TEMA DEL TRABAJO DE TITULACIÓN:

DISEÑO DE MODELO DE SEGURIDAD Y PLAN DE MEJORAS PARA LA SEGURIDAD DE LA RED, EN FUNCIÓN DE LAS VULNERABILIDADES Y AMENAZAS DETECTADAS EN LA EMPRESA CENFORSP. CIA LTDA.

LÍNEA DE INVESTIGACIÓN:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

MODALIDAD DE TITULACIÓN:

PROPUESTA TECNOLÓGICA

CARRERA:

INGENIERÍA EN SISTEMAS

TÍTULO A OBTENER:

ADMINISTRACIÓN DE REDES

AUTOR:

JOAN PAUL ZAMBRANO LOOR

TUTOR:

MGTR. MANUEL RAMÍREZ

Samborondón – Ecuador

2021 - 2022

AGRADECIMIENTO

Agradezco en primer lugar a Dios por brindarme la sabiduría para seguir por el camino del aprendizaje con esfuerzo y constancia.

A mi familia por todo el apoyo brindado en cada paso que he dado. En especial a mis padres que siempre han sido mis guías.

Agradezco también a los docentes que influyeron de manera positiva en mi carrera, compartiendo siempre sus conocimientos, experiencias y a quienes les guardo un profundo respeto y admiración. A la Ing. Ericka Ascencio quien siempre brindó su buena predisposición y soluciones como decana de nuestra facultad. A mi tutor, el Ing. Manuel Ramírez por todos los conocimientos importantes de la especialidad y brindarme su ayuda con excelentes consejos en la elaboración de este proyecto. La Ing. Ana María Arellano, quien siempre estuvo pendiente del desarrollo personal y profesional de los alumnos. Al Ing. David Benavides, por brindarme la confianza y las oportunidades para formar parte de su excelente equipo de trabajo y crecer de manera profesional.

DEDICATORIA

Dedico este trabajo de titulación a mi familia, en especial a mis padres Omar, Debie, Jessica y a mis hermanos Camila, Cristopher e Isaac; ya que son un pilar fundamental en mi vida y siempre me brindan su apoyo incondicional para alcanzar mis metas y sueños.

A Saray Castro, quien me acompañó a lo largo de este camino y siempre me motivó a mejorar en muchos aspectos e influyó de manera positiva en mi vida.

A mi difunto abuelo Misael, quien me inspiró a dar lo mejor de mí, afrontar siempre con buena predisposición los problemas y a quién llevaré siempre en el corazón.

ANEXO N°16

1. CERTIFICACION DE REVISION FINAL

QUE EL PRESENTE PROYECTO DE PROPUESTA TECNOLÓGICA TITULADO:

DISEÑO DE MODELO DE SEGURIDAD Y PLAN DE MEJORAS PARA LA SEGURIDAD DE LA RED, EN FUNCIÓN DE LAS VULNERABILIDADES Y AMENAZAS DETECTADAS EN LA EMPRESA CENFORSP. CIA LTDA.

ACOGIÓ E INCORPORÓ TODAS LAS OBSERVACIONES REALIZADAS POR LOS MIEMBROS DEL TRIBUNAL ASIGNADO Y CUMPLE CON LA CALIDAD EXIGIDA PARA UN TRABAJO DE TITULACIÓN, POR LO QUE SE AUTORIZA A: **JOAN PAUL ZAMBRANO LOOR,** QUE PROCEDA A SU PRESENTACION.

Samborondón, 08-11-2021

Mgtr/ PhD.. Manuel Ramírez Pírez - *Tutor(a)*

ING. MANUEL Ramirez 13:55 (hace 6 minutos)

para mí

Buenas tardes señor Joan Zambrano, luego de revisar su proyecto a partir de las sugerencias del tribunal, le comunicó que puede subir el mismo para su defensa final

saludos

Ing. Manuel Ramírez

--

Universidad Ecotec

Great Place To Work. Certified DIC 2020 - DIC 2021 ECUADOR

Ing. Manuel Ramírez Pírez, Msc

Docente de la Facultad de Ingenierías

PBX: 04 3723400 Ext.: 447

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Yo **Manuel Ramírez Pírez**, tutor del trabajo de titulación" DISEÑO **DE MODELO DE SEGURIDAD Y PLAN DE MEJORAS PARA LA SEGURIDAD DE LA RED, EN FUNCIÓN DE LAS VULNERABILIDADES Y AMENAZAS DETECTADAS EN LA EMPRESA CENFORSP. CIA. LTDA**." elaborado por **Joan Paúl Zambrano Loor**, con mi respectiva supervisión como requerimiento parcial para la obtención del título de Ingeniero en sistemas con énfasis en Administración de redes.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 4 (%) mismo que se puede verificar en el siguiente link: https://secure.urkund.com/old/view/108944976-640894-572826#DcQxDoAgEATAv1BvzO0dcOJXjlUhaiikoTT+XaeYJ9wjLCtBAf8VNDCCGQpVGCzBHBEJGY55Qxjt6u1sde/1CltMYmIskulRiiR3fT8= Adicional se adjunta print de pantalla de dicho resultado.

URKUND

Urkund Analysis Result

Analysed Document: Tesis Joan Zambrano para urkund.docx (D114351107)
Submitted: 10/5/2021 9:58:00 PM
Submitted By: mramirez@ecotec.edu.ec
Significance: 4 %

Sources included in the report:

MARCO TEORICO ANGIE PIN VITERI.docx (D64974726)
Introduccion a la Seguridad Informatica y el Analisis de Vulnerabilidades.docx (D41399833)
PROYECTO DE INVESTIGACION.docx (D54401723)
MONOGRAFIA JANINA JOHANNA ZAMBRANO MAZABANDA.docx (D28995939)
TESIS SEGURIDAD PERIMETRAL ING. DAVID GUEVARA 13-01-2015.docx (D12878027)

Instances where selected sources appear:

17

FIRMA DEL TUTOR
MANUEL RAMÍREZ PÍREZ

RESUMEN

La empresa CENFORSP. CIA LTDA ubicada en la ciudad de Guayaquil, es una entidad privada que no cuenta con ninguna medida de seguridad a nivel LAN y que además contaba con una gran cantidad de vicisitudes que pueden llegar a comprometer de manera crítica la integridad de los datos de la empresa y de acuerdo al levantamiento de información realizado mediante un pentesting se descubrieron a través de una máquina virtual con el S.O. Kali Linux, para detectar las vulnerabilidades en la red mediante el uso de las herramientas dentro de dicha plataforma digital como lo es Nmap y el uso de aplicaciones externas como lo es Wireshark, estas herramientas en su conjunto permitieron detectar la existencia de problemas se encontraban ligados a la configuración interna de cada uno de los servidores, en especial el servidor FTP, el cual contaba con los puertos 21, 22 totalmente abiertos, además, la infraestructura de la institución carece de toda medida de seguridad, partiendo desde que no cuenta con ningún firewall lo que implica que este servidor se encuentre presto a recibir cualquier tipo de amenazas como es el caso de los ataques de denegación de servicios o ataques de fuerza bruta.

A lo largo de esta documentación y en el proceso de investigación se demostró mediante exploits el grado de vulnerabilidad que presenta sus servidores, y partiendo de estos procesos de observación se llegó a punto de denotar la importancia de emplear las distintas normas dictaminadas en las normas ISO 27000 – 27001, en un plan de mejoras que permitió la obtención de buenas prácticas a nivel tecnológico, un levantamiento de información para prevención de futuros ataques y un mejor uso de los recursos tecnológicos disponibles dentro de la empresa o que se encuentran a disposición de todos como sistemas Open Source.

Palabras Claves: ISO 27000 – 27001, exploits, DMZ, ataque de denegación de servicios, ataques de fuerza bruta, pentesting

ABSTRACT

The company CENFORSP. CIA LTDA located in the city of Guayaquil, is a private entity that does not have any security measures at the LAN level and that also had a large number of vicissitudes that could critically compromise the integrity of the company's data and according to the information gathering carried out by means of a pentesting, they were discovered through a virtual machine with the OS Kali Linux, to detect vulnerabilities in the network through the use of tools within said digital platform such as Nmap and the use of external applications such as Wireshark, these tools as a whole allowed to detect the existence of problems were linked to the internal configuration of each of the servers, especially the FTP server, which had ports 21, 22 completely open, in addition, the infrastructure of the institution lacks any security measure, starting from the fact that it does not have any firewall which implies that this server is ready to receive any type of threats such as denial of service attacks or brute force attacks.

Throughout this documentation and in the investigation process, the degree of vulnerability presented by its servers was demonstrated through exploits, and based on these observation processes, it was possible to denote the importance of using the different standards dictated in the ISO standards 27000 - 27001, in an improvement plan that allowed obtaining good practices at a technological level, a collection of information to prevent future attacks and a better use of the technological resources available within the company or that are available to all as Open Source systems.

Keywords: ISO 27000 - 27001, exploits, DMZ, denial of service attack, brute force attacks, pentesting

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

La implementación de nuevas tecnologías de información ha permitido a las empresas desarrollarse de una manera exponencial y de igual manera ha facilitado y agilizado la manera de poder interactuar con los usuarios sin importar cuál sea, su posición geográfica y asimismo ha permitido reducir tiempos y procesos en ciertas tareas logísticas u operacionales.

Si bien es cierto que estos recursos han evolucionado la forma de hacer negocios por el lado de las empresas también es irrefutable argumentar que esta forma de trabajar ha provocado que existan cada vez más vulnerabilidades y amenazas a nivel de integridad, accesibilidad y disponibilidad de la información.

Por tal razón se ha requerido implementar una infraestructura tanto física como lógica, la cual debería ser sumamente robusta y normalizada, por lo que se basará en las pautas dictaminadas en las normas ISO 27001 y 27002, las cuales permitirán tener una guía para la seguridad de la información.

Cabe indicar que la empresa CENFORSP. CIA LTDA., no cuenta con ningún mecanismo de seguridad que garantice el uso idóneo de la información. Lo que acarrea la existencia de contratiempos y problemas en las tareas cotidianas de la compañía y asimismo afecta la manera de manejar la información de la compañía lo que generaría una seria vulnerabilidad en los datos de la compañía.

La presente propuesta se enfrasca en diseñar un plan de mejora en la seguridad de la red de la empresa CENFORSP. CIA LTDA., para esto se propone una amalgama de estrategias y mecanismos adecuados para mantener la confidencialidad, integridad y disponibilidad de la información, a través de una gestión integral de seguridad de la información basada en la norma ISO 27001 y las buenas prácticas de la norma ISO 27002 y en cuanto a la metodología de trabajo se propone el uso de Lean Startup para poder establecer un modelo mediante el cual se establezca la creación de un modelo de seguridad óptimo para los empleados de la empresa de esta forma evitar las malas prácticas utilizadas hasta la actualidad por dichos usuarios.

PLANTEAMIENTO DEL PROBLEMA

La empresa CENFORS. CIA LTDA., ubicada en la ciudad de Guayaquil - Ecuador es una institución privada que no cuenta con ninguna medida de seguridad a nivel de LAN, de acuerdo al levantamiento de información pertinente se encontraron una gran cantidad de vicisitudes que pueden comprometer muy seriamente a la integridad de datos de la empresa. Entre los problemas de mayor realce que se pudo detectar a nivel general está la falta de equipos físicos y/o lógicos que puedan ser empleados como equipos de firewall dedicados y de igual modo se pudo detectar que no existen políticas de seguridad que permitan un mayor control y gestión en las áreas de operación y administración. En cuanto a nivel lógico y técnico se realizó una pesquisa interna en la red de la compañía, para esto se realizó una auditoría interna mediante un Pentesting realizado en Kali Linux; y partiendo de este análisis dinámico se pudo detectar infiltraciones en la red de tipo malware y un sin número de problemas a nivel de servidores, entre los más alarmantes están que ciertos módulos de los servicios de intranet se mantienen bajo el protocolo HTTP; el firewall interno de los servidores se encontraban desactivados y la mayoría de los puertos tanto de los servidores web como el de base de datos se encontraban abiertos.

Cabe resaltar que la compañía cuenta con un departamento TI, el cual debería ser el encargado de mantener el correcto funcionamiento de la red interna, y asimismo brindar el mantenimiento preventivo y correctivo de los equipos informáticos y de igual manera es la entidad dedicada en brindar la seguridad necesaria para establecer reglas y procesos dedicados a salvaguardar el acceso de los datos.

A causa de que la empresa no cuenta con un plan de gestión de seguridad, es probable que sufra una proliferación de múltiples ataques como spammers, worms, botnets y demás, y como consecuencia sufre un gran número de amenazas internas como es el caso de pérdida o fuga de información, secuestro de sesión, denegación de servicios e incluso pueden llegar a ser víctimas de ataques de suplantación de información, sitios o portales.

OBJETIVOS

Objetivo general:

Diseñar un modelo de seguridad y plan de mejoras y para la red, en función de las vulnerabilidades y amenazas detectadas en la empresa CENFORSP. CIA LTDA.

Objetivos específicos:

- Determinar los fundamentos teóricos relacionados a la seguridad en redes de datos,
- Evaluar la seguridad de red con el uso herramientas de escaneo y diagnóstico para la detección de vulnerabilidades,
- Interpretar los resultados en función de la medición de cada indicador analizado en la red.
- Proponer un plan de mejoras que garantice la seguridad y eficiencia de la red LAN de la empresa CENFORSP en base a las directrices dictaminadas por las normas ISO 27000 e ISO 27001.

JUSTIFICACIÓN

Para muchos el recurso más vital y crítico de una institución es la Información y en este caso en particular no es la excepción, si por alguna razón este activo llegaría a estropearse, el daño de la empresa sería irremediable, puesto que se podría que en el peor de los escenarios se podría llegar a comprometer información dedicada tanto de los socios de la compañía, como de los clientes, por lo que es indispensable para esta compañía que cuente con las medidas necesarias para así garantizar la integridad de la empresa.

Tal como se lo mencionó en el exordio del planteamiento del problema se realizó una indagación sobre el departamento de informática de la compañía CENFORSP. CIA LTDA, entre todas las vicisitudes que se pudieron encontrar están: la institución con un sistema de gestión de seguridad; ciertos módulos aplicativos aún mantienen el protocolo HTTP; el servicio de FTP presenta fallas debido a que no se puede acceder a él; los sistemas diseñados salen a producción sin un testeo previo; se carece de un sistema de seguridad de la

información SGSI, lo que provoca fallos en temas de seguridad de la información; y para finiquitar otro punto alarmante es que existen ciertos problemas con la configuración del dominio del servidor de la Base de Datos lo que implica la necesidad de reiniciar el servidor de la BD cada vez y cuando, en resumen se evalúa que los segmentos de Producción, Infraestructura y Desarrollo no son los más adecuados. En cuanto al proceso de logística se evidencia que la existencia de trabajos manuales en muchas de las tareas, por lo que se incide en adaptación de procesos automatizados en sus actividades cotidianas.

Todos estos problemas y falencias intuyen en la necesidad de mejorar la calidad y disponibilidad de sus actividades, por lo que se considera determinante el hecho de acoger la norma internacional ISO 27001 la cual depende de las buenas prácticas proporcionado por la norma ISO 27002 en las actividades del día a día de la empresa.

CAPÍTULO I: MARCO TEÓRICO

En este capítulo se abordarán los fundamentos teóricos relacionados con la información o datos, se habla de su seguridad de los sistemas que pueden poseer formas mediante las cuales no se pueda vulnerar la información. También se habla de los ataques que existen y de cómo se los puede detectar a través de herramientas de uso práctico que permita poner a prueba a todo un sistema y así aportar a que este no sea fácilmente vulnerado y se logre obtener información o simplemente destruir toda la red de datos locales.

1.1. Antecedentes

"Desde 2008, los ciberdelincuentes hayan estado creando malware para atacar dispositivos, tales como routers y otros equipos de red. Cabe señalar que los ataques a dispositivos IoT suelen ser sigilosos, de forma que los usuarios no noten que sus dispositivos están siendo explotados" (Ramírez, 2021).

Por ese motivo surge la importancia de proteger dichos dispositivos y también protegerse de ellos, debido que son los que más ataquen han registrado una de las soluciones presentes es el identificar todos los dispositivos conectados a la red, clasificarlos correctamente y, siempre que sea posible, analizar los riesgos asociados.

"Uno de los casos más conocidos se produjo en 2010 cuando un ciberataque tuvo como objetivo las instalaciones del programa nuclear iraní a través de un malware llamado Stuxnet. Entonces saltaron todas las alarmas. Aquellos entornos industriales, que antes se consideraban seguros y herméticos, se convirtieron en foco de interés" (Galán, 2020).

En estos años la falta de información en procesos existentes a lo largo de la evolución de los sistemas informáticos se vio estancando en preguntas y afirmaciones existentes como el no estar conectado a la red ayuda a la protección industrial e informática de toda la infraestructura o que los atacantes (en este caso llamado delincuentes informáticos) desconocen del tema de ataques a las redes, por ende, no es necesaria su seguridad absoluta, error por el cual el malware pudo cometer grandes conflictos a los entornos industriales.

“En 2014, un nuevo ciberataque, conocido como DragonFly, dio lugar al espionaje de los datos de centrales energéticas de 84 países. El incidente puso en evidencia cómo muchas vulnerabilidades de los sistemas industriales podían ser explotadas desde el interior de las propias infraestructuras” (Galán, 2020).

DragonFly fue considerado un grupo de hackers profesionales de sombrero negro y gris capaces de vulnerar cualquier sistema llamado a su ataque con el nombre de la organización, dicho ataque consiste en el uso de un Sistema de Gestión de Contenidos CMS el cual registra información de las vulnerabilidades de un sistema y además lograr explotarla desde dentro de la misma infraestructura, volviéndola totalmente vulnerable.

“Más recientemente, un nuevo grupo de ciberdelincuentes llamado Sandworm vulneró el interfaz hombre-máquina (HMI) de varios fabricantes de equipamiento industrial a través de las conexiones a Internet que tenían establecidas” (Galán, 2020).

Sandworm al atacar y vulnerar dicha interfaz la cual hace referencia a una ventana que el usuario controla para comunicarse con el sistema invitando a una correcta interacción entre ellos, en la industria es técnicamente, un requisito mediante la cual se aplica más interacción de hombre-máquina, entonces dicha vulnerabilidad afecto lo suficiente a través de una red externa dándole nacimiento a las redes.

En 2019 se presentó un ataque también sin precedentes “Facebook se vio involucrado una vez más en un caso de exposición de datos. Cerca de 419 millones de números de teléfono y de identificación de usuario en Facebook fueron almacenados en un servidor online que no estaba protegido por contraseña” (TICPYMES, 2020).

Lo que hace llegar a la conclusión que ningún sistema por más grande y resguardo que sea se libra del hurto de la información, pese a que los datos personales no sean tan sensibles como las cuentas bancarias, se puede suplantar identidades y en base a eso conseguir mayores medios por los cuales realizar una explotación de información.

