Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE INVESTIGACIÓN PARA LA AUTOMATIZACIÓN DE LA IMPLEMENTACIÓN DE UN SERVIDOR HONEYPOT CON EL OBJETIVO DE DETECTAR, ANALIZAR Y PREVENIR CIBERATAQUES A EMPRESAS GUATEMALTECAS

Jenner Rockael Fernández Morales
Asesorado por el Maestro Ing. Mario Renato Escobedo Martínez

Guatemala, marzo de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE INVESTIGACIÓN PARA LA AUTOMATIZACIÓN DE LA IMPLEMENTACIÓN DE UN SERVIDOR HONEYPOT CON EL OBJETIVO DE DETECTAR, ANALIZAR Y PREVENIR CIBERATAQUES A EMPRESAS GUATEMALTECAS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JENNER ROCKAEL FERNÁNDEZ MORALES
ASESORADO POR EL MAESTRO ING. MARIO RENATO ESCOBEDO MARTÍNEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, MARZO DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
EXAMINADORA	Inga. María Magdalena Puente Romero
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE INVESTIGACIÓN PARA LA AUTOMATIZACIÓN DE LA IMPLEMENTACIÓN DE UN SERVIDOR HONEYPOT CON EL OBJETIVO DE DETECTAR, ANALIZAR Y PREVENIR CIBERATAQUES A EMPRESAS GUATEMALTECAS

Tema que me fuera asignado por la Dirección de la Escuela de Estudios de Postgrado, con fecha 20 de agosto de 2021.

Jenner Rockael Fernández Morales

EEPFI-PP-0165-2022
Guatemala, 12 de enero de 2022

Director
Armando Alonso Rivera Carrillo
Escuela De Ingenieria Mecanica Electrica
Presente.

Estimado Ing. Rivera

Reciba un cordial saludo de la Escuela de Estudios de Postgrado de la Facultad de Ingeniería.

El propósito de la presente es para informarle que se ha revisado y aprobado el Diseño de Investigación titulado: **AUTOMATIZACIÓN DE LA IMPLEMENTACIÓN DE UN SERVIDOR HONEYPOT CON EL OBJETIVO DE DETECTAR, ANALIZAR Y PREVENIR CIBERATAQUES A EMPRESAS GUATEMALTECAS.**, el cual se enmarca en la línea de investigación: **Seguridad - Seguridad**, presentado por el estudiante **Jenner Rockael Fernandez Morales** carné número **200915537**, quien optó por la modalidad del "PROCESO DE GRADUACIÓN DE LOS ESTUDIANTES DE LA FACULTAD DE INGENIERÍA OPCIÓN ESTUDIOS DE POSTGRADO". Previo a culminar sus estudios en la Maestría en ARTES en Ingeniería Para La Industria Con Especialidad En Telecomunicaciones.

Y habiendo cumplido y aprobado con los requisitos establecidos en el normativo de este Proceso de Graduación en el Punto 6.2, aprobado por la Junta Directiva de la Facultad de Ingeniería en el Punto Décimo, Inciso 10.2 del Acta 28-2011 de fecha 19 de septiembre de 2011, firmo y sello la presente para el trámite correspondiente de graduación de Pregrado.

Atentamente,

"Id y Enseñad a Todos"

Mtro. Mario Renato Escobedo Martínez
Asesor(a)

Mtro. Mario Renato Escobedo Martinez
Coordinador(a) de Maestría

UNIVERSIDAD DE SAN CARLOS
ESCUELA DE POSTGRADO
FACULTAD DE INGENIERIA
DE GUATEMALA

Mtro. Edgar Dario Alvaréz Cotí
Director
Escuela de Estudios de Postgrado
Facultad de Ingeniería

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERIA
DIRECCIÓN
ESCUELA DE POSTGRADO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

EEP-EIME-0165-2022

El Director de la Escuela De Ingenieria Mecanica Electrica de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador y Director de la Escuela de Estudios de Postgrado, del Diseño de Investigación en la modalidad Estudios de Pregrado y Postgrado titulado: **AUTOMATIZACIÓN DE LA IMPLEMENTACIÓN DE UN SERVIDOR HONEYPOT CON EL OBJETIVO DE DETECTAR, ANALIZAR Y PREVENIR CIBERATAQUES A EMPRESAS GUATEMALTECAS.**, presentado por el estudiante universitario **Jenner Rockael Fernandez Morales**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería en esta modalidad.

