UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

MODALIDAD: PROPUESTA METODOLÓGICA Y TECNOLÓGICA AVANZADA

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

Trabajo de titulación previo a la obtención del título de Magister en Sistemas de Información

Autor

Sangucho Sandoval David

Tutor

Rubio Peñaherrera Jorge Bladimir MSc.

LATACUNGA – ECUADOR

2020

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación "**Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del CUERPO DE BOMBEROS DE LATACUNGA**" presentado por Sangucho Sandoval Abrahan David, para optar por el título magíster en Sistemas de Información.

CERTIFICO

Que dicho trabajo de investigación ha sido revisado en todas sus partes y se considera que reúne los requisitos y méritos suficientes para ser sometido a la presentación para la valoración por parte del Tribunal de Lectores que se designe y su exposición y defensa pública.

Latacunga, mayo, 25, 2020

……

Mg. Jorge Bladimir Rubio Peñaherrera

CC.: 0502222292

APROBACIÓN TRIBUNAL

El trabajo de Titulación: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del CUERPO DE BOMBEROS DE LATACUNGA, ha sido revisado, aprobado y autorizado su impresión y empastado, previo a la obtención del título de Magíster en Sistemas de Información; el presente trabajo reúne los requisitos de fondo y forma para que el estudiante pueda presentarse a la exposición y defensa.

Latacunga, junio, 12, 2020

……..
MSC. Manuel William Villa Quishpe
CC.: 1803386950
Presidente del tribunal

…….
MSC. Alex Christian Llano Casa
CC.: 0502589864
Lector 2

…….
PhD. Gustavo Rodríguez Bárcenas
CC.:1757001357
Lector 3

DEDICATORIA

A mi abuelita, María Juana Sandoval, una mujer que cuido
mi vida, la cual a pesar de haberla perdido hace algún
tiempo atrás, ha estado siempre cuidándome
y guiándome desde el cielo.
David S.S

AGRADECIMIENTO

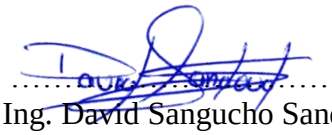
A Dios por darme la fuerza para continuar creciendo
profesionalmente, a la Universidad Técnica de Cotopaxi,
por la apertura que me dio de ingresar nuevamente a sus aulas
para poder obtener un segundo título en mi vida profesional.

David Sangucho Sandoval.

RESPONSABILIDAD DE AUTORÍA

Quien suscribe, declara que asume la autoría de los contenidos y los resultados obtenidos en el presente trabajo de titulación.

Latacunga, mayo, 25, 2020



……

Ing. David Sangucho Sandoval
0503129801

RENUNCIA DE DERECHOS

Quien suscribe, cede los derechos de autoría intelectual total y/o parcial del presente trabajo de titulación a la Universidad Técnica de Cotopaxi.

Latacunga, mayo, 25, 2020

……

David Sangucho Sandoval
0503129801

AVAL DEL PRESIDENTE

Quien suscribe, declara que el presente Trabajo de Titulación: "Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del cuerpo de bomberos de Latacunga", contiene las correcciones a las observaciones realizadas por los lectores en sesión científica del tribunal.

Latacunga, Junio del 2020

.....

MSc. Manuel William Villa Quishpe

CI: 1803386950

UNIVERSIDAD TÉCNICA DE COTOPAXI
DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

Título: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del CUERPO DE BOMBEROS DE LATACUNGA

Autor: Sangucho Sandoval Abrahan David
Tutor: Jorge Bladimir Rubio Peñaherrera. Mg.

RESUMEN

A raíz de la evolución tecnológica que dio realce al desarrollo, progreso e innovación, mejorando así las necesidades diarias de cada uno de los seres humanos, se ha convertido a su vez en una de las mayores amenazas cibernéticas a nivel mundial, teniendo en cuenta que las personas con mayor probabilidad de vulneración son aquellas con poco conocimiento en el manejo de la tecnología, 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, es así como nace la necesidad de implementar un sistema gestor de seguridad en el Cuerpo de Bomberos de Latacunga, donde podemos incrementar políticas de seguridad que permitan el cifrado de datos y limiten el acceso a páginas sociales, mediante un Software denominado Pfsense, y por ende formar a los funcionarios en materia de ciberseguridad y reducir el consumo inadecuado de Internet evitando interrupciones en los servicios/páginas gubernamentales dentro de la institución, a medida que se estableció políticas dentro del firewall se ha conseguido una conexión estable y de mayor velocidad, mediante esta implementación se dio el primer paso hacia la ciberseguridad, logrando tener una navegación en internet segura con el cifrado de paquetes extremo a extremo, mediante los certificados importados de Pfsense.

PALABRAS CLAVE: Cibernéticas; vulneración; ingeniería social; ciberdelincuente; Pfsense; ciberseguridad; inescrupulosas.

UNIVERSIDAD TECNICA DE COTOPAXI
DIRECCION DE POSGRADO

MAESTRIA EN SISTEMAS DE INFORMACIÓN

Title: IMPLEMENTATION OF A SECURITY MANAGEMENT SYSTEM AGAINST POSSIBLE CYBER THREATS IN THE NETWORK OF THE CUERPO DE BOMBEROS DE LATACUNGA.

Author: Sangucho Sandoval Abrahan David
Tutor: Rubio Peñaherrera Jorge Bladimir MSc.

ABSTRACT

As a result of the technological evolution that gave prominence to development, progress and innovation, thus improving the daily needs of each one of the human beings, it has in turn become one of the greatest cyber threats worldwide, taking into account that The people with the highest probability of violation are those with little knowledge in the handling of technology, one of the most common causes is given by deception of social engineering, where the cybercriminal impersonates a person, company or institution in order to obtain confidential information such as passwords, credit card information, among others, is how the need to implement a security management system in the Cuerpo de Bomberos de Latacunga is born, where we can increase security policies that allow data encryption and limit access to social pages, through a software called Pfsense, and therefore train officials in matters of e cybersecurity and reduce inappropriate Internet consumption avoiding interruptions in government services / pages within the institution, as policies were established within the firewall, a stable and faster connection was achieved, through this implementation the first step was taken towards cybersecurity, achieving secure internet browsing with end-to-end packet encryption, using imported Pfsense certificates.

KEYWORD:
Cybernetics; infringement; social engineering; cyber criminal Pfsense; cybersecurity; unscrupulous.

Ibeth Maricela Comina Tayo con cédula de identidad número: 0503639544 Licenciada en: Ciencias de la Educación mención Ingles con número de registro de la SENESCYT: 1020-2017-1893590; **CERTIFICO** haber revisado y aprobado la traducción al idioma inglés del resumen del trabajo de investigación con el título: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del CUERPO DE BOMBEROS DE LATACUNGA de: Abrahan David Sangucho Sandoval, aspirante a magister en Sistemas de Información.

Latacunga, 05, 15, 2020

.....
Ibeth Maricela Comina Tayo
0503639544

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN

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.

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.

El constante crecimiento tecnológico conlleva a estar bajo amenazas que afectan a nuestra infraestructura es por ello que debemos darle la mayor seguridad a la información interna de una empresa en este caso el Cuerpo de Bomberos de Latacunga.

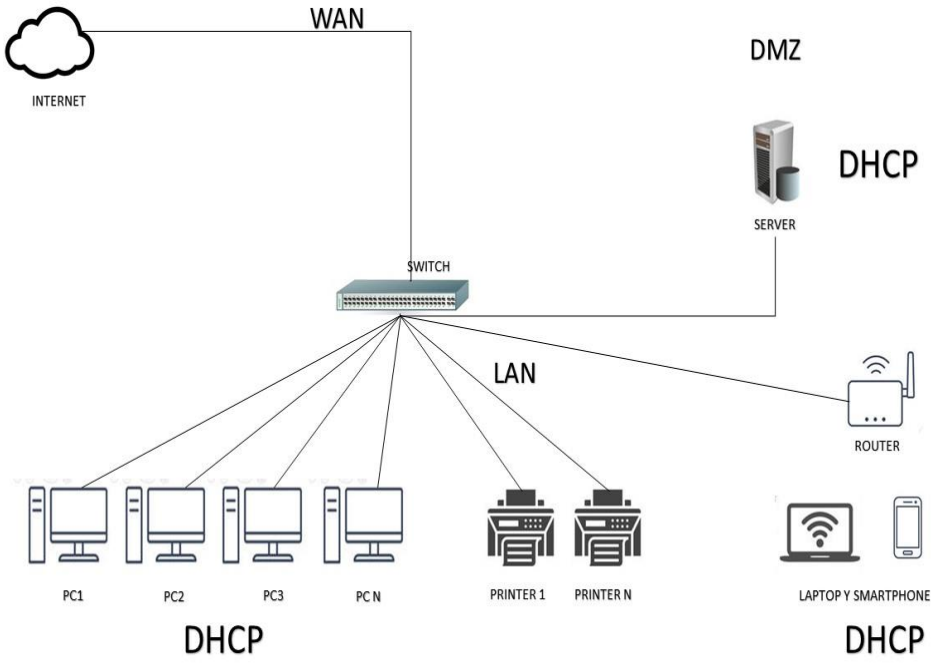
En la actualidad la mayoría de personas no están familiarizadas con la constante lucha día a día en ciberseguridad, es por esa razón que no se preocupan en la necesidad de invertir en seguridad informática, para de esta manera reducir riesgos, ataques y por ende el robo de información.

Una de 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 asechan nuestra institución, **mediante la implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red.**

Con la implementación de este mecanismo en el Cuerpo de Bomberos de Latacunga estamos dando un paso muy importante en el desarrollo de la seguridad de la información, mismo que se requiere de políticas de seguridad y capacitación tanto a los administradores del sistema como a los usuarios de esta infraestructura.

La institución no cuenta con procedimientos ni políticas que orienten a las buenas prácticas en el uso de la tecnología, no ha formado a sus funcionarios en materia de ciberseguridad para prevenir y evitar posibles amenazas, no invierten en herramientas de ciberseguridad.

Figura 1. Situación actual de la infraestructura de red del C.B.L.

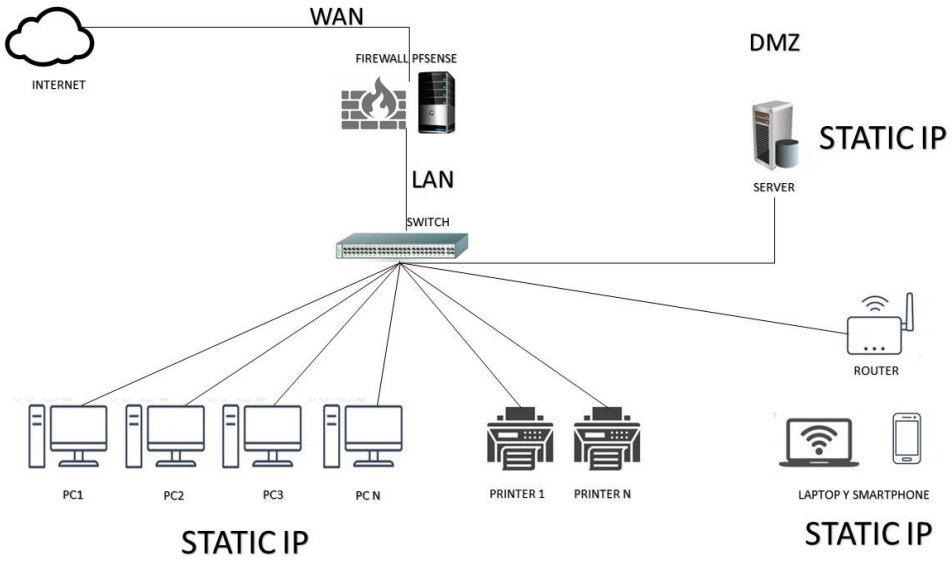


Elaborado por: David Sangucho Sandoval

La finalidad de esta implementación es que el Cuerpo de Bomberos de Latacunga cuente con un sistema contra defensas en primera línea de ataques provenientes de internet hacia la red interna de la institución, logrando de esta manera el acceso únicamente a los servicios que la institución los crea necesarios, dichos servicios lo serán controlados mediante reglas establecidas en un entorno LINUX.

Estos servicios o políticas establecidas se los controlará 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 serán 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.

Figura 2. Propuesta para la infraestructura de red del C.B.L.



Elaborado por: David Sangucho Sandoval.

Mediante esta implementación se conseguirá **Lograr que el CUERPO DE BOMBEROS DE LATACUNGA haga uso seguro y adecuado de los Sistemas de Información, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques.**

Una vez establecidas estas políticas se analizará los paquetes o tráfico que cruza mediante nuestro firewall permitiendo así el bloqueo o liberación de paquetes hacia el interior o exterior de nuestra infraestructura de red.

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.

Tabla 1. Objetivos Específicos.

Objetivo	Actividad (tareas)
1. Objetivo específico 1: Evaluar la efectividad de seguridad actual de la organización políticas, accesos, manejos de información.	1. Analizar e identificar las vulnerabilidades de la empresa.
2. Objetivo específico 2: Definir los mecanismos y controles de seguridad más relevantes	1. Cooperación y responsabilidad individual para el uso seguro de las herramientas de tecnologías de la información y comunicación.
3. Objetivo específico 3: Implementar políticas que mejoren la seguridad de los Sistemas que utilizan los funcionarios	1. Comunicar el problema. Informar internamente a los directivos del problema para tomar alguna acción.
	2. Ser sincero y responsable en caso de que la empresa tenga la culpa.
	3. Proporcionar detalles. Explicar por qué ocurrió la situación y qué se vio afectado.
	4. Comprender qué causó y facilitó la violación de seguridad.
	5. Asegurarse de que todos los sistemas estén limpios
	6. Capacitar a los funcionarios y directivos acerca de cómo prevenir las violaciones futuras.

Elaborado por: David Sangucho Sandoval

Con esta implementación ayudaremos a fomentar una cultura de identificación, prevención y detección de riesgos cibernéticos, se dará a conocer sobre el peligro que representa al no estar preparados para los diferentes ataques maliciosos que existen actualmente y se brindará información de cómo responder ante una acción maliciosa basándonos en minimizar los riesgos, esta acción es importante porque los estudios realizados por empresas especialistas en ciberseguridad señalan que los ataques cibernéticos han evolucionado, los hackers están desarrollando software maliciosos cada vez más sofisticados con el fin de buscar vulnerabilidades en los sistemas interconectados para sustraer información digital con el fin de lograr su objetivo, lo cual con el nuevo conocimiento acerca de la importancia de implementar planes de acción y estrategias para minimizar los riesgos, **el CUERPO DE BOMBEROS DE LATACUNGA tendrá el enfoque necesario para protegerse de amenazas y garantizar la seguridad cibernética.**

La institución no cuenta con procedimientos ni políticas que orienten a las buenas prácticas en el uso de la tecnología, no ha formado a sus funcionarios en materia de ciberseguridad para prevenir y evitar posibles amenazas, no invierten en herramientas de ciberseguridad.

Con la implementación de estos mecanismos de seguridad en el CUERPO DE BOMBEROS DE LATACUNGA, evitamos riesgos de ataques maliciosos en cada uno de los ordenadores de cada área de trabajo, mismos que minimizamos los riesgos y por ende la suspensión de actividades en la mencionada institución, logrando resultados óptimos y evitando vulnerabilidades.

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. [7]

Uno de los **métodos** a utilizar en esta fase será el empírico ya que nos permite usar como instrumento la encuesta, que será dirigida a todos los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA, de igual manera se va emplear en este proyecto el **método** Inductivo, por que asciende de lo particular a lo general.

CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA

1.1 **Antecedentes**. 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 comunicacione, pero, al mismo tiempo, conlleva nuevos riesgos y amenazas que pueden afectar a la seguridad de los sistemas de información. [8]

Dichas intromisiones cibernéticas siempre están presente y cada vez se habla más del tema en distintos congresos o foros mundiales todos llegando a la conclusión que los ataques cibernéticos evolucionan de forma muy frecuente.

Dichas intromisiones logran avanzar desde simples modificaciones de páginas Web, hasta estafas, o temas más complicados como actividades de espionajes.

En febrero de 2015, la firma Kaspersky quien es una empresa que se dedica crear soluciones de seguridad, así como un antivirus quien es su producto estrella que lleva el mismo nombre de la empresa. Esta firma dio a conocer su comentario acerca el ciber-crimen logrado ejecutarse por The Carbanak group, este grupo realizó un sin fin de hurtos a casi cien bancos, robando alrededor de un billón de dinero americano en todo el mundo.

Lo que se analizó fue, que dichos asaltantes cibernéticos descubrieron las flaquezas de los sistemas en las redes privadas, en otras palabras, podían ingresar a sus a sus protocolos de seguridad sin mayores problemas con la finalidad de ingresar a la red privada de la empresa sin autorización alguna.

Los delincuentes lograron realizar registros y transacciones falsas que aparentemente eran transacciones normales para los funcionarios del banco y de forma no lograron ser detectadas por procesos antifraude que tenía la empresa.

Así mismo a finales del 2014, la firma Sony Pictures fue víctima de un ataque cibernético donde los hackers ingresaron al núcleo de la propiedad intelectual de una empresa. Entre los daños ocasionados a la firma Sony se detectó la sustracción de 100 Tera bitios (Mil catorce bitios (bit)) de ciber-información, conteniendo de mails, trailers de películas nuevas y próximos guiones a estrenarse en nuevos proyectos.

Según un informe de la firma Digiware señala que Perú es el quinto país de América Latina que más recibe ataques cibernéticos. Según el estudio, Perú concentra el 11.22% de recepción de ataques cibernéticos, luego aparecen Colombia 21.73%, Brasil con el 19% de recepción de ataques cibernéticos, Argentina con el (13.94%), mientras que Ecuador tiene un porcentaje similar que Perú (11.25%). [9]

En Ecuador se ha implementado un firewall L2 utilizando redes definidas por software (sdn), mediante la dirección de la Universidad Católica del Ecuador en el año 2016, donde se ha evidenciado la importancia de mantener una ligera seguridad en la información, mismo que ha sido implementado a través de un emulador de red denominado Mininet.

1.2 Fundamentación epistemológica. - Las nuevas tecnologías alcanzan no solo a las compañías sino también a los ciberdelincuentes, que transforman vulnerabilidades en riesgos organizacionales. ¿Cómo lograr un cambio de paradigma que permita estar un paso adelante de los ciber atacantes?

En este complejo escenario geo-político en el que operan las organizaciones, y donde cada vez dependen en mayor medida de la tecnología para

sobrevivir en plena transformación digital, resulta indispensable establecer rigurosas medidas de protección para enfrentarse a amenazas cada vez más sofisticadas, y sin embargo, habiendo ya renunciado a la defensa del perímetro en un mundo interconectado, el único paso posible para perdurar se focalizará en desarrollar capacidades de anticipación, protección, respuesta y recuperación de sus activos más esenciales, a través de un marco de gobierno efectivo y condicionado cada vez más por una regulación creciente.

1.2.1 Necesidad de la ciberseguridad. - La Ciberseguridad es un problema latente, del que todos los países parecen estar ocupándose, los profesionales de la ciberseguridad deben tener las mismas habilidades que los atacantes cibernéticos, pero los profesionales de la ciberseguridad deben trabajar de acuerdo con la ley local, nacional e internacional. Los profesionales de ciberseguridad también deben usar sus habilidades con ética.

Esta preocupación por la protección de los datos, se escala también a las organizaciones privadas. Hemos visto como grandes corporaciones, hospitales e inclusos medianos y pequeños empresarios han sido víctimas de ataques de hackers, los que a través de "Malwares" (software o código maligno) copian la información de sus sistemas o la encriptan, para luego lucrar con la venta de la información obtenida, o, con la liberación de los sistemas.

No es casualidad que el mundo entero se esté ocupando de la ciberseguridad de su información, ya que el peligro hoy está a un sólo clic. [10]

1.2.2 Ciberseguridad. - Es el esfuerzo constante por proteger estos sistemas de red y todos los datos contra el uso no autorizado o los daños. A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos. A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización. A nivel del estado, la

seguridad nacional, y la seguridad y el bienestar de los ciudadanos está en juego.[5]

1.2.3 Historia de ciberseguridad. - La Ciberseguridad, se emplea en la detección y amenazas a la Seguridad y esta se brinda básicamente en el uso frecuente de ordenadores y es aquí en donde podemos evidenciar que los "Usuarios" son demasiado vulnerables o descuidados al momento de utilizar sus Computadores ya que al ser tan indispensables para el funcionamiento de una empresa son las más solicitadas a la hora de robar información y búsqueda de datos como cuentas de toda la nómina de los empleados o funcionarios.

En cuanto al primer ciberdelincuente de la historia, puede uno decir que fue un personaje norteamericano que fue denominado "Capitán Crunch", debido a que utilizó un pequeño silbato que venía en una caja de cereal para engañar a la central telefónica con el sonido de dicho silbato, logrando realizar llamadas telefónicas de larga distancia, consiguiendo engañar a las empresas de telefonía con dicho fraude.

A principios de los años 70, se conoció el primer virus de la historia, a través de un mensaje que empezó a aparecer en varios ordenadores de la red ARPANET (la antecesora de Internet)

En octubre de 2016 tuvo lugar un ataque perpetrado por la red de robots o botnet Mirai que, infectando dispositivos del internet de las Cosas (IoT) (fundamentalmente cámaras-IP y routers domésticos), Constituyó una red de dispositivos zombis y lanzó un ataque masivo de denegación de servicio distribuido (DDoS) contra la infraestructura de DNS del proveedor de infraestructura Dyn, afectando a usuarios de empresas tan relevantes como Twitter, Amazon, Tumblr, Reddit, Spotify, Paypal y Netflix, denegándoles el acceso.

En mayo de 2017, sucedió el mayor ataque de la historia, denominado "Wannacry", que afectó más de 200 mil computadores, cerca de 120 países en todo el mundo, dicho ataque fue un "ramsomware", que es un secuestro de información, a través del cual, el ciberdelincuente encripta la información del computador, es decir que lo pone una clave desconocida para que el dueño de la información no la pueda utilizar y pide dinero para entregar dicha clave.