1.2. Conceptos generales

1.2.1. Seguridad

Seguridad es la cualidad de algo o alguien que es o está estable, seguro y bien en su ambiente, significa que una herramienta, máquina o sistema está diseñado y cumple con la función de evitar riesgos o garantizar el buen funcionamiento, "alza la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza" (Pérez & Gardey, 2021).

La seguridad es una herramienta que ayuda a todo sistema, organismo, individuo y sociedad a mantener cualquier riesgo controlado y aísla todo suceso o importuno caso para lograr establecer un correcto funcionamiento en la producción de todo tipo de proceso a seguir por una entidad.

1.2.2. Seguridad informática

Desde el inicio de este subtema se debe tomar en cuenta una confusión que siempre ha existido y es el hecho de que la seguridad informática y la seguridad de la información poseen características importantes que hacen que se diferencien entre sí.

Dicho esto, la seguridad informática se basa en resguardar el medio informático mediante el cual se establece una conectividad. (Castro, 2018) mediante varios autores menciona que la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información. Entonces la seguridad informática es la disciplina que se encarga de generar, diseñar y planificar las normativas, procedimientos, reglas, técnicas y métodos que den paso a la obtención de un sistema informático confiable, veraz y seguro, donde siempre exista una correcta disponibilidad del uso del mismo.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información (Castro, 2018), también del dispositivo físico externo que se usa para recibir y transmitir, los usuarios y protocolos que se están usando en la supervisión de la seguridad informática planificada, pero

siempre la tarea principal es minimizar y en el mejor de los casos eliminar los riesgos para obtener mejor y mayor seguridad dentro de un área asignada.
La clasificación de los campos en los que la seguridad se basa son los siguientes:

- **Usuarios:** Son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar (Castro, 2018), esto se debe a que los usuarios cometen errores y olvidan detalles importantes, suelen tener accidentes y esos sucesos hacen perder totalmente una operación, además de tiempo valioso e importante para la generación de nuevas tareas a realizarse, en la mayoría de los casos las medidas de prevención se van más aplicadas hacia los usuarios que ante cualquier otra situación de ataque externo.
- **Información:** Se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo (Castro, 2018), entonces si esta información llega a ser vulnerada o es obtenida y usada de forma inapropiada, puede llevar a la ruina a cualquier organización o persona de la que dependa su seguridad, por ende, la información es considera el activo principal de toda empresa, organización o individuo
- **La infraestructura:** En sí, es el campo que más se puede proteger dentro de la rama de seguridad informática. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización (Castro, 2018).

Pero también es necesario el cuidado de infraestructura lógica que sea capaz de prevenir todo tipo de ataque que consista en la formulación de ataques o detección de vulnerabilidades otorgadas a través de herramientas de testeo hacia todo sistema operativo.
"La totalidad de los especialistas en seguridad basan sus conocimientos y experticias sobre el aspecto técnico tradicional de la seguridad, esto es en las áreas IT, aunque bastantes de ellos consideran las cuestiones propias como el

nuevo aspecto en las comunicaciones y que hace que actualmente se hable de TIC. Además de tener un enfoque técnico prácticamente, los especialistas únicamente se manejan con las vulnerabilidades y en parte con amenazas en forma de ataques" (ISOTools, 2017).

Con la propuesta de establecer una evaluación de riesgos, se necesita realizar una auditoria o una evaluación a los activos y también de ser necesario revisar contenido basura por parte del área de telecomunicación y seguridad en la red de datos, además se debe identificar cualquier ataque, amenaza y vulnerabilidad que pueda aprovechar y explotar los atacantes hacia estos activos que de por son parte de la información más relevante de la empresa o institución.

1.2.3. Seguridad de la información

Es la disciplina que se encarga de proporcionar la evaluación de riesgos y amenazas, trazar el plan de acción y adecuación para minimizar los riesgos (Figueroa, 2017), esto se da gracias a las normativas, las buenas prácticas o el modo mediante el cual se establece un trato considerado de acuerdo a la información que se requiera resguardar con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información de activos.

A su vez, la seguridad de la información es aquella normativa que se encarga de proteger y garantizar los siguientes aspectos:

- **Confidencialidad:** El poder proteger los aspectos privado de individuos, instituciones u organismos, da por sentado el hecho de que un sistema informático es confiable, más aún cuando lo que se defiende es la información como prioridad de dicho sistema, concluyendo en que un sistema es confiable si defiende y respeta la privacidad de su usuario sin tener registro de sus actividades almacenas en algún apartado. (Excellence, 2018) menciona que la confidencialidad, requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es necesario acceder a la información mediante autorización y control**,** entonces el objetivo de la confidencialidad es prevenir la divulgación no autorizada de la información o recursos perteneciente al usuario del sistema.

- **Integridad:** Supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización (Excellence, 2018). Por lo tanto, su objetivo es el de velar por algún cambio no permitido del recurso o información a través de cualquier medio que se use para poder lograr dicho ataque.
- **Disponibilidad de la información:** Se debe cumplir que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados (Excellence, 2018).

Planteando el objetivo de que la disponibilidad de la información trata de que el sistema informativo siga activo sin ningún riesgo de ser atacado o alterado y además poder permitir el acceso autorizado de los usuarios asignados mientras proteja todos los otros campos al mismo tiempo.

La implementación de la norma ISO 27001 de seguridad de la información, además de reducir el impacto de los riesgos y amenazas, entre otros beneficios, mejora la planificación y la gestión de la seguridad de la empresa (Figueroa, 2017). Debido a esto, el negocio, empresa, institución o individuo se le da la confianza para el continuo avance en el crecimiento y desarrollo de su objetivo principal el cual es crecer económica y moralmente en su camino hacia el éxito frente a cualquier contingencia, dando así una perspectiva de prestigio frente a terceras partes y cumpliendo las normativas establecidas por las normas encargadas de proteger el ambiente sistemático, los equipos encargados del resguardo de la información mediante los cuales se obtiene la disponibilidad necesaria para realizar un trabajo y también la confianza del usuario hacia la institución o sistema operativo en la que posee datos.

1.2.4. Estándares

Los estándares son reglas, medidas y normas que ayudan a mantener el orden y confiabilidad de todo tipo de sistema, organización y sociedad, permiten a todo aquel que conozca de ellos tener un conocimiento básico, basado para la seguridad propia y el de los que están a su alrededor.

En el ámbito de la seguridad informática y de la información para poder proteger el recurso indispensable de la empresa se habla de los estándares principales que se encargan de dar orden a este sector y hace de las redes LAN y seguridad informática de una empresa menos vulnerable y más confiable.

1.2.4.1. Normas ISO 27000

Es un conjunto de estándares internacionales, en este caso delimitado a la seguridad de la información. Esta familia de las ISO comprende de un conjunto de buenas prácticas para la implementación, mantenimiento y mejora de Sistemas de Gestión de Seguridad de la Información (SGSI) (Intedya, 2015).

Los pilares fundamentales de esta son las normas 27001 y 27002; la primera se basa en la gestión de la seguridad apoyada por la identificación continua de riesgos mientras que la segunda es sólo una guía de buenas prácticas, describiendo una serie de objetivos de control y gestión que deberían ser implementados por las organizaciones (Normas ISO, 2021).

Un SGSI es un conjunto de procedimientos y políticas que sirven para estandarizar la gestión de la seguridad de la información (Intedya, 2015). Brevemente explicados, los pilares de la ISO 27000 son:

- **ISO 27000:** Contiene el vocabulario en el que se apoyan las normas.
- **ISO 27001:** Comprende de los requisitos para implementar un SGSI.
- **ISO 27002:** Recopila las buenas prácticas de Seguridad de la Información.
- **ISO 27003:** Es una guía de ayuda de la SGSI. Sirve de apoyo para la ISO 27001.
- **ISO 27004:** Describe una serie de recomendaciones sobre la realización de mediciones para los SGSI.
- **ISO 27005:** Es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información. Incluye ejemplos.
- **ISO 27006:** Requisitos de acreditación para las organizaciones certificadas.
- **ISO 27007:** Es una guía para auditar las SGSI. Establece qué y cuándo auditar, cómo asignar auditores, planificación, ejecución, actividades, etc.

En este trabajo se abordará como principal tema la norma ISO 27001, pero contar con los beneficios otorgados por el pilar de está ayudará a entenderla mejor.

Beneficios:

La gestión de riesgos es un elemento clave en la prevención de fraude, pishing, daños en general, pérdida de datos y muchos otros incidentes de seguridad informática. Sin una gestión de riesgos sólida, la empresa está expuesta a muchos tipos de amenazas.

Hoy en día, la seguridad de la información está constantemente en peligro a un ataque de los nombrados en el párrafo anterior. Un SGSI es un enfoque sistemático para la gestión de información confidencial de la empresa para mantenerlo seguro. El diseño e implementación de la norma ISO 27001 dará confianza a clientes y proveedores que la seguridad de la información de la organización se toma en serio (Normas ISO, 2021).

Gran parte de la información de cualquier empresa se encuentra en sistemas informáticos, sin embargo, la norma ISO 27001 define la información cómo

Un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada […] La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene (Normas ISO, 2021).

Según este concepto, la norma propone un marco de gestión de la seguridad de toda la información de la empresa, incluida la perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones, etc. En este punto, las personas pueden llegar a ser tratadas como activos del SGSI si se cree conveniente (Normas ISO, 2021).

1.2.4.2. Norma ISO 27001

Su objetivo es preservar la información. Se ha demostrado que la implantación de controles y procedimientos realizados frecuentemente no son suficientes sin

un criterio común predefinido, en torno a la compra de productos técnicos sin considerar la información esencial a ser protegida (Normas ISO, 2021).

La International Organization for Standarization (ISO), a través de sus normas ISO e IEC 27000 establece una serie de reglas y normas a seguir para una seguridad de la información empresarial íntegra, desarrolladas en las normas ISO 27001 e ISO 27002 (Normas ISO, 2021).

Sus requisitos aportan un SGSI consistente, orientado a proteger la información sin importar el formato de la misma contra cualquier amenaza, lo que garantiza en todo momento las actividades ininterrumpidas de la empresa. Sus objetivos son preservar la confidencialidad, integridad y disponibilidad de la información (Normas ISO, 2021).

A la hora de implantar un SGSI se debe considerar como eje la evaluación de riesgos. Esto permitirá a la empresa tener la visión necesaria para definir el alcance de la aplicación de la norma, integrando el sistema en la metodología de mejora continua para todas las normas ISO (Normas ISO, 2021).

Existen numerosas metodologías estandarizadas para la evaluación de riesgos, pero la que la norma ISO sugiere es identificar lo siguiente:

- **Los Activos de Información y sus responsables:** Se refiere a todo lo de valor para la organización, incluyendo edificios, equipamientos, ideas, aplicaciones, proyectos, marca, reputación, etc.
- **Las Vulnerabilidades:** Son las debilidades propias del activo que lo hacen susceptible a sufrir ataques o daños.
- **Las Amenazas:** Son aquellas cosas que puedan suceder y dañar el activo de la empresa como desastres naturales, incendios, ataques de malware, etc.
- **Los Requisitos Legales:** Todo requisito contractual que la organización está obligada a cumplir con la gente relacionada a ella.
- **Los Riesgos:** Definir la probabilidad de que las amenazas o vulnerabilidades del activo puedan causar un daño al mismo.

Luego de identificados los puntos vitales del sistema, se procede a realizar un cálculo de riesgo a partir de su probabilidad de ocurrencia e impacto sobre la organización, bajo la fórmula:

Ecuación 1. Fórmula del Riesgo

$$Riesgo = Impacto\ x\ Probabilidad\ de\ la\ Amenaza$$

Con esto se determina qué riesgos deben ser controlados con prioridad.

Una vez identificado esto, la empresa está preparada para definir su política de tratamiento de riesgos según los puntos anteriores y según la dirección de la empresa. Aquí se seleccionarán los controles para cada riesgo, orientados para asumir, reducir, eliminar y transferir el riesgo (Normas ISO, 2021).

El SGSI que propone la ISO 27001 se resume en la siguiente figura:

***Figura 1**. Implementación del SGSi*

Nota. Fuente (Normas-iso.com, 2021)

1.2.4.3. Norma ISO 27002

Según Ostec (s.f), la norma ISO 27002 nació bajo el ala de las organizaciones internacionales ISO (The international Organization for Standardization) e IEC (Ineternational Electrotechnical Commission) con la finalidad de crear un grupo de normas que consoliden las directrices relacionadas al alcance de la Seguridad de la información, en particular la norma ISO/IEC 27002 es la que establece el código de las mejores práctivas diseñadas para apoyar la implementación del Sistema SGSI en todas las organizaciones, el principal objetivo de contar con

esta norma es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización. Esto incluye selección, implementación y administración en controles, tomando en cuenta los entornos de riesgos encontrados en una empresa.

Beneficios de usar esta norma ISO 27002:

Entre las ventajas que pueden llegar a proporcionar esta certificación se tiene:

- Da mayor concienciación sobre la seguridad de la información.
- Mayor control de activos e información sensible.
- Ofrece un mejor enfoque en la implementación en las políticas de control.
- Oportunidad de identificar y hacer frente a falencias en la sistemática de la empresa.
- Reducción de riesgos a corto, mediano y largo plazo.
- El empleo de esta norma podrá convertir un diferencial competitivo a nivel empresarial.
- Ofrece una mejor organización con procesos y mecanismos sistematizados y bien diseñados.
- Promueve reducción de costes en la prevención de incidentes en la seguridad de la información.

En esta sección se pueden utilizar procesos, procedimientos, diagramas, entre otros que según la metodología seleccionada tienen que ser puestas para la mejor comprensión de las diferentes etapas del proyecto.

1.2.5. Modelo de seguridad

Un Modelo de Seguridad y Privacidad de la Información - MSPI, en cualquier entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos (Mintic, 2018).

Ser capaz de establecer pasos, guías y normas para ayudar a gestionar información, buenas prácticas y mejoramiento en los controles individuales de cada usuario es lo que un modelo de seguridad informática tiene como propósito,

por lo general un modelo de seguridad cuanta con muchos ítems guías en base a estándares y criterios basados en casos anteriores en donde se ha planteado o encontrado la misma causa, problema o conflicto, ocasionado por alguna apertura o falla del sistema.

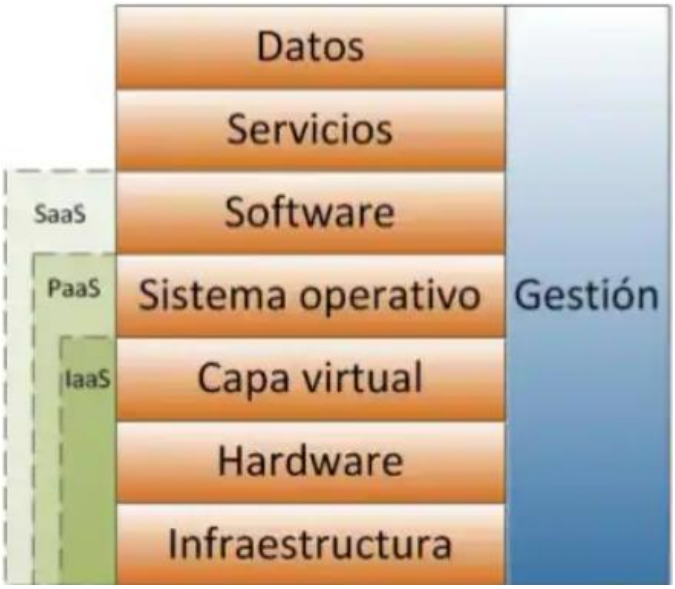

***Figura 2**. Ejemplo de modelo de seguridad.*

Nota. Fuente (Mintic, 2018)

1.2.6. Planes de seguridad

Para que un plan de seguridad informática resulte exitoso, tanto en la etapa de planificación, como en la de aplicación, debe seguir un conjunto de recomendaciones, la viabilidad del plan dependerá en gran medida de la difusión del mismo entre todo el personal de la compañía, lo que aumentará su pericia y capacidad de reacción ante una amenaza (uss, 2018).

Es necesario entender que un plan de seguridad es una idea capaz de ser implementada a tal punto de presentar resultados exitosos al instante, a través de un modelo de seguridad establecido gracias al levantamiento de información de los fallos informáticos de la empresa, para poder generar un plan eficaz se necesita del siguiente procedimiento:

- **Identificar los bienes y patrimonio a resguardar:** en este punto el principal bien a custodiar son los datos e información altamente sensible dentro de la empresa, por lo tanto, se debe dar enfoques tecnológicos

para el cuidado de este recurso, también orientar a los empleados, mejorar el servicio de conexión de red, crear zonas seguras para los servidores y las demás herramientas informáticas.

- **Detectar los riesgos y vulnerabilidades:** se basa en encontrar todo tipo de afectaciones dentro del sistema informático en donde se trata de albergar la información, es de vital importancia el llevar un registro de dichos o posibles ataques además de cómo fueron capaces de llegar al sistema, ya que con ellos se puede ayudar a corregir y mejorar la seguridad del lugar.
- **Establecer prioridades de seguridad informática:** no todo un siempre la empresa cuenta con los recursos y conocimientos para dar un soporte técnico global y completo a todo su sistema de información por ende es necesario la detección de los riesgos para poder establecer un criterio en base a las prioridades de recursos establecidos y así lograr resguardar aquellos activos más importantes y costosos de la institución.
- **Aplicar el plan de seguridad informática:** un plan debe garantizar que la empresa podrá mantenerse operativa y funcional durante la ocurrencia de la eventualidad de seguridad, o al menos permitirá que las operaciones sean recuperadas en el menor tiempo posible (uss, 2018). De tal forma, se facilita la reducción de pérdidas, amenazas y ataques, y se orienta a un avance tecnológico que ayudará a capacitar a más sectores dependientes de la tecnología en general.

1.2.7. Vulnerabilidades

Las vulnerabilidades y amenazas informáticas son un riesgo para los sistemas y la información de la empresa, sobre todo en el entorno actual, altamente digitalizado y dependiente de los servicios TI (Ambit Team, 2020).

Teniendo en cuenta que todo sistema de información y de red es vulnerable, es importante el saber reconocer cuales son las principales vulnerabilidades, amenazas y ataques que más enfrentan los sistemas de red para elevar su nivel de seguridad informática y que los atacantes obtengan mayores dificultades para lograr infiltrarse en la red de la empresa a la cual necesiten robar información.

Los conceptos definidos de vulnerabilidades y amenazas al ser semejantes con su objetivo de irrumpir a una red LAN para la obtención de información valiosa o para simplemente acabar con la sistematización que se llevaba hasta el momento del ataque, no define el motivo por el cual cada una presenta sus diferencias, por lo tanto, se debe definir cuáles son las diferencias entre ambas y las formas más comunes con las cuales ingresan dentro de un sistema.

