = 3 años de garantía |

*Nota.* Servidores por Vigencia Tecnológica para la Unidad Educativa de Fuerzas Armadas del Colegio Militar No.1 “Eloy Alfaro “.

## Factibilidad Técnica y Económica

Una vez determinada la necesidad que presenta la Unidad Educativa de Fuerzas Armadas Colegio Militar No. 1 Eloy Alfaro, se procede a realizar la investigación de 2 herramientas de firewall libre y 2 herramientas de firewall propietario a fin de proponer una solución para el problema planteado.

## Factibilidad Técnica

En el mercado a existen actualmente existe una gran variedad de firewall licenciados y gratuitos, entre los cuales para conocimiento se menciona los siguientes:

### Firewalls Basados en Software Propietario.

- SONICWALL
- FORTINET

**Tabla 2**

*Ficha Técnica de Característica de Firewall Propietario*

| CARACTERÍSTICAS | FORTINET | SONICWALL |
|---|---|---|
| Aceleración de contenido de seguridad | 1 | 2 |
| Firewall | 1 | 1 |
| VPN | 1 | 1 |

| CARACTERÍSTICAS | FORTINET | SONICWALL |
|---|---|---|
| IPS | 1 | 1 |
| Antivirus | 1 | 1 |
| Antispam | 1 | 1 |
| Ajuste de contenido | 1 | 1 |
| Control de aplicaciones | 1 | 1 |
| Inspección de contenido SSL | 1 | 1 |
| Optimización de WAN | 1 | 0 |
| Control inalámbrico | 1 | 1 |
| Evaluación de vulnerabilidad | 1 | 0 |

**Calificación: 1=Desarrollo Interno; 2=Abastecidos por Terceros; 3=No Disponible**

*Nota.* Para el presente análisis se tomará en cuenta las características más representativas al momento de una implementación, a las cuales se ha dado un puntaje del 1 al 5 a fin de determinar el mejor puntaje para la selección del firewall, que se ajuste a las necesidades de la Unidad Educativa.

**Tabla 3**

*Evaluación de Firewall Propietario*

| ORD | CARACTERÍSTICAS | PONDERACIÓN | | MODELOS | | | |
|---|---|---|---|---|---|---|---|
| | | | | FORTINET | | SONICWALL | |
| | | Puntaje | % | Calif | % | Calif | % |
| 1 | Deep Packet Inspección SSL | 5 | 33 | 93,94 | 31 | 100,00 | 33 |
| 2 | Cloud Sandbox MultiEngine | 4 | 27 | 85,19 | 23 | 100,00 | 27 |
| 3 | Deep Memory Inspection | 3 | 20 | 35,00 | 7 | 100,00 | 20 |
| 4 | Cloud Delivered Email Security | 2 | 13 | 100,00 | 20 | 100,00 | 13 |
| 5 | Client Security Antivirus | 1 | 7 | 100,00 | 13 | 100,00 | 7 |
| | Total | 15 | 100% | | | | |

*Nota.* De la investigación realizada se determina que Fortinet tiene cantidades menores de paquetes SSL mientras que en Sonic Wall tiene más completo los paquetes SSL.

Fortinet tiene ciertas fallas al momento de entrar al Cloud sandbox multiengine mientras que en Sonic Wall tiene menos fallas en lo que sería el cloud sandbox multiengine; Fortinet al

momento de que realice una inspección de memoria va a fallar en su totalidad mientras que en Sonic Wall no va a tener ningún tipo de fallas al momento de realizar la inspección de memoria; Fortinet se le puede presentar ciertos inconvenientes cuando se trata de la seguridad del correo en la nube ya que esos inconvenientes son fáciles de modificar mientras que en Sonic Wall tiene una mayor seguridad al momento de subir archivos entre otros en la nube desde nuestro correo electrónico; Fortinet más probabilidades de que se le pueda ingresar a nuestro firewall un virus mientras que en Sonic Wall tiene más capacidades de sobreproteger el firewall.

