Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del Cuerpo de Bomberos de Latacunga

Implementation of a security management system against possible cyber threats in the network of Cuerpo de Bombers de Latacunga

Autor[1] **SANGUCHO SANDOVAL Abrahan David**
ORCID: 0000-0001-5278-9259

Resumen

En la actualidad el internet se ha vuelto un aliado de la humanidad, que conlleva de la mano en las labores diarias de cada uno de los seres humanos, ya sea por temas de educación, trabajo, etc., es por esta razón que como usuarios de esta herramienta tecnológica somos blanco perfecto de los hackers, una de las causas más comunes se da mediante el engaño de ingeniería social, donde el ciberdelincuente se hace pasar por una persona, empresa o institución para poder obtener información confidencial como contraseñas, información de tarjetas de crédito entre otras. En el Cuerpo de Bomberos de Latacunga se realizó una investigación de campo, donde a través del método empírico, mediante la técnica de encueta se obtuvo información relevante que fue analizada estadísticamente permitiendo detectar vulnerabilidades en la red interna de la institución, es así como nace la necesidad de implementar un sistema gestor de seguridad, (firewall por software), donde podemos

Revista Académica y Científica
julio - diciembre
Vol. 2, Nº 3, 2021
pp. 42 - 55
ISSN: 2737 - 6214

https://server.istvicenteleon.edu.ec/victec/index.php/revista

Recibido: 11/07/2021
Aceptado: 20/07/2021

[1] Soporte informático. Dirección Distrital 05D01Latacunga-MAG. asangucho9801.pos@utc.edu.ec

incrementar políticas de seguridad, logrando tener una navegación en internet segura con el cifrado de paquetes extremo a extremo, mediante los certificados importados del firewall Pfsense.

Palabras clave: internet; tecnológica; hackers; ingeniería social; ciberdelincuente; políticas de seguridad.

Abstract

Currently the internet has become an ally of humanity, which leads hand in hand in the daily work of each of the human beings, whether for education, work, etc., it is for this reason that as users of this technological tool we are the perfect target of hackers, one of the most common causes is through deception of social engineering, where the cybercriminal impersonates a person, company or institution in order to obtain confidential information such as passwords, card information credit among others. In the Latacunga Fire Department, a field investigation was carried out, where through the empirical method, through the survey technique, relevant information was obtained that was statistically analyzed to detect vulnerabilities in the internal network of the institution, this is how the Need to implement a security management system (software firewall), where we can increase security policies, achieve safe Internet browsing with end-to-end packet encryption, through certificates imported from the Sense firewall.

Keywords: internet; technological; hackers: social engineering; cybercriminal; security politics.

1. Introducción

Como resultado de la evolución tecnológica que dio protagonismo al desarrollo, el progreso y la innovación, mejorando así las necesidades diarias de cada uno de los seres humanos, se ha convertido a su vez en una de las mayores ciber amenazas a nivel mundial, teniendo en cuenta que las personas con la mayor probabilidad de violación son aquellos con poco conocimiento en la línea de tecnología, una de las causas más comunes está dada por el engaño de la ingeniería social.

La constante evolución de la tecnología y por ende la comunicación entre redes de computadoras va creciendo significativamente, donde todo este contexto se lo denomina ciberespacio, mismo que está relacionado con las

actividades diarias de los seres humanos dentro de este análisis nos vemos involucrados de día en día en una batalla interminable de amenazas cibernéticas, ya que en cada equipo digital se presenta anomalías en el funcionamiento adecuado de los mismos, producto de softwares maliciosos, permitiendo así la filtración de información personal, institucional o empresarial..

2. Metodología

Una de las herramientas tecnológicas más utilizadas hoy en día es el Internet, a su vez se ha convertido en un medio digital inseguro y vulnerable, lo cual conlleva la aceptación de los riesgos mediante la navegación y espionaje de personas u organizaciones que buscan robar información, datos personales, ya sea por diversión, dinero, asuntos políticos, etc.