ID Y ENSEÑAD A TODOS

Ing. Armando Alonso Rivera Carrillo
Director
Escuela De Ingenieria Mecanica Electrica

Guatemala, enero de 2022

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.221.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO DE INVESTIGACIÓN PARA LA AUTOMATIZACIÓN DE LA IMPLEMENTACIÓN DE UN SERVIDOR HONEYPOT CON EL OBJETIVO DE DETECTAR, ANALIZAR Y PREVENIR CIBERATAQUES A EMPRESAS GUATEMALTECAS,** presentado por: **Jenner Rockael Fernández Morales ,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, marzo de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Soberano, Rey de reyes y Señor de señores, fuente de inagotable sabiduría. Gracias por estar siempre conmigo, darme la vida y la salud para poder finalizar con éxito mi carrera universitaria, gracias por hacer realidad uno de mis sueños.
Mis padres	Evelyn Eunice Morales Piedrasanta y Julio Cesar Fernandez Ochoa. Gracias por brindarme su amor, sacrificio y confianza. Sin ustedes no hubiese sido posible alcanzar este éxito, los amo mucho.
Mis hermanos	Ángel Julio César, Aylin Eunice y Eugenia Elizabeth Fernández. Por ser bendición para mi vida.
Mis abuelitos	Roderico Fernández Rodas (q. e. p. d.), José Rodolfo Morales (q. e. p. d.), Eugenia Josefina Ochoa López y María Elizabeth Piedrasanta Juárez.
Mi sobrina y primos	Que este triunfo obtenido sea un ejemplo para ellos.

Mi novia	Nicté Montiel. Gracias por tu amor, comprensión y apoyo incondicional.
Mis tíos	Por su apoyo y cariño.
Mi familia en general	Con mucho cariño.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudios en donde me he formado profesionalmente.
Facultad de Ingeniería	Por los profesionales que puso en mi camino, de los cuales aprendí lo mejor.
Amigos de proyectos	Por esos días y noches de arduo trabajo para terminar los proyectos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

LISTA DE SÍMBOLOS

Símbolo	Significado
e^x	Error de estimación máximo aceptado
n	Muestra de una población
Z_{α}^{x}	Parámetro estadístico del nivel de confianza (NC)
%	Porcentaje
q	Probabilidad de que no ocurra el evento en estudio
p	Probabilidad de que ocurra en evento en estudio
Q	Quetzales
N	Tamaño de la población o universo

GLOSARIO

Cross-Site Scripting	Secuencia de comandos entre sitios
Delay	Tiempo de espera
Denial of Service	denegación de servicio
Frame	Paquete de datos
Hoaxes	Engaños

RESUMEN

Un servidor honeypot un servidor que se construye vulnerable ante ciberataques deliberadamente con el objetivo de llamar la atención de ciberdelincuentes y que estos puedan entrar y pensar que están dentro de un servidor real y productivo. Luego de que un ciber atacante ha caído en esta “trampa” será posible conocer cuáles son sus técnicas de ataque. Con esta información podremos reforzar nuestros servicios reales y protegernos con anticipación a los ciber atacantes.

Mientras más servicios existan en un servidor honeypot mayor será la superficie de ataque que el ciber atacante tratara de explotar y mayor será la información que obtendremos. Sin embargo, implementar toda esta cantidad de servicios conlleva una inversión de tiempo y esfuerzo. En los últimos años ha surgido la infraestructura como servicio, a través de esta podremos implementar y provisionar de forma automatizada todos los servicios necesarios.

1. INTRODUCCIÓN

Internet se ha convertido en los últimos años en una herramienta indispensable en muchos ámbitos de nuestra vida diaria. La utilidad que este tiene va desde simplemente leer correos electrónicos hasta efectuar transacciones bancarias. Sin embargo, también existen actores mal intencionados que buscan causar daño a los usuarios u organizaciones tratando de robar, destruir o secuestrar información valiosa.

Un servidor *honeypot* simula el funcionamiento de un servidor real con el objetivo de distraer al atacante, así como conocer las técnicas y procedimientos que este utiliza para acceder y perpetrar un ciberataque. La información obtenida de un servidor *honeypot* debe ser analizada y utilizada para proteger los sistemas informáticos.

El fin de este trabajo de investigación es mostrar como un servidor *honeypot* puede ser implementado de forma automática para reducir su tiempo de implementación, así como demostrar cuales son las mejoras practicas utilizadas para analizar la información obtenida y que esta pueda ser accedida de forma pública para que empresas guatemaltecas puedan utilizarla para protegerse de ataques cibernéticos.