Si el propietario de una empresa no tiene implementado en su negocio un modelo de buenas prácticas de seguridad digital, que proteja la organización, un ataque como alguno de los que hemos observado puede llevar a perdidas elevadas e incluso al cierre definitivo de la empresa.[11]

1.2.4 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. La formulación de la identidad digital de una persona depende en gran medida del entorno en el que se va a utilizar. Por ejemplo, la información que requiere el centro médico al que acudimos con una dolencia es distinta a la que demanda Amazon para validar una compra. El grado de seguridad y privacidad que debe proteger nuestra información personal depende de la sensibilidad de la misma y de si la ofrecemos de forma voluntaria o forzada. Por ejemplo, comentar de forma neutral en una red social es un contenido que aportamos de forma voluntaria y no constituye información especialmente sensible, por lo que no requiere un control especial. En el caso de que esa información poco sensible se le exija al usuario de forma forzada, como puede ser, el tener que darse de alta como usuario para poder comentar en un blog, se le debe garantizar por lo menos el derecho al anonimato. 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.[11]

1.2.5 Ciclo de vida de la ciberseguridad. - La ciberseguridad es como la salud de una persona: hay que vigilarla y cuidarla constantemente, no vale con realizar intervenciones esporádicas. Por ello, se habla de un ciclo o un proceso, es decir, una estrategia que se aplica constantemente en todo momento y que contiene distintas fases.

Prevención: Requiere una formación continua para conocer las nuevas amenazas que acechan en las redes en cada momento y qué medidas hay que llevar a cabo para evitar poner en peligro la información y los sistemas corporativos.

Las tareas de prevención incluyen:

- El control sobre quién accede a los recursos de la empresa y la asignación de permisos y credenciales al personal en función de los roles desempeñados.
- Establecimiento de medidas técnicas, organizativas y legales para evitar fugas de información de la empresa.
- Definición de una política de seguridad de la red, que debe ser implementada a través de herramientas de software y hardware y que debe ser auditada con frecuencia para garantizar su eficacia.

Detección: De un ataque, que puede tener lugar en tiempo real o después de que haya ocurrido. Esta fase del ciclo de la ciberseguridad reposa sobre dos acciones complementarias:

- La monitorización continua de los sistemas y redes de la empresa para poder identificar lo antes posible los intentos de agresión y limitar el daño que puedan causar.
- La identificación de los puntos flacos en nuestras infraestructuras informáticas que pueden dejarnos expuestos ante conductas maliciosas.

Respuesta: Cuando finalmente la empresa ha sufrido un ciberataque se inicia esta etapa, que conlleva:

- Los sistemas de recuperación, que permiten devolver el estado de los equipos y las aplicaciones al punto de partida anterior a que se haya producido el problema.
- La aplicación de nuevas medidas de seguridad que eviten que la situación se vuelva a producir en el futuro.

Inteligencia: Se trata de compartir la información sobre los ataques con otras empresas e instituciones, así como con organismos relacionados con la seguridad, para conocer mejor la operativa de agresión y hacer más efectiva la respuesta al cibercrimen.[12]

1.2.6 Ataques informáticos. – Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; A fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

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, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.

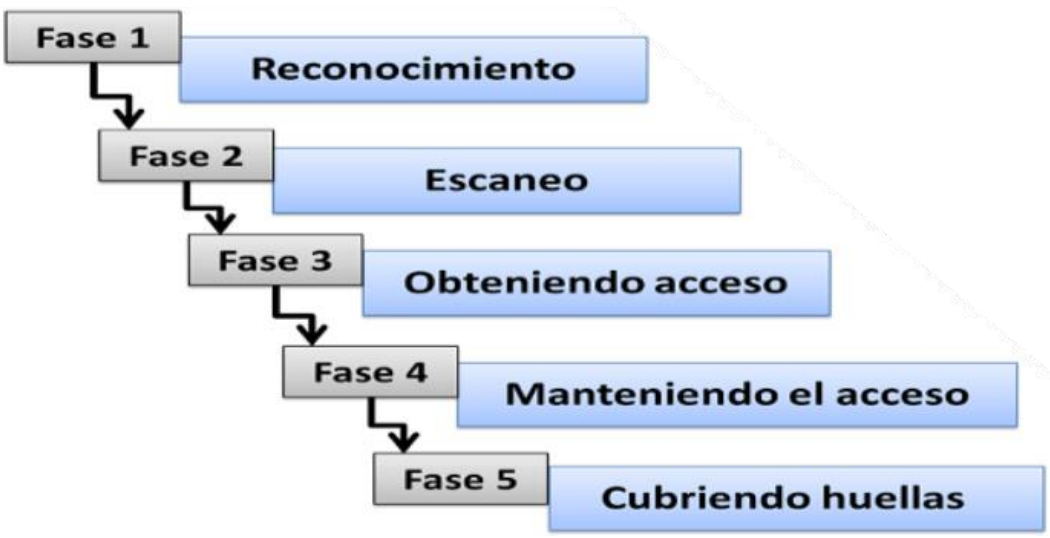
El mundo está viviendo una auténtica evolución tecnológica. Todos los sectores están siendo digitalizados, desde la agricultura o la ganadería hasta la industria, el comercio, el turismo, etc. Este aumento en el uso de tecnología también ha provocado un incremento en la cantidad de ciberataques.

Hace unos años, los objetivos principales de los hackers eran las personas particulares. En la actualidad, la mayoría de ataques informáticos son dirigidos a empresas, así lo demuestran los datos de los ataques informáticos en 2018.

1.2.7 Fases de un ataque informático. – Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. 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:

Figura 3. Fases de un ataque informático.



Fuente: MSN seguridad.

Fase 1: Reconocimiento. Esta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social.

Fase 2: Exploración. 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.

Fase 3: Obtener acceso. 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 y Session hijacking.

Fase 4: Mantener el 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.

Fase 5: Borrar huellas. Una vez que el atacante logró obtener y mantener el acceso al sistema, 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).

1.2.8 Aspectos de ciberseguridad que compromete un ataque. – La seguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos.

Bajo esta perspectiva, el atacante intentará explotar las vulnerabilidades de un sistema o de una red para encontrar una o más debilidades en alguno de los tres elementos de seguridad. Para que, conceptualmente hablando, quede más claro de qué manera se compromete cada uno de estos elementos en alguna fase del ataque, tomemos como ejemplo los siguientes casos hipotéticos según el elemento que afecte.

Confidencialidad. Un atacante podría robar información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, atentando contra la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. Un ejemplo que compromete este elemento es el envenenamiento de la tabla ARP (ARP Poisoning).

Integridad. Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina Bit-Flipping y son considerados ataques contra la integridad de la información. El ataque no se lleva a cabo de manera directa contra el sistema de cifrado, pero sí en contra de un mensaje o de una serie de mensajes cifrados. En el extremo, esto puede convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utiliza cifrado.

Disponibilidad. En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información.[13]

1.2.9 Debilidades de seguridad comúnmente explotadas. – Afortunadamente, en la actualidad existe una gama muy amplia de herramientas de seguridad lo suficientemente eficaces que permiten obtener un adecuado nivel de seguridad ante intrusiones no autorizadas haciendo que la labor de los atacantes se transforme en un camino difícil de recorrer.

Ingeniería Social Los atacantes saben cómo utilizar estas metodologías y lo han incorporado como elemento fundamental para llevar a cabo cualquier tipo de ataque.

Si bien esta técnica es utilizada en cualquier ámbito, en lo que a informática se refiere, consiste en la obtención de información sensible y/o confidencial de un usuario cercano a un sistema u organización explotando ciertas características que son propias del ser humano.

Sin lugar a duda, las personas constituyen uno de los problemas más importantes de seguridad para cualquier organización porque a diferencia de los componentes tecnológicos, son el único elemento, dentro de un entorno seguro, con la capacidad de decidir "romper" las reglas establecidas en las políticas de seguridad de la información. Ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, quien, de esta manera, podrá eludir los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización. Por ejemplo, en este sentido, la confianza y la divulgación de información son dos de las debilidades más explotadas para obtener datos relacionados a un sistema.

Como contramedida, la única manera de hacer frente a los métodos de Ingeniería Social es la educación. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, los administradores de la red y la cúpula mayor, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes para que logren identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente.

Esto no significa que cada uno de los empleados deba realizar cursos de seguridad informática, sino que el proceso de capacitación debe formar parte de las Políticas de Seguridad de la Información y debe ser ejecutada a través de planes dinámicos de concientización.

"Usted puede tener implementada la mejor tecnología, Firewalls, sistemas de detección de intrusos o complejos sistemas de autenticación biométricos... Pero lo único que se necesita es una llamada telefónica a un empleado desprevenido y acceder al sistema sin más. Tienen todo en sus manos" [13]

Contraseñas: Otro de los factores comúnmente explotados por los atacantes son las contraseñas. Si bien en la actualidad existen sistemas de autenticación complejos, las contraseñas siguen, y seguirán, siendo una de las medidas de protección más utilizadas en cualquier tipo de sistema informático. En consecuencia, constituyen uno de los blancos más buscados por atacantes informáticos porque conforman el componente principal utilizado en procesos de autenticación simple (usuario/contraseña) donde cada usuario posee un identificador (nombre de usuario) y una contraseña asociada a ese identificador que, en conjunto, permiten identificarse frente al sistema.

Si bien es cierto que una contraseña que supere los diez caracteres y que las personas puedan recordar, es mucho más efectiva que una contraseña de cuatro caracteres, aun así, existen otros problemas que suelen ser aprovechados por los atacantes.

A continuación, se expone algunos de ellos:

- La utilización de la misma contraseña en varias cuentas y otros servicios.
- Acceder a recursos que necesitan autenticación desde lugares públicos donde los atacantes pueden haber implantado programas o dispositivos físicos como keyloggers que capturen la información.
- Utilización de protocolos de comunicación inseguros que transmiten la información en texto claro como el correo electrónico, navegación web, chat, etcétera.
- Técnicas como surveillance (videoconferencia) o shoulder surfing (mirar por detrás del hombro), entre otras tantas, que permiten evadir los controles de seguridad. [13]

1.2.10 Seguridad. La seguridad se trata de la supervivencia. Es cuando un problema se presenta como una amenaza existencial hacia un objeto referente designado (tradicionalmente, pero no necesariamente, al Estado, incorporando

gobierno, territorio y sociedad). El carácter especial de las amenazas a la seguridad justifica el uso de medidas extraordinarias para hacerlas efectivas. La invocación de la seguridad ha sido la clave para legitimar el uso de la fuerza, pero más generosamente ha abierto el camino para que el Estado movilice o tome poderes especiales para manejar amenazas existentes. Tradicionalmente, al decir "seguridad", un representante estatal declara una condición de emergencia, reclamando así el derecho a usar cualquier medio que sea necesario para bloquear el desarrollo de una amenaza

1.2.11 Ciberseguridad. La ciberdefensa es definida como la capacidad de asegurar, salvaguardar la prestación de los servicios, confidencialidad, integridad y disponibilidad, proporcionados por los sistemas de información y comunicaciones en la fase de operación de los sistemas en producción en respuesta a posibles e inminentes acciones maliciosas originadas en el ciberespacio. La ciberseguridad está enfocada en la protección de la información y sistemas que se utilizan para almacenar o gestionar información y sus tres pilares fundamentales; son la confidencialidad, la integridad y disponibilidad. Concepto que engloba todas las actividades defensivas en las que se utilizan como medio aquellos relacionados con las infraestructuras TIC Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y herramientas Seguridad de la Información Seguridad del personal, Seguridad de la Documentación, Seguridad de las TIC, Ciberseguridad tecnológica que pueden utilizarse para proteger los activos de la organización y los usuarios en el entorno de ciberespacio.

La ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución de la tecnología de la información y comunicación (TIC), que ha acelerado el proceso de globalización y periódicamente sorprende con su constante innovación. Ejemplo de ello, lo encontramos en el incremento de la cantidad de aparatos

conectados al ciberespacio, lo que ha dado origen a la denominada internet de las cosas. [5]

1.2.12 Ciberataque. El término ciberataque es bastante complejo, ya que diariamente tanto la sociedad como las tecnologías de la información están en continuo cambio, por lo que una definición se quedaría obsoleta en cuestión de poco tiempo. Y, aunque existan muchas definiciones del término, oficiales o no, ninguna abarcará todos los conceptos que desde otro punto del planeta puedan verse como absolutamente necesarios. Realmente es complicado dar una definición exacta porque depende de muchas variables, y sobre todo si la definición se pretende crear para la aceptación en la comunidad internacional, ya que entre las naciones tienen conceptos diferentes en la mayoría de los sentidos.

El término de ciberataque se ha usado para todo tipo de actividad extraña dentro de los confines del internet, desde las protestas online hasta actos reales de guerra en campos de batalla reales. Incluso los mismos expertos en el tema caen presa a la hora de dar una definición más que valida del concepto, debido a la intangibilidad de los conceptos.

Normalmente se llama ciberataque a todo hecho malicioso que conlleve el uso de Internet. Para intentar definirlo bien hay que comenzar por distinguirlo de un ataque convencional y físico.

La primera diferencia que encontramos es la fuerza que se usa en los ataques, mientras que en un ataque convencional usamos las fuerzas cinéticas, como puede ser una bomba o el uso de una espada, y que por tanto está ligado a la física y al terreno en el que se encuentren. Mientras que en un ciberataque se usa cualquier tipo de acción informática de cualquier fuerza, y no tiene fronteras y es apolítico, queriendo decir que no proviene de una sola ideología, esto quiere decir que puede estar en múltiples lugares a la misma vez y propagarse en cuestión de segundos.

Hay muchas maneras para llevar a cabo un ciberataque, ya sea por ejemplo infectando los ordenadores o las redes con virus y gusanos que controlen, ralenticen o dañen los ordenadores; o bien mediante la explotación de los programas espía para encontrar posibles puntos débiles dentro del sistema, o robar la información; enviando ataques de denegación de servicio (DDoS) , con o sin la ayuda de botnets, para saturar tanto páginas web como redes e infraestructuras críticas.

En seguridad informática, se entiende como un ataque de denegación de servicios (DoS por sus siglas en inglés Denial of Service, o DDoS de Distributed Denial of Service) como el ataque a un sistema de ordenadores o a una red que es capaz de causar que un servicio o un recurso sea inaccesible para los usuarios legítimos. Normalmente, lo primero que causa es la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o bien una sobrecarga de los recursos de computación del sistema de la víctima. Este ataque se genera mediante la saturación de los puertos con flujo de información, lo que produce una sobrecarga en el sistema y este por defecto lo "deniega". Los ataques pueden realizarse de muchas formas diferentes, pero todos tienen algo que les une, todos usan la familia de protocolos TCP/IP para llevarse a cabo. Más concretamente, el DDoS, que es una ampliación del DoS, se produce generando grandes flujos de información desde puntos diferentes de conexión, lo que lleva a cabo la sobrecarga y por tanto la denegación del servicio. Esta técnica, gracias a su sencillez tecnológica, es la más usada por los crackers para llevar acabo cualquier tipo de ciberataque

Microsoft define Botnet como: El término bot es el diminutivo de robot. Los delincuentes distribuyen software malintencionado (también conocido como malware) que puede convertir su equipo en un bot (también conocido como zombi). Cuando esto sucede, su equipo puede realizar tareas automatizadas a través de Internet sin que lo sepa. Los delincuentes suelen usar bots para infectar una gran cantidad de equipos. Estos equipos crean una red, también conocida como botnet. Los delincuentes usan botnets para enviar mensajes de

correo electrónico no deseados, propagar virus, atacar equipos y servidores y cometer otros tipos de delitos y fraudes. Si su equipo forma parte de una botnet, el equipo puede volverse más lento y puede estar ayudando a los delincuentes sin darse cuenta.

1.2.13. Ciberdefensa. Se define a la Ciberdefensa como la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques.

El grado de conocimiento que necesita un atacante para realizar una agresión a los sistemas de información ha decrecido a lo largo del tiempo, debido al aumento de la calidad, cantidad y disponibilidad de herramientas ofensivas.

Actualmente, es relativamente fácil encontrar en internet herramientas de ethical hacking basadas en el uso de conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas, sin hacer daño. Existen también herramientas de informática forense y de seguridad informática, entre otras, que son utilizadas con mala intención. Todo ello conforma un escenario de nuevos riesgos para el que es necesario que los distintos gobiernos desarrollen planes o estrategias, y se contemple la Ciberdefensa como un riesgo al que es preciso hacer frente para mejorar la seguridad nacional.

La Ciberdefensa es definida por La OTAN como: El desarrollo de la capacidad de prevenir, detectar, defenderse y recuperarse de los ataques cibernéticos. Por lo tanto, la defensa se centra en el uso de métodos tecnológicos para identificar una intrusión no autorizada, localizar el origen del problema, evaluar los daños, evitar la propagación de los daños dentro de la red, y en la medida necesaria, la reconstrucción de los datos y de los equipos que se encontraban dañados. Defensa implica la capacidad de colocarse en el camino de penetración, identificar tal intento, y frustrar a través de la interrupción y suspensión de las tareas. [6]

1.2.14. Virus Informático. "Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador. Aunque no todos son tan dañinos.

1.2.15. Firewall. El firewall es un dispositivo que apoya el bloqueo de conexiones entrantes y salientes de una red, esto con el fin de limitar accesos no deseados que puedan vulnerar los equipos de la red. Existen firewall de red o de host, los de red son implementados para proteger los equipos y sistemas de información de una red y los de host protegen a los equipos de cómputo o servidores directamente desde su núcleo de conexiones. Para los equipos con firewall de host el aseguramiento tecnológico es clave ya que por medio de este se minimiza las posibles intrusiones y se bloquea accesos por medio de vulnerabilidades que afecten las aplicaciones o programas que estén en los equipos de cómputo o servidores, los firewall de host permiten por medio de reglas restringir conexiones externas a servicios y puertos del equipo, el firewall de red restringe tráfico de red y limita desde el perímetro accesos vulnerables a los sistemas.

1.2.15.1- Cómo actúa. - Un sistema firewall tiene una serie de reglas definidas y es así su forma de funcionar. Puede autorizar o bloquear una conexión, según lo tengamos configurado. También puede redireccionar la misma.

Por ejemplo, podríamos permitir únicamente que se autoricen las conexiones que tengamos configuradas previamente y bloqueando el resto. Con esto nos aseguraríamos tener nuestro equipo seguro, pero debemos de definir con precisión qué queremos autorizar para que no suframos problemas.

Básicamente podríamos decir que su utilidad es la de proteger nuestro equipo de posibles intrusos que puedan conectarse y robarnos datos personales, información, etc. Es por ello que su función es la de preservar nuestra

seguridad y privacidad, proteger nuestra red y mantener a salvo la información guardada en el equipo.

También nos protege frente a posibles usuarios no deseados que puedan acceder a nuestra red o equipo, Además, evita posibles ataques de denegación de servicios.

Un firewall bien configurado nos podría defender ante ataques IP address, Spoofing o ataques source routing, por ejemplo.

Si no disponemos de un firewall, aunque tengamos un antivirus bien configurado y de calidad, dejaríamos siempre una puerta abierta a posibles amenazas. Es por ello que es un buen complemento a nuestros programas de seguridad.

Un sistema firewall tiene una serie de reglas definidas y es así su forma de funcionar. Puede autorizar o bloquear una conexión, según lo tengamos configurado. También puede redireccionar la misma.

Nosotros le damos las reglas básicas al firewall. Si el tráfico cumple con las reglas que se han configurado, podría entrar o salir. Si por el contrario no cumple con las normas que hemos establecido, quedaría bloqueado sin llegar a su destino.

Podemos, por tanto, filtrar direcciones, administrar los accesos a los usuarios que queramos o no que se conecten, hacer un filtrado de protocolo (por ejemplo, que sólo se conecte a páginas https), controlar el número de conexiones que se realizan desde un mismo punto, controlar qué aplicaciones pueden conectarse a la red y las que no, etc.

Sin embargo, un firewall tiene sus limitaciones. Nos puede proteger frente a amenazas de Internet, pero por ejemplo no podría evitar que alguien introduzca un USB en nuestro equipo y robe información.

El Firewall es capaz de bloquear las páginas web peligrosas, con contenidos no adecuados e inmorales, protegiendo así tanto nuestro ordenador de las diferentes amenazas que asolan la red como a todas las personas que se conecten a Internet, especialmente a los más pequeños, que son los usuarios más vulnerables. [17].

1.2.16. Antivirus. Un antivirus es una aplicación que trata de detectar y eliminar los virus informáticos, es decir, aquellos programas maliciosos que pueden ingresar en un ordenador y producir daños tales como la pérdida de efectividad del procesador, la supresión de archivos, la alteración de datos, la exposición de información confidencial a usuarios no autorizados o la desinstalación del sistema operativo.

Los antivirus regularmente se deben configurar para ser actualizados automáticamente para que las firmas puedan ser comparadas con los nuevos códigos maliciosos que existan. La comparación de encabezados de los archivos hace que el antivirus detecte si es malicioso o no, igualmente su comportamiento en el sistema ya que los virus regularmente toman el comportamiento de procesos del sistema y actúan como tal, por ello regularmente se debe analizar comportamiento y efecto para determinar si es un virus o un proceso normal del sistema

1.2.17. Tipos de Antivirus. Al igual que no hay virus similares, tampoco existen sistemas antivirus iguales. Vitriago identifica los tipos de sistemas antivirus así:

- **Anti-espías o antispyware.** Esta clase de antivirus tiene el objetivo de descubrir y descartar aquellos programas espías que se ubican en la computadora de manera oculta.

- **Anti pop-Ups.** Tiene como finalidad impedir que se ejecuten las ventanas pop-ups o emergentes, es decir a aquellas ventanas que surgen repentinamente sin que el usuario lo haya decidido, mientras navega por Internet.

- **Anti-Spam.** Se denomina spam a los mensajes basura, no deseados o que son enviados desde una dirección desconocida por el usuario.

1.3. Fundamentación del estado del arte. – En España entre los años 2011 y 2015, se incrementó la capacidad, tanto de planeamiento como de ejecución en tres niveles: político estratégico, operacional y táctico / técnico.

Este trabajo de investigación se ha construido como un estudio de casos sobre la ciberseguridad en España, estimando su relevancia y su naturaleza en relación con la propuesta de un modelo de organización de la ciberseguridad en España, el cual pueda ser realizable y tenga un impacto positivo en el incremento de los niveles de la seguridad nacional.