**Firewalls Basados en Software Libre.**

- ZONEALARM
- IPFIRE

**Tabla 4**

*Ficha Técnica de Características de Firewall Libre*

| CARACTERÍSTICAS | ZONEALARM | IPFIRE |
|---|---|---|
| Aceleración de contenido de seguridad | 1 | 1 |
| Firewall | 1 | 1 |
| VPN | 0 | 1 |
| IPS | 0 | 1 |

| CARACTERÍSTICAS | ZONEALARM | IPFIRE |
|---|---|---|
| Antivirus | 1 | 1 |
| Antispam | 1 | 1 |
| Ajuste de contenido | 1 | 1 |
| Control de aplicaciones | 1 | 1 |
| Inspección de contenido SSL | 0 | 0 |
| Optimización de WAN | 0 | 1 |
| Control inalámbrico | 1 | 1 |
| Evaluación de vulnerabilidad | 1 | 1 |

**Calificación: 1=Desarrollo Interno; 2=Abastecidos por Terceros; 3=No Disponible**

*Nota:* Vista que existe gran variedad de firewalls en el mercado y tomando en cuenta la necesidad de la institución, únicamente se procederá a tomar en cuenta dos de cada uno a fin de verificar la factibilidad técnica, operativa y económica de los mismos.

**Tabla 5**

*Evaluación de Firewall Libre*

| ORD | CARACTERÍSTICAS | PONDERACIÓN | | MODELOS | | | |
|---|---|---|---|---|---|---|---|
| | | | | ZONEALARM | | IPFIRE | |
| | | Puntaje | % | Calif | % | Calif | % |
| 1 | Deep Packet Inspección SSL | 5 | 33 | 81,81 | 27 | 100,00 | 33 |
| 2 | Cloud Sandbox MultiEngine | 4 | 27 | 100 | 13 | 100,00 | 27 |
| 3 | Deep Memory Inspection | 3 | 20 | 85 | 17 | 100,00 | 20 |
| 4 | Cloud Delivered Email Security | 2 | 13 | 100,00 | 20 | 100,00 | 13 |
| 5 | Client Security Antivirus | 1 | 7 | 100,00 | 13 | 100,00 | 7 |
| | Total | 15 | 100% | | | | |

*Nota*: De lo investigado se puede definir que : ZoneAlarm tiene menos cantidades de paquetes SSL, mientras que en IPFire tiene los paquetes más completos de SSL.; ZoneAlarm tiene ciertas fallas al momento de entrar al Cloud sandbox multiengine, mientras que en IPFire no tiene fallas al momento de utilizar cloud sandbox multiengine; ZoneAlarm al momento de que

realice una inspección de memoria va a tener ciertas dificultades al momento de inspeccionar la memoria, mientras que en IPFire no va a tener ningún tipo de fallas al momento de que la inspección de memoria se vaya a realizar; ZoneAlarm se le puede presentar ciertos inconvenientes al momento de cargar cierta cantidad de información en la nube del correo correspondiente, mientras que el IPFire al momento de cargar documentos en la nube no va a tener ningún inconveniente, ni demoras.; ZoneAlarm tanto como el IPFire tiene un buen servicio de antivirus para los clientes ya que al momento de ejecutar cualquier programa lo analiza y le muestra el análisis al usuario

**Factibilidad Económica**

Para definir los costos de la implementación de un firewall basado en Software, para la Unidad Educativa de Fuerzas Armadas Colegio Militar No. 1 Eloy Alfaro, en los siguientes cuadros se establecerá la inversión que se debe realizar a fin de que la institución pueda asignar el presupuesto correspondiente.

**Tabla 6**

*Costos de Inversión en Hardware*

| HARDWARE | CANTIDAD | DETALLE | VALOR UNITARIO | VALOR TOTAL CON IVA |
|---|---|---|---|---|
| Servidor | 1 | Ubtek Xeib E2324g de 16gb y 4tb en disco | 2030,26 | 2273.89 |