Las acciones más efectivas de poner en práctica la seguridad de la información y por ende el de una empresa muchas veces se ve obligado a limitar webs, servicios, características de software que vienen siendo una puerta de entrada hacia lo más preciado de nuestra empresa, como es la información, datos etc., es así como reduciremos en un 90% las vulnerabilidades que día a día asechas nuestra institución, mediante la implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red.

Estos servicios o políticas establecidas se los controla mediante un servidor FIREWALL y se los identificará a la red LAN y por otra parte los servidores denominado como zona desmilitarizada (DMZ), denegando accesos no permitidos hacia la red interna del Cuerpo de Bomberos de Latacunga, las políticas establecidas son controladores de dominio, servidores de correo electrónico, servicios web institucionales, acceso a internet, interfaces de web, servidores y plataformas de servicios públicos, enlaces entre instituciones, entre otros.

Todos los paquetes que entren o salgan de la red del Cuerpo de Bomberos de Latacunga pasaran a través de nuestro sistema gestor de seguridad, examinando así cada paquete y bloqueando aquellos que no cumplen con las políticas establecidas.

Uno de los componentes de seguridad que se requieren dentro de una organización es el firewall, un elemento que permite controlar el tráfico de red tanto hacia fuera como dentro de la misma, sin embargo, debido al costo de estos equipos o a la complejidad de programación de los mismos, muchas

empresas optan por obviar este elemento importante, dejando de esta manera expuesta su información a múltiples amenazas de seguridad. (Adrián, 2016)

El uso de las Tecnologías de la Información y la Comunicación se ha incorporado de forma generalizada a la vida cotidiana. Este nuevo escenario facilita un desarrollo sin precedentes del intercambio de información y comunicaciones, pero, al mismo tiempo, conlleva nuevos riesgos y amenazas que pueden afectar a la seguridad de los sistemas de información. (Agesic, 2018)

La seguridad está en nuestras manos, nuestra actividad en la red configura nuestra identidad digital, que está compuesta por el rastro de datos que vamos dejando mientras navegamos y utilizamos servicios online.

Cuando la información que vertemos en las redes es de carácter sensible, entramos en terrenos que exigen más control. En el caso de que la ofrezcamos voluntariamente, ese control y la obligación de estar informados sobre los peligros que ello conlleva recae sobre nosotros, algo que ocurre al subir fotos personales y de niños a redes sociales públicas. Si nuestra información se nos exige, entonces debemos asegurarnos de que el proveedor del servicio es de absoluta confianza, y conocer las condiciones de prestación del mismo. (administracionvirtualdotblog, 2018)

Uno de los pasos más importantes en seguridad, es la educación.

Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados

El mundo está viviendo una auténtica evolución tecnológica, todos los sectores están siendo digitalizados, desde la agricultura o la ganadería hasta la industria, el comercio, el turismo, etc. Este aumento en el uso de tecnología también ha provocado un incremento en la cantidad de ciberataques.

2.1. Fases de un ataque informático

Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

La siguiente imagen muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado.

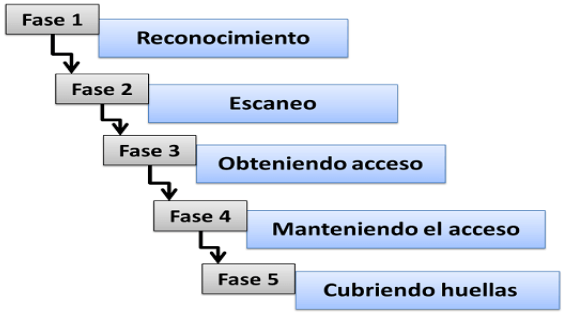

Ilustración 1: fases de un ataque informático
Fuente: E. Cárdenas 2012

2.1.1 Fase 1 Reconocimiento

El Esta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona u organización.

Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social.

2.1.2 Fase 2 Escaneo

En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

2.1.3 Fase 3 Obteniendo acceso

Lo En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración.

Algunas de estas técnicas que el atacante puede utilizar son ataques de Buffer, DoS, DDos, Password filtering.

2.1.4 Fase 4 Manteniendo acceso

Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet.