2. ANTECEDENTES

Los ataques cibernéticos en el año 2021 en el continente americano han aumentado un 70 % según el último informe Inteligencia de amenazas de la reconocida empresa de ciberseguridad *Check Point*.

> Este mismo informe también nos cuenta que en Guatemala en el año 2020 se contabilizaban 1012 ataques a organizaciones semanalmente en junio, a comparación del mes de noviembre del mismo año que se registraron 1673. Estos son números realmente alarmantes tomando en cuenta que ocurren muchos más ataques que no son reportados y por lo tanto no se registran en estos informes. (Ciberseguridad, 2021, párrs. 1 - 11)

> Un *honeypot* es un dispositivo de seguridad que está diseñado para atraer actividades cibernéticas maliciosas a sí mismo. Los datos capturados son usados para estudiar y entender cómo operan los ciber atacantes y subsecuentemente mejorar la seguridad de nuestra infraestructura tecnológica. Un *honeypot* no tiene ningún recurso verdaderamente valioso, sino todo lo contrario, es un recurso de seguridad cuyo valor radica en ser investigado, atacado y comprometido. (Spitzner, 2002, p. 32)

> Los orígenes de los *honeypots* se remontan a conceptos y usos militares, pero aparecieron por primera vez en el área de seguridad informática en la década de los 80s. Un investigador describe la caza de un hacker en 1986 con la idea de monitorear la actividad de un intruso en un sistema real, este proveyó como cebo informes militares falsos para atraer al atacante a un área particular de su sistema. Si bien este no fue el honeypot

> que conocemos hoy, fue el primer intento de atrapar moscas con miel. (Stoll, 1988, p. 22)

El primer honeypot como se conoce hoy en día, que hizo uso de un entorno simulado fue descrito por Cheswick en 1992, en el cual nos relata el rastreo del hacke holandes Berfed en 1991. A finales de los 90s, lo intentos de atraer y observar a los atacantes sobresalieron con la introduccion de varias herramientas y productos comerciales.

> Una de las primeras formas de clasificar a los honeypots fue por su nivel de interaccion. Un honeypot de baja interaccion dara al ciber atacante acceso muy limitado al sistema, es decir, no tendra acceso en profundidad y unicamente se emularan una pequeña cantidad de protocolos y servicios de red. Un honeypot de alta interaccione es todo lo contrario, en lugar de simplemente emular ciertos protocolos y servicios, el ciber atacante cuenta con sistemas muy parecidos a sistemas reales, por lo que es muy poco probable que piense que esta siendo observado y engañado. (Seifert, 2006, p. 95)

3. PLANTEAMIENTO DEL PROBLEMA

3.1. Contexto general

Como resultado de la pandemia COVID-19 muchas empresas guatemaltecas han aumentado la cantidad de sistemas informáticos con el fin de poder adaptarse a esta situación. Como resultado de esto ahora tenemos muchas personas realizando teletrabajo y empresas ofreciendo sus productos o servicios en línea. Muchas de estas implementaciones fueron improvisadas y sin tomar en cuenta aspectos básicos de seguridad informática, debido a que no se tuvo tiempo necesario para realizar un planeamiento apropiado. Todo esto ha aumentado la superficie que los cibercriminales pueden aprovechar ejecutar delitos informáticos.

3.2. Descripción del problema

Actualmente en Guatemala no existe una fuente confiable y de libre acceso a información sobre ataques cibernéticos locales, existen empresas que ofrecen servicios de seguridad informática y consultoría a grandes empresas, sin embargo, esto tiene un costo que medianas y pequeñas empresas no se pueden dar el lujo de pagar. Esto provoca que cientos de organizaciones sufran ciberataques que provocan el robo de información, la perdida de confiabilidad de sus clientes y la más importante, perdidas monetarias.

3.3. Formulación del problema

En la actualidad pocas empresas guatemaltecas cuentan con una herramienta dedicada a recolectar información sobre potenciales ataques ejecutados por *hackers*, los cuales pueden llegar a comprometer seriamente la continuidad del negocio y uno de sus activos más importantes: la información.

3.3.1. Pregunta central

¿Qué tan efectivo puede ser la automatización de la implementación servidor honeypot para generar información que ayude a prevenir ataques cibernéticos a empresas guatemaltecas?