La investigación presentó en primer lugar la evolución de los incidentes de ciberseguridad en España entre 2011 y 2015, encuadrándolos en un contexto general, ya que gran parte de las ciber amenazas son compartidas por otros Estados. [14]

En el 2013 en Quito en empresa de contabilidad ARMAS & ASOCIADOS, se implementó un firewall sobre plataforma LINUX, el sistema planteado reúne los requisitos de ser un sistema de uso simple desde el punto de vista del usuario, pero reúne la complejidad suficiente dentro de sus procesos internos, para ser una solución lo suficientemente segura, todos los procesos adicionales se realizan dentro del sistema de seguridad, son totalmente transparentes para

el usuario, es decir el usuario no se percatará que dentro del sistema se realizan verificaciones adicionales de seguridad. [15]

1.4 Conclusiones Capítulo I

- Uno de los factores principales dentro de una organización, empresa u hogar, es la seguridad de la información, es por eso que se ha detallado dentro de este capítulo todo lo referente a lo que concierne las vulnerabilidades dentro de la misma, factores importantes, riesgos, ataques, etc., se ha evidenciado también la implementación de soluciones hacia los diferentes tipos de ataques que se vive diariamente, dando soluciones óptimas.
- Se ha podido evidenciar de cierta forma algunos ataques causas y consecuencias producto de ataques maliciosos hacia instituciones que de una u otra manera lograron penetrar hacia la red LAN, dando como resultado pérdidas millonarias de dinero.
- El uso inadecuado de los sistemas informáticos, el engaño y debilidades empleados por los atacantes es cada vez más sofisticado, donde los propios usuarios en la mayoría de las ocasiones son los responsables de abrir brechas para que los ciberdelincuentes actúen con total libertad.

CAPÍTULO II. PROPUESTA

En el Cuerpo de Bomberos de Latacunga se ha evidenciado un alto riesgo de vulnerabilidades, ya que no cuenta con una infraestructura de red adecuada, no dispone de ningún tipo de seguridad, es ahí que se evidencia la falta de prevención ante los problemas informáticos. 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.

Muchos de nosotros no tomamos importancia a los riesgos que conlleva este tema, asumimos que simplemente es una inversión de dinero que no tiene sentido, pero a medida que pasa el tiempo la amplia variedad de amenazas que afectan a nuestros equipos informáticos siempre conllevan a una única consecuencia, que los sistemas dejan de funcionar.

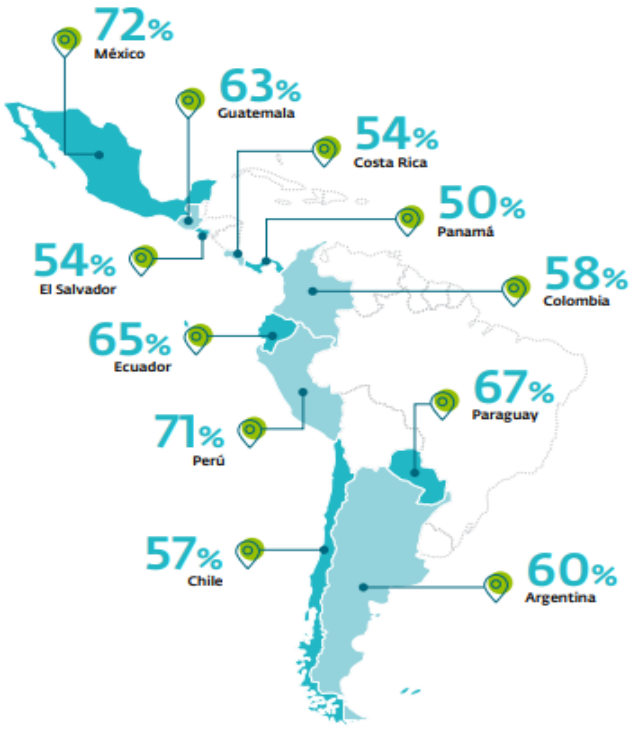
Uno de los lugares más importantes y útiles es el internet, que contiene todo tipo de información y ciencia, es de ahí donde muchos usuarios conocidos como piratas informáticos, buscan hacer negocio atacando de forma remota a los ordenadores de muchos usuarios que navegan en Internet.
Más allá de las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

La importancia de la información para el logro de los objetivos en las organizaciones, le ha significado ser considerada en muchos casos como el activo más importante. Debido al valor que se le atribuye, es objeto de diversas amenazas como el robo, falsificación, fraude, divulgación y destrucción, entre muchas otras.

Según ESET-security-report-LATAM, 2 de cada 5 Empresas de Latinoamérica sufrieron una infección de malware en 2018, y el 10% Disminuyó la cantidad de casos de ransomware respecto del año anterior, mientras que el año 2018 se consolidó como medio de infección la minería de criptomonedas, en líneas generales, los códigos maliciosos son un problema que va en aumento para los usuarios en la región. Tal es así que un análisis sobre la cantidad de archivos maliciosos vistos durante 2018 da cuenta de un crecimiento del 7%, llegando a más 750 millones solo en países de Latinoamérica. Para mostrar aún más la significancia de este crecimiento, si comparamos los primeros meses de 2019 con lo que vimos en los primeros meses de 2018, la cantidad de archivos únicos

ya fue superada en casi un 30%, por encima de los 360 millones de archivos maliciosos registrados.

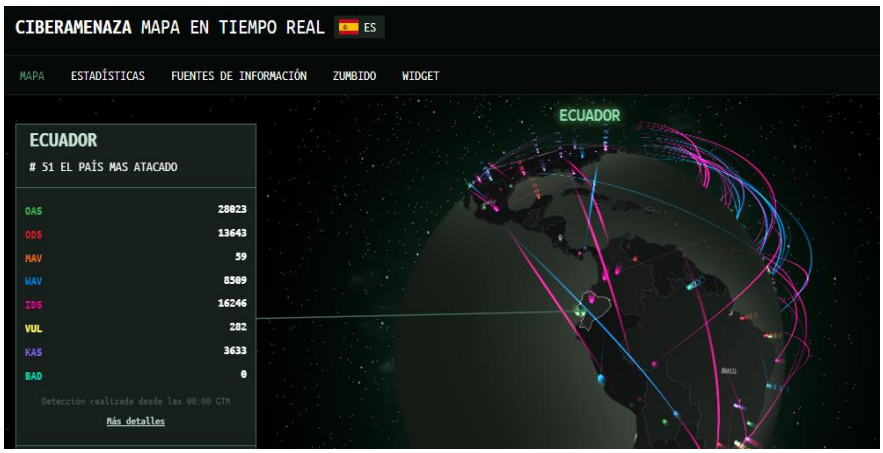
Figura 4. Incidentes de seguridad por país.



Fuente: ESET security.

Mientras que en el 2020 según Kaspersky Security ecuador se encuentra en la posición número 51 como el país más atacado de américa Latina.

Figura 5. Incidentes en tiempo real.



Fuente: KASPERSKY Security.

Es por esta razón por la que ambas empresas recomiendan implementar por lo menos medidas básicas que protejan las instituciones, estas pueden ser mediante antivirus, firewall y backups.

Los riesgos a los que está expuesta dicha información conducen a la necesidad de desarrollar ambientes confiables, pero conseguirlo es un problema complejo y multifactorial. Por esta razón, se han desarrollado enfoques de seguridad como la defensa en profundidad, que tiene como propósito proteger la información a través de la aplicación de controles en distintas capas.

Una de estas capas es el perímetro, el límite lógico que divide la red corporativa de otras redes, incluyendo Internet. En la llamada seguridad perimetral, el firewall continúa teniendo vigencia como mecanismo de protección de las redes y ha sido un elemento imprescindible desde su aparición hace 25 años. [16]

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, en el Cuerpo de Bomberos de Latacunga se va a implementar un firewall por software, qué va a actuar como primera barrera de protección ante cualquier amenaza cibernética.

2.1- Diagnóstico del problema. – En la actualidad el Cuerpo de Bomberos de Latacunga no cuenta con un sistema de seguridad tanto por hardware como por software, las conexiones hacia la red se los realiza de una manera directa, no existe un control sobre los funcionarios, mucho menos a personas ajenas a la institución, la falta de medidas de seguridad en la institución es un problema que está en constante crecimiento, el libre acceso a la red institucional a puesto a los directivos en constante amenaza, la institución no cuenta con medidas de seguridad que garanticen la protección de información, y privacidad de la misma.

El Cuerpo de Bomberos de Latacunga en los últimos se ha visto afectado en el incremento de acciones que violan la privacidad, los recursos etc., debido a la falta de seguridad institucional, los funcionarios, directivos y la población en general se conectan hacia la red LAN a través del servicio WIFI que ofrece la institución.

El acceso a internet se lo realiza de una manera libre, cualquier persona que se conecta a la red institucional puede acceder a todo contenido web, e incluso al libre acceso a los recursos compartidos que dispone la institución, esto impide el normal funcionamiento de los procesos internos a los que se dedica, y por ende ha existido la perdida de información.

Otro de los problemas que atraviesa la institución es el software actual instalado es la mayoría de sus ordenadores, mismo que es Windows 7 en sus diferentes versiones, el cual el 14 de enero del 2020, llega el fin del soporte oficial para este sistema operativo, esto implica que ya no se repararán todos los bugs y errores descubiertos en esta versión. Quiere decir que Microsoft no vigilará que Windows 7 sea un sistema seguro. Esta es otra de las razones a la que la institución quedará expuesta a vulnerabilidades a niel de software, quedando así expuestos a fallos o agujeros de seguridad, mismos que al ser explotados por los hackers, ponen en peligro a todos los funcionarios que siguen usando esta versión de software, el sistema quedará abandonado y los problemas de seguridad crecerán.

Otro de los inconvenientes que eh encontrado es la configuración interna de red, todos los equipos sin excepción disponen de un entorno DHCP, incluyendo al sistema de vigilancia institucional, mismo que es un grave riesgo de seguridad si un usuario malintencionado se conecta a la red.

Los funcionarios de la institución no están formados en materia de ciberseguridad, el internet está lleno de peligros, trampas y virus ocultos. Protegerse de estas amenazas a veces no resulta fácil, no está por demás saber de antemano si una página web que vamos a visitar es segura y si está libre de riesgos para nuestro equipo informático.

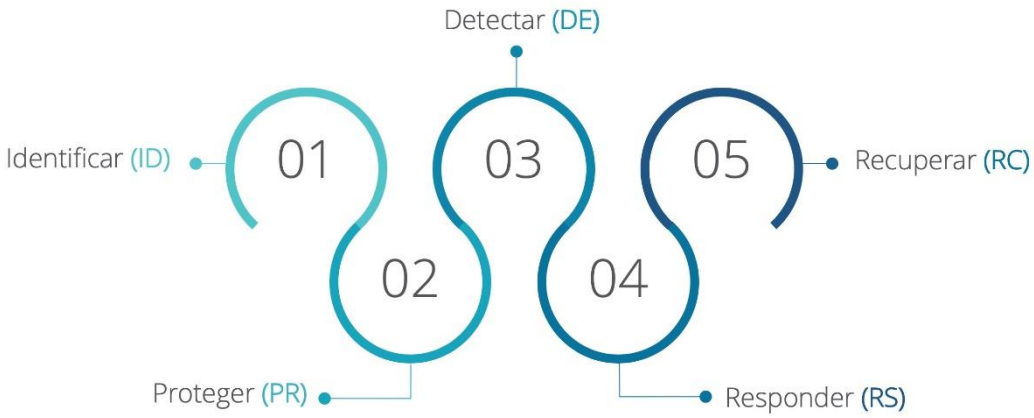
2.2- Métodos específicos de la especialidad a emplear en la investigación:

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, pero también podemos incorporar algunas nuevas reglas que complementen a las ya existentes. Teniendo en cuenta que la seguridad al 100% no existe, pero hay muchas formas de prevenir posibles incidentes, o reducirlos al máximo posible.

2.2.1- Método CSF (Cybersecurity Framework). Este método está enfocado a las empresas de distintos tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos. Les proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

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.

Figura 6. Núcleo de CSF.



Fuente: Instituto Nacional de Normas y Tecnología.

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. La comprensión del contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos relacionados con la ciberseguridad permiten que una organización se centre y priorice sus esfuerzos, de acuerdo con su estrategia de administración de riesgos y sus necesidades comerciales.

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.

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

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.

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. [19]

Prepararse para el futuro tecnológico nunca fue fácil, especialmente cuando se trata de materia de ciberseguridad. El entorno de Tecnologías de la Información siempre ha sido inestable y las amenazas cada vez son mayores, la mejora y el aumento de estrategias en ciberseguridad deberían ser priorizadas en el 2020.

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.

2.2.2.-Estrategias: Para enfrentar estas amenazas, es muy importante identificar tu privacidad, no solo personal sino también a nivel empresarial y por ende la seguridad de la información, y la mejor manera de hacerlo es emplear estrategias de seguridad personal, más confiables y eficientes.

1. **Implementar protocolos de seguridad:** Para protegerse de los ataques de informáticos, las empresas deben crear un protocolo adecuado que los empleados puedan seguir y responder de una manera positiva ante posibles amenazas en la red. Además, es obligación del encargado de TI. Informar a los funcionarios y obligarlos a mantenerse al margen de sitios web no seguros, así como a no abrir ni responder mensajes spam y correos electrónicos de remitentes desconocidos.

   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. **Ad-Blockers:** Esto puede ser una opción para crear una campaña integral de concientización sobre la seguridad cibernética y capacitación, centrada específicamente en los ataques de phishing. Si los funcionarios están bien informados sobre las amenazas de phishing, se darán cuenta de lo que deben observar en términos de protección de seguridad, lo que significa que es más probable que omitan este tipo de mensajes.

Además, se puede implementar ad-blockers en los navegadores de cada uno de los funcionarios, los scripts utilizados en el cryptojacking normalmente provienen de anuncios, por lo que un bloqueador de anuncios puede proporcionar una protección significativa.

3. **Seguir las normas de privacidad de datos:** Esto significa que cada vez más empresas asumirán el reto de garantizar la seguridad de sus datos. Mientras el GDPR (Reglamento General de Protección de Datos) entró en vigencia en el 2018, existe una fuerte expectativa de aumento en los requisitos en todo el mundo. Creemos que la privacidad de los datos seguirá siendo un problema importante en el 2019, por lo que debe cumplir con su misión de seguir las pautas y mantener sus datos confidenciales lo más seguros posible.

2.2.3.- Adopción tecnológica: Las instituciones están adoptando con entusiasmo la innovación tecnológica, y la mayoría dice que los beneficios superan cualquier riesgo que se presente.

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.

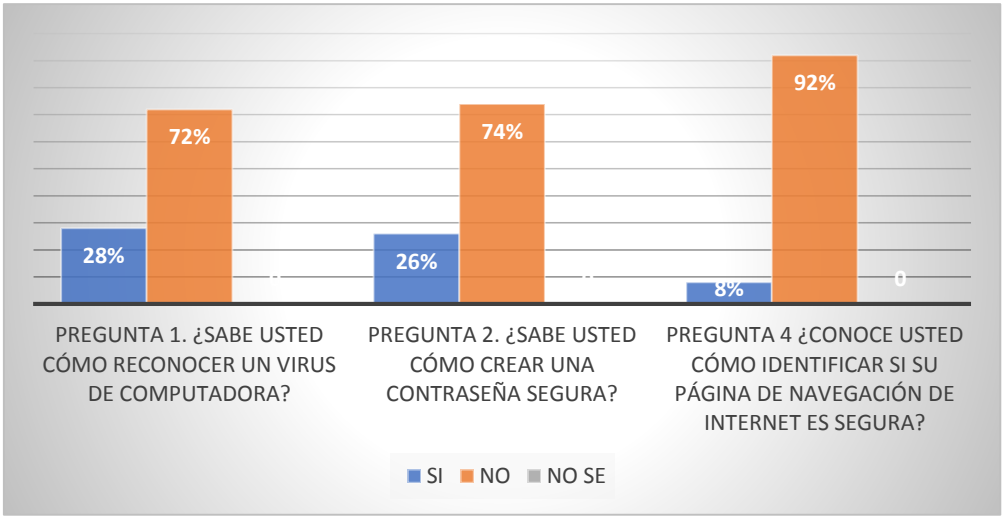
Incluso sectores tradicionales como el de la manufactura esperan que casi el 50% de los productos que desarrollan sean "inteligentes" o "conectados" de alguna manera, según Cisco Network Academi, para el 2020 se tiene previsto la conexión de 50 000 millones de aparatos electrónicos, abriendo nuevos agujeros vulnerables a la seguridad personal.

En el Cuerpo de Bomberos de Latacunga no existen políticas que aplique al buen uso de la tecnología, ni mucho menos conocimientos básicos que orienten a la

ciberseguridad, y por ende a la protección de datos personales de cada uno de los funcionarios.

2.2.4.- Toma de decisiones. A través del método empírico empleado para la obtención de resultados estadísticos, mediante el instrumento aplicado que fue la encuesta, 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.

Figura 7. Resultados de los conocimientos en ciberseguridad del Cuerpo de Bomberos de Latacunga



Elaborado por: David Sangucho Sandoval.

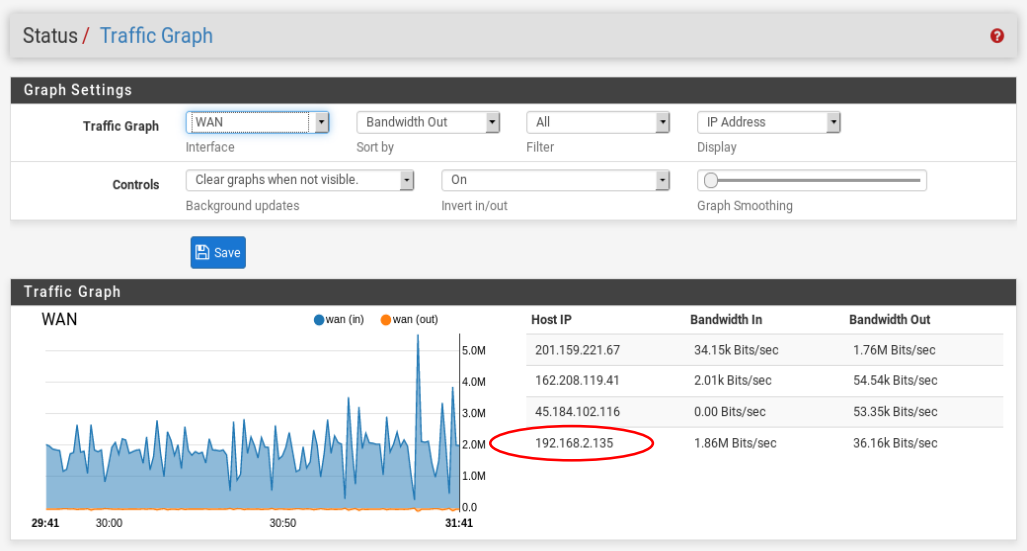
En lo que respecta a la escasez de conocimiento, hay varias brechas de inseguridad, la mayoría de compañías e instituciones no cuentan con personal de Tics, mucho menos con expertos en seguridad de la información, lo que demuestra el desconocimiento en ciberseguridad interna y externa, esto conlleva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

Cuerpo de Bomberos de Latacunga reconoce que carecen de preparación para responder a filtraciones de datos y por ende a estar inmunes a cualquier ataque.

Por esta razón se ve la necesidad de implementar un sistema gestor de seguridad Firewall, en este caso será mediante software, como es **pfSense**.

Mediante las pruebas establecidas en la infraestructura del Cuerpo de Bomberos de Latacunga se ha evidenciado el libre acceso a la red de todo tipo de personas, ya que este carecía de seguridad, dando como resultado el consumo excesivo de ancho de banda en el router marca D-link modelo DIR-615, mismo que provoca lentitud en el internet en las estaciones de trabajo de los funcionarios que pertenecen a la institución.

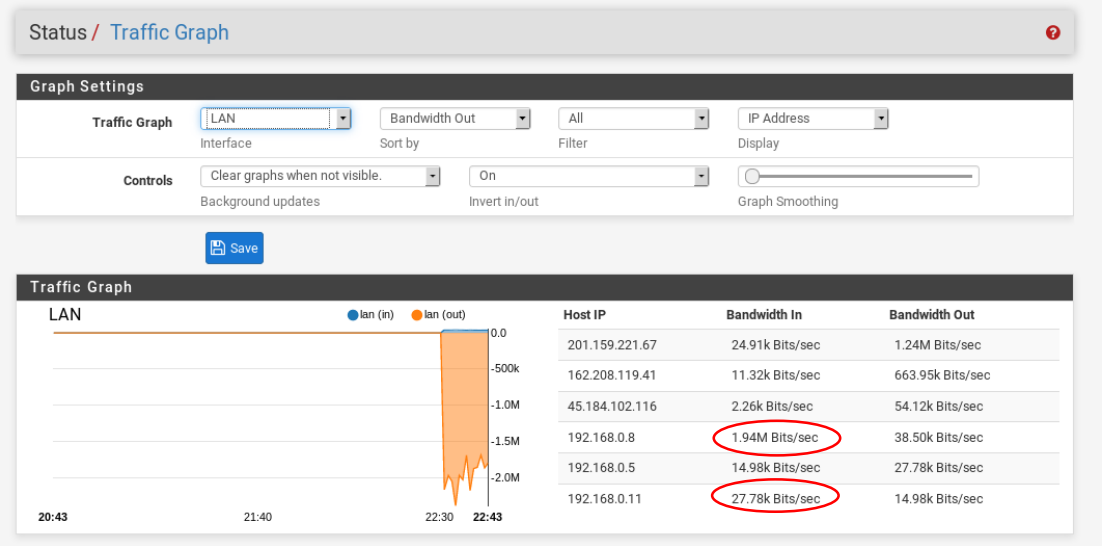
Figura 8. Ancho de banda en la infraestructura del Cuerpo de Bomberos de Latacunga



Elaborado por: David Sangucho Sandoval.

Podemos evidenciar el tráfico de la entrada de infraestructura WAN oscila entre 4 y 5 megas en fibra óptica dando el pico máximo del proveedor, cuya dirección IP pertenece a la 192.168.2.135, donde también se realizó un monitoreo de red, para evidenciar el consumo en la interfaz LAN.