2.1.5 Fase 5 Cubriendo huellas

Intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS). (Cárdenas, 2012)

2.2. Principios de la seguridad informática

2.2.1 Confidencialidad

Requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es necesario acceder a la información mediante autorización y control. La confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

2.2.2 Integridad

Es prevenir modificaciones no autorizadas, la información se mantendrá inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar mediante autorización.

2.2.3 Disponibilidad

La capacidad de permanecer accesible en el sitio, en el momento y en la forma en que los usuarios que estén autorizados lo requieran. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible. (pmg-ssi, 2018)

2.3. Método CSF

Muchos de los riesgos se deben a la falta de conocimientos en materia de ciberseguridad, ignoramos todo lo que son capaces de hacer los ciber-delincuentes y como consecuencia, realizamos conductas que pueden convertirnos fácilmente en víctimas.

Uno de los lugares más importantes y útiles es el internet, que contiene todo tipo de información y ciencia, es de ahí donde muchos usuarios conocidos como piratas informáticos, buscan hacer negocio atacando de forma remota a los ordenadores de muchos usuarios que navegan en Internet.

Más allá de las típicas infecciones con las que nos podemos encontrar, por ejemplo, una de las más sonadas en el 2017 como es el ransomware, una vía de acceso muy utilizada por los piratas informáticos para comprometer los archivos, sistemas, etc., y por ende la infraestructura de red.

Tener nuestra institución protegida frente amenazas es importante, para ello existen numerosos tipos de hardware y software orientados a defendernos de posibles ataques, cada uno de ellos puede estar configurado en diferentes plataformas.

Con el avance de la tecnología estamos cada vez más expuestos a los ataques a los que tenemos que hacer frente sean más difíciles de predecir, mismos que es de vital importancia trabajar arduamente día tras día para mejorar las medidas de seguridad, teniendo en cuenta que la seguridad al 100% no existe, pero hay muchas formas de prevenir posibles incidentes, o reducirlos al máximo posible.

El método CSF (Cybersecurity Framework), está enfocado a las empresas de distintos tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos.

La nueva versión 1.1 del CSF fue publicada el 16 de abril de 2018. El documento ha evolucionado para ser aún más informativo, útil e inclusivo para todo tipo de organizaciones.

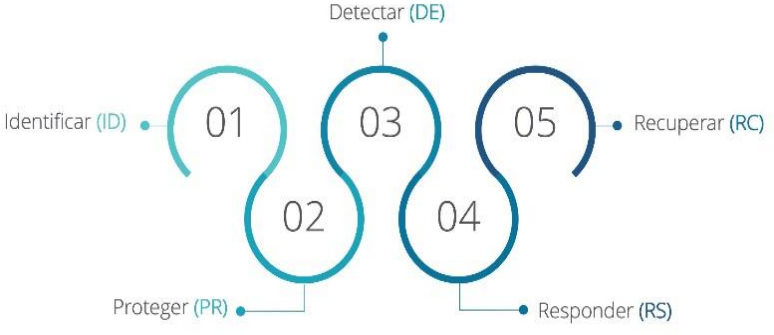

Ilustración 2: Núcleo de CSF
Fuente: Cyberframework

2.3.1 Identificar

Ayuda a desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y las capacidades.

2.3.2 Proteger

Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Esta función contempla la capacidad de limitar o contener el impacto de un potencial evento de ciberseguridad.

2.3.3 Detectar

Define las actividades necesarias para identificar la ocurrencia de un evento de ciberseguridad., permitiendo el descubrimiento oportuno de los mismos.

2.3.4 Responder

Incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente.

2.3.5 Recuperar

Identifica las actividades necesarias para mantener los planes de resiliencia y para restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Esta función es compatible con la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad. (nist.gov, s.f.)

En una encuesta reciente, casi el 68% de los líderes de IT admitieron que su negocio había sufrido al menos un ataque cibernético en 2018. Y el estudio también reveló que el 19% de las empresas encuestadas no tenía ningún plan para lidiar con un ciberataque. Estos son datos inquietantes para la mayoría de las empresas.