3.3.2. Preguntas auxiliares

En coherencia con la pregunta central, se formulan las siguientes preguntas auxiliares:

- Pregunta 1

¿Qué porcentaje de tiempo se logra reducir realizando la implementación de un servidor honeypot por medio de automatización?

- Pregunta 2

¿Cuáles son los ataques cibernéticos que pueden ser prevenidos gracias a la implementación de un servidor honeypot?

- Pregunta 3

¿Existe una fuente confiable y de libre acceso a información acerca de ataques cibernéticos?

3.4. Delimitación del problema

El presente trabajo se desarrollará en hardware propio, tendrá una duración 6 meses y abarcará el área de Guatemala.

4. JUSTIFICACIÓN

La línea de investigación en la que este trabajo se enfoca es la automatización y seguridad de redes con la idea de aportar datos relevantes para la prevención de ataques cibernéticos.

Hoy en día las empresas reaccionan a los ataques cibernéticos de manera reactiva, es decir, cuando estos ya han ocurrido, esto provoca que el tiempo de recuperación sea de horas o incluso días, provocando a las empresas perdidas monetarias, con este trabajo se pretende que las acciones se tomen de manera preventiva para tratar de minimizar el tiempo sin operación.

Se espera que este trabajo sea útil y apoye con datos relevantes a las pequeñas y medianas empresas en Guatemala para que estas sean capaces de controlar y detener las amenazas cibernéticas que se puedan presentar. Otro beneficio que puede ser obtenido de este trabajo es que puede servir de guía para las empresas que piensen implementar sus propios servidores honeypot.

5. OBJETIVOS

5.1. General

Automatizar la implementación de un servidor un Honeypot como herramienta de prevención y detección de ciberataques en empresas guatemaltecas.

5.2. Específicos

- Reducir el tiempo de implementación de un servidor honeypot por medio de automatización.

- Prevenir la mayoría de los ataques cibernéticos gracias a los datos obtenidos en un servidor honeypot.

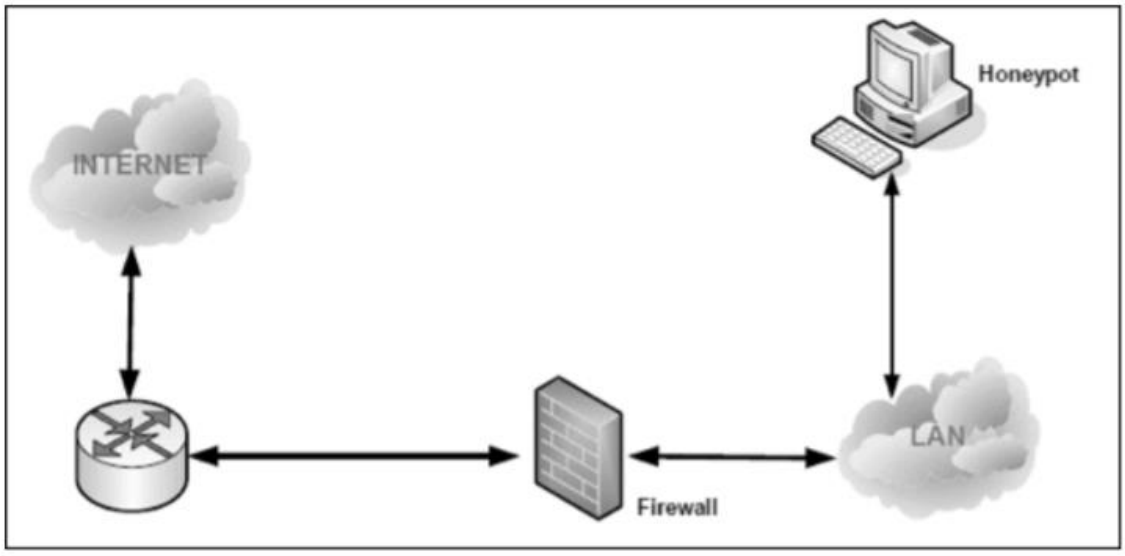
- Crear una fuente confiable y de libre acceso a información acerca de ataques cibernéticos.

6. NECESIDADES POR CUBRIR Y ESQUEMA DE LA SOLUCIÓN

Este trabajo viene a ayudar a aquellas empresas que no cuentan con un departamento de seguridad informático ya que estas no tendrán que realizar ninguna implementación dentro de su infraestructura, sino que se proveerán datos más fáciles de digerir como direcciones IP maliciosas que se deben bloquear, vulnerabilidades que se deben parchear inmediatamente, etc. Toda esta información será publica y accesible por medio de redes sociales.