Vulnerabilidad "es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un (*agujero*) que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño" (Ambit Team, 2020), en otras palabras, se puede catalogar como vulnerabilidad a cualquier falencia que pueda comprometer la seguridad informática, ya sea desde fallas humanas, errores en la configuración o falta de robustez en el diseño de red.

1.2.7.1. Tipos de vulnerabilidades en seguridades informática

Existen diferentes tipos de vulnerabilidades que se deben tomar en cuenta para así saber qué medidas de contingencia se pueden considerar para salvaguardar la seguridad informática de la institución a tratar.

- **Vulnerabilidad de desbordamiento de buffer:** este tipo de vulnerabilidad se realiza cuando una aplicación no tiene la capacidad de controlar la cantidad de datos que se registran en el buffer, lo que desembocaría que los bytes sobrantes se almacenen en diferentes zonas de la memoria y así se reescriba en el contenido original (S2 Grupo, 2020), la peligrosidad de esta vulnerabilidad es que le brinda al atacante la posibilidad de obtener todos los derechos de superusuario o administrador,
- **Vulnerabilidad de race condition:** esta vulnerabilidad se lleva a cabo cuando múltiples subprocesos tienen acceso a un recurso compartido en el mismo tiempo y espacio (S2 Grupo, 2020), este paradigma implicaría que servidores como samba se encuentren comprometidos, ya que estos al funcionar básicamente como un árbol de recursos serían las víctimas ideales para este llevar a cabo este exploit,

- **Vulnerabilidad de XSS (Cross Site Sripting):** este exploit es usado en ataques que permiten ejecutar scripts diseñados en lenguajes como VBScript y JavaScript, por lo que servidores como apache y tomcat serían los targets por defecto para esta vulnerabilidad (S2 Grupo, 2020), este script básicamente da puerta abierta a ataques a nivel web como es el caso de los phishing.
- **Vulnerabilidades de inyección SQL:** esta vulnerabilidad se produce cuando se inserta alguna sentencia SQL en algún script SQL ya programado lo que implicaría una alteración a nivel de la funcionalidad de la base de datos (S2 Grupo, 2020), en resumen, se puede deducir que este script le permitirá al atacante tener control total de todas las DB equiparadas en dicho servidor.
- **Vulnerabilidades de Denegación de Servicios:** este paradigma se utiliza con el propósito de que los usuarios no puedan acceder a este servicio, esto se debe al continuo y excesivo consumo de ancho de banda de red o de recursos conectados al sistema (S2 Grupo, 2020), básicamente este ataque se centra en lanzar múltiples peticiones al mismo tiempo en el puerto específico al servicio que se quiera vulnerar.

1.2.8. Amenazas

Se define como amenaza informática a toda acción que aprovecha una vulnerabilidad para colapsar un sistema informático, cabe resaltar que la mayoría de estas vicisitudes proviene en gran manera de ataques externos (Ambit Team, 2020).

Las amenazas son ataques informáticos que por general buscan no solo infiltrar un sistema informático para obtener información, sino que también busca destruir totalmente el sistema informático con el propósito de cumplir con la función con la que fueron programados, existen diferentes tipos de ataques o amenazas informáticas como las que se presentan a continuación:

1.2.8.1. Tipos de amenazas

Por lo general, todo sistema informático tiende a ser atacado, con o sin intención de afectar la integridad del conjunto de equipos encargados, resguardar la integridad de la información que se almacena dentro de un conjunto de sistemas. Esos ataques pueden ser realizados ya sea por un ente externo a la empresa como interno por parte de los mismos usuarios al no poseer los conocimientos necesarios capaces de adaptarlos a un sistema estandarizado y totalmente autónomo donde lo que es indispensable es el uso de códigos, encriptación y autentificación de identidad, muestra de archivos y sobre todo protección de confiabilidad hacia el usuario.

Pero en ocasiones por el ingreso a sitios pocos protegidos, por el mal uso de los puertos de acceso a la red propia del sistema en donde se encuentra la información del usuario o la falta de equipos que sirvan y cumplan la función de proteger la infraestructura completa de toda la localidad en donde se resguarda la información valiosa de la empresa, se presenta en ocasiones la probabilidad de encontrarse con ataques por parte de virus informáticos u otras aplicaciones informáticas las cuales, como principal prioridad cumple con el encargo de malgastar los recursos de la maquina o dispositivo informático que posea el usuario y el peor de los casos acabar totalmente con el software (parte intangible del equipo), o filtrar información hacia una red globalizada, a tal punto, de llegar a ser utilizada para actos vandálicos o el incriminar (perjuicio) social hacia el atacado.

un virus informático es un programa que tiene como objetivo dañar o cambiar el funcionamiento de la computadora. Esta es una definición bastante clara, pero el virus informático no siempre tiene que ser un programa completo, puede ser hasta cierto punto fragmentos de un programa (Castro, 2018), entonces se establece que un virus informático es un medio mediante el cual un atacante puede aprovechar la vulnerabilidad que deja este y filtrar información necesaria para sus actos maliciosos.

- **Virus informáticos**

Según (Vieites, 2013), se define al virus informático, como un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o autorreplicación, el cual trata de reproducirse de forma acelerada para extender su alcance. Se dice que los virus fueron creados como método de prevención de ataques, anticipación de posibles controversias y alteradores de la realidad virtual, pero al ver la efectividad de ataque y el intento desesperado de las empresas por deshacerse del inconveniente, pasaron a ser parte de un mercado laboral en base a la obtención de información o recursos que sirvan para moldear la realidad de las actividades de una empresa, persona, incluso videos juegos, saliendo beneficiados unos y perjudicados otros, además también los utilizan para beneficio auditorio de los organismo que son monitoreados por el estado de su país.

Un virus informático puede hacer demasiadas tareas para atentar contra la integridad informática, por ejemplo, la eliminación archivos ya sea documentos, imágenes, audios, videos, con una fecha aleatoria como método random, evitar accesos a las computadoras para corromper la disponibilidad e ingreso del usuario a la máquina y terminal de ejecutar su contenido malicioso, robo de información no especifica, bloquear las funciones de un sistema operativo o de programas dentro del ordenador, pc o equipo dentro de la red local donde se estableció el virus.

También Vieites (2013), indica que existen varios tipos de virus que se los puede definir de la siguiente manera:

- **Virus de sector de arranque (BOOT):**

En los diskettes, CDs y memorias externas, el sector que se encarga del arranque del equipo se llama BOOT. Esta es la sección concreta de un disco en la que guarda información sobre las características y contenido del mismo. Cuando se habla de arranque en un disco duro se denomina Master BOOT o MBR; existen determinados casos en donde un virus o software malintencionado se aloja en este sector, permitiéndole ejecutarse cada vez que el equipo arranque. Este tipo de virus se denomina Virus de BOOT (Sánchez, 2010).

Estos virus deben pesar menos de 512 Kb ya que es el tamaño máximo de asignación del sector del disco o diskette que se ejecuta antes del booteo. El usuario arranca el equipo, este procede a leer los 512 Kb asignados al booteo, ejecutando el virus, luego procede al sistema operativo o, caso contrario, a hacer notar la ausencia de uno, mientras que el virus ha infectado ya la memoria del equipo (Borghello, 2021).

Se puede considerar a este tipo de virus como uno de los más peligrosos de todos, puesto que debido a su mecanismo los usuarios suelen desconocer que se encuentran infectados, asimismo son difíciles de eliminar debido al cifrado o daño excesivo dentro del código existente, por lo que resultaría más sencillo y práctico formatear el disco de instalación.

- **Virus de archivos ejecutables:**

Este tipo de virus se adjunta al código de un archivo ejecutable, desviando el código de su ejecución para arrancar, luego retornando al código del huésped, ejecutando el archivo deseado por el usuario y el virus pasa desapercibido. Una vez alojado en la memoria, este puede infectar a otros ejecutables que sean abiertos en la computadora (Borghello, 2021).

Ejemplos de este virus son el Chernovil, Darth Vader y PHX, por citar unos cuantos, el nivel de peligrosidad de este tipo de virus se centra en el hecho de que este virus al tener la capacidad de adosarse a un archivo ejecutable, el usuario no suele darse cuenta de lo sucedido, y una vez realizado este proceso el virus aloja a la memoria y puede llegar a infectar a otros archivos ejecutables que se encuentren abiertos en ese equipo.

- **Virus de macros:**

Estos infectan archivos de información generados por aplicaciones que cuentan con lenguajes de programación de macros. En la actualidad estos son los más expandidos ya que todos los usuarios realizan intercambios de documentos para hacer su trabajo. Los primeros antecedentes de estos virus fueron las macros de Lotus 123 porque eran lo suficientemente poderosas para permitir este tipo de implementación. Por usar el lenguaje de programación Word Basic, la difusión masiva de los primeros virus de este tipo, desarrollados a principios de los 90’s, fueron para Microsoft Word.

Estos virus marcaron un hito en la historia: Terminaron con el paradigma de “los únicos archivos que pueden infectarse son ejecutables”, volviendo obsoletas a todas las tecnologías antivirus hasta ese momento (Borghello, 2021).

Básicamente los virus macros al estar añadidos en documentos de textos tienen la capacidad de expandirse a gran velocidad, provocando anormalidades en los documentos de texto, como es el caso de archivos con palabras faltantes o con palabras nuevas poniendo de este modo en peligro los datos almacenados.

- **Virus de lenguajes de Script:**

Es un tipo de virus de archivos, escritos en lenguajes de scripting varios como el VBS, JavaScript, BAT, PHP, etc. Además de esto, infectan a otros scripts como archivos de servicio y comandos de Windows o Linux, o forman parte de un virus con múltiples componentes. Estos virus tienen la capacidad de infectar otros archivos con formatos como el HTML ya que este permite la ejecución de scripts (Eset, 2020).

Dentro de un Servidor Apache que aloje varios servicios web a nivel de Intranet o Extranet este virus podría ser sumamente fatal puesto que tendría la capacidad de infectar todos los módulos diseñados.

- **Malware:**

Es el término usado para referirse a cualquier tipo de software malicioso (malicious software), diseñado para infiltrarse y ejecutarse en su dispositivo sin su conocimiento.

Existen muchos tipos de malware, cada uno con distintos objetivos, sin embargo, todas las variantes trabajan activamente en contra de la persona afectada (AVAST, 2021). Algunos tipos de malware son:

- **Gusanos:**

Están diseñados para proliferarse. Un gusano infecta al equipo y se replica, extendiéndose a dispositivos adicionales mientras permanece activo en todos los sitios infectados. Algunos de estos malware actúan como vectores para instalar malware adicional, otros sólo están diseñados para extenderse sin causar daño intencionado en las máquinas por cuales pasan, aunque siguen saturando redes con su demanda de ancho de banda (AVAST, 2021), lo que implicaría ciertas falencias en el tráfico de red, de igual manera podría generar

agujeros de seguridad tanto en el sistema operativo como a nivel de aplicaciones.

- **Spyware:**

Este software acumula la información sobre el equipo o red en la que se aloja para luego enviársela al atacante. Es un tipo de software comúnmente usado por los hackers para supervisar la actividad de internet de una persona, recopilando datos personales, bancarios, de redes, etc. Con el propósito de cometer fraude o robo de identidad o, en algunos casos, chantajear a la víctima (AVAST, 2021), la amenaza central de este virus está correlacionado con el hecho de que el mecanismo viola la integridad y privacidad del usuario a través de un levantamiento de información a nivel de extranet, lo que implicaría que los ataques que se puedan realizar sean sumamente versátiles y altamente intrusivos.

- **Ramsomware:**

Este software actúa como “nota de rescate”. El secuestrador en este caso es el hacker, y el ramsomware se usa para bloquear o denegar el acceso al dispositivo y a sus archivos a menos que se le pague un rescate. Cualquier persona o grupo, natural o empresarial, que guarde información esencial en sus dispositivos corre el riesgo de enfrentarse a esta amenaza (AVAST, 2021), lo que fluctúa en el hecho de que los principales targets de este tipo de eventualidades sean las grandes compañías, ya que al contener servidores que contengan data crítica y sensible ocasiona que el pago de desbloqueo sea prácticamente inevitable.

- **Keyloggers:**

Este tipo de software identifica, registra y graba la pulsación de teclas o clicks del mouse; esta información, luego es recolectada por la persona que lo haya instalado, Existen en forma hardware o software.

Los keyloggers físicos son dispositivos que se instalan entre la computadora y el teclado, difíciles de identificar por el usuario promedio, aunque sencillo identificarlos a simple vista si se presta atención. Tienen distintas capacidades de almacenamiento y son, por lo general, usados por empresas para controlar a ciertos empleados (Borghello, 2021), usualmente esta herramienta está centrada básicamente en el robo de información, en especial los datos privados del usuario como es el caso de usuarios, contraseñas, números de tarjetas y pines

de bancos, por tal razón, es una herramienta que está enfocada en los delitos cibernéticos.

- **Bombas de tiempo:**

Son virus programados para activarse en determinado momento definido por su creador, una vez infectado el sistema, no se activará ni causará ningún tipo de daño antes del día previamente definido. Actúa al momento de ejecutar el archivo .exe integrado al programa descargado, de acuerdo a una acción o fecha estipulada y se almacena en la memoria del computador con varios efectos que pueden ser el consumo excesivo de recursos del sistema, la destrucción rápida o disimulada de ficheros, ataque a la seguridad del sistema implementando derechos de acceso o uso de la máquina para ciberterrorismo (AAAPN, 2021).

Todos los virus mencionados cumplen con la denegación del servicio del equipo para llegar a la obtención de la información, pero algunas de ellos como se puede apreciar en su conceptualización constan con la habilidad de autopropagarse a través del navegador para realizar un ataque masivo hacia las demás localidades dentro de su cobertura de avistamiento, todas estas cualidades, hacen de los virus informáticos un tema de cuidado y protección, y para ello se necesita plena autosugestión y conocimientos en base a seguridad para poder detener y denegar su avance o al menos mantenerlos controlados.

1.2.9. Herramientas para detectar vulnerabilidades

Entre las herramientas de pentesting más utilizadas para auditar y encontrar las vulnerabilidades por donde pueden acceder amenazas que afectan a cualquier sistema informático, se tiene:

Para la parte de redes:

- **Metodología de Cisco PPDIOO. –** Esta metodología está diseñada para definir las actividades pertinentes en cada fase del ciclo de vida de una red, para así ayudar a asegurar la excelencia de los servicios.

  El objetivo principal del PPDIOO es definir las actividades mínimas requeridas, lo que permite optimizar el desempeño de una red (S F, 2011).

  Al usar esta herramienta dentro de la empresa se obtiene el funcionamiento de la red LAN, como están distribuidos los equipos en las diferentes capas jerárquicas, la infraestructura física y lógica de los

dispositivos conectados a la red y los servicios otorgados por estos hacia los hosts finales.

- **WireShark. –** es un analizador de red open source que tiene como funcionalidad captar lo que sucede en la red, lo que implica que se puede diseccionar todos los paquetes de red a tal punto que se pueda encapsular a toda la información requerida a nivel de paquetes individuales.

  Una vez obtenido el respaldo de la red gracias a la metodología utilizada, se procede a analizar la red física de la empresa mediante este aplicativo, el cual presenta una variedad de características que ayudan a entender todas las vulnerabilidades existentes de forma física o a nivel de hardware y configuración de los dispositivos conectando a la red local de CENFORSP. CIA LTDA.

  Entre las principales características de esta herramienta están (Arguello , 2020):

  - Identificar amenazas y vulnerabilidades en una red.
  - Observar un tráfico de red para así depurar redes complejas.
  - Filtrar le tráfico de acuerdo a sus protocolos, puertos y demás parámetros.
  - Permite capturar paquetes y guardarlos en un archivo

iPerf3.- es un programa diseñado para medir capacidad de ancho de banda entre dos o más equipos a nivel local o a nivel de Internet. Entre los beneficios que esta herramienta puede llegar a ofrecer están (Redes Zone, 2021):

Cuenta con la capacidad de mostrar el estado de la conexión entre dispositivos conectados entre sí, se usa en la empresa para verificar la velocidad de obtención de información mediante el medio definido y comparar la velocidad con la cual se genera el envió de un paquete de un host a otro.

Para la parte de seguridad informática:

- **Kali-Linux. -** más que una herramienta es un sistema operativo open source, estructurado de tal manera que ya cuenta con las herramientas establecidas o preinstaladas para auditoria de redes e informática. Es la

versión actualizada de backtrackLinux, es un derivado de Debían por lo que su gestor de paquetes es apt-get, convirtiéndolo en un sistema operativo por defecto para un pentesting o autoría.

Para definir el ataque dirigidos hacia los servidores de la empresa CENFORSP. CIA LTDA, se usan las herramientas establecidas dentro del sistema operativo para el avance de los requerimientos para la captación de vulnerabilidades de la red LAN, comenzado con:

- **Escaneo de puerto usando Nmap. -** Nmap es la mejor herramienta de escaneo de puertos y descubrimiento de hosts que existe actualmente. Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red (De-Luz, 2021), es capaz de examinar qué dispositivo están habilitado, además de verificar si dichos equipos o hosts en la red local tienen algún puerto abierto y saber qué sistema operativo está utilizando un determinado objetivo al que se le procederá a realizar dicho escaneo.

  Para lograr la obtención de los puertos habilitados y deshabilitados del sector siempre es necesario tener a disposición un escaneador que permita distinguir entre los puertos seguros por los cuales el filtrado de información pertinente sea el correcto, ajustándose a todas estas características y acoplándose al esquema planteado Nmap es una herramienta que permite realizar un escaneo de puertos a los diferentes hosts, ver qué servicios tenemos activos en dichos hosts gracias a que nos dirá el estado de sus puertos, podremos saber qué sistema operativo está utilizando un determinado equipo, e incluso podremos automatizar diferentes pruebas de pentesting para comprobar la seguridad de los equipos (De-Luz, 2021).

  Para comprobar cuál es el estado de los puertos dentro de la red local y los hosts disponibles primero se debe entender como es la vista de los puertos y como se presentarán los resultados antes de hacer la auditoría informática. Entre los estados de los puertos tenemos:

  - **Open (abierto):** estado inicial de todo puerto en un dispositivo, (De-Luz, 2021) menciona que los pentesters podrán utilizar este puerto

abierto para explotar el sistema, debido a que se está aceptando conexiones TCP o UDP.