Figura 9. Consumo excesivo de ancho de banda en la LAN del Cuerpo de Bomberos de Latacunga



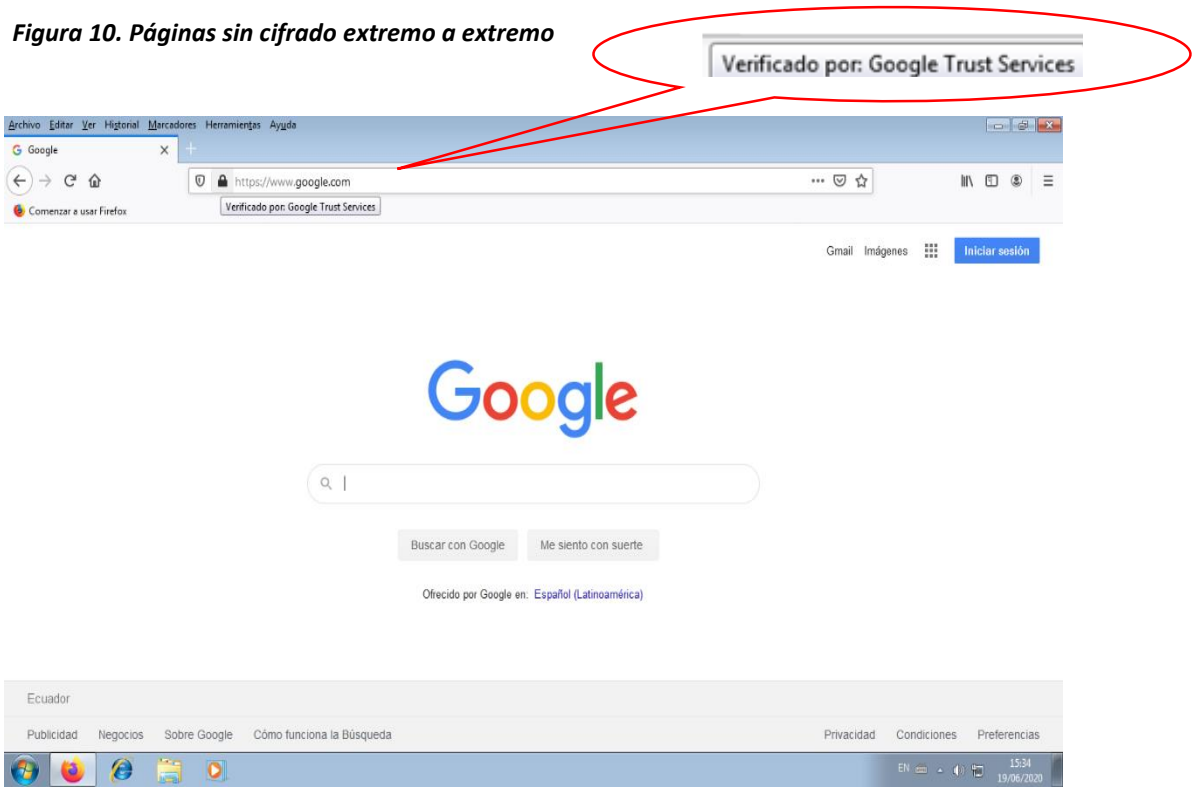
Elaborado por: David Sangucho Sandoval.

La gráfica anterior corresponde a la infraestructura LAN del Cuerpo de Bomberos de Latacunga, donde la dirección correspondiente a la 192.168.0.8, correspondiente al Router, consume la mayoría de ancho de banda, debido a las conexiones sin restricciones, mientras que la dirección IP 192.168.0.11, correspondiente a la estación de trabajo del área financiera, se evidencia que el ancho de banda es apenas 27,7 kb, lo cual ocasiona la inestabilidad en los trabajos diarios de la institución, y el malestar constante de los funcionarios y por ende las quejas hacia el área de sistemas.

Del mismo modo al encontrarse bajo infraestructura crítica el Cuerpo de Bomberos de Latacunga está expuesto a múltiples riesgos y amenazas, como profesionales, conviene reconocer y saber qué es una Infraestructura Crítica de la que depende nuestra calidad de vida y por ende la institución, conocer cómo y con qué criterios se protegen la infraestructura de red, esto nos permitirá detectar nuestras vulnerabilidades, en el Cuerpo de Bomberos de Latacunga, otro problema que se detectó que cómo usuarios de la web nos vemos expuestos a todo tipo de amenazas, siempre que estemos conectados habrá ataques malintencionados que busquen

acceder a nuestros datos aprovechándose de vulnerabilidades en este caso de infraestructura y por ende en las comunicaciones que establecemos día a día.

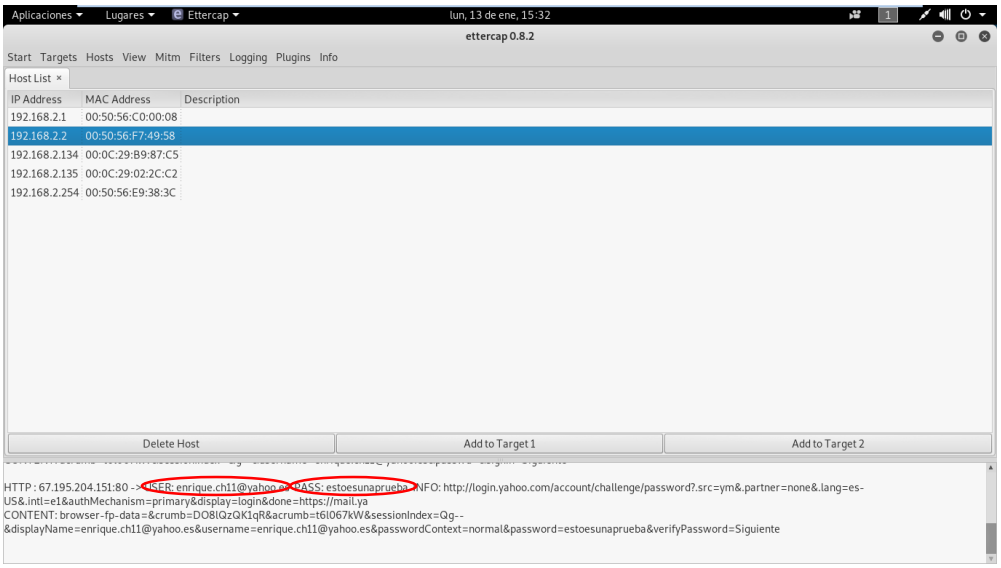
Figura 10. Páginas sin cifrado extremo a extremo



Elaborado por: David Sangucho Sandoval.

Se realizó mediante método de experimentación la simulación de un ataque de tipo MITM por sus siglas en inglés (Man in the middle), que consiste en intervenir la comunicación que establecen dos partes un emisor y un receptor, sin que éstas puedan percibir la intromisión, el atacante puede estar ubicado de forma física o lógica, obteniendo como tal las credenciales de los usuarios, denominado como víctimas, la causa común es la carencia de sistemas de seguridad, y softwares obsoletos.

Figura 11. Robo de credenciales a funcionarios del Cuerpo de Bomberos de Latacunga



Elaborado por: David Sangucho Sandoval.

2.3. Diseño experimental. – La elección de esta metodología se lo realizo mediante las pruebas de validación, El objetivo de esta investigación experimental es descubrir las causas de un fenómeno, en este caso las vulnerabilidades que existen dentro de la institución, dichas pruebas se lo realizaron mediante el procedimiento de denegación de servicios y hombre en el medio.

2.4- Descripción metodológica de la valoración económica, tecnológica, operacional y medio ambiental de la propuesta

2.4.1- Valoración económica. Para la implementación de la propuesta se optó por la utilización de software libre, porque es versátil y practico, se lo puede ejecutar directamente desde un pendrive o un CD player, aparte de ofrecer una versión para máquinas virtuales, en caso que se utilice sistemas virtualizados en tu empresa o en casa, obteniendo una red más segura.

2.4.2- Valoración tecnológica. PfSense es una solución de firewall avanzado de software libre para la implementación en equipos hardware con una potencia equivalente que se equipara a las grandes soluciones de firewall del mercado, sus productos se basan en las plataformas más

fiables y están diseñados para proporcionar los más altos niveles de rendimiento, estabilidad y confianza.

2.4.3- Valoración ambiental. La manipulación y el funcionamiento de este tipo de dispositivos, son amigables con del entorno natural y las nuevas alternativas de cambio con tecnología verde, están ayudando mucho a cambiar un escenario que se prevé difícil para el medio natural, la tecnología y el medio ambiente son dos áreas que están más relacionadas de lo que nos podemos llegar a imaginar. Es así que al implementar esta solución encontramos la manera en la que la tecnología forme parte de la solución y no del problema.

2.5. Conclusiones Capítulo II.

- El Cuerpo de Bomberos de Latacunga no está preparado para enfrentar una ola de ataques con distintos niveles de sofisticación, lo que provoca que la institución esté abierta a ataques, cuyos resultados pueden ser dañinos a su reputación y por ende el resultado será la pérdida de datos.
- El Cuerpo de Bomberos de Latacunga carece de conocimientos de ciberseguridad, no cuenta con estrategias que orientes a sus funcionarios a asumir la responsabilidad de proteger los activos institucionales contra las amenazas cibernéticas.
- Otro de los problemas en la institución es el uso de software obsoleto, y por ende el descuido en la actualización de parches de seguridad o migración de sistemas operativos recomendados por el fabricante, donde se presenta una oportunidad que personas mal intencionadas puedan causar pérdida y exposición de datos confidenciales.

CAPÍTULO III. APLICACIÓN Y/O VALIDACION DE LA PROPUESTA

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.

El cambio no solo es asociado a las distintas políticas y a los procedimientos, sino también a las capacidades humanas para estar preparados y poder responder ante un ataque informático.

3.1- Resultados del diagnóstico del problema realizado. Los resultados obtenidos con la implementación de este Software pfsense cumplen estándares de calidad, ya que aparte de ser un software Open Sourse, es gratuito, y 100% confiable y seguro.

Todos los paquetes son filtrados por el servidor de seguridad pfSense para validar la información entre las direcciones de origen y destino, para luego ser verificadas por las reglas definidas por el administrador para determinar si los paquetes deben ser reenviados o bloqueados.

Un firewall viene siendo como un cuello de botella por el que todo el tráfico de Internet entrante y saliente debe pasar, para poder ser controlado, un cortafuegos bien instalado, configurado y administrado evitan en gran escala que los hackers puedan acceder hacia la red LAN y por supuesto ayudan a mantener a salvo los datos confidenciales de su empresa.

Un firewall trabaja como un agente de seguridad quien identifica cada paquete de datos antes de que este le permita el acceso, actúa como "barrera" manteniendo a un lado a los usuarios sin autorización, controla el uso de Internet, bloqueando o desbloqueando accesos inapropiados o apropiados.

3.1.1.- Técnica de investigación

3.1.1.1.- Entrevista

Esta técnica utilizada para la llegar al problema se lo aplico a toda la población del Cuerpo de Bomberos de Latacunga, es decir a 53 funcionarios que laboran en la mencionada institución, misma que arrojo información necesaria para poder realizar la implementación de un gestor de seguridad.

3.1.1.2. Resultados del diagnóstico del problema. – Una vez validado el instrumento técnico en mi propuesta metodológica en el Cuerpo de Bomberos de Latacunga, se ve la necesidad de solventar estos inconvenientes de acuerdo a los resultados obtenidos mediante la tabulación de datos de cada una de las preguntas reflejadas en la encuesta dirigida hacia los servidores de la institución en mención.

Los funcionarios tienen dificultades con respecto a al reconocimiento de virus en sus ordenadores, cuando navegan en la red no identifican si una página es segura o no, de igual manera las contraseñas utilizadas en sus cuentas personales son de poca seguridad y no las cambian periódicamente.

Figura 12. Vulnerabilidades en la infraestructura del Cuerpo de Bomberos de Latacunga

Elaborado por: David Sangucho Sandoval.

3.2 Resultados de los métodos específicos. Una vez realizada la encesta a los funcionarios del Cuerpo de Bomberos de Latacunga, se procedió al análisis de cada una de las preguntas planteadas, donde se analizó cada uno de los requerimientos para la implementación de un sistema gestor de seguridad, que garantice no solo la protección de información, sino que también sirva como base fundamental en los funcionarios de la institución y tomen conciencia al momento de estar frente a una amenaza cibernética.

Para la implementación de un sistema gestor de seguridad (pfSense) se garantiza que es uno de los mejores sistemas operativos orientado a firewall, este SO está basado en FreeBSD y tiene una gran cantidad de usuarios por todo el mundo, aunque su uso es gratuito, la empresa que está detrás proporciona equipos hardware para ser utilizados como firewall en pequeñas y medianas empresas.

Con la implementación de este software que protege el exterior con el interior de una red, se establece que a pesar de que cualquier empresa está expuesta a sufrir cualquier tipo de ataque, decidir no protegerse y reducir la inversión que se realiza en ciberseguridad hace a cualquier organización más vulnerable y, por tanto, con más posibilidades de sufrir un ciberataque.

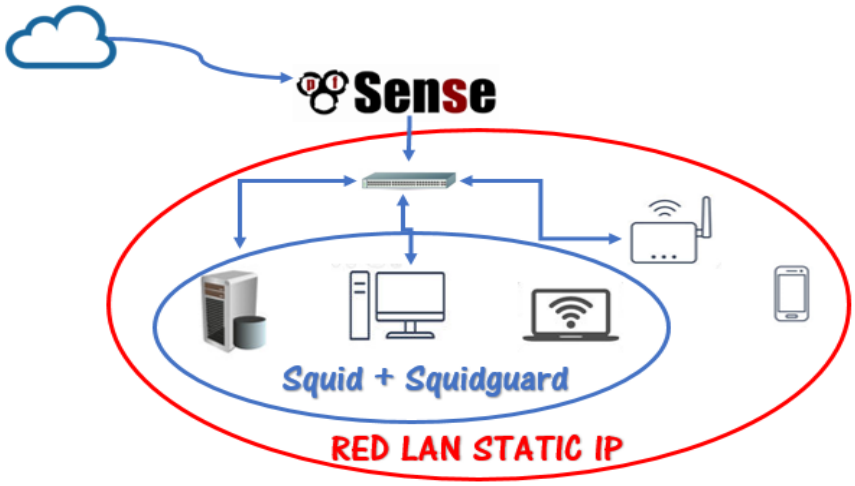
Su instalación y configuración nos permite configurar acorde a las necesidades institucionales, tales como servidor VPN, portal cautivo, etc., en este caso implementar funciones de Firewall dentro de nuestra red.

Bajo este criterio se determina usar una de sus principales características que es un servidor proxy bajo su herramienta SQUID.

1. Configuración de IP estática en la red LAN.
2. Creación de certificados de seguridad SSL para conexiones web.
3. Ejecución de certificados para validación de Squid en cada estación de trabajo para filtración de tráfico https.
4. Configuración de Squid Proxy utilizando Man in the middle mediante el puerto 3128, con filtración de protocolos http y https para capturar el tráfico del puerto 80 y 443.

5. Configuración de Squidgard para filtrado web por listas negras, esto quiere decir que tenemos una gran lista de urls y dominios al que podemos denegar o permitir acceso al usuario, que contienen virus y que hay páginas que se dedican a instalar spyware.

Figura 13. Arquitectura pfSense del Cuerpo de Bomberos de Latacunga



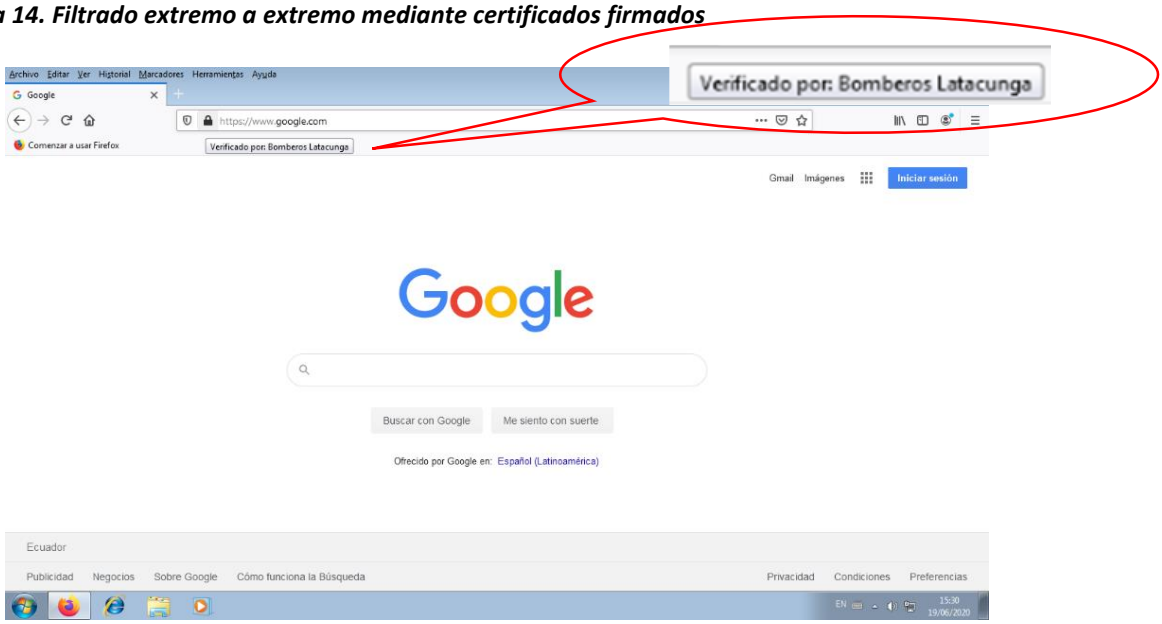
Elaborado por: David Sangucho Sandoval.

3.3. Resultado del diseño experimental que demuestra la validación de la propuesta. - Después de la implementación de este software (FIREWALL), en la LAN del Cuerpo de Bomberos de Latacunga, donde nos permite filtrar en su totalidad el tráfico entrante y saliente entre estas dos redes LAN y WAN, si el tráfico entrante o saliente cumple con una serie de Reglas establecidas por la herramienta Squid + Squidguard, entonces el tráfico podrá acceder o salir de nuestra red o HOST sin restricción alguna. En caso de no cumplir las mismas el tráfico entrante o saliente será bloqueado.

La metodología a aplicar en esta investigación es el método experimental, donde trata de un proceso que se utiliza para investigar fenómenos, adquirir nuevos conocimientos o corregir e integrar conocimientos previos. Se utiliza en 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.

Mediante la aplicación de la metodología experimental se procede a realizar las pruebas de implementación, dando como resultado el filtrado extremo a extremo, mediante las políticas de conexión de paquetes SSL, mismo que Pfsense desvía los paquetes al servidor proxy, donde analiza las reglas de Squid.

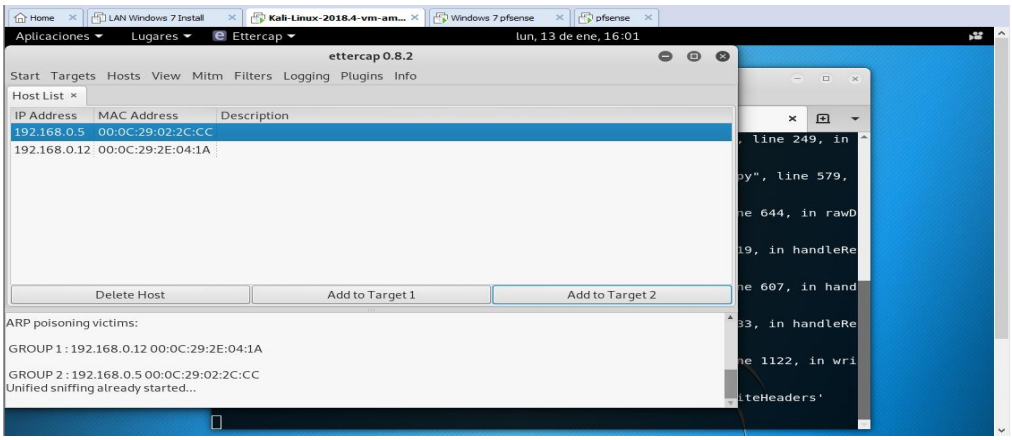
Figura 14. Filtrado extremo a extremo mediante certificados firmados



Elaborado por: David Sangucho Sandoval.

3.4. Pruebas del software. – Se procede a realizar las pruebas correspondientes empleando estrategias de **hacking ético,** donde con el software Pfsense, cumple con las reglas de firewall, mismo que no permite el acceso, denegando al atacante obtener las credenciales del usuario.

Figura 15. Pruebas MITM con Squid en pfSense en la LAN del Cuerpo de Bomberos de Latacunga

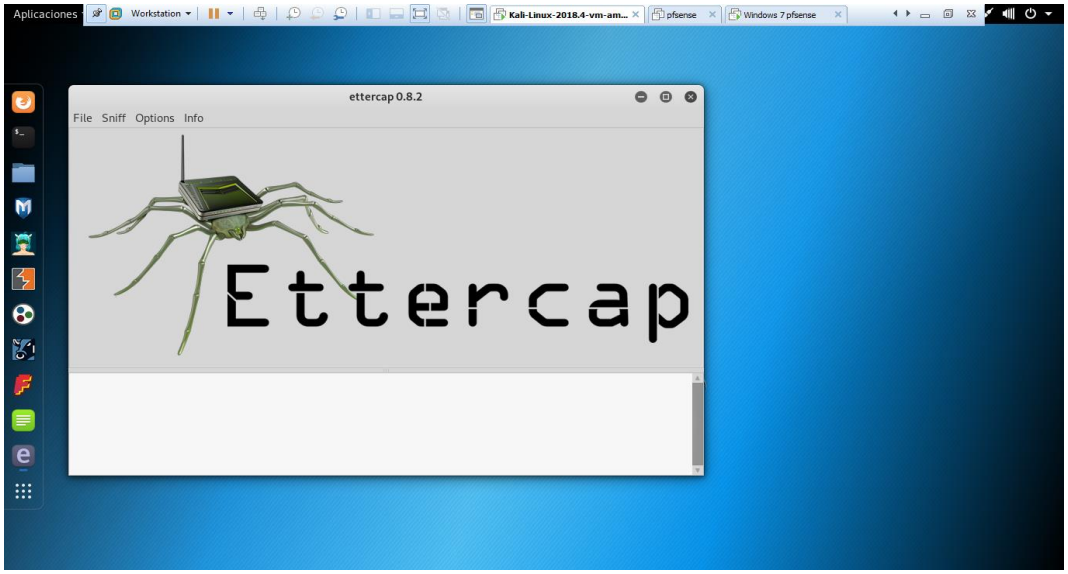


Elaborado por: David Sangucho Sandoval.

Los detalles completos de las pruebas del software se encuentran detalladas en el Anexo 4.

3.5. Validación de la propuesta. – Se realizan las pruebas correspondientes de funcionamiento antes, como después de la implementación del software gestor de seguridad, mediante la herramienta ETTERCAP, donde se obtiene los resultados esperados, mediante la utilización de hacking ético (hacker de sombrero blanco), permitiéndonos identificar y reparar posibles vulnerabilidades, lo que previene eficazmente la explotación por hackers maliciosos (hacker de sombrero negro).

Figura 16. Herramienta utilizada para ataques MITM



Elaborado por: David Sangucho Sandoval.

Para la validación de la propuesta se utilizó herramientas que se detallan a continuación:

- Computador con sistema operativo Linux en su distribución Kali versión 2018.4. (atacante)
- 2 computadores con sistema operativo Windows 7 (victimas)
- Computador son sistema operativo pfSense
- Conexión a internet

Los resultados correspondientes se detallan en el Anexo 3 y 4.