A continuación, se muestra la topología que será implementada

Figura 1. **Esquema de la solución**



Fuente: elaboración propia, utilizando Microsoft Visio 2016.

7. MARCO TEÓRICO

El presente capítulo presenta la base teórica de este trabajo, definiendo los conceptos básicos de automatización en tecnologías de la información y ciberseguridad, para luego dar paso a la definición y tipos de honeypots existentes.

7.1. Automatización

La automatización en tecnologías de la información, algunas veces llamada automatización de la infraestructura es el uso de software para crear instrucciones y procesos repetibles con la idea de reducir la interacción humana con los sistemas. El software de automatización trabaja dentro de las fronteras de esas instrucciones, herramientas y marcos para completar las tareas con poca o nula intervención humana.

La automatización es clave para la optimización y la transformación digital de las tecnologías de la información. Los ambientes deben ser modernos, dinámicos y capaces de escalar rápidamente y la automatización nos provee todas estas bondades.

Todas las tareas relacionadas con tecnologías de la información pueden ser automatizadas en algún grado. Así la automatización se puede aplicar a diferentes áreas, desde automatización de redes de datos, infraestructura, aprovisionamiento de servicios en la nube, entre otros.

7.2. Infraestructura como código

Infraestructura como código es una forma de gestionar la infraestructura de tecnologías de la información que se basa en prácticas del desarrollo de software. “Destacan las rutinas repetibles para el aprovisionamiento y cambios en sistemas y su configuración. Los cambios se realizan en el código, luego con el uso de la automatización, estos se prueban y aplican a los sistemas” (Morris, 2016, p. 53).

7.2.1. Beneficios de la infraestructura como código

A continuación, se listan algunos de los beneficios de la Infraestructura como código.

- El aprovisionamiento automático reduce el riesgo de error humano.
- Ayuda a los equipos de TI a enfocarse en la creación de software en lugar del aprovisionamiento y mantenimiento de la infraestructura actual.
- Es posible reducir costos automatizando la eliminación de recursos no usados.
- Se mantiene la consistencia en las configuraciones al utilizar plantillas previamente revisadas y aprobadas.
- Se mejora la seguridad al automatizar la verificación continua del cumplimiento de estándares de seguridad.

- Se facilita la colaboración de varias personas del equipo en la elaboración de código al estar almacenado en un repositorio que permite la administración de versiones.

7.2.2. Herramientas para el desarrollo de infraestructura como código

La creciente utilización de infraestructura como código ha impulsado a varias empresas que ofrecen servicios de nube a desarrollar sus propias herramientas para cubrir las necesidades de sus clientes. Cada herramienta ofrece su propia interfaz y lenguaje de programación. Algunas de las herramientas más utilizadas son las siguientes:

7.2.2.1. Terraform

Terraform es una herramienta consistente y confiable de infraestructura como código de código abierto que proporciona un flujo de trabajo mediante CLI (command line interface) consistente para administrar cientos de servicios en la nube, proporcionando acceso a datos compartidos de estado y secretos, controles de acceso para aprobar cambios en la infraestructura, según su web oficial (Terraform, 2021).

7.2.2.2. AWS cloud formation

CloudFormation nos permite modelar, aprovisionar y gestionar recursos pertenecientes a AWS y otros proveedores manejándolos como infraestructura como código. Permite automatizar la administración de recursos a través de toda la organización con las integraciones de servicios de AWS que ofrecen controles

de gobernanza y distribución de aplicaciones llave en mano, según su web oficial (AWS CloudFormation, 2021).

7.2.2.3. Google cloud deployment manager

Google Cloud Deployment Manager es un servicio de implementación de infraestructura como código que automatiza la creación y administración de los recursos de Google Cloud. Permite escribir plantillas flexibles y archivos de configuración utilizándolos para crear implementaciones de varios servicios de Google Cloud como Cloud Storage, Compute Engine, y Cloud SQL para trabajar juntos, según su web oficial (Cloud Deployment Manager, 2021).

7.2.2.4. Chef infra

Chef Infra es un software de administración de infraestructura como código que elimina los esfuerzos manuales y garantiza que la infraestructura se mantenga consistente y compatible durante su vida útil, incluso en los entornos más complejos, heterogéneos y de gran escala. Permite definir que las configuraciones se corrijan automáticamente si un sistema difiere del estado definido, según su web oficial (Chef Infra, 2021).