- **Close (cerrado):** son útiles para indagar si es que existe o no un host levantado a través de él, de cara al administrador del sistema, es recomendable filtrar estos puertos con el firewall para que no sean accesibles. De cara al pentester, es recomendable dejar estos puertos "cerrados" para analizar más tarde, por si ponen algún servicio nuevo (De-Luz, 2021).
- **Filtered (filtrado):** en este estado Nmap no puede determinar si el puerto está abierto, porque hay un firewall filtrando los paquetes de Nmap en dicho puerto. Estos puertos filtrados son los que aparecerán cuando tengamos un firewall activado (De-Luz, 2021). Por eso es uno de los estados más seguros de la red pese a que la llegada de información es un poco retardada.
- **Open | Filtered (abierto y filtrado):** el intentar usar este tipo de puertos es una de las denegaciones más comunes, debido a que Nmap no sabe si el puerto está abierto o filtrado. (De-Luz, 2021) menciona que esto ocurre porque el puerto abierto no envía ninguna respuesta, y dicha falta de respuesta podría ser por el firewall. Este estado aparece cuando usamos UDP y IP.
- **Close | Filtered (cerrado y filtrado):** en este estado no se sabe si el puerto está cerrado o filtrado por lo tanto se lo conoce como niegue absoluto de la información, existen como accesibles para su posible alcance que ocurren a través del IP Idle Scan.

- **MetaSploit vulnerabilidad a nivel lógico. -** es una herramienta poseedora de múltiples cualidades que permiten atacar a una red, servicio o sistema informático con el objetivo de un caso de estudio, auditoría o deshabilitación de servicios (Rizaldos, 2018). Es muy completa porque tiene gran cantidad de exploits, que son vulnerabilidades conocidas, Un **exploit** es un ataque que usa una vulnerabilidad de software para causar algún tipo de efecto no deseado en el sistema objetivo, como instalar malware o dar al hacker el control u otro tipo de acceso. Incluso si existe

una determinada vulnerabilidad, no hay ningún peligro inmediato hasta que alguien averigua cómo crear un exploit para ella (Belcic, 2020).

Estos ataques vinculados directamente a una vulnerabilidad especifica son creados a partir de lenguaje de programación como Rugby, C++, Java Script y Python, este último es un sistema muy sencillo de utilizar debido a la gran facilidad a nivel de programación con el que se puede desarrollar. **Python** y todas las herramientas necesarias para la creación de aplicaciones disponibles están en todas las plataformas principales. Por lo tanto, es una opción **multiplataforma**, bastante tentadora para los desarrolladores que no quieren preocuparse por pagar altos costos de desarrollo y también dar a conocer a demás atacantes lo que en simple contexto es la vulnerabilidad específica y como se la ataca.

Un dato interesante de esta herramienta es la forma con la que permite interactuar con otras aplicaciones externas, para que en conjunto se pueda explotar al máximo la mayor debilidad que se presente dentro de cualquier sistema, además también permite transportar el malware generado a cualquier otro sistema operativo o formato, ya sea Windows o Unix, debido a que este labora en Linux como atacante principal.

Para poder demostrar la efectividad de cada una de estas herramientas dentro de la empresa, se planea utilizar una simulación que permita detectar ataques establecidos por defectos y así vincularlos a los registrados dentro de la institución, de tal manera que, se exponen las afectaciones actuales de la empresa y como solucionarlo mediante un plan de seguridad informáticas orientado por las normas ISO 27002.

1.2.10. Infraestructuras vulnerables

Los sistemas modernos ya no son herméticos. La integración con redes Internet los exponen a las mismas vulnerabilidades que cualquier otro sistema TI como por ejemplo nuevos dispositivos IoT, segmentación de redes, configuraciones por defecto, gestión de privilegios y accesos remotos, cifrado de comunicaciones y datos, vulnerabilidades en interfaces Web de aplicaciones, parcheado y sistemas operativos obsoletos (Galán, 2020),

Entonces considerando el concepto anterior se dice que una red no será totalmente vulnerable debido a que dentro de los sistemas e infraestructura de las TI siempre se encuentra un medio por el cual se pueda llegar a obtener la información solicitada o necesario para destruir la confiabilidad de la red a la que se quiere deshabilitar. Por ello también es indispensable saber qué tipos de servicios se ofrece dentro de la empresa, porque son factores que los atacantes utilizan para generar vulnerabilidades dentro de la infraestructura de la red, entre estos servicios tenemos:

- **Servidores informáticos**

En el mundo tecnológico, es necesario tener un registro de todo servicio ofrecido dentro de la red local, los dispositivos alojados en una zona segura y encargados de la prestación de servicios hacia los demás componentes o dispositivos finales de la red LAN son los servidores, los cuales usando un sistema cliente-servidor que se encarga de proporcionar los servicios ya sea web, base de datos, recursos compartidos y demás opciones dependiendo de las necesidades de la empresa en donde se instala dicho servidor, los servidores usados en la compañía CENFORSP. CIA LTDA son los siguientes:

- **Servidor web. – "**Se ocupa de guardar la información en formato HTML de los sitios**,** donde se incluye texto, imágenes, videos y todo tipo de datos. Mediante un explorador web, los usuarios puedan visualizar todo esto en sus pantallas" (Colaborador de DocuSign, 2020).

  También gestión información en formatos alternativos como PHP, JSP; estos se ven reflejado en SUN java SWS, y son usados debido a su alto rendimiento y alcance dentro del mercado actual por su código abierto. Uno de los principales servidores web es el Apache debido a que es un sistema multiplataforma que brinda buen soporte, estabilidad y seguridad además de ser didáctico y sencillo en su uso.

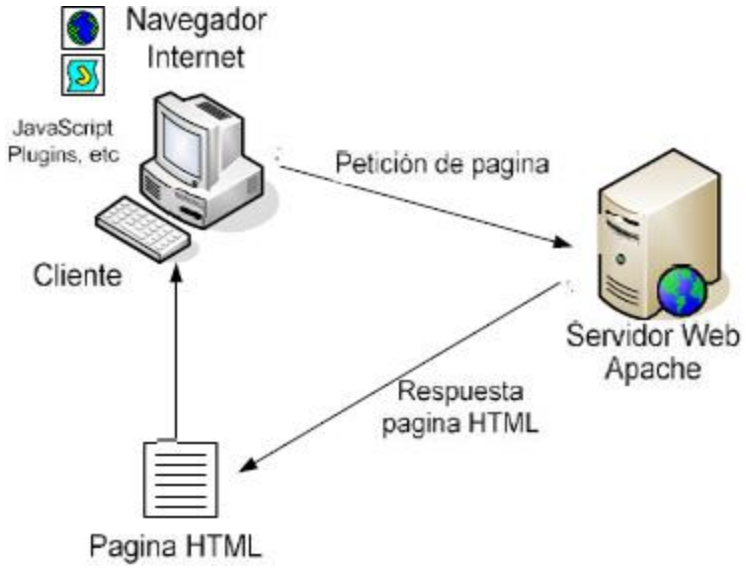

***Figura 3**. Vista del servidor web*

Nota. Fuente (Anonymous, 2013)

También existen otros servidores web como Microsoft IIS (adaptable solo en Windows) que permite transformar un host en un servidor web, pero en una pequeña escala y también están los Lighttpd (veloz en sentido de paquetería) este funciona para empresas que soliciten registros rápidos.

- **Servidor de base de datos. – "**Son dispositivos diseñados para almacenar grandes cúmulos de información y poder gestionar los datos uno por uno. También son capaces de analizar, manipular y alojar los datos de acuerdo a los requerimientos del usuario" (Colaborador de DocuSign, 2020).

El tener una base de datos disponible para cada institución es uno de los ideales de la tecnología actual debido que el tener un lugar donde almacenar información para poder administrarla, analizarla y compartirla permitirá un crecimiento en el mercado laboral y se entenderá también la importancia de la información frente a toda situación.

Un ejemplo claro es que "usualmente está controlada por un software que nos ayuda con la administración, en el caso de WordPress, es común utilizar MySQL como software para la administración de la base de datos. Muchas veces pensamos que el contenido de WordPress se encuentra en archivos HTML, sin embargo, la mayor parte del contenido de las

entradas, páginas, comentarios, etc. están guardados en una base de datos" (Marreros, 2019).

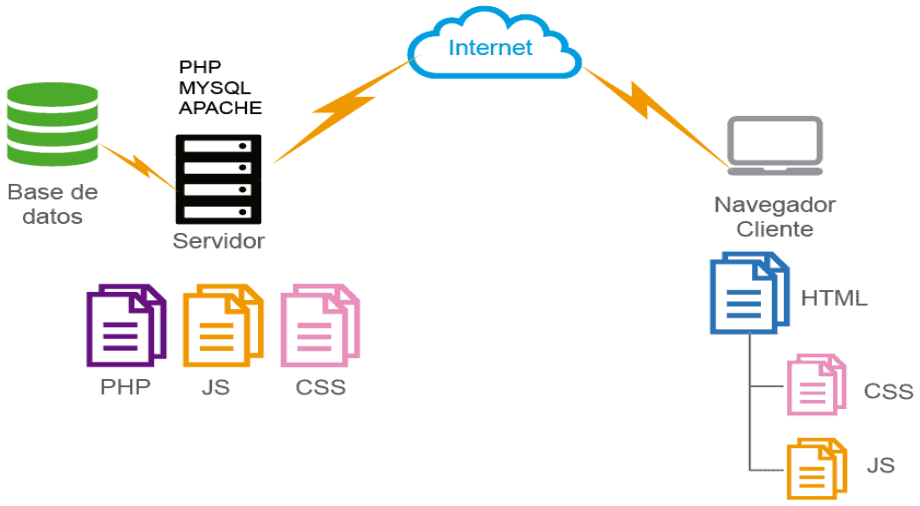

***Figura 4**. Vista del servidor de base de datos.*

Nota. Fuente (Marreros, 2019)

Entre las bases de datos más comunes que se presentan en la actualidad por su gran capacidad de registro y monitoreo de todos los campos posibles son mySQL, Maria Db, PostgreSQL, presentes en todo ambiente laboral.

- **Servidor de transferencia de archivos (FTP). –** Si hay un proyecto comercial y se desea expandir en sentido tecnológico los servicios otorgados ya sea internet, carpetas compartidas, transferencia de información y demás, se debe elegir entre adquirir o contratar servicios de alojamiento, almacenamiento y demás dependiendo de las necesidades de la empresa, para tener mayores probabilidades de éxito. "Además, al contratar servicios de este tipo, las copias de seguridad mantendrán a salvo tu información y evitarás que, por fugas, negligencia, malas prácticas o por ciberdelincuencia pierdas lo que es importante para tu organización" (Colaborador de DocuSign, 2020).

  En síntesis, el servidor FTP tiene la capacidad de realizar una conexión rápida y directa con el servidor, por ende, resulta ideal para la

transferencia de archivos de manera bidireccional en ambientes multiplataformas.

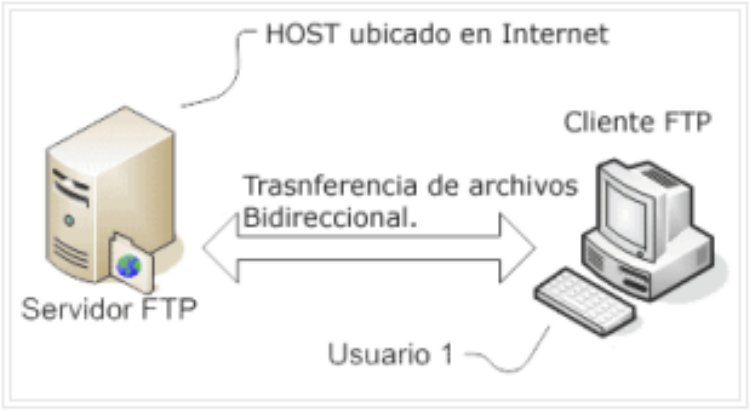

***Figura 5**. Modelo de trabajo del Servidor FTP*

Nota. Fuente (Wordpress, 2013)

1.2.11. Sistema de gestión de seguridad de la información

Toda entidad junto con sistema de operación necesita una manera, estrategia, planificación y forma de mantenerse a salvo en base a los ataques que se les avecine después de cierto tiempo, llevar un control preventivo ayuda a que todo el organismo se mantenga seguro

y de llegarse a dar el caso de haber afectaciones actuales ya dentro del sistema informático usar métodos correctivos para defenderlo.

Un sistema de gestión para la seguridad de la información es un método de cuidado que permite ordenar, estudiar y analizar la estructura y diseño de los sistemas de información, también el establecer los procedimientos, reglas y pasos de trabajo para mantener su seguridad y confidencialidad, incluso dispone de controles para llevar medición de la eficacia de lo establecido anteriormente. La idea es alcanzar un nivel de riesgo menor que el soportado por la institución, para preservar la confidencialidad, integridad y disponibilidad de la información (Vargas A. , 2013).

Figura 6.- *Sistema de Gestión de la Seguridad Informática*

Nota: Fuente (Vargas & Castro Mattei, 2020)

1.2.11.1. Diseño de modelado y la infraestructura lógica del conflicto

Para el adecuado diseño de políticas TI se propone la confección de una lista de chequeo que contenga, por ejemplo: la infraestructura TI crítica para la organización, el nivel de preparación de los recursos humanos que interactúan con las infraestructuras TI, los elementos de configuración de cada servicio, así como de la infraestructura subyacente que lo soporta, la lista de alertas que se consideren y las respuestas ante las mismas, las principales métricas de rendimiento asociadas al cumplimiento de los SLA, las tareas comunes de gestión: salvas, gestión de fallas, gestión de cambios, aprovisionamiento de servicios, creación y borrado de usuarios, así como los requisitos de calidad, asociados al negocio: sus estrategias y metas junto a las principales restricciones asociadas a los servicios, entre otros (Peña & Anías, 2020).

De acuerdo al plan expresado se menciona la acometida de actividades pertinente para el comienzo de la creación del diseño para un modelo de seguridad y plan de mejora informática, partiendo desde el uso de la información obtenida en el paso anterior y adaptándola a los estándares elegidos que

fomentan el buen uso de las seguridades en las redes de telecomunicaciones, también se usan las estrategias necesarias para la generación de ítem a cumplir una vez el diseño de seguridad esté listo, la metodología a utilizar es la que se visualiza a continuación:

1.2.11.2. Plan de Diseño a través de SGSI

Un Sistema de Gestión de Seguridad de la Información según la ISO27001 genera una garantía con la que sabemos que podemos realizar una adecuada gestión de la seguridad de la información en la organización (LOZANO & CORREA, 2020). De tal manera que, de realizar una evaluación para luego un análisis que permita tratar de forma adecuada cada gestión de trabajo permitida dentro de cada área afectada de la red local dentro de compañía.

Este sistema de gestión informático crea un procedimiento de mejora que evoluciona junto a los cambios que se pueden producir en la empresa, por su gran flexibilidad y adaptación del sistema, diciendo que los procesos de economía y tecnología son los que avanzan a una gran velocidad.

Para ello es necesario seguir un proceso conocido como Ciclo Deming el cual describe etapas que se realizan para cumplir con el SGSI y de esta manera establecer un uso automatizado de desarrollo que permita la autonomía de dicho diseño de seguridad en la red.

1.2.11.3. Ciclo Deming (PHVA)

El diseño de un plan de mejoras para la seguridad de la red, en función de las vulnerabilidades y amenazas detectadas en la empresa CENFORSP. CIA LTDA basado en un modelo de seguridad usando los, estándares ISO 27000 e ISO 27001, consta de las siguientes características a trabajar para su correcta generación como propuesta tecnológica, frente a la obtención del título universitario:

- **Planear:** se establece los respectivos procesos de lo que se quiere llegar a mejorar con énfasis en los objetivos planteados y el método de medición que se tomará para evaluar el avance que se estima dentro de la institución, se llega al criterio de que aplicar las normas y estándares

mencionados e implementarlos dentro de un diseño estructurado de un sistema de protección digital para la seguridad informática de una empresa, que se encarga de dar control y servicio de enseñanzas de seguridades físicas y que posee mucha información pertinente, necesita un plan de protección que conste de dispositivos adicionales específicamente encargados de la protección de la red.

- **Hacer:** para poder realizar lo planeado se trata de crear una esquematización de lo ocurrido actualmente dentro de la empresa, y mediante un análisis de lo sucedido y las prácticas generadas gracias al estándar otorgado en los criterios de ayuda establecer una solución óptima fácil y accesible para la pronta instalación de dicho diseño dentro de la organización
- **Verificar:** para el proceso de verificación en el caso del proyecto estimado siempre es necesaria la utilización de verificadores de sistemas, el tratar de atacar a la red y saber hasta dónde permite nuestro a avance será la principal herramienta para verificar que tan seguro es el sistema y si realmente ha aumentado la seguridad de las empresas, estos resultados ayudarán a establecer el crecimiento e importancia de este proyecto de seguridad informática dentro de un sistema poco convencional.
- **Actuar:** Una vez realizado la respectiva verificación, se objeta para realizar mantenimientos preventivos que eviten el avance de nuevas vulnerabilidades, si los resultados no cumplen con las expectativas y los objetivos predeterminados, se realizan las correcciones y modificaciones necesarias. Por otro lado, se toman las decisiones y acciones adecuadas para mejorar continuamente el desarrollo de los procesos.

Dentro de la obtención de análisis de la información de los datos establecidos por los pasos a anteriores, se obtiene una metodología de fases agrupadas para el análisis de riesgos de amenazas frente a las vulnerabilidades encontradas en la organización.

Para ello, identificar los activos críticos de los sistemas de información que pueden suponer un riesgo para la empresa, realizando un análisis de riesgos. Análisis que nos llevará a obtener una imagen rigurosa de los riesgos a los que

se encuentra expuesta la empresa (INCIBE, 2017). Estas fases son las siguientes:

Figura 7.- *Fase de análisis de riesgo*

Fuente: (INCIBE, 2017)

Fase 1. - Definir el alcance del análisis de riesgos: se trata de analizar riesgos en todos los campos de la institución, pueden ser todos los servicios, departamentos, actividades entre otros sectores donde la prioridad es saber cuáles son los riesgos hacia las partes de cada parte de la empresa.

Fase 2. – identificar y valorar los activos de información: los datos obtenidos de la fase anterior sirven para identificar los movimientos por parte de los atacantes de la red y amenazas que darán paso a incontables inconvenientes a la red local y por ende a la empresa.

Fase 3. – Identificar las amenazas: el saber qué tipo de amenazas son las que están atacando a la integridad de la red, permite brindar una solución palpable hacia los encargados de solventar dichos conflictos, de tal manera que es aconsejable crear una red poco vulnerable, donde no haya que establecer auditorias de manera seguida para que así que se mantenga un margen de confidencialidad y el ahorro de recursos no estimados por la empresa.

Fase 4. – Estudio y análisis de las características de los activos: en esta fase se estudia las posibles herramientas con las que la empresa u organización cuenta para la generación de un sistema de defensa informática frente a los ataques, amenazas y vulnerabilidades detectadas, por lo general el uso de aplicaciones informáticas, supera por mucho a los dispositivos que flaquean a la red en los ámbitos de información y penetración a la red local, debido a que, se busca usar software de libre acceso de la información para el ahorro de activos. En el caso de CENFORSP. CIA LTDA. Existe la problemática de que al no poseer ciertos recursos informáticos ni tener amplios conocimientos en el ámbito de redes, carecen de activos capaces de elevar la seguridad informática dentro de la empresa.