**Tabla 7**

*Costo de Inversión en Software Firewall Propietario*

| CARACTERÍSTICAS | DETALLE | |
|---|---|---|
| | **FORTINET** | **SONICWALL** |
| Costos para pequeñas empresas empiezan desde | $430 a $1400 | $50 hasta $80,000 |
| Costo analizado por la NSS Labs (Numero de Seguridad Social) | $2000 | $5400 |
| Costo de licencia por 1 año | $1,600.00 | $249.00 |
| Costo de licencia por 3 años | $4,200.00 | $485.00 |
| Costo por soporte | $180.00 | $177,28 |
| Transferencia de conocimientos | $500 | $860 |
| *INVERSION APROXIMADA A 1 AÑO* | $5680 | $6766,28 |

**Tabla 8**

*Costos de Inversión en Software Firewall Libre*

| CUADRO COSTO DEL FIREWALL | ZONEALARM | IPFIRE |
|---|---|---|
| Costo por soporte | $44.95/año | N/A |
| Transferencia de conocimiento | 1500 | |

**Consolidado de Gastos para Definir el Presupuesto**

**Tabla 9**

*Propuesta con Software Firewall Propietario*

| GASTOS | VALOR |
|---|---|
| Hardware | $2273,89 |
| Software | $6361,6 |
| *TOTAL* | $8635,49 |

**Tabla 10**

*Propuesta con Software Firewall Libre*

| GASTOS | VALOR |
|---|---|
| Hardware | $2273,89 |
| Software | $0,00 |
| *TOTAL* | $2273,89 |

**Factibilidad Operativa**

Una vez realizado el análisis técnico y económico se procederá a seleccionar la mejor propuesta, a fin de elaborar el manual técnico y de usuario mismo que será entregado al Jefe de Área investigada (Tic´s), a fin de que puedan tomar el presente análisis para implementar una solución de Firewall basado en Software libre.

# Capitulo IV

## Conclusiones, Recomendaciones

### Conclusiones

- Se recabó la información necesaria de los sistemas de protección perimetral que existen actualmente en el mercado con lo que se definió los tipos de firewall que se ajustan a las necesidades de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 “Eloy Alfaro”.
- Luego de analizar las herramientas de protección perimetral basadas en software libre como software propietario se llegó a la conclusión que la herramienta de firewall más conveniente para el área de las Tic´s de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 “Eloy Alfaro”, es el Firewall IPFire basado en software libre, debido a que cumple todas las características técnicas de seguridad de la institución, así como también los bajos costos encontrados en el mercado actual.
- Después de haber analizado el firewall más conveniente para el área de las Tic´s de la Unidad Educativa de las Fuerzas Armadas Colegio Militar No.1 “Eloy Alfaro”, el firewall que salió seleccionado es el IPFire, ya que cumple con las necesidades del área de las Tic´s, por lo que se procede a realizar un manual técnico que facilite la implementación del Fireware sugerido, de la misma manera se procede a entregar un manual de usuario que sirva como guía para las operaciones de seguridad que la institución requiera.

**Recomendaciones**

- Después de la investigación realizada se recomienda utilizar el software IPFire, basado en software libre, ya que cumple con las expectativas plateadas por la institucion.

- Se recomienda realizar la gestión para solicitar el presupuesto necesario en base al estudio presentado, que permita ejecutar la implementación del software IPFire como protección perimetral para la institución.

- Una vez implementada la solución de protección perimetral se recomienda al personal de las Tic`s verificar e instalar las actualizaciones que se publican semestralmente a fin de que se utilice los nuevos parámetros de seguridad que la herramienta genera.

- Es importante que se planifique la capacitación previa a la implementación del software, a fin de que el personal pueda utilizar todos los beneficios de seguridad que IPFIRE, presenta.

## Glosario

**AAA:** Protocolo de Autenticación, Autorización, Contabilidad; (Authentication, Authorization, Accounting).

**Adware:** Programa publicitario malicioso, sus palabras en inglés ad(adversiting) y ware (programa informático).

**Blackling:** Copia de respaldo de la información almacenada en un dispositivo electrónico.

**Blogs:** Pagina Web en donde se publica artículos.

**Buffer Overflow:** Es un error de programación cuando copian una gran cantidad de datos y que no alcanzan a almacenarlos.