7.2.2.5. Red hat ansible automation platform

Ansible Automation Platform proporciona un marco empresarial para construir y operar la automatización de la infraestructura de TI a escala. Esta permite a los usuarios de una organización crear, compartir y administrar la automatización, desde el desarrollo y las operaciones hasta los equipos de red y seguridad, según su web oficial (Red Hat Ansible Automation Platform, 2021).

7.2.3. Herramientas para el versionado de código

El control de versiones es la práctica de dar seguimiento y administrar cambios en el código de software. Un sistema de control de versiones ayuda a los equipos de TI a gestionar los cambios al código fuente a lo largo del tiempo. A medida que los entornos de desarrollo se han acelerado, los sistemas de control de versiones ayudan a los equipos de TI a trabajar de forma más rápida e inteligente. Las herramientas más utilizadas son:

7.2.3.1. Git

> Git es un sistema de control de versiones de código abierto y gratuito diseñado para manejar desde proyectos pequeños a muy grandes, con velocidad y eficiencia. La característica de Git que realmente lo distingue de casi todos los demás sistemas es su modelo de ramificación. Git permite tener múltiples ramas que pueden ser completamente independientes entre sí. La creación, fusión y eliminación de esas líneas de desarrollo solo toma unos segundos, según su web oficial. (Git, 2021, p. 159)

7.2.3.2. CVS

CVS es un sistema de control de versiones que permite registrar el historial de archivos y documentos de código. Ofrece un modelo cliente/servidor que permite a los desarrolladores en diferentes ubicaciones geográficas funcionar como un solo equipo. El historial de versiones se almacena en un único servidor central y las maquinas cliente tienen una copia de todos los archivos en los que están trabajando los desarrolladores, según su web oficial.

7.2.3.3. Apache subversion (SVN)

Subversión es un sistema de control de versiones de código abierto que se caracteriza por su confiabilidad como un lugar seguro para almacenar datos valiosos, la sencilles de su modelo de uso y su capacidad para satisfacer las necesidades de una amplia variedad de usuarios y proyectos, desde individuos hasta operaciones empresariales a gran escala, según su web oficial. (Subversion, 2021, p. 54)

7.2.3.4. Mercurial

Mercurial es un “sistema de control de versiones de código abierto. Gestiona de forma eficaz archivos y documentos de código de toda magnitud. Mercurial está escrita en Python. Tiene un alto rendimiento y escalabilidad con capacidades avanzadas de ramificación, fusión y un desarrollo colaborativo toralmente distribuido” según su web oficial (Mercurial, 2021, p. 45).

7.2.3.5. Monotone

Monotone tiene la misma función y distribución de los sistemas anteriores. Proporciona un almacén de versiones transaccionales de archivos sencillos, Emplea versiones criptográficas para resguardar la seguridad en la infraestructura del cliente. Se ejecuta en todos los sistemas operativos utilizados hoy en día y este licenciado bajo GNU GPL, según su web oficial (Monotone, 2021).

7.3. Fundamentos de ciberseguridad

Es muy común hoy en día que se confundan los términos seguridad de la información con ciberseguridad. En el pasado, la seguridad de la información se encargaba de proteger la confidencialidad, integridad y disponibilidad de los datos de una organización. Desafortunadamente eso ya no es suficiente. Las organizaciones, sin importar su tamaño, son un objetivo. Con esto podemos decir que ciberseguridad es el proceso de proteger los datos de una organización, previniendo, detectando y respondiendo a ciberataques.

7.3.1. Amenaza

Una amenaza es cualquier daño potencial que puede ser causado a un activo de una organización, a través del acceso no autorizado a un sistema de información, la destrucción, divulgación o modificación de información y la denegación del servicio (NIST, 2021).

7.3.2. Vulnerabilidad

Una vulnerabilidad es una debilidad en el diseño, implementación, software, código fuente o la falta de un mecanismo en un sistema. La correcta implementación de medidas de ciberseguridad puede mitigar una vulnerabilidad y reducir el riesgo de explotación. Las vulnerabilidades pueden presentarse en los siguientes sistemas:

7.3.2.1. Vulnerabilidades en aplicaciones

Las aplicaciones contienen cientos de funcionalidades, generalmente las aplicaciones son configuradas para usabilidad en lugar de seguridad. Por esta razón los atacantes tienen una gran superficie de ataque.