3.6. Valoración de la propuesta. - Para valoración de la propuesta en el Cuerpo de Bomberos de Latacunga se considera analizar desde los siguientes puntos de vista:

- Económico
- Tecnológico
- Ambiental

3.6.1 Valoración económica. – Para la implementación del sistema gestor de seguridad se ha tomado en cuenta los siguientes entornos.

3.6.1.1 Gastos directos

Tabla 2. Gastos directos.

DETALLE	CANTIDAD	V. UNITARIO	TOTAL
Computadores	4	$ 450	$ 1800
Licencias Windows (incluido con el hardware)	2	$ 0	$ 0
Licencias pfSense	1	$ 0	$ 0
Licencia Kali	1	$ 0	$ 0
Navegadores	2	$ 0	$ 0
Internet	1 año	$ 25	$ 300
TOTAL			**$ 2100**

Elaborado por: David Sangucho Sandoval.

El valor de la implementación del software gestor de seguridad del Cuerpo de Bomberos de Latacunga asciende los $2.100,00 que ha sido obtenido mediante el Hardware utilizado para realizar las pruebas correspondientes.

Tabla 3. Gastos directos.

DETALLE	CANTIDAD	V. UNITARIO	TOTAL
Resma de papel bond	2	$ 4	$ 8
Cuaderno	$ 2	$ 1.50	$ 3
Impresiones	500	$ 0.05	$ 25

Copias	100	$ 0.05	$ 5
Lápiz	2	$ 0.50	$ 1
Borrador	2	$ 0.30	$ 0, 60
Esferos	2	$ 0.50	$ 1
Carpeta	5	$ 0.80	$ 4
Anillados	8	$ 1.00	$ 8
TOTAL			**55.60**

Elaborado por: David Sangucho Sandoval.

3.6.1.2 Gastos indirectos.

Tabla 4. Gastos indirectos.

DETALLE	TOTAL
Movilización	$ 200
Alimentación	$ 80
TOTAL	$ 280

Elaborado por: David Sangucho Sandoval.

3.6.1.3 Gastos Totales.

Tabla 5. Gastos totales.

DETALLE	TOTAL
Total gastos directos	$ 2155.60
Total gastos indirectos	280
Imprevistos	200
TOTAL	$ 2635.60

Elaborado por: David Sangucho Sandoval.

3.7. Valoración tecnológica. Con la implementación de este sistema gestor de seguridad en el Cuerpo de Bomberos de Latacunga estamos aportando en la optimización del acceso a Internet, se está administrando los accesos de la red

LAN hacia la WAN, centralizando los accesos y controlando la seguridad de la institución, con esta solución cumplimos estándares de calidad y a su vez utilizamos licencias Open Sourse y lo configuramos específicamente para operar en su potente plataforma firewall y su administración es totalmente amigable desde la interfaz web, también se economiza costos en el mismo instante que se configura de una manera adecuada transformamos un ordenador común en un potente firewall eficaz y seguro.

3.8. Valoración ambiental. - 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, de ahí partimos en la implementación de este sistema gestor de seguridad para el Cuerpo de Bomberos de Latacunga que no tendrá ningún impacto malicioso con el medio ambiente.

3.9 Discusión de la Aplicación y Validación de la propuesta. – A lo largo de la investigación de esta propuesta a favor del Cuerpo de bomberos de Latacunga se pudo evidenciar ciertas vulnerabilidades dentro de la institución, donde al no existir barreras de seguridad, así como también el libre acceso a la navegación web, acceso público hacia la red institucional, misma que estaba siendo un blanco preciso a terceras personas no autorizadas capten la señala wifi y por lo tanto provocaban reducción de velocidad de carga de datos de Internet y generando mal estar en los funcionarios al momento de acceder a las plataformas institucionales de atención al público.

Todo este análisis se obtuvo mediante un estudio minucioso hacia la infraestructura institucional, es ahí donde nace la necesidad de implementar un sistema Gestor de seguridad (firewall) que garantice la seguridad de los datos institucionales, así como también el uso adecuado del internet, estableciendo políticas de seguridad (reglas) a través del software implementado (pfSense).

Otro agujero de seguridad se filtró en 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.

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.**

3.10- Conclusiones del capítulo III.

- Con la implementación del sistema gestor de seguridad se priorizaron las páginas de navegación de ciertos funcionarios que acceden a páginas institucionales para brindar servicio a la comunidad.
- La ejecución de certificados firmados mediante pfSense se logró el cifrado extremo a extremo entre el cliente y el servidor.
- Con la implementación de este software se brindará las diversas necesidades de seguridad de la información y comunicación dentro de la red LAN, así como también se tendrá una puerta de control de accesos que comunica la red WAN con la red LAN, también se controlará el acceso a la navegación e ingreso a ciertos sitios.
- Su interfaz de pfSense es sencilla, tanto la parte de instalación por consola como el configurador web.
- Las características necesarias para el uso de este sistema son de requerimientos mínimos de hardware, esto es una de las ventajas principales para la institución, ya que no hay necesidad de adquirir un computador de última tecnología, puesto que dentro del parque informático de la institución existe Hardware en el cual se puede realizar la instalación y configuración.

Conclusiones generales.

- El poco conocimiento de los funcionarios sobre materias de ciberseguridad mantenía un margen de inseguridad en la infraestructura institucional.
- 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.
- Aunque la empresa no disponga de acceso a Internet, se debería establecer políticas de seguridad para la red interna y de esta manera administrar todo el acceso de los funcionarios a sitios específicos de la red y proteger la información.

Recomendaciones.

- Establecer políticas de respaldo continuo de información.
- Se recomienda al encargado de TIC's monitorear las actividades del firewall, así como también la modificación de reglas establecidas dentro del mismo.
- Se recomienda al administrador del firewall actualizar constantemente la lista de sitios denegados de navegación para evitar filtraciones de páginas no deseadas.
- Verificar los diferentes elementos de seguridad y configuraciones en los sistemas operativos y tener en cuenta las políticas de seguridad y la buena configuración del sistema que permita tener un grado de confianza para poder generar un buen funcionamiento en los ordenadores.
- Ejecutar los certificados de seguridad firmados por el software pfSense una vez que se haya migrado o cambiado de sistema operativo, para que el ordenador siga siendo protegido en su totalidad.

Bibliografía

[1] Robert Vargas Borbúa, Rolando P. Reyes Chicango, Luis Recalde Herrera, «Ciberdefensa y ciberseguridad, más allá del mundo virtual,» *Latinoamericana de Estudios de Seguridad,* pp. 31-45, 2017.

[2] C. C. N. d. España., «CCN-CERT IA-09/16 Ciberamenazas 2015/Tendencias 2016,» *CCN-Cert,* 2015-2016.

[3] P. &. F. A. Singer, *Cibersecurity and Cyberwar,* 2014.

[4] R. V. H. L. R. &. R. R. Borbúa, «Ciberdefensa y ciberseguridad,» *Revista Latinoamericana de Estudios de Seguridad,* 2017.

[5] S. C, « Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier.,» *Revista Latinoamericana de Estudios de Seguridad,* p. 8, 2017.

[6] G. SACK y J. S. IERACHE, «Controles de seguridad propuesta inicial de un framework en el contexto de la ciberdefensa,» *XXI Congreso Argentino de Ciencias de la Computación,* 2015.

[7] B. F. J. ADRIÁN, «Diseño e implementación de un firewall l2 utilizando redes definidas por software,» p. 8, 2016.

[8] Agesic, *Marco de ciberseguridad,* 2018.

[9] ANTONIO INOGUCHI ROJAS, ERIKA LIZET MACHA MORENO, «GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ,» 2016.

[10] «Crowe,» 02 04 2018. [En línea]. Available: http://aechile.cl/2016/10/06/ciberseguridad-una-necesidad-del-mundo-actual/. [Último acceso: 14 10 2019].

[11] 25 10 2018. [En línea]. Available: https://administracionvirtualdotblog.wordpress.com/2018/10/25/primera-entrada-del-blog/. [Último acceso: 15 10 2019].

[12] «Telefónica,» 2019. [En línea]. Available: https://www.fundaciontelefonica.com/empleabilidad/. [Último acceso: 16 10 2019].

[13] E. Cárdenas, «Anatomía de un ataque informático,» 2012.

[14] A. V. Fernández, «La Ciberseguridad en España 2011 – 2015,» 2015.

[15] J. P. E. Morocho, «Implementación de un Firewall sobre plataforma LINUX en la empresa de contabilidad Armas&Asociados,» 2013.

[16] M. Á. Mendoza, «Por qué es necesario el firewall en entornos corporativos,» *Welivesecurity.com,* 2014.

[17] J. Jiménez, «Qué es un firewall y por qué es importante para nuestra seguridad,» *redeszone.net,* 2017.

[18] Caiza D Cisnero A, Méndez P Villa H., «Implementación de un prototipo como,» *Cumbres,* pp. 9-16, 2017.

[19] https://www.nist.gov/cyberframework/online-learning/five-functions.

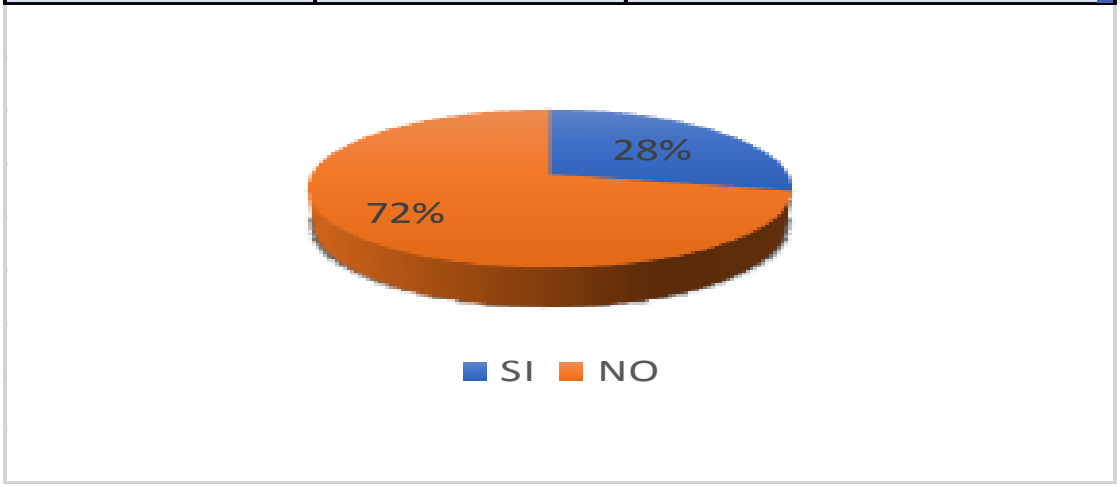
ANEXO 1

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA ENCUESTA

Encuesta dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

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

OPCIÓN	VALOR	PORCENTAJE
SI	15	28%
NO	38	72%
TOTAL	53	100%



Análisis de datos

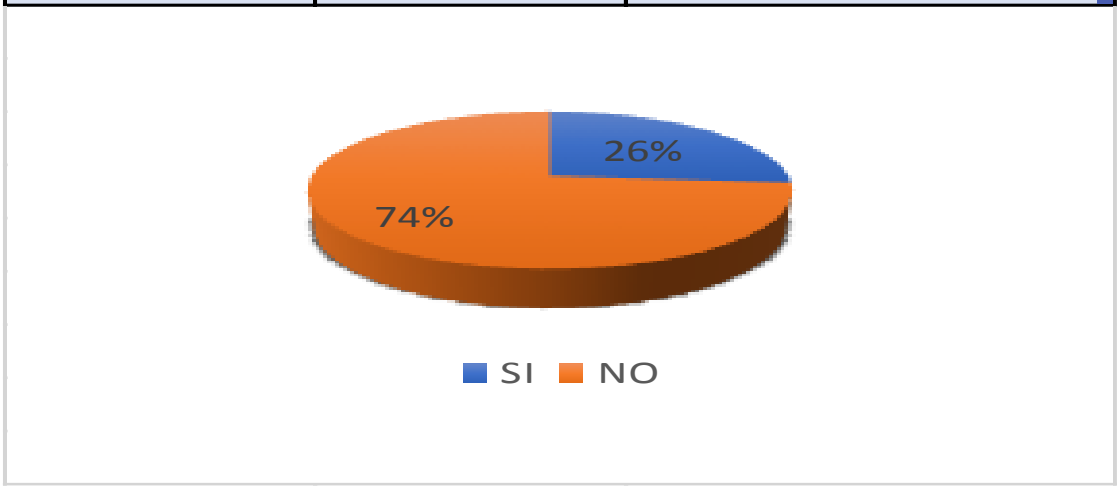
El 100% de los funcionarios encuestados corresponden a un total de 53 personas que, al momento de responder esta pregunta, 15 personas correspondiente al 28% tienen conocimientos claros sobre como reconocer un virus de computadora, mientras que el 72% de funcionarios no tienen conocimientos sobre como identificar un virus.

Interpretación de resultados

De la encuesta realizada claramente se puede evidenciar que el 72% de los funcionarios están siendo un blanco perfecto ante una amenaza cibernética.

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

OPCIÓN	VALOR	PORCENTAJE
SI	14	26%
NO	39	74%
TOTAL	53	100%



Análisis de datos

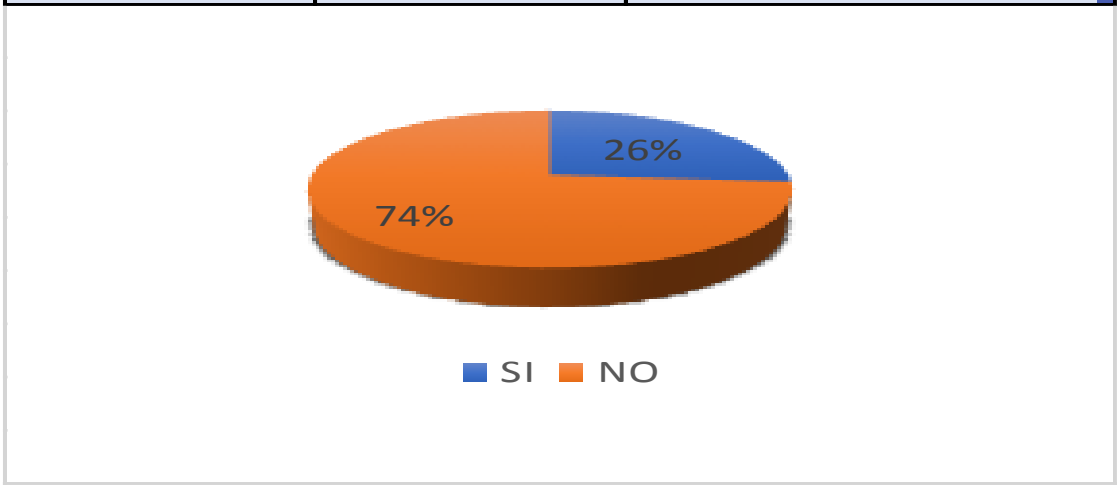
Del 100% de funcionarios encuestados, solo 14% de los mismos tiene conocimientos de sobre cómo crear una contraseña segura, mientras que el 74% correspondiente a los 39 funcionarios respectivamente no tienen conocimientos sobre los caracteres a utilizar para generar una contraseña segura.

Interpretación de resultados

De los resultados obtenidos de esta pregunta se refleja claramente que la mayoría de funcionarios no están familiarizados en crear contraseñas seguras que garanticen el ingreso seguro a sus cuentas personales, simplemente utilizan contraseñas de nivel de seguridad bajo, mismos que estas propensos a ser violentadas.

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

OPCIÓN	VALOR	PORCENTAJE
SI	14	26%
NO	39	74%
TOTAL	53	100%



Análisis de datos

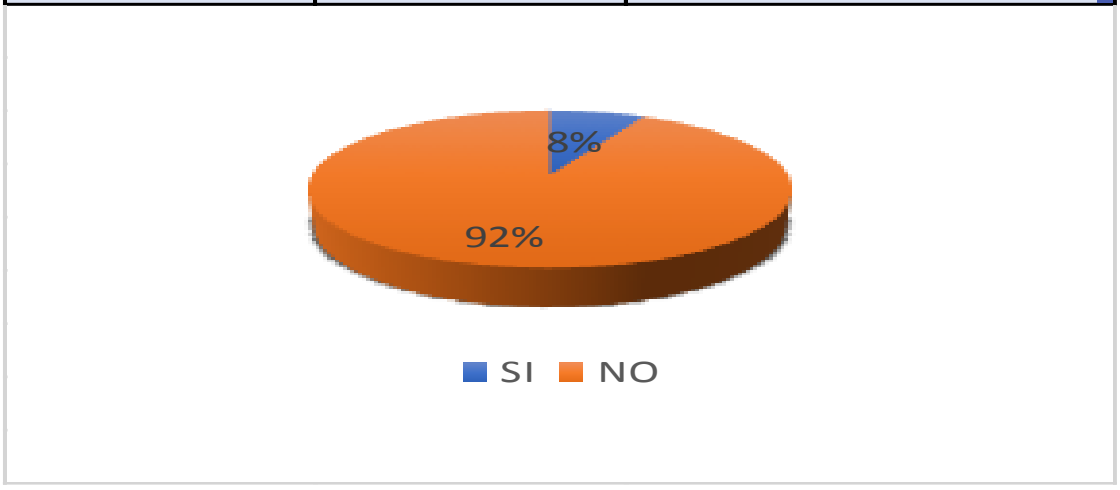
De acuerdo al 26% de los resultados positivos de esta pregunta, 14 funcionarios cambian frecuentemente las contraseñas de sus cuentas personales, mientras que el 74% no realiza este proceso.

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 no hay conocimientos en crear una contraseña segura lógicamente reduce la preocupación de cambiar frecuentemente sus contraseñas personales.

PREGUNTA 4 ¿Conoce usted cómo identificar si su página de navegación de internet es segura?

OPCIÓN	VALOR	PORCENTAJE
SI	4	8%
NO	49	92%
TOTAL	53	100%



Análisis de datos

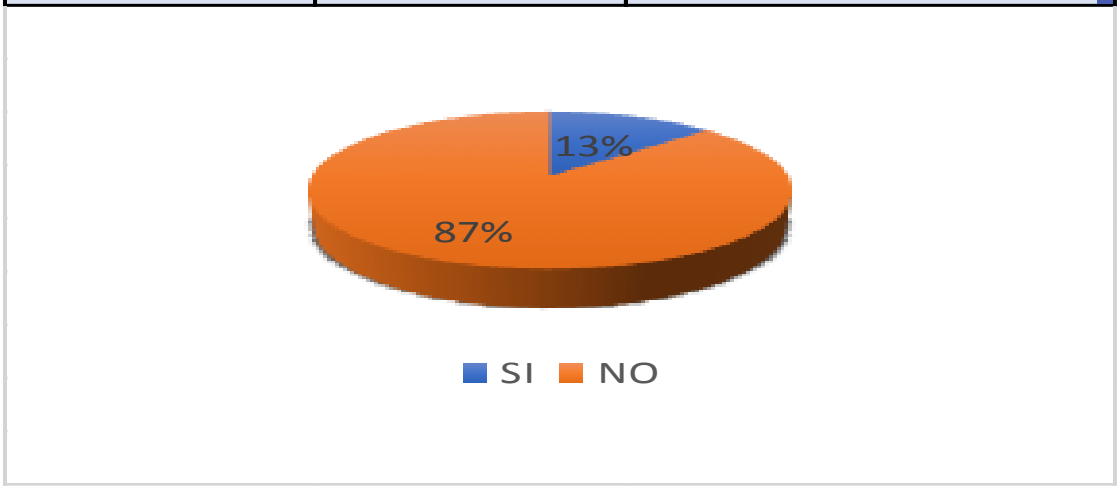
De un total de 53 funcionarios que laboran en el Cuerpo de Bomberos de Latacunga, solo 8% de personas son capaces de poder identificar una página segura dentro del navegador de internet, mientras que el 92% del personal desconoce de este tema.

Interpretación de resultados

Según la interpretación de datos en esta pregunta la mayoría de funcionarios no están formados en entornos de seguridad informática, ya que, siendo una institución pública, la mayoría de funcionarios deberían estar con un nivel de conocimientos informáticos medio, en entornos de navegación web, y así evitar la propagación de virus en la infraestructura institucional.

PREGUNTA 5 ¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?

OPCIÓN	VALOR	PORCENTAJE
SI	7	13%
NO	46	87%
TOTAL	53	100%



Análisis de datos

Según los resultados obtenidos en la encuesta aplicada en el Cuerpo de Bomberos de Latacunga, el 7% de funcionarios alguna vez respondieron positivamente a esta pregunta, mientras que el 87% de la institución hizo caso omiso a este tipo de virus informático.

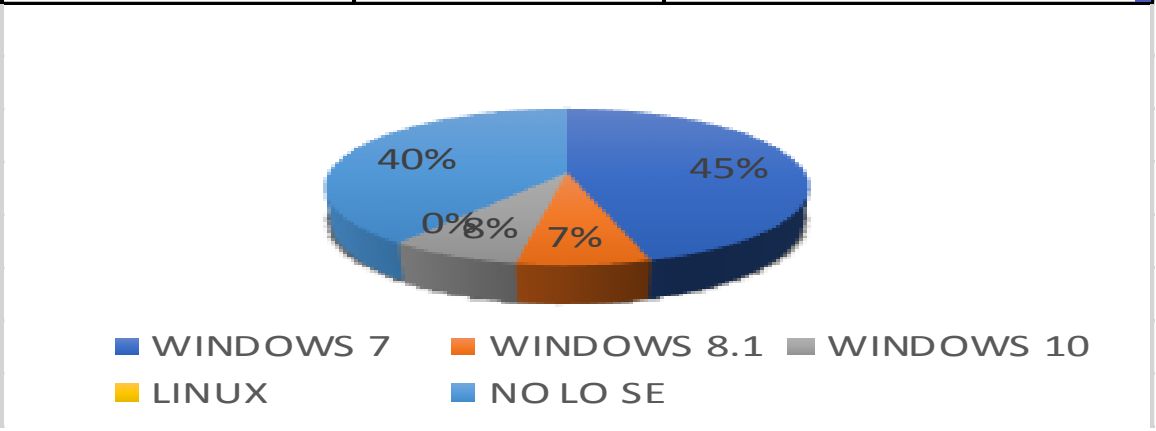
Interpretación de resultados

Según el análisis de datos en esta pregunta podemos apreciar que el 13% de funcionarios no distingue un correo fraudulento y entrega sus credenciales a los ciberdelincuentes, sin saber que están siendo objeto de robo de información no solo personal si no institucional, infección de dispositivos, pérdidas económicas, entre otros.