**Ciberpunk:** Se referencian a ciber (Avances científicos) y punk (rebelión y transgresion).

**Cracker:** Cuando una persona ingresa a nuestro equipo y red sin ningún tipo de autorización.

**Criptografía:** Técnica comunicacional en conceptos matemáticos o algoritmos para poder transformarles en mensajes.

**Fortinet:** Dispositivo para la seguridad de las redes que prevén amenazas emergentes y sofisticadas.

**Freeradius:** Acrónimo de Servicio de Usuario de Acceso Telefónico de Autenticación Remota (Remote Authentication Dial-In User Service).

**Freeware:** Software libre o de distribución libre.

**Hardware:** Componentes físicos que contiene el equipo.

**Insiders:** Es un ataque que ser realiza dentro de la empresa por medio de un empleado

**IP:** Dirección de Protocolo Interno**.**

**IPFire:** Es un firewall de código abierto para plataforma GNU/LINUX.

**IPS:** Sistema de Prevención de Intrusos o Intrusion Prevention System.

**IpTables:** Es un módulo de Linux que su función es filtrar paquetes de la red.

**ISP:** Internet Service Provider o Proveedor de servicios de internet.

**Lammer:** Persona que se dice pirata informática que utiliza programas de fácil uso para los hackers.

**Licencia AGLP:** Affero General Public Licence.

**Licencia Apache:** Apache License o Apache Software License.

**Licencia BSD:** Berkeley Software Distribution.

**Licencia Creative Commons:** Bienes Comunes Creativos.

**Licencia GLP:** Licencia Publica General GNU.

**Malware:** Software Malicioso.

**Publicaciones PUSH:** Tecnología que permite que se envié mensajes a los teléfonos celulares automáticamente.

**RAE:** Real Academia Española.

**RAM:** Random Access Memory.

**Rootkits:** Software malicioso que permite el acceso de un equipo a otro software.

**SEO:** Search Engine Optimization u Optimización para motores de búsqueda.

**Software:** Conjunto de programas o aplicaciones que hacen lo posible que funcione el equipo.

**OEM:** Original Equipament Manufacturer o Fabricante de Equipo Original.

**SonicWall:** Proveedor de sistemas de seguridad, que permite controlar, gestionar y proteger tu red con facilidad.

**SQL:** Structured Query Language o Lenguaje de Consulta Estructurado

**SSL:** Secure Sockets Layer o Capa de Sockets Seguros

**Tic´s:** Tecnología de la Información y la Comunicación

**Ubiquiti:** Software de fácil instalación hacia nuestra nube para realizar mantenimiento de la infraestructura de red UniFi WIFI.

**UNIX:** Sistema operativo que controla los recursos del equipo y asigna a cada usuario.

**VPN:** Virtual Private Network o Red Privada Virtual.

**WAN:** Wide Área Network o Red de Área Amplia.

**ZoneAlarm:** Cortafuego producido por Check Point, incluye un sistema de detección de intrusos y de virus, troyanos o gusanos.

## Bibliografía

Anónimo. (2019). *EcuRed.* Obtenido de https://www.ecured.cu/Cracker

APD, R. (20 de 04 de 2019). *APD*. Obtenido de https://www.apd.es/tipos-de-seguridad-informatica/

Arevalo, A. P. (01 de 2010). *UNIVERSIDAD MICHOACANA DE SAN NICOLAS DE HIDALGO.* Obtenido de https://www.fcca.umich.mx/descargas/apuntes/academia%20de%20informatica/INTRODUCCION%20-%20ADM.%20CENTROS%20DE%20COMPUTO%20PEREZ%20AREVALO.pdf

*Argentina.gob.ar.* (30 de 12 de 2020). Obtenido de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte

*Atico34.* (2022). Obtenido de https://protecciondatos-lopd.com/empresas/sistema-prevencion-intrusiones-ips/#:~:text=Los%20sistemas%20de%20protecci%C3%B3n%20contra,firmas)%20de%20intentos%20de%20intrusi%C3%B3n.

*ayudaley.* (09 de 04 de 2021). Obtenido de https://ayudaleyprotecciondatos.es/2021/04/09/troyanos/#:~:text=Un%20troyano%20o%20caballo%20de%20Troya%20es%20una%20variedad%20de,el%20control%20de%20tu%20computadora.