2.4. Estrategias

Se debería implementar restricciones a cada estación de trabajo, independientemente del cargo que ocupe el funcionario, esta medida de seguridad puede parecer demasiado simple, pero es algo que pocas empresas realmente lo hacen.

Este protocolo ha sido expuesto reiteradamente por expertos en ciberseguridad, pero muchas personas continúan ignorando esta regla, asumiendo que es algo que **"todo el mundo sabe"**. De hecho, educar a sus empleados, funcionarios, etc., es el primer gran paso hacia la ciberseguridad efectiva y eficiente y garantizar un entorno online seguro.

2.5. Adopción tecnológica

En el 2019 se ha incrementado considerablemente la adopción de nuevas tecnologías, no sola a nivel de hardware, si ni también a nivel de software, entre ellas la computación en la nube, productos digitales patentados y dispositivos conectados a IoT.

Según Cisco Network Academi, para el 2020 se tiene previsto la conexión de 50 000 millones de aparatos electrónicos, abriendo nuevos agujeros vulnerables a la seguridad personal.

2.6. Tipos de investigación

En el siguiente estudio se realizó una investigación de campo, donde a través del método empírico, mediante la técnica de encueta, y el método experimental, que trata de un proceso que se utiliza para investigar fenómenos, adquirir nuevos conocimientos o corregir e integrar conocimientos previos. Se utilizó la investigación científica y se basa en la observación sistemática, la toma de mediciones, la experimentación, la formulación de pruebas y la solución a la hipótesis.

2.7. Toma de decisiones

A través del método empírico empleado en el Cuerpo de Bomberos de Latacunga, para la obtención de resultados estadísticos, mediante el instrumento aplicado que fue la encuesta aplicada a toda la población del Cuerpo de Bombero de Latacunga, es decir a 53 funcionarios que laboran en la mencionada institución, a lo que arrojo información necesaria para poder realizar la implementación de un gestor de seguridad.

Se evidencia claramente el poco o nulo conocimiento en ciberseguridad, donde eh escogido las preguntas más relevantes para medir que tan familiarizados se encuentran sobre el tema de estudio, de acuerdo a los resultados obtenidos nos podemos dar cuenta la magnitud del problema al que la institución está sometida, y si a esto le sumamos los sistemas obsoletos, pues esto conlleva a las principales causas de las vulnerabilidades corporativas.

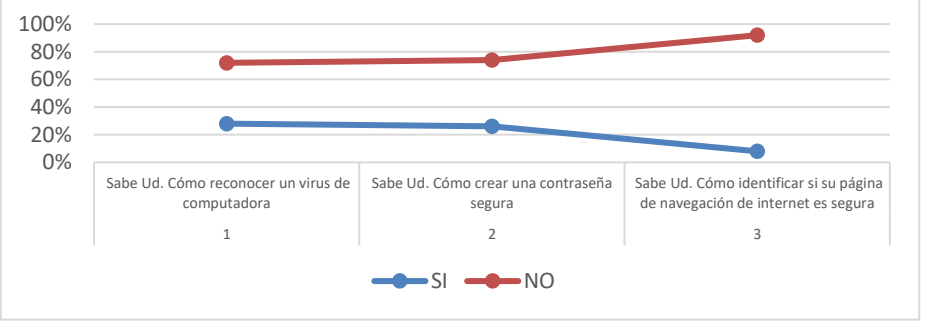

Ilustración 3: Conocimientos en ciberseguridad en el C.B.L
Fuente: Sangucho, D (2021)

En lo que respecta a la escasez de conocimiento, hay varias brechas de inseguridad, la mayoría de compañías e instituciones no cuentan con personal de Tics mucho menos con expertos en seguridad de la información, lo que demuestra el desconocimiento en ciberseguridad interna y externa, esto conlleva a que no se sienten preparados para hacer frente a amenazas comunes.

3. Resultados

En estos últimos años, todos los países subdesarrollados han implementado sistemas de seguridad ya sea por Software o Hardware, iniciando así el cambio hacia el recibimiento del internet de las cosas (IoT), donde reflejan cambios sustanciales en las nuevas tecnologías de la información y comunicación que se incorporan a las redes LAN de distintas, industrias y empresas, e incluso se han tomado acciones para sus hogares.