Mientras que el 87% de los funcionarios están conscientes de que este tipo de corros son Span.

PREGUNTA 6 ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

OPCIÓN	VALOR	PORCENTAJE
WINDOWS 7	24	45%
WINDOWS 8.1	4	8%
WINDOWS 10	4	8%
LINUX	0	0%
NO LO SE	21	40%
TOTAL	53	100%



Análisis de datos

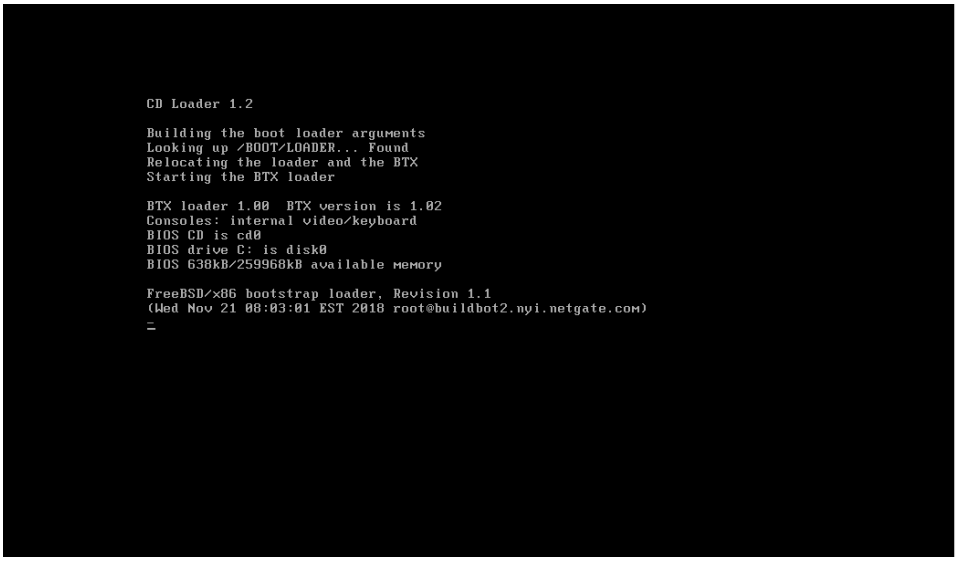
Según los resultados obtenidos en la encuesta podemos observar que en la actualidad existe una mayor cantidad de usuarios con Windows 7, a esto se asemeja un porcentaje similar, que no distingue el Sistema Operativo instalado en su computador.

Interpretación de resultados

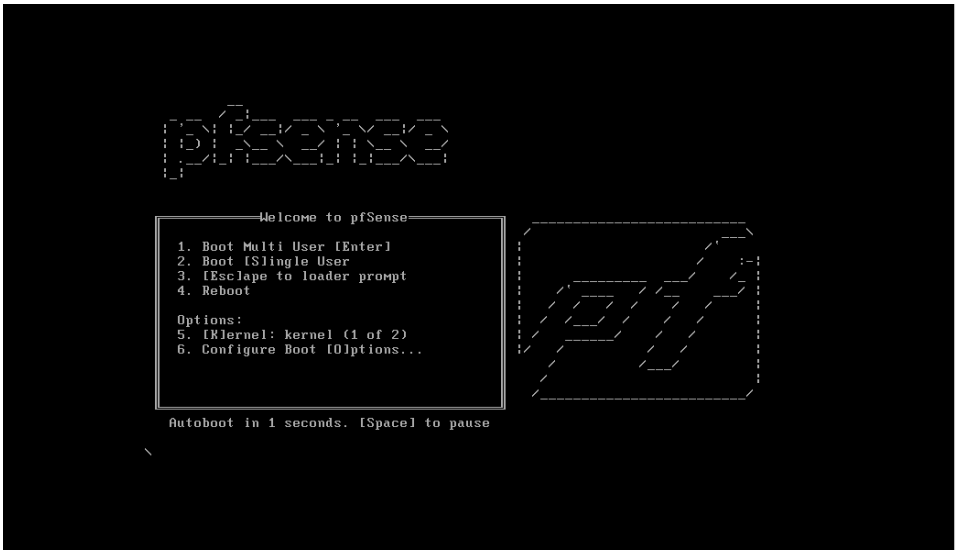
De acuerdo a los datos obtenidos en esta pregunta podemos apreciar que un 45% de funcionarios tiene instalado como Sistema Operativo Windows 7 en sus ordenadores, lo que significa que para este año las vulnerabilidades van a aumentar en un porcentaje mayor al del año 2019, debido a que en Enero del 2020, Microsoft deja de brindar soporte técnico a este Sistema Operativo, mientras que el 40% de funcionarios no tiene conocimientos bajo que plataforma está trabajando su ordenador, bajo este criterio la institución se ve en una alta probabilidad de riesgo, debido a que los funcionarios no están preparados en su totalidad sobre temas tecnológicos.

ANEXO 2

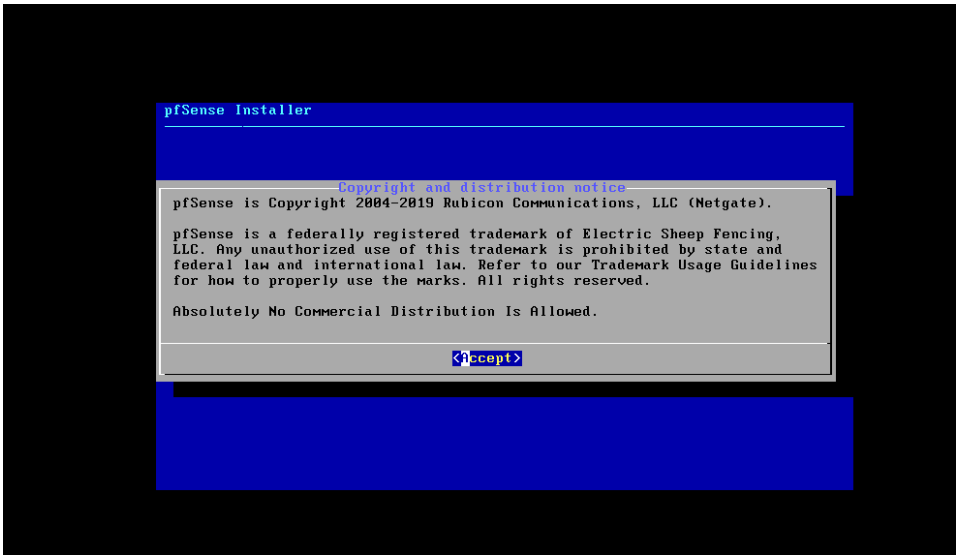
INSTALACIÓN DE PFSENSE



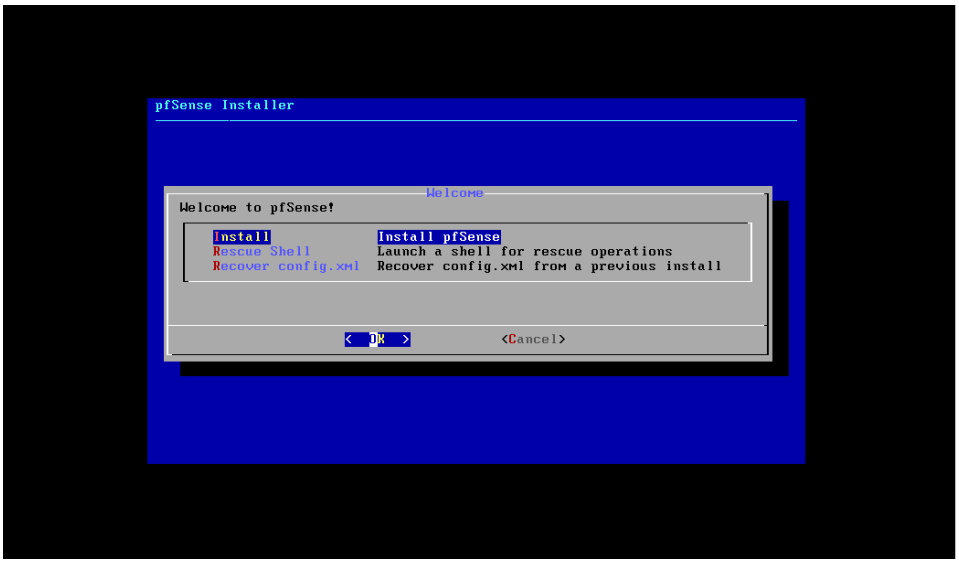
Inicialización del instalador



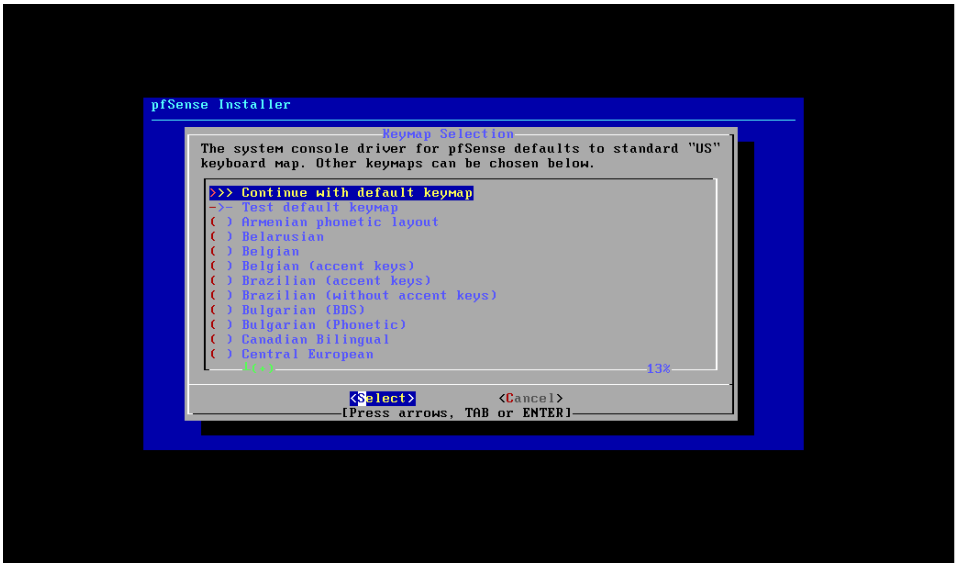
Aceptación de términos



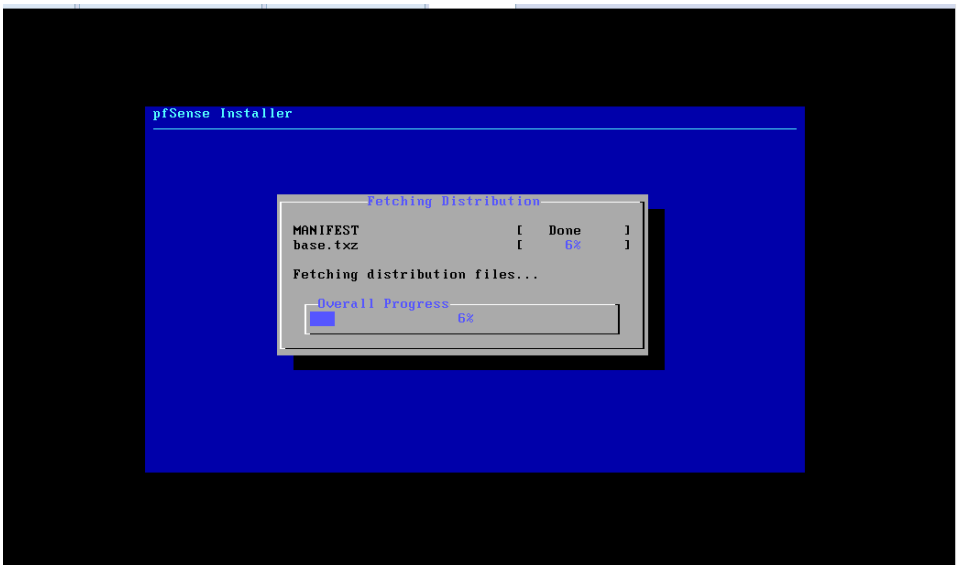
Selección de opción a ejecutar



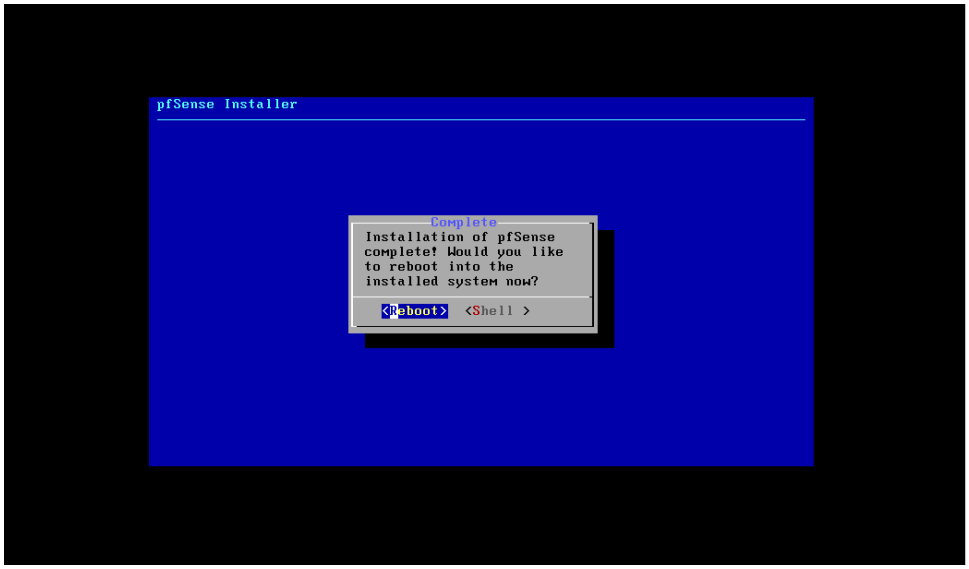
Selección de opción de instalación



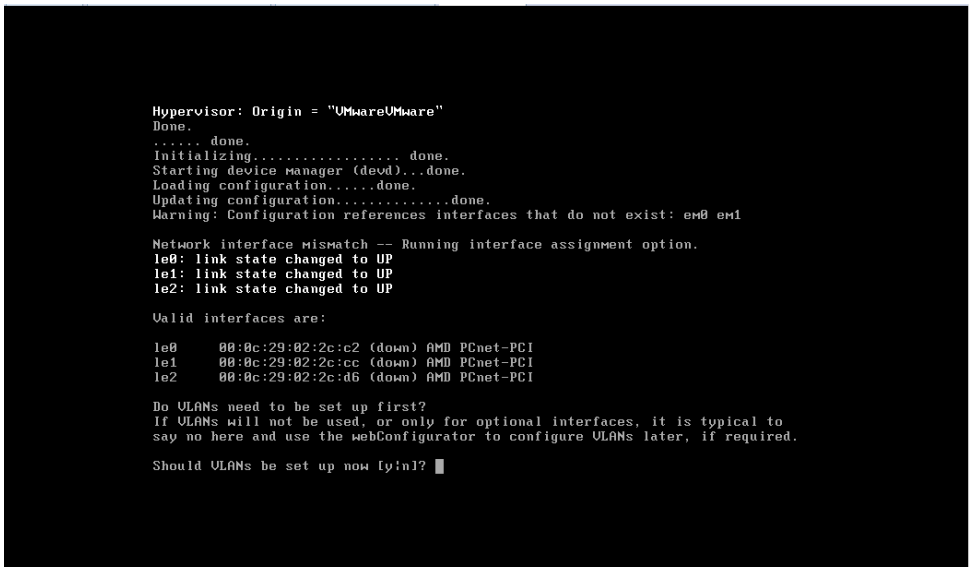
Proceso de instalación



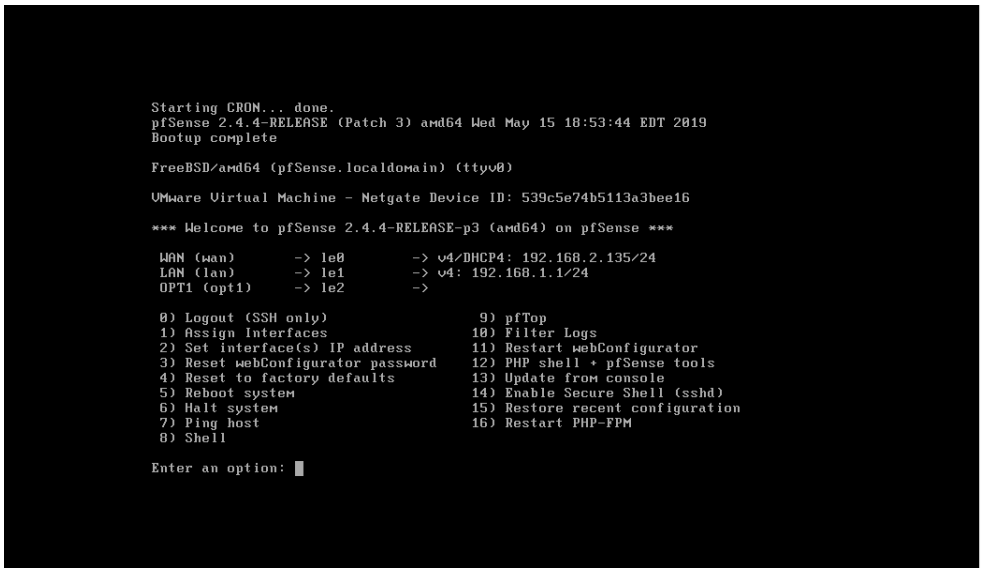
Finalización de la instalación



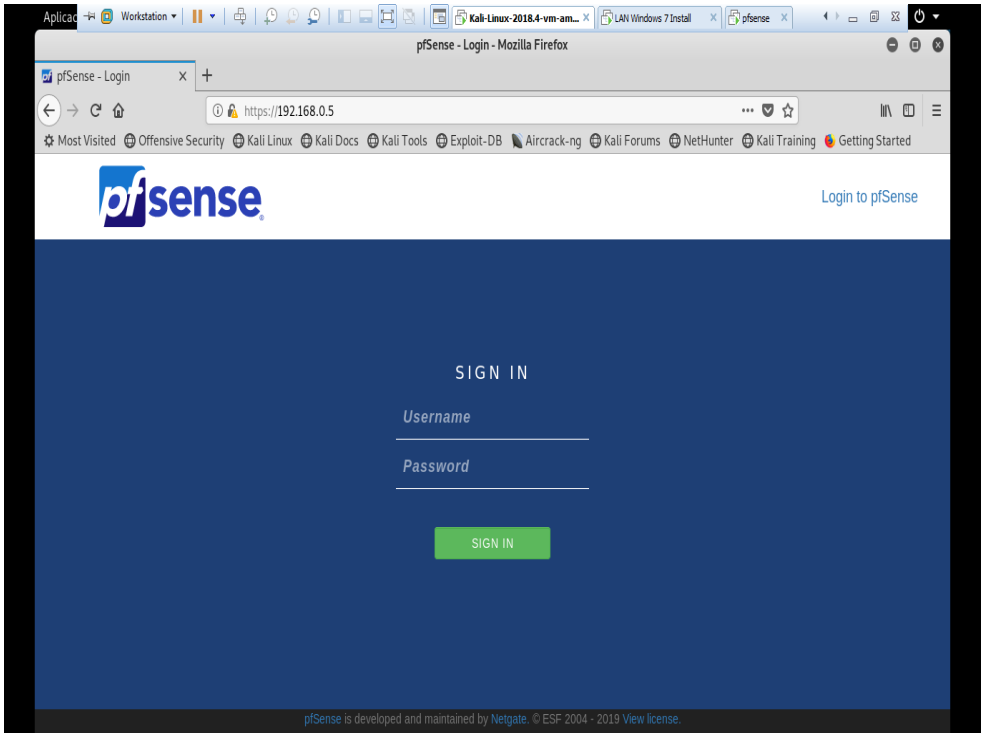
Asignación de interfaces de Red



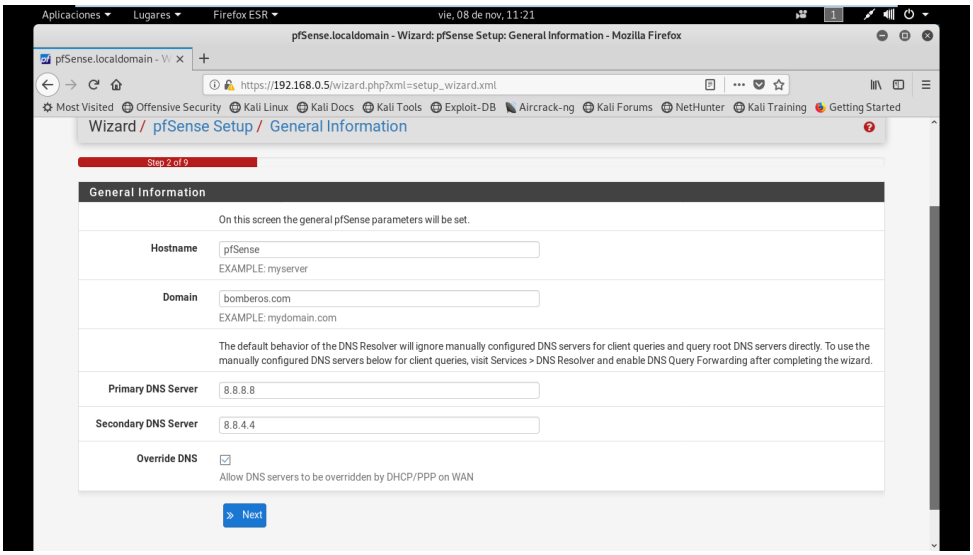
Asignación de Ip. A las interfaces



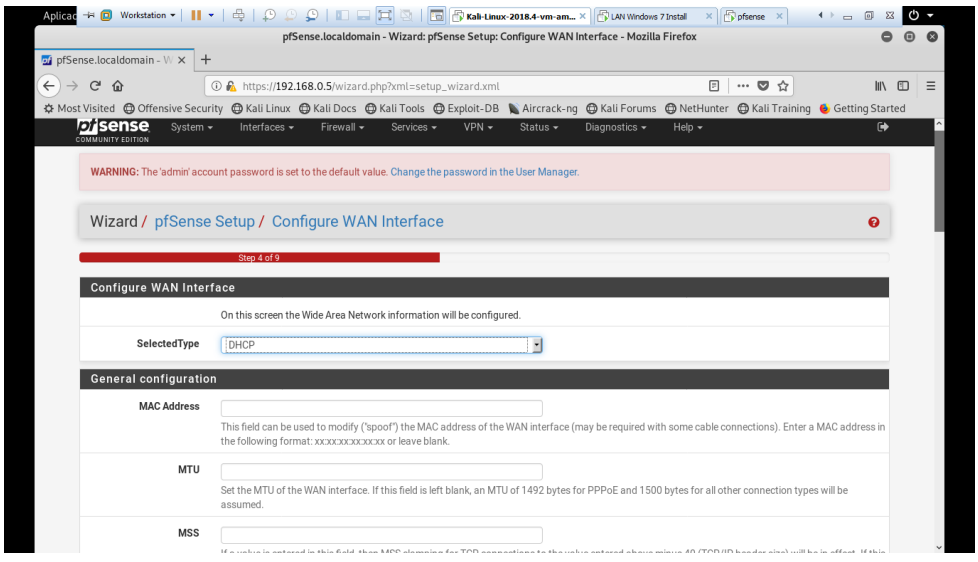
Ingreso a pfsense a través de la interfaz web