*BBVA API_Market*. (29 de 10 de 2014). Obtenido de https://www.bbvaapimarket.com/es/mundo-api/las-5-licencias-de-software-libre-mas-importantes-que-todo-desarrollador-debe-conocer/

Belcic, I. (20 de 09 de 2021). *Academy.* Obtenido de https://www.avast.com/es-es/c-spam#topic-1

Bilski. (15 de 11 de 2020). *Caracteristicass.de.* Obtenido de caracteristicass.de/antivirus/

Bohorquez, M., & Paez , L. (2017). DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL EN LAS NSTALACIONES DEL CONSORCIO EXPANSION PTAR SALITRE, SEDE BOGOTÁ D.C. *DISEÑO DE UN SISTEMA DE SEGURIDAD PERIMETRAL EN LAS NSTALACIONES DEL CONSORCIO EXPANSION PTAR SALITRE, SEDE BOGOTÁ D.C*. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/15322/1/DISE%C3%91O%20DE%20UN%20SSP.pdf

Briceno, G. (14 de 05 de 2022). *Euston96*. Obtenido de euston96.com/adware/

Briceño V., G. (14 de 05 de 2022). *EUSTON.* Obtenido de https://www.euston96.com/malware/

Briceño, G. (14 de 05 de 2022). *Euston96*. Obtenido de https://www.euston96.com/spyware/

*Ciberseguridad.* (2021). Obtenido de https://uciberseguridad.es/sistema-de-prevencion-de-intrusos-ips/#:~:text=El%20sistema%20de%20prevenci%C3%B3n%20de,e%20intentar%20detener%20esa%20actividad.

*Cisco* . (2020). Obtenido de https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

*concepto*. (5 de 08 de 2021). Obtenido de https://concepto.de/software-libre/

Content, R. (30 de 04 de 2019). *rockcontent.* Obtenido de https://rockcontent.com/es/blog/tipos-de-software/

*EJEMPLOS*. (2020). Obtenido de https://ejemplos.net/ejemplos-de-software-propietario/

Felipe. (01 de 07 de 2021). *hostingplus.* Obtenido de https://www.hostingplus.pe/blog/caracteristicas-de-hardware/

Felipe. (14 de 01 de 2022). *hostingplus*. Obtenido de https://www.hostingplus.pe/blog/cuales-son-las-caracteristicas-del-software-propietario-y-sus-tipos/

*Fundacion MAPFRE.* (2019). Obtenido de https://www.fundacionmapfre.org/publicaciones/diccionario-mapfre-seguros/software-de-seguridad-fraudulento/#:~:text=En%20el%20%C3%A1mbito%20de%20los,que%20el%20usuario%20busca%20protegerse.

Gabriela, B. (14 de 05 de 2022). *EUSTON*. Obtenido de https://www.euston96.com/firewall/

GEEKFLARE. (27 de julio de 2020). *GEEKFLARE.* Obtenido de GEEKFLARE: https://geekflare.com/es/firewall-introduction/

*Grupo Atico34*. (10 de 09 de 2020). Obtenido de https://protecciondatos-lopd.com/empresas/software-libre/#Concepto_de_software_libre

*Hornetsecurity.* (2022). Obtenido de https://www.profesionalreview.com/hardware/#%C2%BFQue_es_el_hardware_cual_es_su_funcion_y_su_definicion

*HORNETSECURITY.* (2022). Obtenido de https://www.hornetsecurity.com/es/knowledge-base/gusanos-informaticos/?_adin=02021864894

Iliana, G. (17 de 02 de 2022). *Cinconoticias*. Obtenido de https://www.cinconoticias.com/ejemplos-de-software-libre/

Jiménez, J. (31 de 08 de 2021). *Redes Zone.* Obtenido de https://www.redeszone.net/tutoriales/seguridad/sistema-deteccion-intrusos/

José, L. R. (03 de 07 de 2019). *247tecno.* Obtenido de https://247tecno.com/software-tipos-ejemplos-caracteristicas/

Llamas, J. (07 de 01 de 2021). *conomipedia*. Obtenido de https://economipedia.com/definiciones/software-propietario.html

*Locura Informatica Digital*. (2021). Obtenido de https://www.locurainformaticadigital.com/2018/02/12/spyware-que-es-definicion-tipos/

Macías, M. Á. (10 de 10 de 2021). *Orange*. Obtenido de https://blog.orange.es/consejos-y-trucos/que-son-las-licencias-de-software-y-que-tipos-hay/#:~:text=Con%20las%20licencias%20de%20software,y%20cualquier%20otra%20consideraci%C3%B3n%20necesaria.