Fase 5. – Estimación de amenazas por cada activo: obtener una probabilidad en la cual se establece el rango de daño que una amenaza especificada puede atentar contra la red y a su vez a la compañía, y además si existe una posibilidad de solventar dicha amenaza, a través del proceso de solución de vulnerabilidades encontradas en la red. Por esa razón al diseñar un modelado de seguridad informática dentro de la localidad antes mencionada, se hace realidad la probabilidad de disminuir constantemente los apartados que ocasionan conflictos al sistema de telecomunicaciones e información.

Fase 6. – Tratar aquellos casos que superen un límite: una vez estimados los riesgos, amenazas y vulnerabilidades dentro de la red de área local, se pasa a encontrar vías optimas de solución frente al esquema de análisis esperado, a través de activos, métodos y estrategias nuevas establecidas gracias al análisis realizado en las fases anteriores.

Los estándares en los que se va a basar para la realización diseño de un modelo de seguridad y plan de mejoras para la seguridad de la red, en función de las vulnerabilidades y amenazas detectadas en la empresa CENFORSP. CIA LTDA. basado en los estándares ISO 27000 e ISO 27001, tal y como se estima en el tema de la propuesta, por lo tanto, se plantea una explicación de dichos estándares y normas.

En este capítulo se analizaron los conceptos teóricos asociados al objeto de estudio, es necesario destacar que todo proyecto que implique la detección de problemas de seguridad debe estar alineado a las normas iso 27000. A partir de ello se aplicará en la presente investigación, las normas 27001 y 27002 mismas que están vinculadas a las necesidades de la empresa. Adicionalmente se utilizará la metodología PPDIOO para organizar el proceso de comprobación, detección y mejoramiento de la red informática de la empresa como herramientas.

1.3. Marco Legal

El Código Orgánico Integral Penal del Ecuador indica:

TÍTULO IV - Infracciones en Particular

Capítulo Segundo - Delitos Contra los Derechos de Libertad

Sección Novena – Delitos contra el derecho a la propiedad indica en:

Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Capítulo Tercero - Delitos Contra Los Derechos Del Buen Vivir

Sección Tercera - Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en

ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 232.- Ataque a la integridad de sistemas informáticos. **-** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos

que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS

TITULO PRELIMINAR

Capítulo I - Principios Generales

Art. 5.- Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

TITULO V - de las infracciones informáticas

Capítulo I - de las infracciones informáticas

Art. 57.- Infracciones informáticas. - Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley. Reformas al Código Penal Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos enumerados:

"Art. - El que, empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. - Obtención y utilización no autorizada de información. - La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

"Art. ...- 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo enumerado:

"**Art. ...- Falsificación electrónica**. - Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho. El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

Art. 61.- A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos enumerados:

"Art. ...- Daños informáticos. - El que dolosamente, de cualquier modo, o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o

cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica. La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art. ...- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Art. 62.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos enumerados:

"Art. ...- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. ...- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente: "Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente: "... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

En este capítulo se analizaron los conceptos teóricos asociados al objeto de estudio, es necesario destacar que todo proyecto que implique la detección de problemas de seguridad debe estar alineado a las normas ISO 27000. A partir de ello se aplicará en la presente investigación, las normas 27001 y 27002, mismas que están vinculadas a las necesidades de la empresa.

Adicionalmente se utilizará la metodología PPDIOO para organizar el proceso de comprobación, detección y mejoramiento de la red informática de la empresa con herramientas y técnicas como métodos de aislamientos de servidores en zonas desmilitarizadas y herramientas como lo son Wireshak (analizadores de redes) y Nmap (escaneadores de puertos) que permitan dar un constante monitorio a las posibles vulnerabilidades dentro de la empresa y también usar manera viables de protección y buenas prácticas de seguridad informática proporcionadas por la norma ISO 27002, para que no haya necesidad de corregir o perder todo tipo de información en base a un ataque generado, siguiendo siempre todas las leyes constitucionales que se le permiten a una persona capaz de manipular un ordenador.

Estos conceptos planteados dentro de la documentación permiten al usuario la comprensión y uso de planes de seguridad usando ciclo Deming (PHVA), capaces de reducir, avisar, proteger y solventar la información de la empresa de todo tipo de vulnerabilidades ya sean físicas como lógicas, actuales o futuras, pueden ser aplicadas para moldear la seguridad informática comenzando con las vulnerabilidades existentes como lo son la inseguridad en los puertos de comunicación, la falta de conocimientos tecnológicos por parte de los empleados de la empresa y la poca aplicación de las normas ISO en seguridad de la información.

CAPÍTULO 2: METODOLOGÍA DEL PROCESO DE DESARROLLO DE LA PROPUESTA TECNOLÓGICA

En este punto de la propuesta tecnológica, se establece los criterios principales mediante los cuales se llegó a la obtención de información referente a el diseño de un modelado de sistema de seguridad informática, para ello se debe interpretar el ambiente mediante el cual se está estableciendo el conflicto y utilizar metodologías, o enfoque que ayuden al investigador adquirir la suficiente información capaz de permitirle dar un análisis estratégico del contenido.

2.1. Enfoque de la investigación

Debido a que los objetivos de la investigación plantean diferentes tipos de análisis a cuestionar, tanto cualitativos por el uso de las descripciones de las vulnerabilidades y amenazas donde se resalta el hecho de conceptualizar cual es el pertinente problema que amedranta la seguridad informática y la conceptualización de las redes LAN de la empresa en cuestión y cuantitativas por el uso de parámetros que permitan establecer que tan segura es la red local del lugar en donde se presentan irregularidades y hostigamientos, por lo tanto, se establece que el enfoque investigativo de esta propuesta tecnológica es de forma mixta, donde se visualiza el uso de ambas cualidades tanto cuantitativas como cualitativas.

Enfoque Mixto: no es simplemente una mezcla en la cual las características particulares de cada enfoque se borran o se vuelven relativas. La riqueza de la investigación mixta consiste en aprovechar las bondades y fortalezas de cada enfoque (Salas, 2019).

Debido a esto, se plantea una relación entre características basadas en la utilidad de ambos componentes, para una mejor obtención de información al diseñar un modelo de seguridad informática usando los criterios posibles a explorar y generar un concepto sólido y fiable que tenga un alcance de estimación elevado y así llegue a ser usado a futuro por más empresas y organizaciones que dispongan de dicho esquema, frente a futuras amenazas

digitales, las cuales van a ser predeterminantes de una sociedad tecnológica avanzada en futuras generaciones.

2.2. Tipo de Investigación

Los tipos de investigación son la manera de saber qué tipo de adaptación debo tomar para establecer la adquisición de variables dentro de un tema de investigación, estos se fomentan junto al enfoque investigativo, donde se establece el modelo que se usa como guía para el desarrollo investigativo de la propuesta tecnológica del desarrollo de un diseño de modelo de seguridad y plan de mejoras en una red LAN dentro de una institución.

Para el desarrollo se optó por usar una investigación descriptiva que, junto a su método de observación, servirán para el análisis y obtención de información, y también un modelo de investigación explicativa que sirve para identificar causas y problemas en base a la obtención de parámetros y uso de herramientas que en el caso del proyecto seria las de herramientas técnicas que nos sirva para identificar los problemas, amenazas y vulnerabilidades existentes dentro de la organización o negocio para luego poder describirlas.

Investigación descriptiva. – La investigación descriptiva analiza las características de una población o fenómeno sin entrar a conocer las relaciones entre ellas (Arias, 2021). Entonces el tipo de investigación descriptiva se encarga de evaluar los campos necesarios para poder cumplir con los objetivos, plantean sin preguntar por qué o de donde salió el problema desde antes de que se aconteciera, o saber cómo se relacionan las variables entre sí.

En este caso la investigación descriptiva servirá para poder describir de forma precisa las vulnerabilidades y amenazas que aquejan la seguridad perimetral de la zona desmilitarizada de la empresa CENSFORSP. CIA LTDA, es importante destacar que esto es posible gracias al empleo de diferentes técnicas y métodos como es el caso de:

- **Método de observación**: El más eficaz para llevar a cabo la investigación descriptiva. Se utilizan tanto la observación cuantitativa (recopilación objetiva de datos que se centran principalmente en números y valores) como la observación cualitativa (mide características de los elementos a

investigar) (Arias, 2021). En este caso se utilizó NMAP como herramienta de observación, ya que con este implemento se podrá escanear el equipo target deseado y de este modo poder observar cuáles son sus vulnerabilidades a nivel lógico, para esto bastaría utilizar el comando Nmap más la dirección ip del equipo que se quiera auditar.

```
nmap [ip]
```

Figura 8.- *escaneo rápido de puertos en un host.*

Nota: *fuente* (De-Luz, 2021)

Investigación Explicativa. - según (Mejia, 2020) la investigación explicativa es un tipo de investigación cuya finalidad es hallar las razones o motivos por los cuales ocurren los hechos del fenómeno estudiado, observando las causas y los efectos que existen, e identificando las circunstancias. Entonces con este tipo de investigación se puede dar explicaciones detalladas de los riesgos que puede ocurrir cuando se tenga una amenaza y se explote una vulnerabilidad dentro de la empresa, de manera que a esta investigación le debe preceder varias investigaciones como las descriptivas que aportan datos importantes y de esta manera se puede realizar un proceso explícito y exacto de la situación en un lapso de tiempo determinado. En este apartado en particular se llevó a cabo el proceso de investigación explicativa a través del resultado de mapeo de puertos, ya que con esta incidencia se podrá determinar las vulnerabilidades dentro del servidor que se desee auditar.

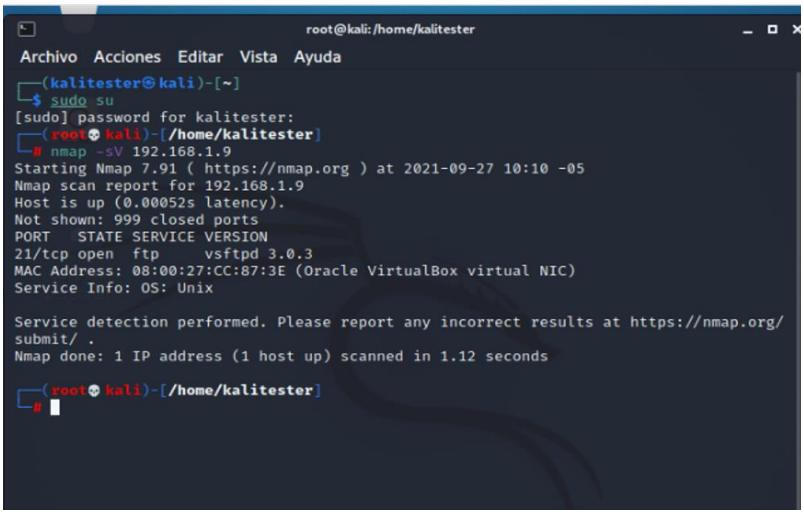

Figura 9.- *lista de estados de los puertos.*

Nota: *fuente* (De-Luz, 2021)

2.3. Período y lugar

La empresa CENFORSP. CIA LTDA es encargada de proporcionar capacitaciones profesionales para guardias de vigilancia y seguridad privada, donde no solo se encargan de capacitar a las personas que buscan una oportunidad laboral de ese ámbito sino también resguardan su información confidencial y su record policial y demás datos personales que sirven como previo requisito para su inscripción, en la actualidad se han presentado cometimientos y acciones delictivas en contra del personal laboral y también hacia los clientes del curso de capacitación, tanto de forma física como también el hurto de identidad perjudicando así la reputación y la confiabilidad de la empresa. Estos ataques directamente a la red LAN actual se establecieron justo por la deficiente seguridad informática presente de la compañía.

Figura 10.- *logo de la compañía CENFORSP. CIA LTDA*

Nota: *dirección: Av. Del ejército y Luis Urdaneta, esquinero*

2.4. Variables

Las variables de la propuesta tecnológica se basan en el ámbito tecnológico de la información en dónde su principal uso es el identificar el fin de los acontecimientos principales que ocurrieron tras el porqué de las vulnerabilidades y amenazas presentes por falta de una buena seguridad de la red informática en

forma local. Para ello debemos estudiar el concepto y operación de las varias mencionadas.

- ✓ **Conceptualización. -** es un ámbito conceptual existente, datos que ya han sido propuestos o antecedentes predominantes de la variable.
- ✓ **Operacionalización. –** es la manera con la que se miden los datos de red en cierto modo usando instrumentos herramientas he indicadores que permitan tener un registro de las actividades establecidas para el análisis de las variables en cuestión, tanto las dependientes como independientes.

Variables	Conceptualización	Indicadores	Instrumentos Y/O Métodos.
Vulnerabilidades y Amenazas informáticas detectadas dentro de la institución.	Las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas (INCIBE, 2017).	**Amenazas:** Uso no autorizado de Sistemas Informáticos, Robo de Información, Suplantación de identidad, Denegación de Servicios (DoS), Ataques de Fuerza Bruta, Alteración de la Información, Divulgación de Información. **Vulnerabilidades:** Errores de configuración, Errores en la gestión de recursos, Errores en los sistemas de validación, Errores que permiten el acceso a directorios y puertos permitidos, Errores en la gestión y asignación de permisos. Falla en servidores informáticos dentro de la DMZ.	"**Network Mapper" Nmap. -** Mapeo de red. Reconocimiento y cateo de la red local. **Nessus. -** programa de escaneo de vulnerabilidades en diversos sistemas operativos. **Metasploit. -** es un proyecto de código abierto para la seguridad informática, que penetra en las defensas levantadas de la red **Metodología de Cisco PPDIOO. –** pasos a seguir para la reestructuración de la red.
Fallo de seguridad de la red LAN.	Según (Molinetti, 2020) estas redes suelen incorporar métodos de conexión directa a internet vía Wi-Fi, lo que facilita el rendimiento en el trabajo, pero también abre las puertas a posibles riesgos si no se toman en cuenta medidas sólidas de seguridad y buenas prácticas internas.	Conflictos con direcciones IP, Tarjetas de red defectuosas. Fallas en switches o Routers, Insuficiente Ancho de Banda.	**WireShark.-** es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones **iPerf3.-** diagnosticar de análisis de una red completa, de forma física como lógica.

Tabla 1: *Variables de la propuesta tecnológica*

2.5. Métodos empleados e instrumentos de la investigación.

Tener un análisis real de la situación que aqueja a la compañía mediante el levantamiento de información requerido obtenido mediante el escaneo de puertos y del direccionamiento IP de cada uno de los hosts de la empresa, permitirá determinar un plan de estrategia que permita salvaguardar la integridad informática de la compañía, es importante destacar que dicho estratagema puede centrarse tanto en términos técnicos como a nivel de recursos humanos, puesto que en teoría solo bastaría contar con equipos de seguridad externos, también hay que tomar en cuenta la gestión de información manejada por los usuarios finales, como es el caso de claves inseguras, contraseñas repetidas en varios servicios de intranet, falta de conocimientos de seguridad a nivel de usuarios y demás.

2.5.1. Procesamiento y análisis de la información.

El procedimiento y análisis del trabajo de investigación o propuesta tecnológica del diseño del modelo de seguridad y plan de mejoras a una red LAN, será realizado a través de metodologías, pasos y fases a seguir con proceso de seguimiento y estrategias que permitan el aporte de información valiosa y exacta para el mejoramiento de una red informática, se da uso de los siguientes pasos antes del diseño del modelo de seguridad informática.

Una vez definido el enfoque o metodología donde se va a comenzar el procesamiento y análisis de la información, se describen los pasos mediante los cuales se dará la obtención de dichos datos, tanto de las amenazas que amedrantan a la cooperación como también las vulnerabilidades existentes en la actualidad, mediante los cuales se llegará a un correcta reparación, rediseño y reestructuración de la red LAN de CENFORSP. CIA LTDA.

Dentro de los pasos para el desarrollo de las actividades que se llevaran a cabo para la culminación de la propuesta tecnológica, se presentan los siguientes puntos visibles capaces de orientar el diseño del modelo de seguridad y plan de mejoras para la seguridad de la red, en función de las vulnerabilidades y amenazas detectadas en la empresa CENFORSP. CIA LTDA. basado en los estándares ISO 27000 e ISO 27001

2.5.2. Preparación para en análisis de vulnerabilidades

Como antesala para realizar la explotación de un servidor mediante una máquina virtual generada con Kali-Linux donde se usa la herramienta descargada de Metasploit db, es determinante comprobar dos parámetros claves, los cuales se detallan a continuación:

- Los equipos tanto de testeo, como el servidor se encuentren en la misma red, para facilitar los procesos técnicos de la instalación de los exploits dentro de la máquina atacante y la obtención de las direcciones Ip correspondientes de cada servidor de la empresa CENFORSP. CIA LTDA.

  En las imágenes se aprecia el terminal de Kali y de Ubuntu FTP, la máquina Kali será quien realiza el ataque de exploit hacia el servidor FTP el cual por defecto tiene disponible sus puertos.

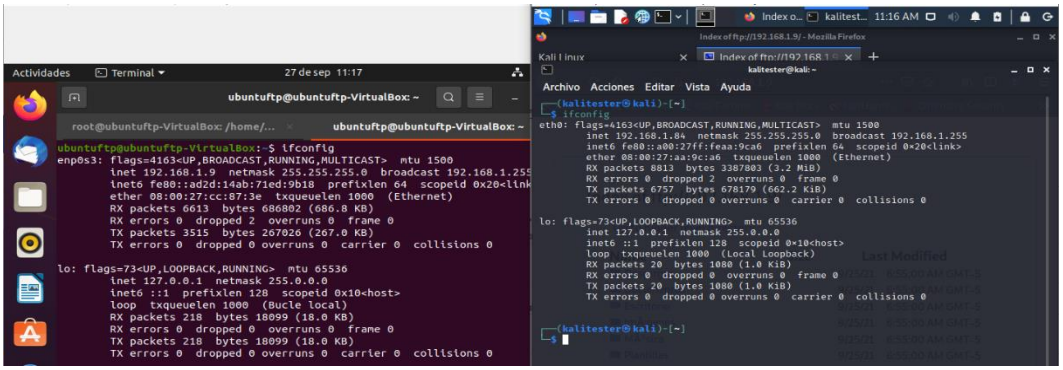

Figura 11.- *verificación de direcciones de red entre servidor FTP y el equipo de tester.*

Nota. Elaborado por Joan Zambrano.

- Lo siguiente es que el servicio FTP se encuentre activo lo que se puede observar a través del comando ***service vsftpd status*** y asimismo que se encuentre funcional, antes de realizar el ataque para verificar si es que realmente haya un cambio después de realizar la configuración pertinente.