7.3.2.2. Vulnerabilidades en sistemas operativos

El software del sistema operativo se carga en estaciones de trabajo y servidores. Los atacantes pueden buscar vulnerabilidades en los sistemas operativos que no han sido parcheados o actualizados.

7.3.2.3. Vulnerabilidades debidas a configuraciones erróneas

La mala configuración de un sistema puede considerarse también una vulnerabilidad. Esto puede ser, dejar puertos innecesarios abiertos, dejar datos sensibles sin cifrar, no usar contraseñas seguras, entre otros.

7.3.3. Exploit

Un *exploit* puede ser un código, una herramienta, una técnica o un proceso que toma ventaja de una vulnerabilidad que conduce a un acceso no autorizado, una escalación de privilegios, perdida de integridad o una denegación de servicio en un sistema. Los *exploits* son bastante dañinos porque la mayoría de software tiene vulnerabilidades y los ciber atacantes constantemente están tratando de tomar ventaja de ello. Aunque la mayoría de las organizaciones intenta buscar y corregir estas vulnerabilidades, la mayoría carece de recursos para asegurar sus sistemas. Algunas veces estas vulnerabilidades no son conocidas, esto se

conoce como una vulnerabilidad de día cero. Este tipo de vulnerabilidades son difíciles de controlar ya que existe un rango de tiempo entre el día que la vulnerabilidad es descubierta y el día en que un parche está disponible para corregir la vulnerabilidad.

7.3.4. Riesgo

Riesgo es la probabilidad perdida financiera, afectación o daño de la reputación de una organización derivado de un ataque cibernético. Existen tres elementos básicos para calcular el riesgo: activos, amenazas y vulnerabilidades. Un activo es cualquier artículo de valor económico propiedad de una persona individual o de una organización. Los activos pueden ser tangibles, como enrutadores, servidores, discos duros, computadoras portátiles, entre otros, o los activos pueden ser no tangibles, como fórmulas, bases de datos, hojas de cálculo, secretos comerciales y tiempo de procesamiento. Sin importar de que tipo de activo hablemos, si el activo se pierde o es comprometido, puede haber un costo económico para la organización. Una amenaza es cualquier agente, condición o circunstancia que puede causar daño, perdida o comprometer un activo. Desde otro punto de vista las amenazas pueden ser categorizadas como eventos que pueden afectar la confidencialidad, integridad o disponibilidad de los bienes de la organización. Las amenazas pueden resultar en la destrucción, divulgación, modificación, corrupción de datos o denegación de servicio. Algunos ejemplos de amenazas que puede enfrentar una organización son los siguientes:

7.3.4.1. Desastres naturales

Cualquier daño que pueda ser causado por inclemencias del clima se considera una amenaza, entre ellos podemos mencionar: huracanes, tormentas, incendios, inundaciones, terremotos y otros eventos naturales.

7.3.4.2. Ciberataques

Un ciberataque puede ser llevado a cabo por una persona externa o interna de la organización, quien no está autorizada y ataca intencionalmente la infraestructura, los componentes, sistemas o datos. Los ciberataques también pueden ser dirigidos a infraestructuras críticas de un país como plantas de agua, plantas eléctricas, plantas de gas, refinerías de petróleo, refinerías de gasolina, plantas de energía nuclear, plantas de gestión de residuos, entre otros. Stuxnet es un ejemplo de una herramienta de este tipo diseñada para este objetivo.

7.3.4.3. Virus y malware

En esta categoría entran una gran cantidad de software y herramientas que son maliciosas y están diseñadas para dañar o destruir un sistema o información.

7.3.4.4. Divulgación de información confidencial

Cada vez que ocurre una divulgación de información confidencial, puede ser una amenaza crítica para una organización si dicha divulgación causa pérdidas de ingresos, genera responsabilidades potenciales o proporciona una ventaja competitiva a un adversario.

7.3.4.5. Ataques de denegación de servicio o denegación de servicio distribuido

Este es un ataque a un sistema o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Hoy en día la mayoría de estos ataques

se lanzan a través de botnets, mientras que en el pasado se utilizaban herramientas como Ping of Death o TearDrop.

7.3.5. Actores de amenaza

Los actores de amenaza son las personas o grupos de personas que ejecutan un ciberataque o son responsables de un incidente de ciberseguridad que impacta a una organización o individuo. Hay varios tipos de actores de amenaza.