Ofimatico Empresarial. (14 de marzo de 2012). *Ofimatica Empresarial*. Obtenido de Ofimatica Empresarial: https://sis19upt.blogspot.com/2012/03/software-libre-y-software-propietario.html

*Panda Security.* (2019). Obtenido de https://www.pandasecurity.com/es/security-info/phishing/

*Panda Security.* (2020). Obtenido de https://www.pandasecurity.com/es/security-info/worm/

Pathak, A. (07 de 04 de 2022). *GEEKFLARE*. Obtenido de https://geekflare.com/es/hardware-vs-software-cloud-firewall/

Perdigón Llanes, R. (31 de 1 de 2022). Evaluacion del rendimiento de cortafuegos basados en software libre. *Revista digital de ciencia, ingenieria y tecnologia*, 31. Obtenido de https://novasinergia.unach.edu.ec/index.php/novasinergia/article/view/307

Pérez, J., & Gardey, A. (2021). *Definicion de.* Obtenido de https://definicion.de/software/

Porto, J. P., & Merino, M. (2017). *Definición.de.* Obtenido de https://definicion.de/adware/

*Profesional Review.* (2019). Obtenido de https://www.profesionalreview.com/hardware/#%C2%BFQue_es_el_hardware_cual_es_su_funcion_y_su_definicion

Quispe, Y. A. (07 de 08 de 2020). *Slideshare*. Obtenido de https://es.slideshare.net/yonathanalexisquispe/sistemas-operativos-libres-y-licenciados

*RentAdvisor.* (2020). Obtenido de https://www.rentadvisor.com.co/seguridad-informatica-caracteristicas/

Revista Gerencia. (abril de 2018). *Revista Gerencia.* Obtenido de Revista Gerencia: http://www.emb.cl/gerencia/articulo.mvc?xid=4657&ni=cibercrimen-chile-en-el-5%B0-lugar-del-ranking-de-ataques-informaticos-en-latinoamerica

*Santander.* (2020). Obtenido de https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.

*Seguridad de la Información.* (26 de 01 de 2017). Obtenido de https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Sergio, R. G. (8 de 10 de 2017). *innovacion.* Obtenido de https://revistainnovacion.com/nota/2143/proteccion_perimetral_10_puntos_clave_para_una_exitosa_implementacion/

*Significados.* (2020). Obtenido de https://www.significados.com/spyware/

*Significados.* (2020). Obtenido de https://www.significados.com/hacker/

*Significados.* (2020). Obtenido de https://www.significados.com/encriptacion/#:~:text=La%20encriptaci%C3%B3n%20es%20un%20procedimiento,que%20un%20tercero%20los%20intercepte.

*SoftwareLab.org.* (2021). Obtenido de https://softwarelab.org/es/que-es-malware/

Soporte en Computo. (08 de marzo de 2018). *Soporte en Computo.* Obtenido de Soporte en Computo: https://pedro2110.wixsite.com/tecnicoensoporte/post/tipos-de-seguridad-informatica

*UNIR.* (30 de 07 de 2020). Obtenido de https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

*Universidad Nacional de Lujan .* (2020). Obtenido de https://www.unlu.edu.ar/doc/seginfo/como_protegerse_del_phishing.pdf

Valerio, Y. (23 de 07 de 2021). *freelancermap.* Obtenido de https://www.freelancermap.com/blog/es/que-hace-hacker-etico/

*Verizon.* (2022). Obtenido de https://espanol.verizon.com/info/definitions/antivirus/#:~:text=Un%20antivirus%20es%20un%20tipo,real%20contra%20ataques%20de%20virus.

# Anexos