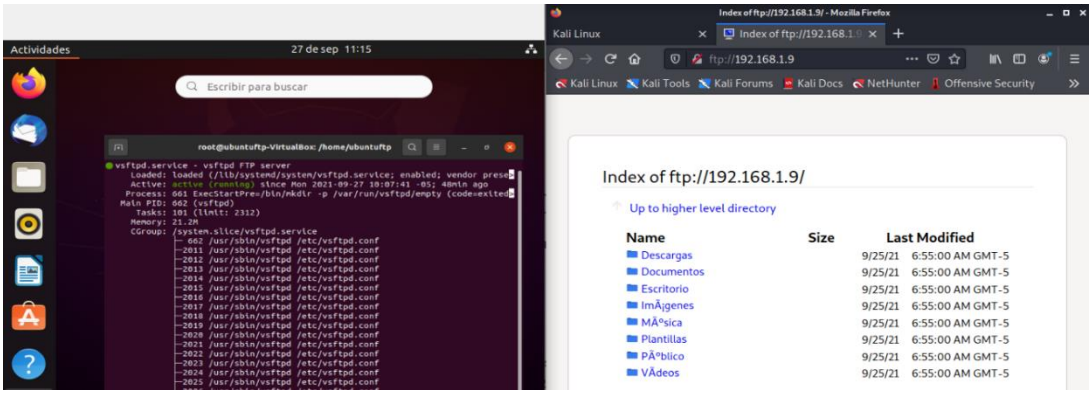

Figura 12.- *verificación del servicio FTP*

Nota. Elaborado por Joan Zambrano.

Continuando con el manual para la operación de explotación a uno de los servidores disponibles, como lo es el servidor de transferencia de archivos que posteriormente se vio su inicialización y uso dentro de uno de los hosts de la empresa, se procede a realizar el respectivo ataque con los siguientes pasos:

1. **Escaneo de puertos:** para empezar el pentesting requerido, es necesario realizar un escaneo de puertos desde el equipo que funcionará como testeador, para esto se utiliza el comando **Nmap -sV (dirección ip)** (al equipo al cual va dirigido el metasploit), puesto que con este comando se podrá determinar el estado de los puertos del equipo que se recibe la infiltración y también se aprecia la versión del protocolo que se está usando, además del servicio que está brindando dicho puerto al momento de estar disponible.

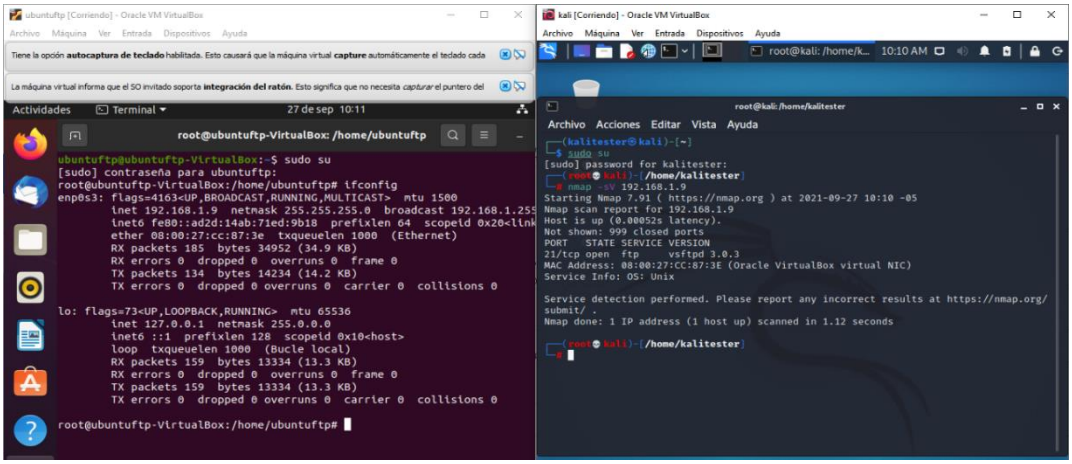

Figura 13.- *escaneo al puerto FTP*

Nota. Elaborado por Joan Zambrano.

2. Una vez que se haya detectado los puertos que estén habilitados, se procede a buscar los exploits que más se ajusten a la versión del protocolo de los puertos disponibles, en este caso se usará el puerto 21/tcp en su versión vsftpd 3.0.3, para esto se debe acceder al web site https://www.exploit-db.com/search y en el apartado de metasploit se busca la versión del protocolo que se quiera explotar, presentando lo siguiente:

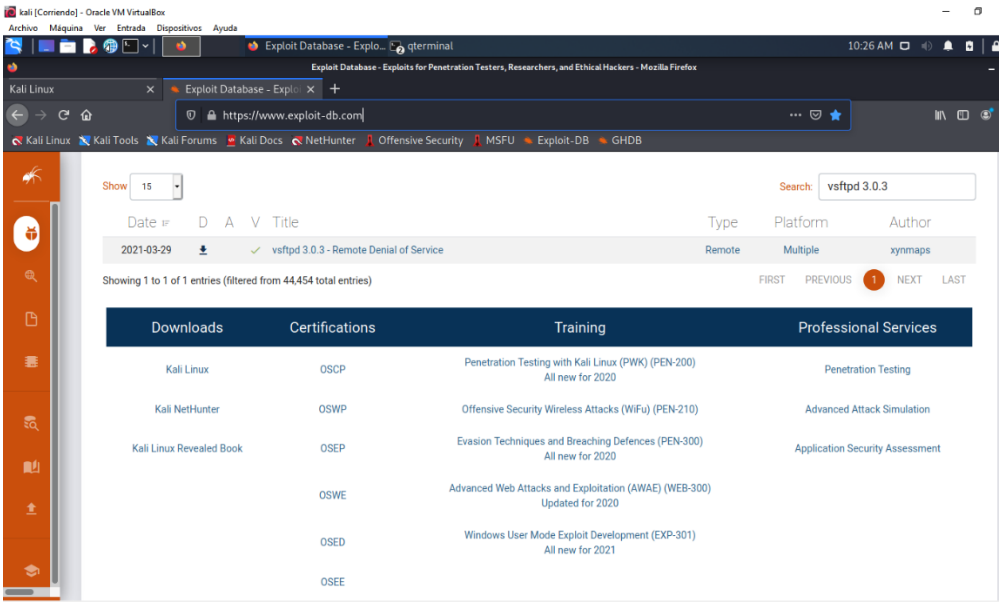

Figura 14.- *búsqueda del exploit para el ataque de vulnerabilidad*

Nota. Elaborado por Joan Zambrano.

3. Una vez que ya se haya realizado la búsqueda pertinente, se selecciona el metasploit que mejor se ajuste a lo requerido ya sea con la misma versión o con una versión pasada ya que los parchados por lo general dependen de la plataforma o servicio brindado, en este caso se optó por un ataque de denegación de servicios, para esto se procede a descargar el script, donde se presenta el siguiente cuadro que permite acceder a la descarga del exploit que realiza la denegación del servicio de transferencia de información.

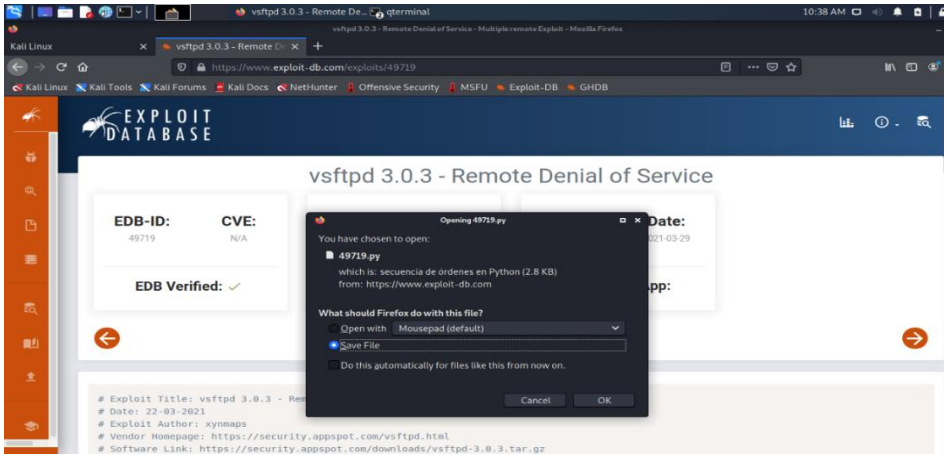

Figura 15.- *descarga del script para el ataque de denegación de servicio*

Nota. Elaborado por Joan Zambrano.

4. Ya descargado el archivo se lo ejecuta dentro de la máquina del atacante, para esto se debe determinar qué tipo de script se va a compilar, en este caso al ser desarrollado en Python se tendrá que ejecutar **Python 49719.py** (número del script) **dirección Ip** (192.168.1.9), dando como resultado la ejecución del DoS con su respectivo banner de presentación, y la dirección y el puerto a quien se le está realizando el ataque.

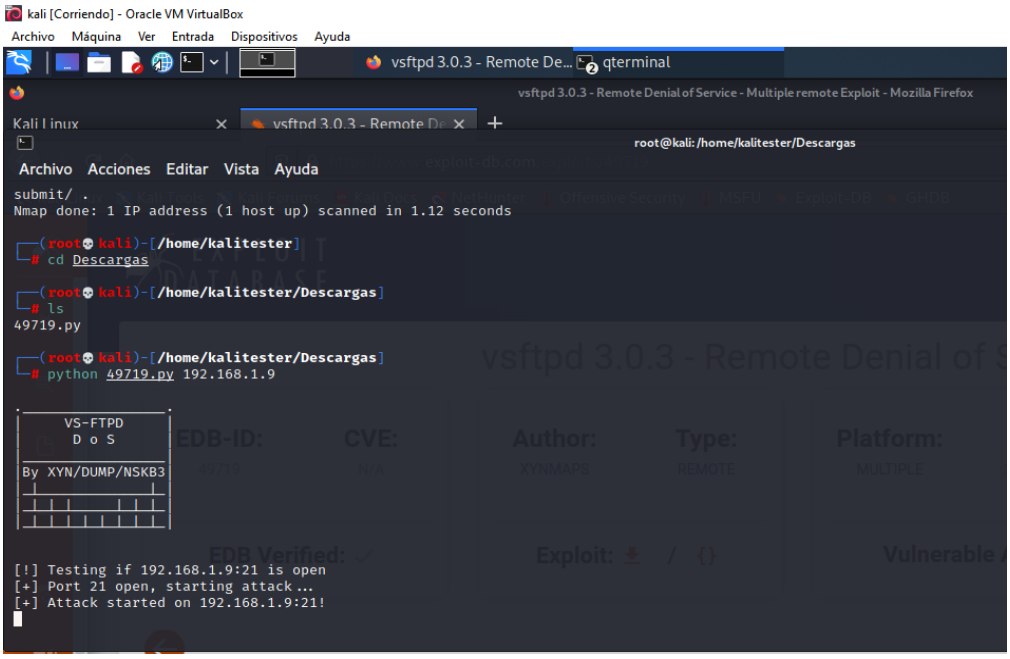

Figura 16.- *ejecución del script para el metasploit requerido*

Nota. *Elaborado por Joan Zambrano.*

5. El script que posee el exploit al ser ejecutado, comenzará a enviar por debajo múltiples sesiones, en un tiempo determinado como se establece dentro de la configuración del exploit descargado, lo que implicaría que otros usuarios no se puedan conectar al servicio de FTP, aunque el servidor este activo, y por ende, se demuestra que el servicio dejo de funcionar correctamente debido a que tiene un colapso de sesiones enviadas de manera Background como se lo refleja en la Figura 5, donde se presenta que el servicio está activado y a la vez no se puede usar el servicio por parte de los hosts disponibles dentro de la empresa.

   Debido a esto se llega a la conclusión de que el servidor FTP de la empresa CENFORSP. CIA LTDA., fue vulnerado por un ataque de denegación de servicio haciendo que su tiempo de producción decaiga y que no se pueda dar uso de la transferencia de archivos dentro de la red LAN de la empresa.

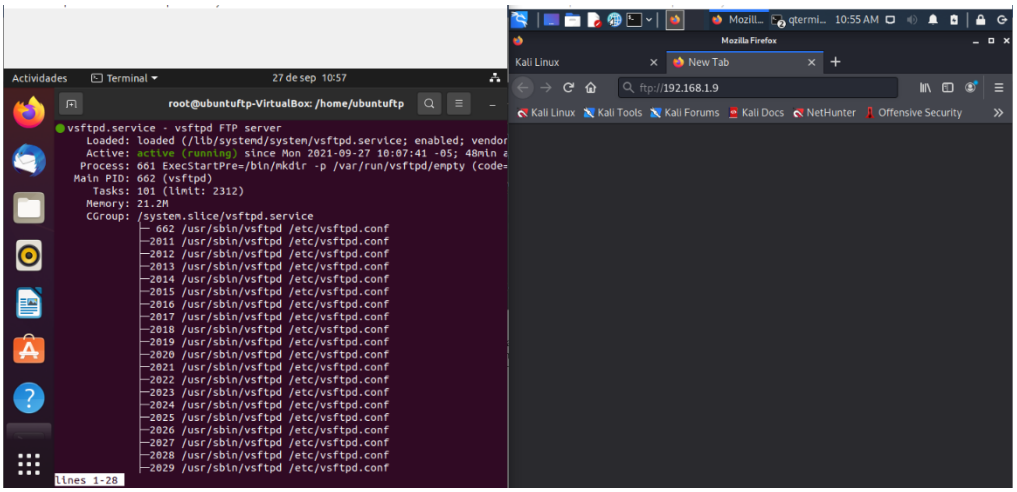

Figura 17.- *ataque de denegación de servicio en proceso*

Nota. Elaborado por Joan Zambrano.

A continuación, se trata de plasmar la codificación paso a paso de lo que guarda el exploit que fue descargado de la plataforma de exploit_db.

- El ataque de denegación de servicios es posible debido al que el script está funcionando bajo las funciones de sockets, multihilos, subprocesos y tiempo.

```
import socket
import sys
import threading
import subprocess
import time
```

Figura 18.- *importación de librerías usadas para el desarrollo del script*

Nota. Elaborado por Joan Zambrano.

- En síntesis, este script se divide en tres procesos principales: el primero es verificar si realmente hay una vulnerabilidad en el puerto 21, para esto se usará **sys. argv** y en caso de que exista alguna vulnerabilidad las cadenas argv [1], argv [2] y argv [3] mantendrá datos por debajo lo que implicaría que el testing realizado a la compuerta que se quiera atacar se encuentre vulnerable.

```
def main():
        global target, port, start
        print banner
        try:
                target = sys.argv[1]
        except:
                print usage
                sys.exit()
        try:
                port = int(sys.argv[2])
        except:
                port = 21
        try:
                conns = int(sys.argv[3])
        except:
                conns = 50
        print("[!] Testing if {0}:{1} is open".format(target, port))
```

Figura 19.- *prueba de vulnerabilidad en el puerto 21*

Nota. Elaborado por Joan Zambrano.

- Apenas el script haya entrado esta vulnerabilidad envía subprocesos al puerto específico, para esto utiliza la función de multihilos dentro de un bucle, tal como se lo detalla en la Figura 8, lo que provocaría un desbordamiento de sesiones al servidor FTP.

```
def loop(target, port, conns):
        global start
        threading.Thread(target=timer).start()
        while 1:
                for i in range(1, conns + 3):
                        t = threading.Thread(target=attack, args=(target,por
                        t.start()
                        if i > conns + 2:
                                t.join()
                                break
                                loop()

t = threading.Thread(target=loop, args=(target, port, conns,))
t.start()
```

Figura 20.- *envío de subprocesos multihilos en un ciclo repetitivo*

Nota. Elaborado por Joan Zambrano.

- Y ya para finalizar, el script envía todos estos subprocesos ilimitados por cada 900 milisegundos lo que garantiza que el desbordamiento sea efectivo

```
def timer():
        start = time.time()
        while 1:
                if start < time.time() + float(900): pass
                else:
                        subprocess.Popen("pkill ftp", shell=True, stdout=subprocess.
                        t = threading.Thread(target=loop, args=(target, port,))
                        t.start()
                        break
```

Figura 21.- *envío de subprocesos por cada 900 milisegundos*

Nota. Elaborado por Joan Zambrano

CAPÍTULO 3: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

De acuerdo al levantamiento de información realizado tanto a nivel físico como a nivel lógico se puede presentar un análisis e interpretación de resultados. El cual estará orientado a partir tanto del diagrama de red de la compañía CENFORSP. CIA LTDA como las configuraciones básicas de sus equipos de red.

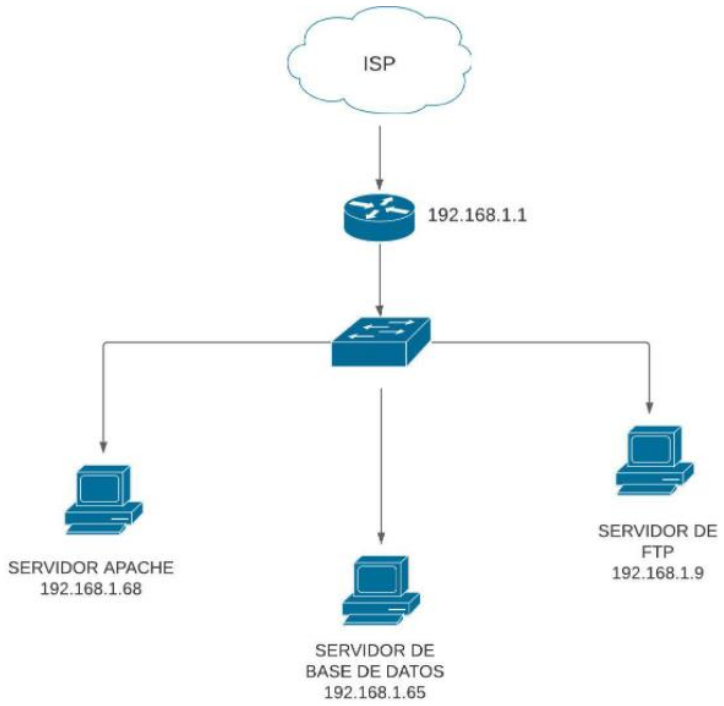

Figura 22.- *Diseño de red actual de la empresa CENFORSP. CIA LTDA.*

Nota. Elaborado por Joan Zambrano.

Tal como se lo demostró previamente se puede deducir que el sistema de red no cuenta con dispositivos de protección externos, que filtren la información de entrada o salida de la red, por ende, no existe una medida que tenga la capacidad de evitar los diversos ingresos de amenazas, como es el caso de los malwares, spywares, worms, rasomwares y demás vicisitudes, para poder dar un análisis de resultado más preciso se presentará la siguiente tabla de indicadores para la generación de una infraestructura de red física segura.