Con la implementación del Software pfsense se cumplen estándares de calidad, ya que aparte de ser un software Open Sourse, es gratuito, y 100% confiable y seguro.

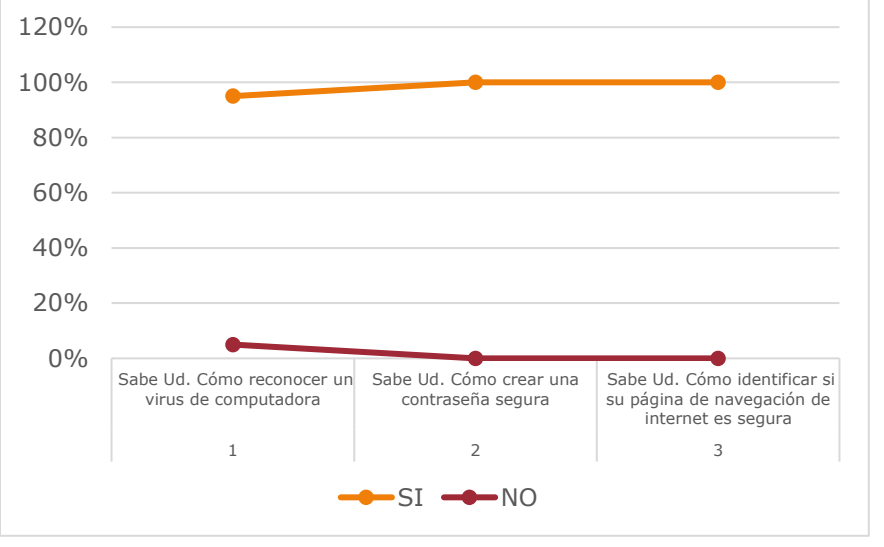

Ilustración 4: Implementación de ciberseguridad en el C.B.L
Fuente: Sangucho, D (2021)

Como se observa en la gráfica, la metodología aplicada en esta investigación es el método experimental, donde el funcionario está ya en capacidad de no ser víctima de engaño, mucho menos por suplantación de identidad. A continuación, se muestra los resultados obtenidos en la encuesta:

PREGUNTA 1. ¿Sabe usted cómo reconocer un virus de computadora?

OPCIÓN	VALOR	PORCENTAJE
SI	48	91%
NO	5	9%
TOTAL	53	100%

Ilustración 5: Encuesta a los funcionarios del C.B.L
Fuente: Sangucho, D (2021)

Análisis de datos

El 100% de los funcionarios encuestados corresponden a un total de 53 personas que, al momento de responder esta pregunta, 48 personas correspondiente al 91% tienen conocimientos claros sobre como reconocer un virus de computadora, mientras que el 5% de funcionarios no tienen conocimientos sobre como identificar un virus.

Interpretación de resultados

De la encuesta realizada claramente se puede evidenciar que el 91% de los funcionarios ya está en capacidad de reconocer un virus de computadora y no son blanco de una amenaza cibernética

PREGUNTA 2. ¿Sabe usted cómo crear una contraseña segura?

OPCIÓN	VALOR	PORCENTAJE
SI	52	98%
NO	1	2%
TOTAL	53	100%

Ilustración 6: Encuesta a los funcionarios del C.B.L
Fuente: Sangucho, D (2021)

Análisis de datos

Del 100% de funcionarios encuestados, solo 2% de los mismos no tiene conocimientos de sobre cómo crear una contraseña segura, mientras que el 98% correspondiente a los 52 funcionarios respectivamente tienen conocimientos sobre los caracteres a utilizar para generar una contraseña segura.

Interpretación de resultados

De los resultados obtenidos de esta pregunta se refleja claramente que la mayoría de funcionarios están ya familiarizados en crear contraseñas seguras que garanticen el ingreso seguro a sus cuentas personales.

PREGUNTA 3 ¿Cambia frecuentemente las contraseñas de sus cuentas personales?