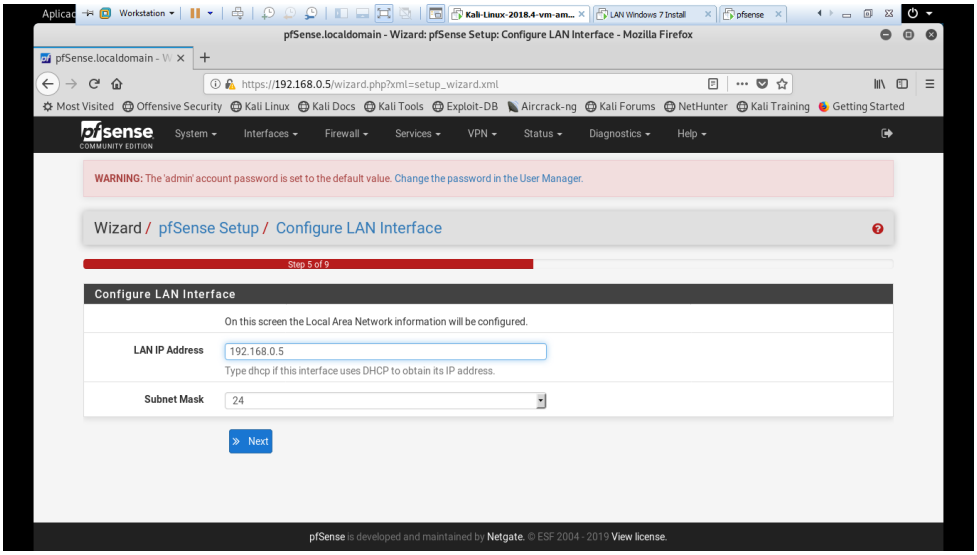
Asignación de DNS



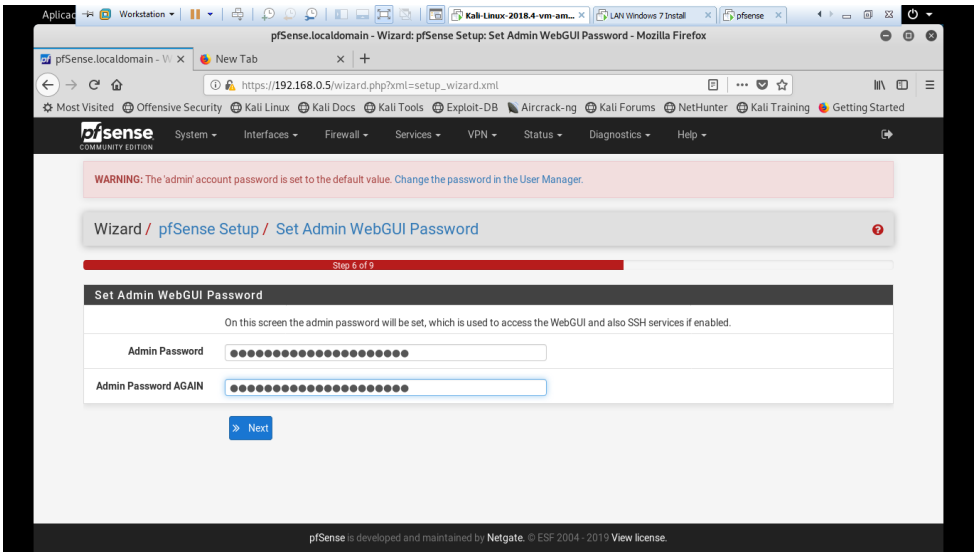
Configuración interfaz WAN



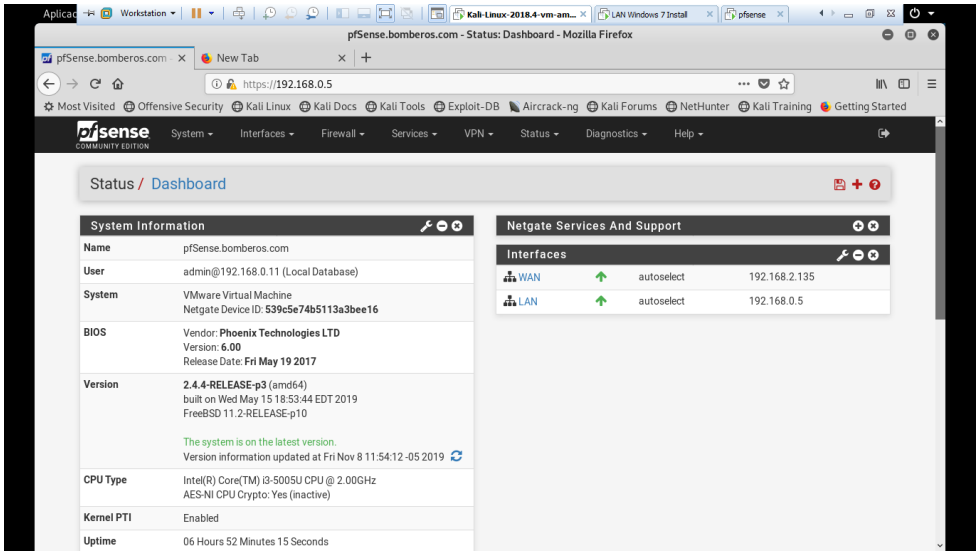
Configuración de interfaz LAN



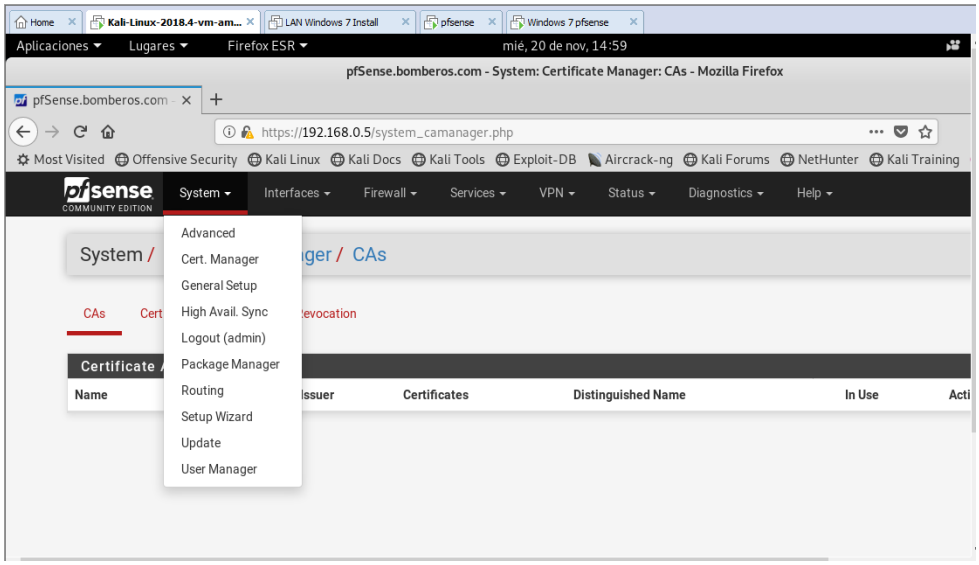
Configuración interfaz de Usuario



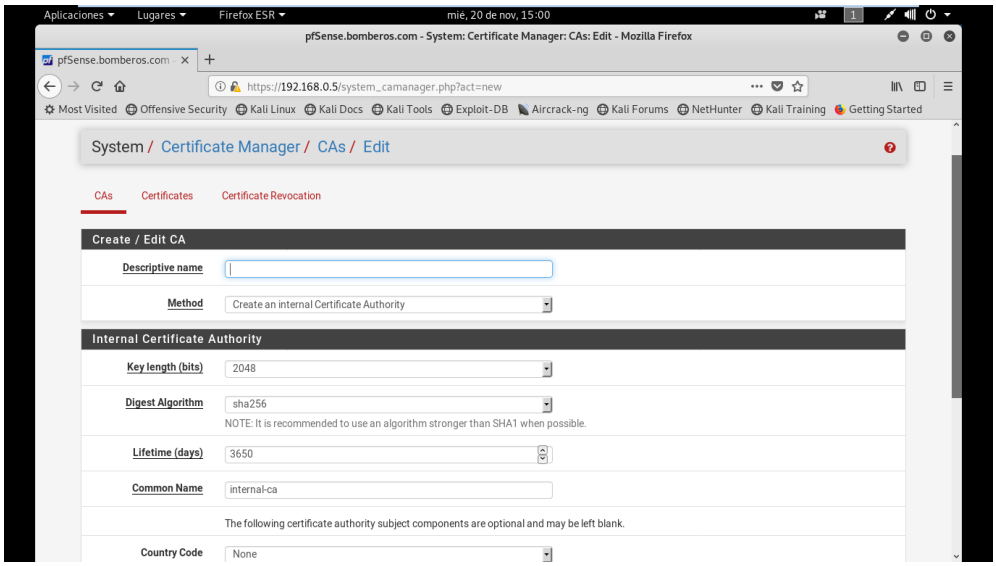
Interfaz gráfica Pfsense con tarjetas de red



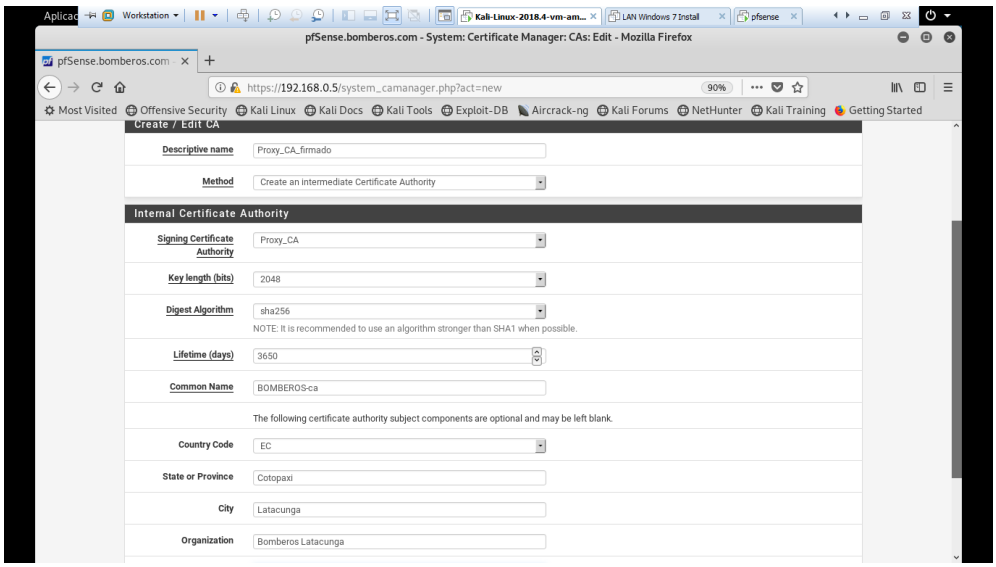
Configuración de certificados MITM



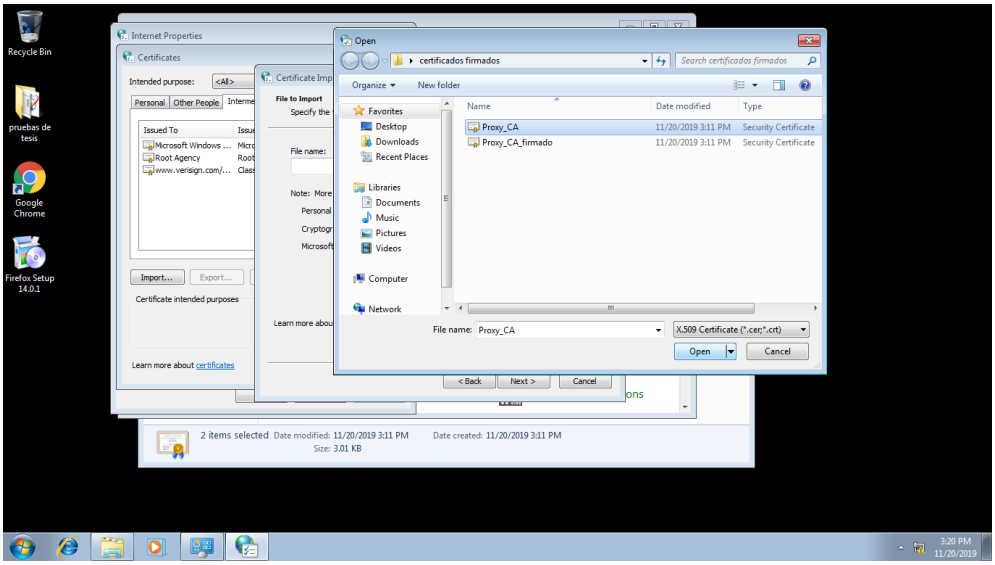
Configuración de certificados



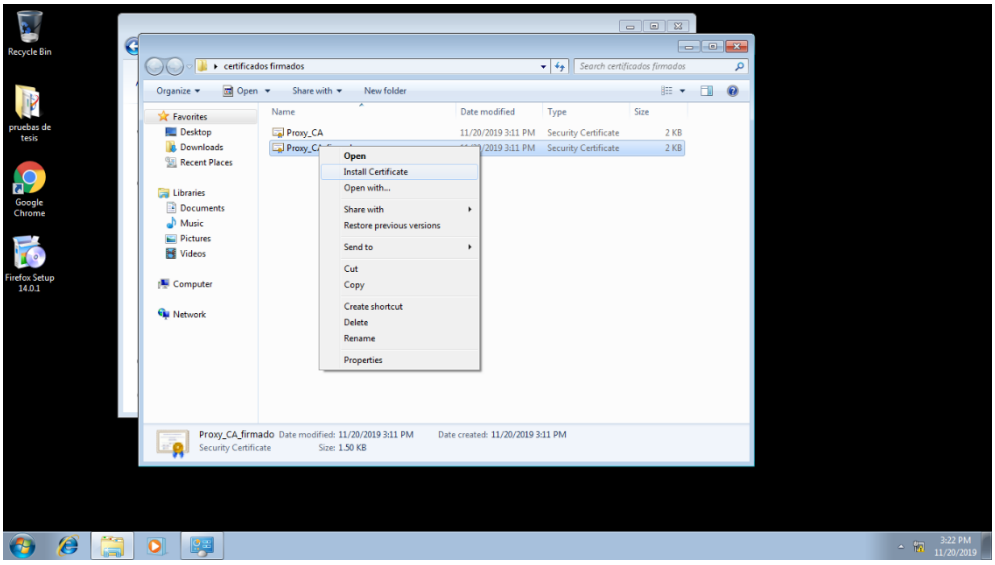
Firmado de certificados



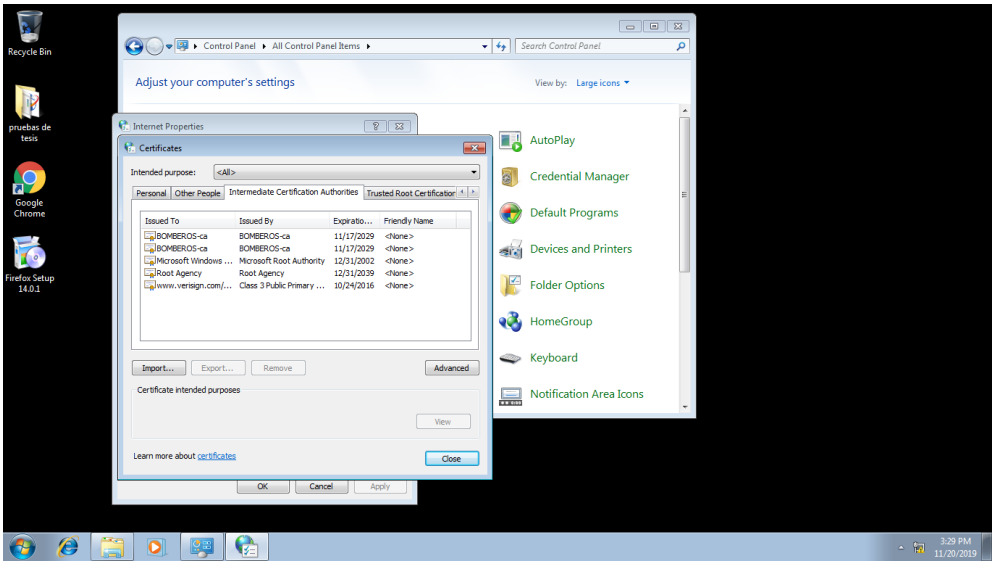
Importación de certificados



Instalación de certificados

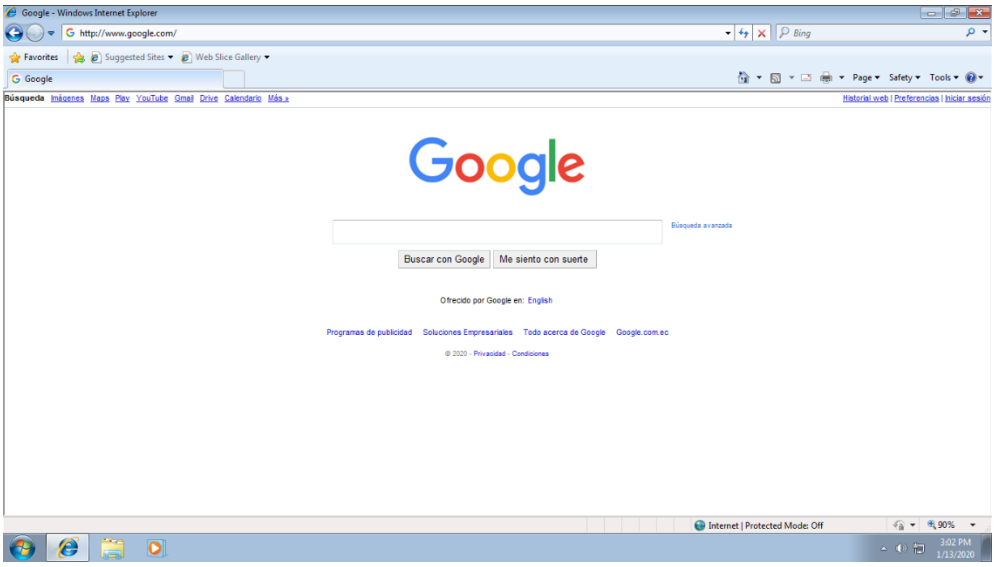


Certificados instalados satisfactoriamente

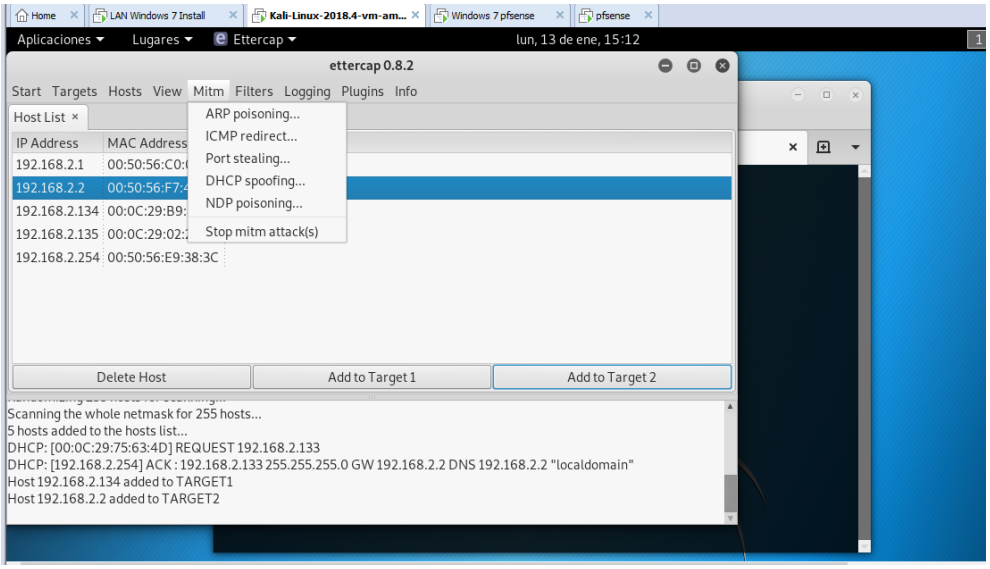


ANEXO 3

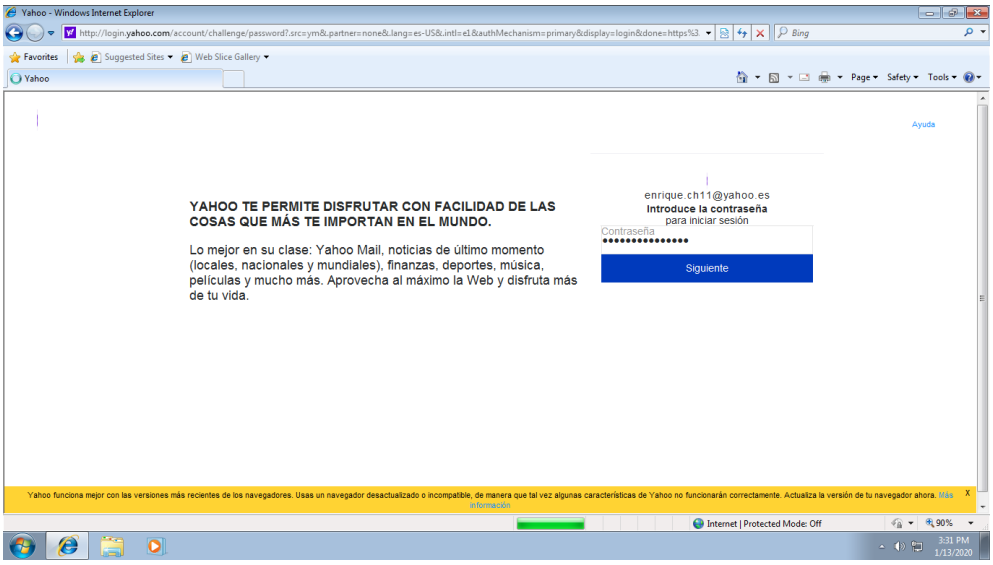
VULNERABILIDADES ANTES DE INSTALAR PFSENSE