3.1. Indicadores de fallo en la red

Los indicadores mencionados son los que permiten realizar un estudio a nivel físico y lógico de la red dentro de la empresa, lo cual permitirá realizar un análisis situacional de cómo se está estructurada la seguridad informática y cuáles son las medidas de prevención que se usan para no ser vulnerados por algún intruso virtual, amenaza o ataque, y así poder estudiar si dentro de CENFORSP. CIA LTDA es necesaria la implementación de un plan de mejora en la seguridad de dicha empresa.

Indicadores	Resultados	
	Sí	No
Falla en servidores informáticos dentro de la empresa.	X	
Conflictos con direcciones IP	X	
Tarjetas de red defectuosas	X	
Fallas en switches o Routers	X	
Insuficiente Ancho de Banda.	X	

***Tabla 2**. Indicadores a nivel de red física*

Una vez realizado el análisis en la infraestructura física de la red, se puede determinar los amplios problemas de red dentro de la compañía, las cuales fueron demostrados mediante las herramientas estipuladas en la estructura del marco teórico, como consecuencia la empresa CENFORSP. CIA LTDA presenta un 100% de falencias de seguridad a nivel de equipos, lo que refleja la alta vulnerabilidad tanto a nivel interno como a externo de la red LAN de la empresa, lo que se traduce en que atacantes pueden acceder a la información están dentro o fuera de la red.

En cuanto al nivel lógico se realizó el análisis partiendo bajo los siguientes parámetros.

Indicadores	Resultados	
	Sí	No
Uso no autorizado de puertos de red	X	
Robo de Información.	X	
Denegación de Servicios (DoS).	X	
Ataques de Fuerza Bruta.	X	
Alteración de la Información.	X	

***Tabla 3**. Indicadores a nivel de red lógico*

De acuerdo al análisis de la tabla de los indicadores lógicos, se puede deducir a través del manual técnico de la simulación del ataque al servidor FTP presentado como prueba de vulnerabilidad a la red, en la metodología de la propuesta, que la empresa CENFORSP. CIA presenta un alto índice de fallas informáticas, ya que se demostró que ataques como denegación de servicios puede comprometer seriamente la integridad de los servidores, en este caso en particular se realizó esta prueba en un servidor de transferencia de archivos.

Como se logra apreciar es un sistema de red que no cuenta con dispositivos de protección externa que filtre la información y evite el ingreso de malware dentro de los sistemas operativos de cado uno de los servidores de la empresa, y como consecuencia dicha empresa es filtrada digitalmente con facilidad sin que note la existencia de dichos ataques. En conclusión, el análisis de los resultados previos por parte del uso de modalidad que sirven para gestionar de forma administrativa e informática, la situación actual de la red y seguridad de la información de la empresa CENFORSP. CIA LTDA, no es válida, ya que presenta un 100% de falencias de seguridad a nivel lógico, debido la falta de dispositivos externos de seguridad perimetral, que ayude a la verificación de paquetería emitidas ya sea dentro o fuera de la empresa y se defiende gracias a la demostración que se apreciará en el capítulo posterior.

CAPÍTULO 4: IMPLEMENTACIÓN DE LA SOLUCIÓN TECNOLÓGICA

Para poder establecer una mejora en la integridad en la seguridad informática de la empresa CENFORSP. CIA LTDA es necesario entender que la implementación de equipos de protección externa es una forma de viabilizar el uso de la tecnología en el ambiente de seguridad informática como un recurso fundamental para la protección y reanimación del mundo informático en las empresas laborales.

Pero antes de proceder a realizar la implementación de las soluciones factibles otorgadas por el investigador es necesario la creación de un modelo de seguridad para la red mediante un plan de mejoras presentado como pasos que se llevan a cabo para toma decisiones frente a la ejecución de controles o tácticas que ayuden a la evolución y mejoramiento de las políticas o procedimientos que se realizan en la empresa, esto en función de las vulnerabilidades y amenazas detectadas gracias al uso de herramientas detectoras de estas brechas digitales.

4.1. Plan de mejoras para la seguridad informática

Un Sistema de Gestión de Seguridad de la Información según la ISO27001 establece la necesidad de seguir un proceso conocido como Ciclo Deming el cual describe etapas que se realizan para cumplir con el SGSI y de esta manera establecer un uso automatizado de desarrollo que permita autonomía de dicho diseño de seguridad en la red.

Y para ello se genera la creación de un nuevo diseño de red para solventar a la falta de esquematización y protección del diseño anterior, presentando soluciones técnicas formuladas por la investigación y criterio del autor el cual se basa en las normas de seguridad informática establecidas para no alterar el proceso estandarizado ya creado, por lo tanto, se tiene:

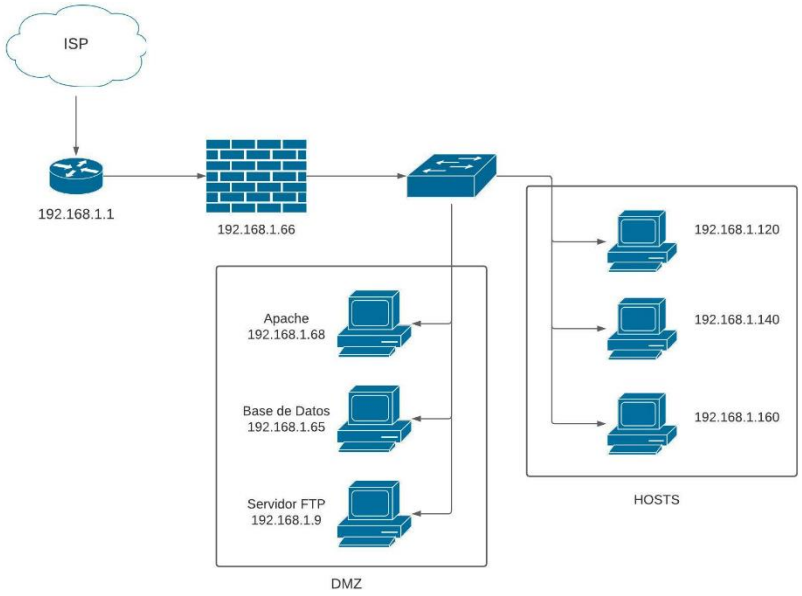

Figura 23. *Diseño propuesto para el mejoramiento de la seguridad informática.*

Nota. Fuente Joan Zambrano.

Debido a que el diseño de la red anterior a este presentaba fuertes decadencias en la protección de la seguridad informática dentro de la empresa, la solución más viable es la implementación de dispositivos externos que posean como principal función el de proteger siempre y constantemente la seguridad de la información, además de cumplir con los estándares de seguridad informática como claves encriptadas, configuraciones avanzadas de seguridad en dispositivos finales y trasladación de información a través de etiquetado de paquetes, pero el principal uso de un cortafuegos externo se plantea como el rediseño en la estructuración de la seguridad informática de la empresa CENFORSP. CIA LTDA, quedando como resultado final la siguiente esquematización:

El utilizar el firewall como dispositivo de protección a nivel de capa 3 dentro de la jerarquía de estructuración de redes locales ayuda a que todo paquete de información no pueda ingresar o salir de la red sin antes establecerse una verificación, y si se desea vulnerar la red, este dispositivo es capaz de enviar alertas a cada uno de los hosts dentro de la red para que estos procedan con su protección interna de manera inmediata.

En el punto de vulnerabilidad de la empresa, ésta no es totalmente vulnerable, pero si sube el nivel de seguridad al punto de prevenir ataques futuros o cualquier

anomalía presentada a nivel lógico y además gana el suficiente tiempo para que se pueda traspasar la información y mantenerla segura, por ende, se considera una de las mejores cualidades en diseño y estructuración de redes y seguridad informática la solución técnica a la infraestructura existente presentada en esta propuesta académica.

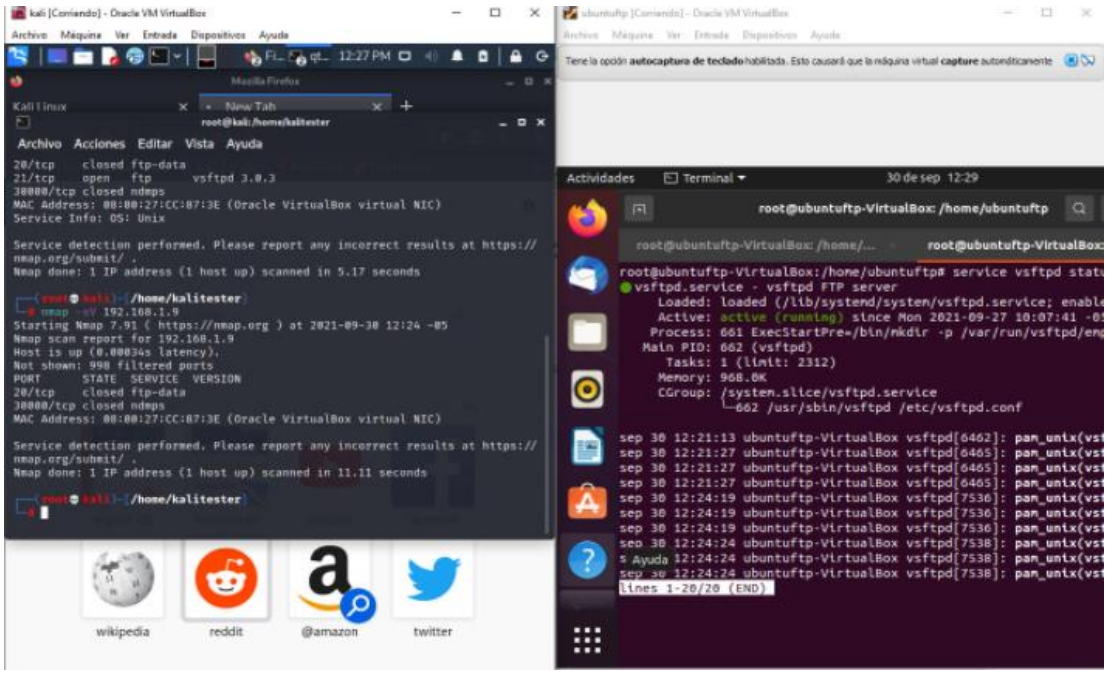

Figura 24. *Presentación de nuevo escaneo de puerto.*

Nota. Elaborado por Joan Zambrano.

Una vez aplicada la solución técnica a la infraestructura mostrada se origina la situación de saber si esto permitió o no mejorar el sistema informático de la empresa, por lo tanto, es necesario un nuevo escaneo de redes a través de las herramientas Nmap para auditar y saber si es que la situación después de la mejora proporcionada en la simulación de la localidad, protege con eficiencia a todo el sistema de información.

Entonces se realizó como prueba hacia el servidor atacado con anterioridad y este presentó como resultado un análisis de puerto donde dos puertos se encuentran totalmente cerrados y los demás permanecen filtrados, de tal manera que se demuestra que la confidencialidad de la red se volvió más segura y menos vulnerable, además se observa que mientras todos los puertos están bloqueados el servicio permanece activo y en correcto funcionamiento.

Por lo tanto, una vez concluida la explicación del proceso que se llevó para generar un plan capaz de mejorar la manera en cómo se cubre gran parte de la seguridad informática dentro de la empresa CENFORSP. CIA LTDA, según dicho proceso comenzamos con el punto de planeación del diseño de mejoras en la seguridad informática, empezando con los aspectos a seguir para cumplir con el reajuste de la protección a la información y concluimos con la verificación de todo el sistema de seguridad mejorado, como se ve a continuación:

I. **Identificar las vulnerabilidades dentro de la empresa,**

   Esto se realiza a través del uso de herramientas digitales encontradas en sistemas operativos como Kali-Lunix, en donde se presentan una gran cantidad de herramientas del monitoreo de la red o sistema informático, con el objetivo de probar que tan protegido se encuentra un sistema y en caso de estar en conflictos, dar soporte y solución.

II. **Determinar riesgos y amenazas que amedranten a estas vulnerabilidades,**

   El conocer cuáles son los posibles ataques y de donde proceden, permiten generar estrategias de protección y seguridad a la empresa, esta solución se puede realizar utilizando plataformas donde se encuentren registrados los diferentes ataques, explotaciones o amenazas que generan, gran cantidad de hackers ya sea como logro o burla, un ejemplo de ello se encuentra en la plataforma exploit_db.

III. **Indagar soluciones tecnológicas que respeten el uso de las normas definidas (ISO 27000-27001),**

   Encontradas las vulnerabilidades y determinado el accionar de las amenazas existentes en las brechas de seguridad dentro de la empresa, esta puede tomar las medidas necesarias dentro de la ley, para que se garantice en todo momento los tres aspectos importantes de la norma ISO 27000-27001, las cuales son confidencialidad, integridad y disponibilidad de los activos de información, por ello se debe estar constantemente al tanto de cada movimiento, accionar o actividad tecnológica alrededor del entorno empresarial para tener ideas y soluciones que puedan mantener a salvo a la empresa, como se presenta actualmente con el uso de un firewall y protección en zona desmilitarizada para mantener aislados a los

servidores, comandos de prevención dentro de las herramientas encontradas en Kali-Linux y demás estudios de herramientas.

Cabe recordar que, si toda vulnerabilidad tiene un ataque, cada ataque tiene su solución, basta con entender la amenaza y los principios de cómo fue creada, para establecer una solución que la mantenga a raya o la elimine.

IV. Adaptar la red informática de acuerdo a las soluciones propuestas,

Debido a la cantidad de pruebas presentadas en la documentación como lo es diseño de la infraestructura física antes de la generación de la propuesta, como también el uso del manual técnico generado a partir de una simulación de los elementos encontrados en la empresa, se entiende el problema actual y se prioriza aumentar el rendimiento de estos puntos establecidos mediante requerimientos que cumplan con las normas definidas encargadas de la seguridad informática de las empresas.

V. Verificar los cambios dentro de la estructura física y lógica de la red,

Al momento de implementar las propuestas planteadas en el capítulo anterior, es indispensable verificar si estas funcionan y son capaces de dar solvencia a las vulnerabilidades encontradas con anterioridad, y a partir de allí también se debe monitorear la nueva red generada y ver si el riesgo a ser vulnerada es igual o menor junto a los indicadores determinados para la seguridad informáticas y la red física de la empresa

VI. Configurar dispositivos de acuerdo a las buenas prácticas establecida en el estándar ISO 27002,

Partiendo de los puntos críticos estipulados en la norma ISO 27002, hay que considerar ciertos aspectos fundamentales como es el caso de la implementación de contraseñas seguras y robustas para el acceso a servicios a nivel de intranet, por lo que se sugiere implementar algoritmos criptográficos seguros. También se sugiere usar los recursos internos que cuenta cada uno de los servidores para resguardar su integridad, como es el caso de sus firewalls internos, en cuanto a la parte de redes con los demás equipos encontrados en la red LAN se recomienda verificar su configuración a nivel de configuración de protocolos y enrutamiento, como también el cerrar los puertos físicos que no se estén usando.

VII. Brindar asesoría técnica a los empleados del uso de los dispositivos de red y la creación de contraseñas dentro de la empresa, según las buenas prácticas establecida en el estándar ISO 27002,

Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir.

Una vez solucionado el problema técnico, ahora hay que dar enfoque a la solución de parte de los usuarios (empleados de la empresa), debido a que su principal inconveniente frente a estos ataques se debe a la falta de conocimientos de TI y seguridad informática, por ello se presenta un esquema que da uso de las normas ISO27000, sobre todo la norma ISO27002 la cual da secciones en base a un sistema seguro y los recursos y conocimientos necesarios para poder lograr dicho ambiente de seguridad informática laboral.

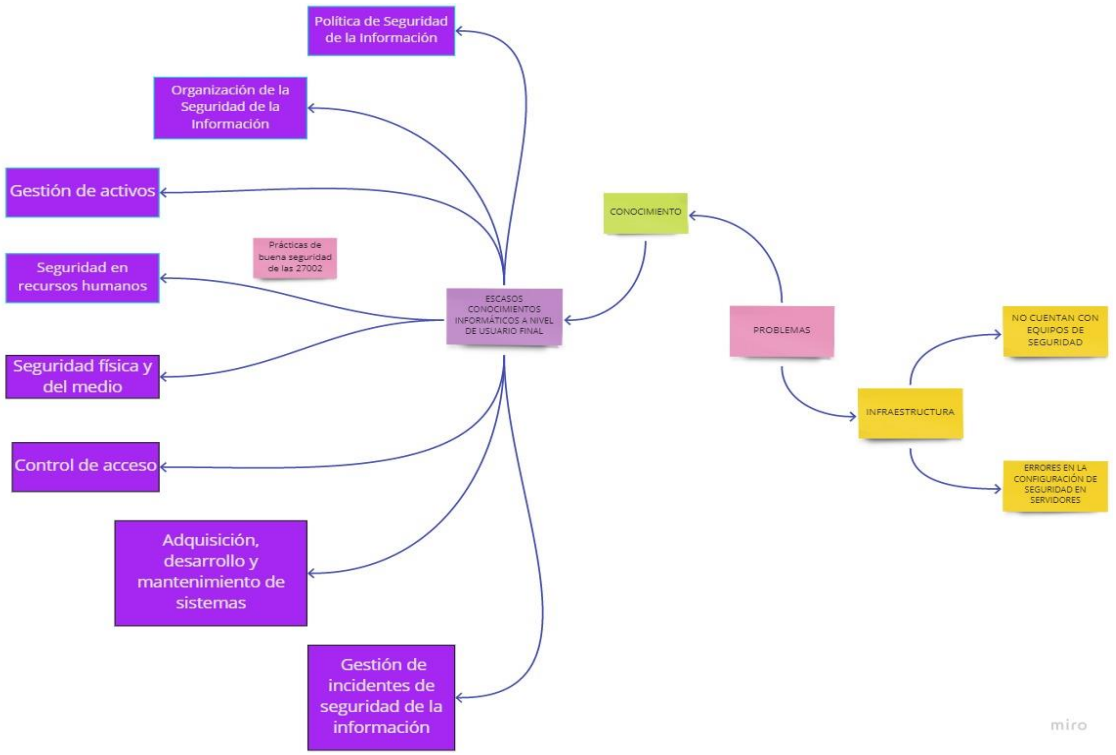

Figura 25. *Flujograma de secciones de la norma ISO27002 para seguridad informática.*

Nota. Elaborado por Joan Zambrano.

VIII. Monitorear y revisar el sistema de gestión de seguridad de la información.

Como punto final se debe establecer un periodo de revisión del sistema de gestión de seguridad de la información, debido a que, como la tecnología avanza en los ámbitos de protección de la información también cada vez descubren nuevas maneras de vulnerar la información, como consecuencia, no se podrá obtener una garantía en la cual se determine que el plan de seguridad establecido funcionará. Utilizar el sistema de prevención a fallas y aprender de las amenazas anteriores generará mayor cantidad de entendimiento a futuros ataques dirigidos a los sistemas informáticos de la empresa.