OPCIÓN	VALOR	PORCENTAJE
SI	52	98%
NO	1	2%
TOTAL	53	100%

Ilustración 7: Encuesta a los funcionarios del C.B.L
Fuente: Sangucho, D (2021)

Análisis de datos

De acuerdo al 98% de los resultados positivos de esta pregunta, 52 funcionarios cambian frecuentemente las contraseñas de sus cuentas personales, mientras que el 2% no realiza este proceso.

Interpretación de resultados

De acuerdo al análisis de datos en esta pregunta, podemos apreciar que los resultados son similares a los de la pregunta anterior, ya que si hay conocimientos en crear una contraseña segura lógicamente incrementa la preocupación de cambiar frecuentemente sus contraseñas personales.

4. Discusión

Antes de la implementación del Sistema Gestor de Seguridad en el Cuerpo de Bomberos de Latacunga, los funcionarios tenían dificultades con respecto al reconocimiento de virus en sus ordenadores, cuando navegaban en la red no identificaban si una página es segura o no, de igual manera las contraseñas que utilizaban en sus cuentas personales eran de poca seguridad y no las cambian periódicamente.

Uno de los agujeros de seguridad que se filtró es el poco conocimiento de los funcionarios de la institución, quienes no estaban al día en cuestión de seguridad informática, puesto que en la actualidad la mayoría de instituciones no le dan mucha importancia a la evolución de ciberataques, no forman a sus empleados en materias de seguridad, ni mucho menos invierten en ello.

La evolución de la tecnología día a día va más allá de nuestras ideas, a ello se suma el avance científico, mismo que cada día se crean nuevas tecnologías que son amigables con el medio ambiente, así también la creación de nuevas vulnerabilidades va de la mano con todo este avance tecnológico, en la actualidad no solo estamos siendo blanco de la tecnología si no también quien esta tras de ello, con el envío masivo de phishing, que actualmente ha tomado lugar en todo el país, con el robo de información, dinero, etc., que por el nulo conocimiento de este tipo de correos, mensajes, llamadas, la victima entrega sus credenciales sin saber que están siendo víctimas de estafa.

A medida que se fue ejecutando esta propuesta se podía evidenciar el interés por el aprendizaje sobre este tema por parte de los funcionarios, ya que con la puesta en práctica de algunas reglas establecidas en la institución se pudo lograr el objetivo planteado dentro de este estudió, teniendo en cuenta que el sentido común juega un papel fundamental para no caer en errores que provoquen un mal funcionamiento de los equipos.

De esta manera se puede evidenciar los resultados obtenidos en este documento como en un principio los conocimientos por parte de los funcionarios son nulos, una vez aplicada varias metodologías, entre ellas la formación en ciberseguridad, con preguntas tan sencillas para personas expertas en la rama tecnológica pero poco entendibles para personas con pocos conocimientos tecnológicos, se está dando el primer paso a conocimientos en ciberseguridad, donde los funcionarios están capacitados para no caer en engaños tecnológicos, a ser más cautelosos con sus datos personales, a adoptar una metodología eficiente de principios de ciberseguridad.

5. Conclusiones

La implementación del firewall nos permite tener un sistema con la potencia y confiabilidad de pfSense mejorando el nivel de seguridad dentro de la red local, y con una gran ventaja económica ya que este es un software open sourse basado en FreeBSD.

El software pfSense al ser open sourse nos proporciona una seguridad continua a diferencia de implementar un firewall por hardware, que aparte de ser demasiado costoso su duración de licencia es de un año.

Referencias bibliográficas

- (s.f.). Obtenido de nist.gov: https://www.nist.gov/cyberframework/online-learning/five-functions.
- *administracionvirtualdotblog*. (25 de 10 de 2018). Obtenido de https://administracionvirtualdotblog.wordpress.com/2018/10/25/primeraentrada-del-blog/
- Adrián, B. F. (2016). En B. F. Adrián, *Diseño e implementación de un firewall l2 utilizando redes definidas por software* (pág. 8).
- Agesic. (2018). *Marco de ciberseguridad.*
- Cárdenas, E. (2012). *Anatomía de un ataque informático.*
- *pmg-ssi*. (2018). Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/