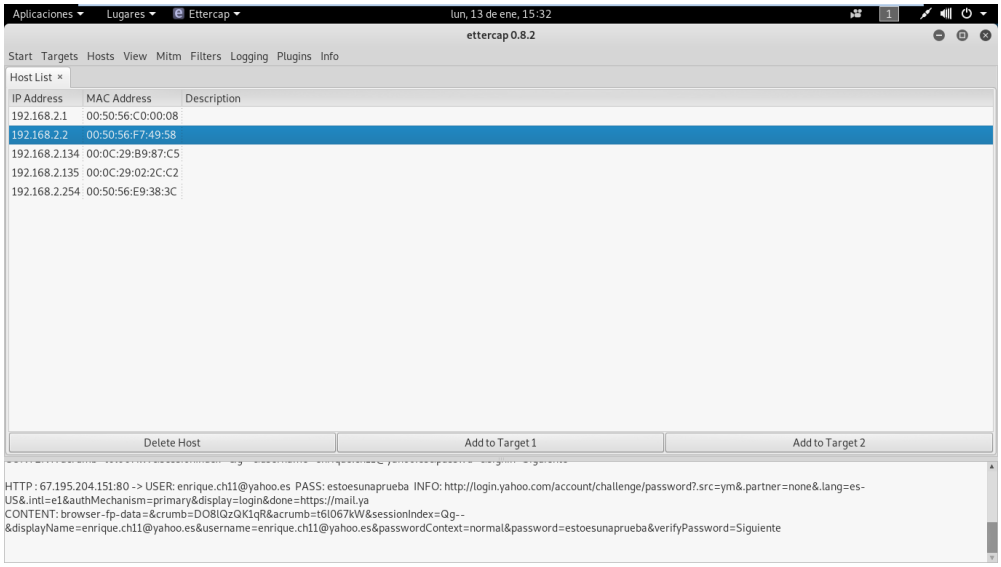
Envenenamiento tabla ARP con KALI LINUX



Ingreso de credenciales de correo Yahoo en el ordenador victima



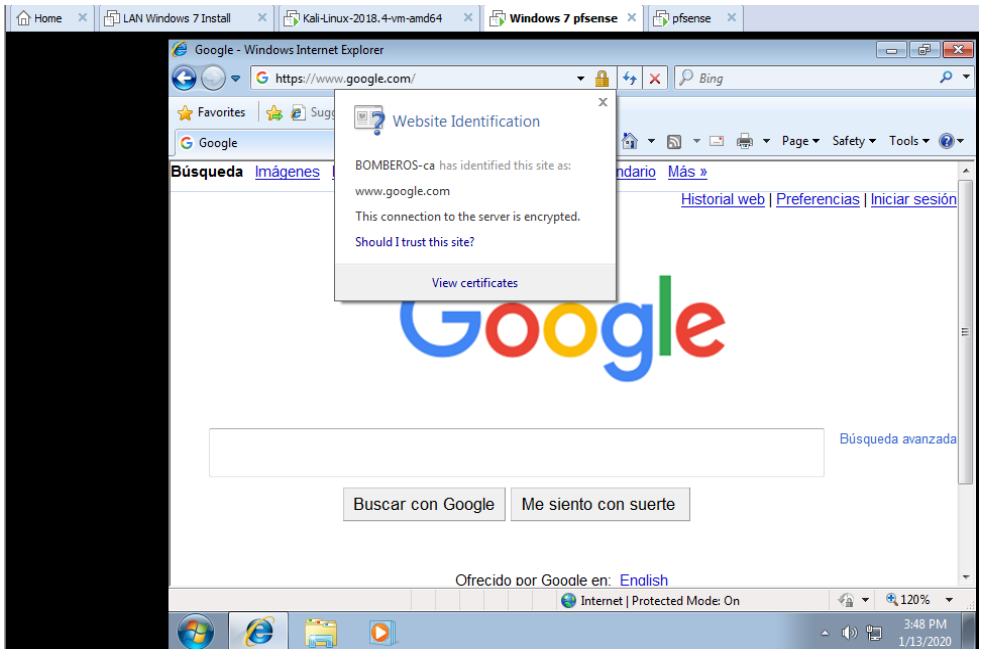
Obtención de credenciales del correo en la máquina del atacante



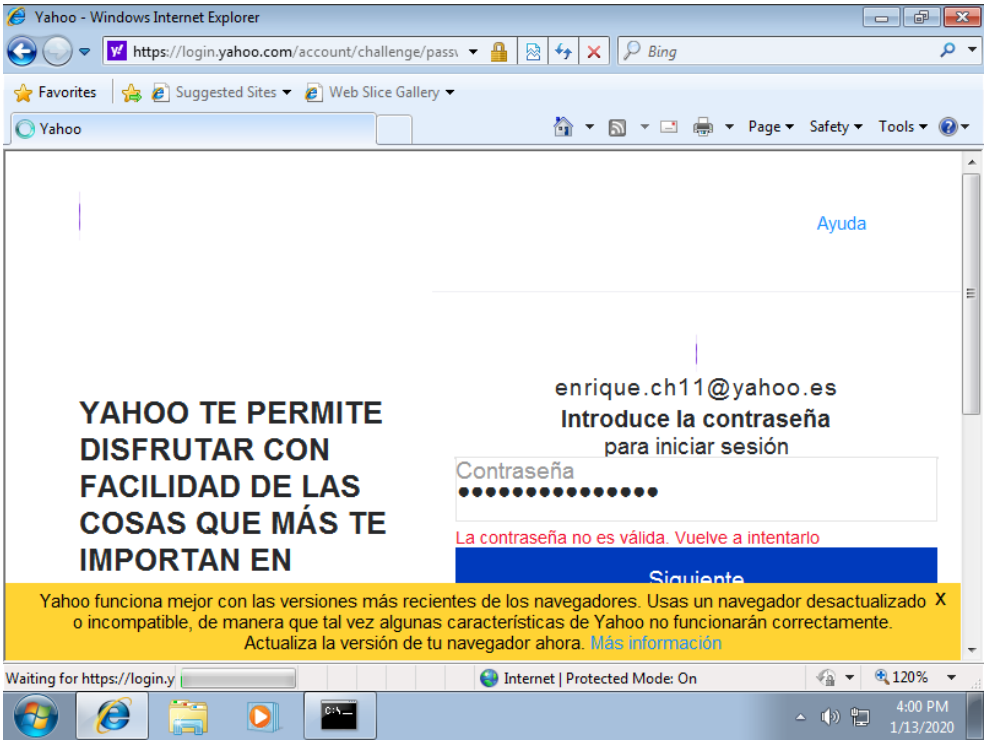
HTTP : 67.195.204.151:80 -> USER: enrique.ch11@yahoo.es PASS: estoesunaprueba

ANEXO 4

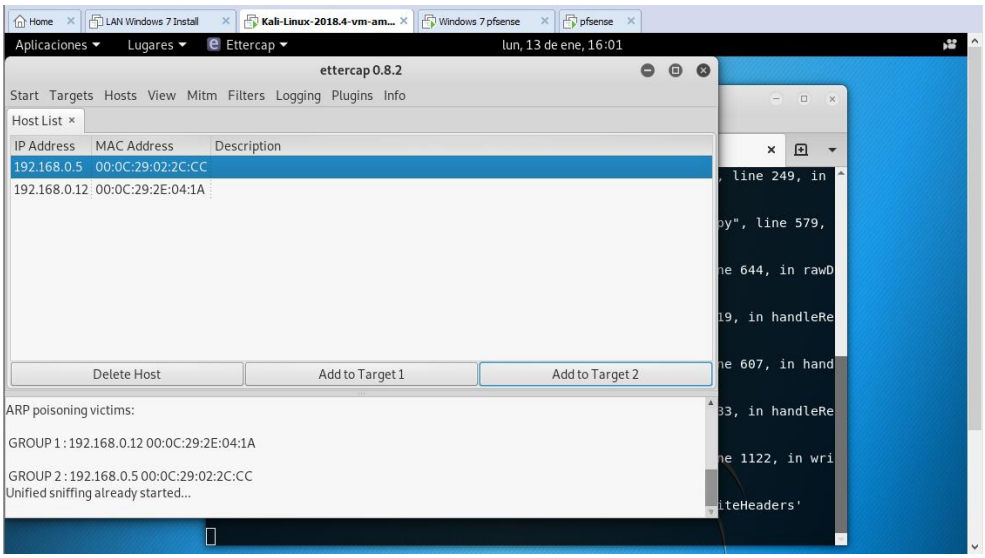
CERTIFICADOS FIRMADOS POR PFSENSE



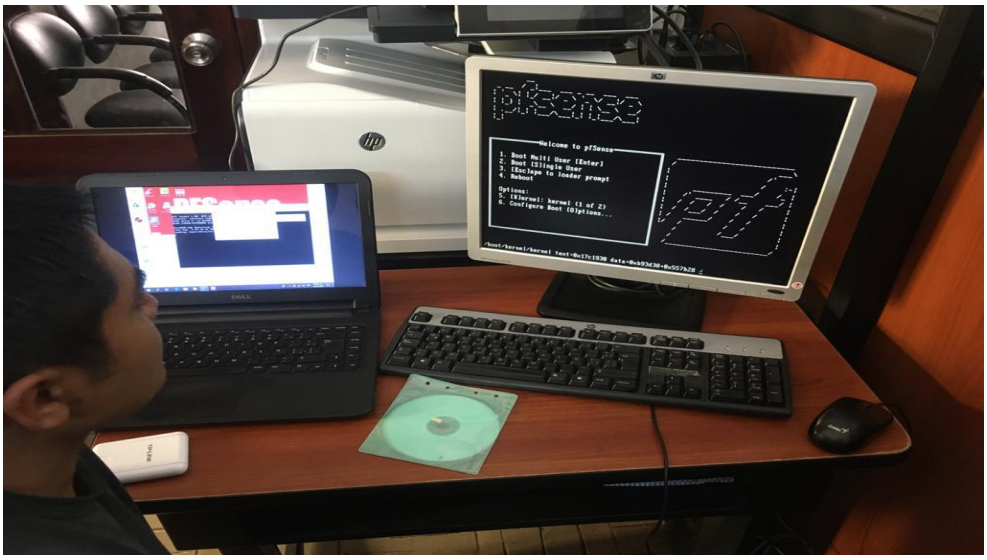
Ingreso de credenciales de correo Yahoo en el ordenador victima

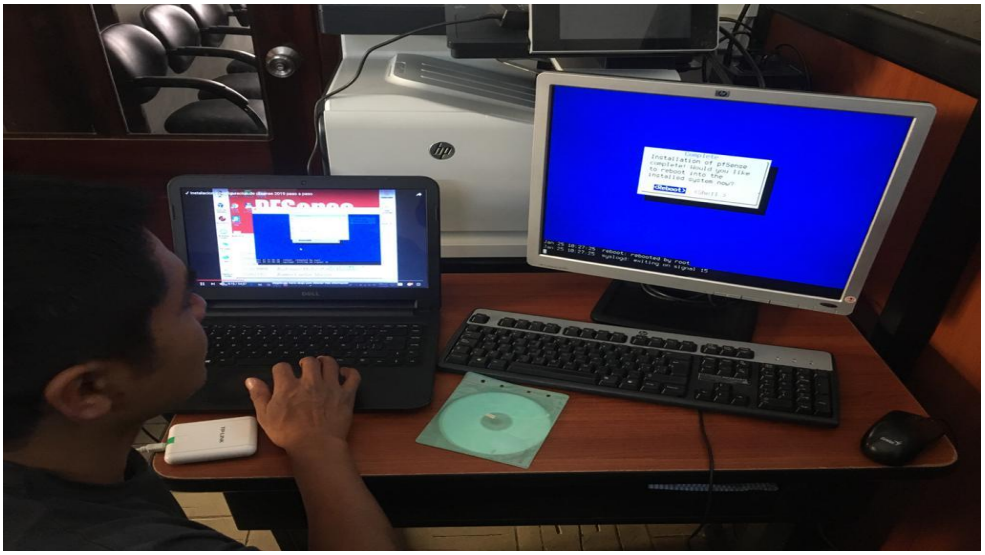


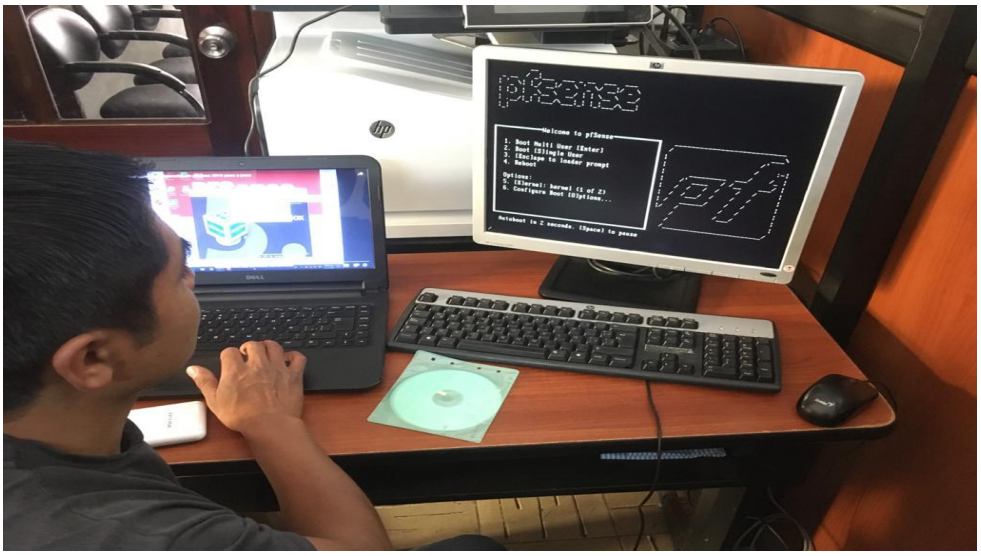
En la máquina del atacante no se obtiene las credenciales de la víctima gracias a los certificados y filtrado de paquetes de Pfsense.



Implementación y pruebas en el Cuerpo de Bomberos Latacunga







ANEXO 5
ENCUESTAS AL PERSONAL INSTITUCIONAL

Universidad Técnica de Cotopaxi

UNIVERSIDAD TÉCNICA DE COTOPAXI

Posgrado

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

		SI	NO
1.	¿Sabe usted cómo reconocer un virus de computadora?	[ ]	[X]
2.	¿Sabe usted cómo crear una contraseña segura?	[ ]	[X]
	Cómo: _____		
3.	¿Cambia frecuentemente las contraseñas de sus cuentas personales?	[ ]	[X]
4.	¿Conoce usted cómo identificar si su página de navegación de internet es segura?	[ ]	[X]
	Cómo: _____		
5.	¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?	[X]	[ ]

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 [X]
- Windows 8.1 [ ]
- Windows 10 [ ]
- Linux [ ]
- No lo sé [ ]

Universidad Técnica de Cotopaxi

UNIVERSIDAD TÉCNICA DE COTOPAXI

Posgrado

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

		SI	NO
1.	¿Sabe usted cómo reconocer un virus de computadora?	☐	☒
2.	¿Sabe usted cómo crear una contraseña segura?	☐	☒
	Cómo: _____		
3.	¿Cambia frecuentemente las contraseñas de sus cuentas personales?	☐	☒
4.	¿Conoce usted cómo identificar si su página de navegación de internet es segura?	☐	☒
	Cómo: _____		
5.	¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?	☐	☒

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 ☒
- Windows 8.1 ☐
- Windows 10 ☐
- Linux ☐
- No lo sé ☐

Universidad Técnica de Cotopaxi

UNIVERSIDAD TÉCNICA DE COTOPAXI

Posgrado

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

		SI	NO
1.	¿Sabe usted cómo reconocer un virus de computadora?	✓	
2.	¿Sabe usted cómo crear una contraseña segura?	✓	
	Cómo: Combinando signos números y letras.		
3.	¿Cambia frecuentemente las contraseñas de sus cuentas personales?	✓	
4.	¿Conoce usted cómo identificar si su página de navegación de internet es segura?		X
	Cómo: _____		
5.	¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?		X

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 ✓
- Windows 8.1
- Windows 10
- Linux
- No lo sé

Universidad Técnica de Cotopaxi

UNIVERSIDAD TÉCNICA DE COTOPAXI

Posgrado

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

		SI	NO
1.	¿Sabe usted cómo reconocer un virus de computadora?	[ ]	[X]
2.	¿Sabe usted cómo crear una contraseña segura?	[ ]	[X]
	Cómo: _____		
3.	¿Cambia frecuentemente las contraseñas de sus cuentas personales?	[ ]	[X]
4.	¿Conoce usted cómo identificar si su página de navegación de internet es segura?	[ ]	[X]
	Cómo: _____		
5.	¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?	[ ]	[X]

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 [X]
- Windows 8.1 [ ]
- Windows 10 [ ]
- Linux [ ]
- No lo sé [ ]

Universidad Técnica de Cotopaxi

Posgrado

UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

		SI	NO
1.	¿Sabe usted cómo reconocer un virus de computadora?	[ ]	[X]
2.	¿Sabe usted cómo crear una contraseña segura?	[X]	[ ]
	Cómo: Debe contener letras Mayusculas, minusculas, números, simbolos		
3.	¿Cambia frecuentemente las contraseñas de sus cuentas personales?	[X]	[ ]
4.	¿Conoce usted cómo identificar si su página de navegación de internet es segura?	[ ]	[X]
	Cómo: _____		
5.	¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?	[ ]	[X]

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 [X]
- Windows 8.1 [ ]
- Windows 10 [ ]
- Linux [ ]
- No lo sé [ ]

Universidad Técnica de Cotopaxi

UNIVERSIDAD TÉCNICA DE COTOPAXI

Posgrado

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

		SI	NO
1.	¿Sabe usted cómo reconocer un virus de computadora?	[ ]	[X]
2.	¿Sabe usted cómo crear una contraseña segura?	[X]	[ ]
	Cómo: Mayusculas, Minusculas, Numeros, Signos (@ - -).		
3.	¿Cambia frecuentemente las contraseñas de sus cuentas personales?	[X]	[ ]
4.	¿Conoce usted cómo identificar si su página de navegación de internet es segura?	[X]	[ ]
	Cómo: Los candados que aparece en la esquina de la ventana.		
5.	¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?	[ ]	[X]

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 [ ]
- Windows 8.1 [X]
- Windows 10 [ ]
- Linux [ ]
- No lo sé [ ]

Universidad Técnica de Cotopaxi

UNIVERSIDAD TÉCNICA DE COTOPAXI

Posgrado

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

		SI	NO
1.	¿Sabe usted cómo reconocer un virus de computadora?	[ ]	[X]
2.	¿Sabe usted cómo crear una contraseña segura?	[ ]	[X]
	Cómo: _____		
3.	¿Cambia frecuentemente las contraseñas de sus cuentas personales?	[ ]	[X]
4.	¿Conoce usted cómo identificar si su página de navegación de internet es segura?	[ ]	[X]
	Cómo: _____		
5.	¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?	[X]	[ ]

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 [X]
- Windows 8.1 [ ]
- Windows 10 [ ]
- Linux [ ]
- No lo sé [ ]

Universidad Técnica de Cotopaxi

Posgrado

UNIVERSIDAD TÉCNICA DE COTOPAXI

DIRECCIÓN DE POSGRADO

MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TÍTULO: Implementación de un sistema gestor de seguridad ante posibles amenazas cibernéticas en la red del "CUERPO DE BOMBEROS DE LATACUNGA"

ENCUESTA

La siguiente encuesta va dirigida a los funcionarios del CUERPO DE BOMBEROS DE LATACUNGA

Instrucciones:

- Lea detenidamente las preguntas para que pueda responder de una forma adecuada
- Marque una sola alternativa dentro del cuadro [X]

	SI	NO
1. ¿Sabe usted cómo reconocer un virus de computadora?	[ ]	[X]
2. ¿Sabe usted cómo crear una contraseña segura?	[ ]	[X]
Cómo: _____		
3. ¿Cambia frecuentemente las contraseñas de sus cuentas personales?	[ ]	[X]
4. ¿Conoce usted cómo identificar si su página de navegación de internet es segura?	[ ]	[X]
Cómo: _____		
5. ¿Ha respondido alguna vez un correo electrónico, en el cual le solicitaron datos personales?	[ ]	[X]

6. ¿Qué versión de Windows está instalada en el equipo que normalmente utiliza?

- Windows 7 [ ]
- Windows 8.1 [ ]
- Windows 10 [ ]
- Linux [ ]
- No lo sé [X]

ANEXO 6
AVAL DE IMPLEMENTACIÓN

República del Ecuador

CUERPO DE BOMBEROS DE LATACUNGA
JEFATURA

AVAL DE IMPLEMENTACIÓN

Yo, Ángel Rodrigo Baño Gamboy, con número de cédula 0502155476, Jefe del Cuerpo de Bomberos de Latacunga (E).

CERTIFICO:

En forma legal que el Sr. **Abrahan David Sangucho Sandoval** con número de cédula **0503129801**, estudiante de la maestría en Sistemas de Información de la Universidad Técnica de Cotopaxi, desarrolló la propuesta cuyo título versa "IMPLEMENTACIÓN DE UN SISTEMA GESTOR DE SEGURIDAD ANTE POSIBLES AMENAZAS CIBERNÉTICAS EN LA RED DEL CUERPO DE BOMBEROS DE LATACUNGA"

Es todo cuanto puedo certificar en honor a la verdad y autorizo al peticionario hacer uso del presente certificado de la manera ética que estimare conveniente.

Latacunga, 30 de abril de 2020.

Atentamente,

Abnegación y Disciplina

Cptn. (B) Ing. Ángel Rodrigo Baño Gamboy.
JEFE DEL CUERPO DE BOMBEROS DE LATACUNGA (E)

Sánchez de Orellana 11-109 y Marqués de Maenza
(03) 2809-080 / (03) 2813-520 (03) 2811-227
www.bomberoslatacunga.gob.ec EMAIL: jefatura@bomberoslatacunga.gob.ec