Una vez ya planteado el cimiento teórico se procedió a evaluar la seguridad de red de la empresa CENFORSP. CIA LTDA, para esto se tuvo que hacer uso de un tester, por lo que se procedió a virtualizar un equipo que tenga Kali Linux como sistema operativo y adicionalmente se hizo uso de un escaneador de puertos, en este caso se optó por NMAP, el cual dio como resultado que ciertos puertos críticos se encontraban habilitados, por ende se dedujo que el sistema de seguridad perimetral que presentaba la compañía era sumamente ineficiente; y para validar este argumento se procedió a realizar un exploit de tipo de denegación de servicios al servidor FTP y así mostrar que a pesar de que el servicio se encontraba habilitado el ingreso a sus recursos no era posible.

Debido a todas estas problemáticas se diseñó un plan de mejoras destinado para fortalecer la seguridad informática de la compañía. En rasgos generales esta planeación está sustentada bajo la estructura PHVA, por lo que esta planeación parte desde la identificación de vulnerabilidades hasta el monitoreo del sistema de gestión de seguridad de la información asegurando de este modo cubrir cualquier tipo de vulnerabilidad o amenaza que pueda aparecer dentro de la institución a analizar.

Todo esto concluye con un modelo de seguridad preventiva (VASM), generado por el autor, debido a que este se basa en la manipulación del plan de mejoras de ocho pasos creado para poder verificar la amenaza, analizará a tal punto de saber cómo funciona, solucionarla de acuerdo a los principios de las normas ISO

27000 y monitorear la red informática para establecer un sistema de protección que prevenga ataques y de tiempo suficiente de poder estudiar cada una de sus controversias.

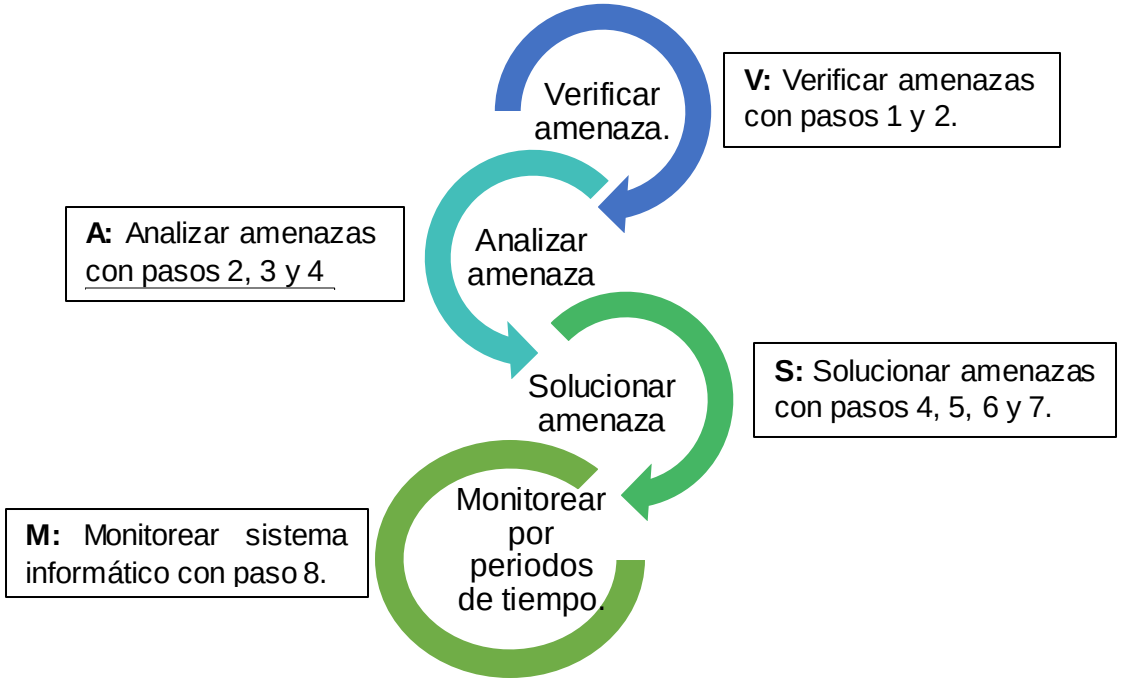

Figura 26. *Modelo de seguridad informática VASM.*

Nota. Elaborado por Joan Zambrano.

Tal como se esbozó a lo largo de la tesis, se determina que se cumplió con todos los objetivos trazados, ya que debido a la naturaleza de la propuesta se tuvo que seguir un paso secuencial, investigativo y práctico. Puesto que para la elaboración de este documento fue determinante realizar en primer lugar un levantamiento de información teórico, ya que con el cumplimiento de este punto le permite tanto a los lectores como a los investigadores interesados en este tópico tener un panorama general del tema a tratar.

CONCLUSIONES

Como conclusión del presente proyecto de titulación se obtuvo lo siguiente:

- Los conceptos basados en la fundamentación de redes informáticas, sistemas informáticos, seguridad informática junto a las normas de seguridad de la información, fueron de vital utilidad para dar una correcta idea del ámbito tecnológico en el cual se enfoca el proyecto actual, para la generación de un modelado de seguridad basado en un plan de mejoras para la seguridad informática de la empresa CENFORSP. CIA LTDA frente a vulnerabilidades y amenazas existentes.
- Mediante una evaluación a la seguridad de red con el uso de herramientas de escaneo y diagnóstico para la detección de vulnerabilidades como Kali Linux, se llegó a la conclusión de que la empresa contaba con un gran número de vulnerabilidades tanto de forma física como lógica, a tal nivel que incluso puertos físicos estaban disponibles para el ingreso de cualquier dispositivo a la red. Se realizó un análisis en donde se consideró uno de los ataques más realizados y sencillos para cualquier atacante, el cual es denegación de servicios, a través de los puertos lógicos disponibles, el cual en la documentación se presenta con éxito, probando la falta de seguridad informática en la empresa.
- Se interpretaron los resultados en función de la medición de cada indicador analizado en la red y se finiquita que es necesaria la implementación de un plan de mejoras capaz de solventar y dar un bienestar técnico en el ámbito físico y lógico a toda la empresa y así asegurar a todo aquel individuo que realice un contrato con la institución la seguridad de su información personal, además de establecer el crecimiento económico, tecnológico y social en el país.
- Al proponer un plan de mejoras que garantice la seguridad y eficiencia de la red LAN de la empresa CENFORSP en base a las directrices dictaminadas por las normas ISO 27000 e ISO 27001, se determina que es necesario optimizar varios aspectos físicos y lógicos en la seguridad de la red y a su vez realizar la implementación y ejecución del modelo de

seguridad preventiva VASM que servirá como una solución segura, creativa e innovadora para el beneficio de la empresa.

RECOMENDACIONES

Con respecto a determinar los fundamentos teóricos relacionados a la seguridad en redes de datos, el actualizar los conocimientos en base a ataques futuros, foros tecnológicos, noticias en la implementación de teorías o casos en donde la tecnología y la seguridad son primicia, es recomendable que se tengan presentes, debido a que la tecnología siempre se encuentra en constante desarrollo y crecimiento, por ende para crear un sistema menos vulnerable es necesario llevar un estudio periódico de temas actuales en la tecnología.

Al evaluar la seguridad de red con el uso herramientas de escaneo y diagnóstico para la detección de vulnerabilidades, se recomienda no solo el uso de herramientas Open Source, sino que también implementar mecanismo o software privado o con licencia, ya que estos presentan un nivel mayor de protección al no ser fácilmente adquiridos y además dejan un registro por cada compra o permiso de uso, lo que da un inicio de búsqueda si se quiere detectar al atacante.

Interpretar los resultados en función de la medición de cada indicador analizado en la red, debe ser necesario realizar un amplio uso de indicadores que ayuden a la medición exhaustiva del comportamiento tanto de la red física como lógica, por eso es recomendable establecer un índice de indicadores que ayuden a distribuir toda una red completa por partes para orientar directamente la solución al lugar afectado, además de establecer una redundancia inmediata si se trata de un servicio disponible.

Al proponer un plan de mejoras que garantice la seguridad y eficiencia de la red LAN de la empresa CENFORSP en base a las directrices dictaminadas por las normas ISO 27000 e ISO 27001, es recomendable orientarse también al uso de normas, estándares y status que amplíen el alcance de lo que se quiere resguardar.

Como respecto a criterio recomendable para la empresa se tiene:

- Contar con un sistema de firewall ya sea físico o virtual que permita en tiempo real controlar el tráfico tanto de entrada como salida de datos.

- En caso de tener la necesidad de abrir algún puerto de un servidor en específico se debe tomar las medidas necesarias para evitar ataques o intrusiones de terceros.
- Se recomienda realizar auditorías periódicas para tener un mayor control lógico de la infraestructura de la empresa.
- Se recomienda adoptar los estándares dictaminados en las normas ISO 27001 para así garantizar la integridad lógica de la compañía.

REFERENCIAS Y BIBLIOGRAFÍAS

BIBLIOGRAFÍA

AAAPN. (23 de Agosto de 2021). *AAAPN*. Obtenido de Asociación de Agentes Aduanales de Piedras Negras: http://www.aaapn.mx/aniv50/blog/tecno/7-00007.php

Aguilera , P. (2010). *Seguridad Informática.* Editex.

Aguilera López, P. (s.f.). *Seguridad Informática.* 2021.

Ambit Team. (10 de Noviembre de 2020). *ambit-bst.* Obtenido de ambit-bst.: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Anonymous. (29 de Enero de 2013). *Historia de la web.* Obtenido de Historia de la web: http://charliedaw2236.blogspot.com/

Areitio, G., & Areitio, A. (2009). *Información. Informática e Internet: del ordenador personal a la Empresa 2.0.* Visión Libros.

Arias, E. R. (05 de Febrero de 2021). *economipedia.* Obtenido de economipedia: https://economipedia.com/definiciones/investigacion-descriptiva.html

AVAST. (23 de Agosto de 2021). *Avast*. Obtenido de Internet Security: https://www.avast.com/es-es/c-malware

BAHILLO, L. (18 de Mayo de 2021). *marketing4ecommerce*. Obtenido de marketing4ecommerce.net: https://marketing4ecommerce.net/historia-de-internet/

Borghello, C. (23 de Ago de 2021). *Noticias sobre seguridad de la información*. Obtenido de Segu.Info: https://www.segu-info.com.ar/virus/tipos_virus

Calvo , L. (3 de Noviembre de 2020). *Go Daddy*. Obtenido de https://es.godaddy.com/blog/lean-startup/

Cámara Valencia. (2019). *camaravlencia*. Obtenido de https://www.mastermarketing-valencia.com: https://www.mastermarketing-valencia.com/marketing-digital/blog/internet-historia-evolucion/

Carazo, J. (30 de Mayo de 2017). *economipedia.* Obtenido de economipedia.: https://economipedia.com/definiciones/metodo-lean-startup.html

Castro, R. (17 de Octubre de 2018). *3ciencias*. Obtenido de 3ciencias: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Chuquitarco, M. (2017). *Diagnostico de vulnerabilidades de redes inalambricas en el Ecuador.* Quito.

Cisco. (2017). *Informe anual sobre ciberseguridad.*

Colaborador de DocuSign. (2 de Abril de 2020). *docusign.* Obtenido de docusign.: https://www.docusign.mx/blog/tipos-de-servidores

De-Luz, S. (10 de Junio de 2021). *redeszone*. Obtenido de redeszone: https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

Excellence, I. (01 de Febreo de 2018). *pmg-ssi.* Obtenido de pmg-ssi.: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Figueroa, J. (15 de Diciembre de 2017). *Polo de conocimiento*. Obtenido de Polo de conocimiento: file:///C:/Users/Intel/Downloads/420-1655-2-PB.pdf

Galán, J. (26 de Octubre de 2020). *interempresas.Ciberseguridad.* Obtenido de interempresas.Ciberseguridad: https://www.interempresas.net/Ciberseguridad/Articulos/317135-Infraestructuras-criticas-y-la-vulnerabilidad-digital.html

Hernández, S., & Avila, D. (Diciembre de 2021). *repository.uaeh.* Obtenido de repository.uaeh: https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/19887/turismo-metodos-empiricos-investigacion.pdf?sequence=1&isAllowed=y#:~:text=La%20importancia%20de%20lo%20emp%C3%ADrico,de%20las%20hip%C3%B3tesis%20previamente%20formuladas.

INCIBE. (20 de Marzo de 2017). *incibe.* Obtenido de incibe: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

INCIBE. (19 de Septimbre de 2019). *incibe.* Obtenido de incibe: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Intedya. (01 de Septiembre de 2015). *International Dynamic Advisors*. Obtenido de INTEDYA: https://bit.ly/385YiGP

LosVirus.es. (23 de Agosto de 2021). *LosVirus*. Obtenido de Cómo eliminar un Dialer: https://losvirus.es/dialers/

LOZANO, M., & CORREA, M. (2020). *repository.ucc*. Obtenido de repository.ucc: https://repository.ucc.edu.co/bitstream/20.500.12494/16502/1/2020_Analisis_Vulnerabilidades_Infraestructura.pdf

Marreros, J. (06 de Diciembre de 2019). *webempresa.* Obtenido de webempresa: https://www.webempresa.mx/blog/estructura-de-base-de-datos-en-wordpress.html

Mejia, T. (27 de Agosto de 2020). *lifeder.* Obtenido de lifeder: https://www.lifeder.com/investigacion-explicativa/

Molinetti, S. (23 de Septiembre de 2020). *empresas.blogthinkbig.* Obtenido de empresas.blogthinkbig: https://empresas.blogthinkbig.com/medidas-de-seguridad-en-una-red-lan/

Normas ISO. (Agosto de 2021). *Normas-iso.com*. Obtenido de https://www.normas-iso.com/iso-27001/

Peña, M., & Anías, C. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. *redalyc.org*, 48. Obtenido de https://www.redalyc.org/journal/3442/344263272003/html/

Prieto, A., Lloris, A., & Torres, J. C. (1989). *Introducción a la Informática.* McGraw-Hill.

Quiroz Zambrano, S. (2017). *Seguridad informática.* Manta.

Ramírez, A. (13 de Septiembre de 2021). *interempresas.* Obtenido de interempresas: https://www.interempresas.net/Ciberseguridad/Articulos/366603-Llega-la-ciber-inmunidad-un-paso-de-gigante-en-la-proteccion-del-IoT.html

Rizaldos, H. (22 de Octubre de 2018). *openwebinars*. Obtenido de openwebinars: https://openwebinars.net/blog/que-es-metasploit/

Romero Castro, M. I. (2019). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Jipijapa.

Sain, G. (2015). Historia de Internet. *Pensamiento Penal*.

Salas, D. (04 de Junio de 2019). *investigaliacr.* Obtenido de investigaliacr.: https://investigaliacr.com/investigacion/el-enfoque-mixto-de-investigacion/

Sánchez, M. (2010). *Virus y seguridad tecnológica en la docencia.* Córdoba.

softoware. (12 de Mayo de 2015). *softoware.* Obtenido de softoware: http://es.softoware.org/project-management-software/download-zimbra-collaboration-suite-open-source-edition-for-linux.html

TICPYMES. (13 de Febrero de 2020). *computing.* Obtenido de computing: https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-mas-grandes-de-decada.1.html

un fantasma en el sistema . (06 de Mayo de 2020). *un fantasma en el sistema* . Obtenido de https://www.unfantasmaenelsistema.com/2020/05/analisis-de-vulnerabilidades-con-nessus/

V., A. C. (s.f.). *archivo.ucr.ac.cr*. Obtenido de archivo.ucr.ac.cr: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

Vargas, A. (2013). *archivo.ucr.ac*. Obtenido de archivo.ucr.ac: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

Vargas, A. C., & Castro Mattei, A. (2020). *Sistemas de Gestión de Seguridad de la Información.*

ISOTools Excellence. (2017) *¿Seguridad informática o seguridad de la información? Recuperado el 05 de marzo de 2017, de http://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/*

Vieites, Á. G. (2013). *Auditoría de seguridad informática. Bogotá, Colombia: Ediciones de la U.*

5 ANEXOS

5.1 ENCUESTA

Modelo de seguridad y plan de mejoras para la empresa CENFORSP

La presente encuesta está dirigida a todos los colaboradores de la empresa CENFORSP. El cuestionario en mención tiene como objetivo evaluar las necesidades de la empresa en función a la seguridad informática.

1- **¿A qué departamento pertenece?**

_____

2- **¿Qué tan importante es para usted la seguridad de la información?**

Muy importante ☐

Poco importante ☐

No es importante ☐

3- **¿La empresa brinda programas de capacitación sobre riesgos informáticos?**

Si ☐ No ☐

4- **¿Es usted capaz de identificar o virus/malware informático?**

Si ☐ No ☐

5- **¿Con qué frecuencia realiza usted cambios de contraseñas?**

Siempre ☐ A veces ☐ Casi nunca ☐ Nunca ☐

6- **¿Tiene software antivirus instalado en su computadora?**

Si ☐ No ☐ No sé ☐

7- **¿Utiliza usted un software firewall en su ordenador?**

Si ☐ No ☐ No sé ☐

5.2 ENTREVISTA

Esta entrevista está dirigida a un miembro del centro de capacitación profesional para guardias de vigilancia y seguridad privada CENFORSP.

Nombre: Raúl Quito.

Cargo: Subgerente.

1. **¿Qué tan importante es para usted la seguridad de la información?**
   Es vital, ya que es lo que nos va a respaldar como empresa y nuestro trabajo en general. Es algo primordial.
2. **¿La empresa invierte presupuesto en ciberseguridad?**
   No. Hemos descuidado esa parte, pero ahora veo que es un punto a mejorar.
3. **¿La empresa cuenta con alguna medida para la seguridad de la información en la red?**
   No, solamente los accesos a los routers wifi.
4. **¿Le interesa tomar medidas para mejorar la seguridad de la información en la empresa?**
   Sí, todo lo que sea seguridad es siempre una buena inversión.
5. **¿Conoce acerca de las normas ISO 27000 para la seguridad de la información?**
   He escuchado sobre ellas, pero no las conozco a fondo.
6. **¿Los empleados son capaces de identificar virus/malware?**
   No todos, la mayoría no. Solamente los que son especializados en sistemas.
7. **¿Los empleados hacen uso adecuado de contraseñas y datos importantes de la empresa?**
   He tenido inconveniente con alguno de los empleados, pero creo que la mayoría si hace buen uso de las contraseñas.
8. **¿Cuentan con un plan de prevención de riesgos informáticos?**
   No, pero estamos pensando en implementar alguno que se acomode al presupuesto.