7.3.5.1. Script kiddies

Estas son las personas que usan scripts o herramientas de hacking existentes. Ellos no tienen la experiencia para escribir sus propios scripts. Este término no se relaciona necesariamente con la edad de la persona. El término se considera despectivo.

7.3.5.2. Grupos de delincuencia organizada

Su principal objetivo es robar información, estafar a las personas y ganar dinero. Estos grupos están continuamente adaptándose, buscando nuevas formas de explotar el uso de datos personales o archivos comerciales confidenciales

7.3.5.3. *Hackers* patrocinados por el estado

Estas personas están interesadas en robar información, incluyendo datos de propiedad intelectual y datos de investigación y desarrollo de grandes empresas, agencias gubernamentales. Un ejemplo de un ataque patrocinado por

el Estado es el malware Stuxnet que se creó para dañar las capacidades de enriquecimiento nuclear de Irán. Luego de esto los países se dieron cuenta de que podían utilizar ciberataques para lograr sus objetivos políticos, comerciales y militares.

7.3.5.4. Hacktivistas

Estas personas ejecutan ciberataques motivados por una causa social o política. Las técnicas que utilizan van desde ataques de denegación de servicio, filtraciones de información y la replicación de sitios web.

7.3.5.5. Grupos terroristas

Estos grupos llevan a cabo ciberataques motivados por causas políticas o religiosas. Su principal objetivo es causar daño a infraestructuras nacionales criticas como plantas de energía, transporte u operaciones de gobierno para intimidar a una nación o población civil.

7.3.5.6. Hackers

Originalmente, el termino *hacker* fue usado para un entusiasta de los computadores. Un *hacker* era una persona a la que le gustaba comprender el funcionamiento interno de un sistema, una computadora o una red de computadores. Con el tiempo, la prensa comenzó a describir a los *hackers* como individuos que irrumpían en sistemas informáticos con intenciones maliciosas. La industria respondió desarrollando el término *cracker*, que es la abreviatura de hacker criminal. Con toda esta confusión sobre como distinguir los chicos buenos de los chicos malos, el término *hacker* ético fue acuñado. Un *hacker* ético es una persona que ejecuta pruebas de seguridad y análisis de vulnerabilidades con la

idea de ayudar a las organizaciones a asegurar su infraestructura tecnológica. Las intenciones de los *hackers* son varias. Algunas son legítimas, mientras que otras pueden considerarse fuera de la ley. Por esta razón se han categorizado a los *hackers* de la siguiente manera.

7.3.5.6.1. Hackers de sombrero blanco

Los *hackers* de sombrero blanco ejecutan actividades de *hacking* ético con la idea de ayudar a las empresas a asegurar su infraestructura tecnológica. Su creencia es que las empresas deben evaluar su postura de seguridad de la misma manera que un *hacker* con malas intenciones lo haría para comprender mejor sus vulnerabilidades.

7.3.5.6.2. Hackers de sombrero negro

Los *hackers* de sombrero negro son criminales que irrumpen en redes de computadoras con malas intenciones, también pueden liberar malware que destruye archivos, retiene computadoras como rehenes, roba contraseñas, números de tarjetas de crédito y cualquier tipo de información personal.

7.3.5.6.3. Hackers de sombrero gris

Los *hackers* de sombrero gris usualmente se ubican entre un *hacker* de sombrero blanco y negro ya que ejecutan tareas de ambos. Algunas veces encuentran vulnerabilidades en un sistema sin el permiso de la empresa, algunas veces pueden explotar esta vulnerabilidad de manera maliciosa, o también pueden reportarla al encargado de seguridad informática para que esta sea corregida.

7.3.6. Inteligencia de amenazas

Se conoce como inteligencia de amenazas al conocimiento acerca de amenazas existentes o emergentes para los activos de una organización. La inteligencia de amenazas incluye contexto, mecanismos, indicadores de compromiso, implicaciones y consejos prácticos. El principal objetivo de la inteligencia de amenazas es informar a las organizaciones acerca de los riesgos e implicaciones asociadas con amenazas cibernéticas. La inteligencia de amenazas es útil en el sentido de que ayuda a las organizaciones a trabajar proactivamente frente a las amenazas cibernéticas en lugar de hacerlo reactivamente.

Hoy en día existen bastantes plataformas de inteligencia de amenazas enfocadas en proveer información útil como indicadores de compromiso, IPs o direcciones web maliciosas y patrones de explotación.

7.3.7. Malware

La palabra malware se refiere a todo software malicioso que puede causar daño a los activos informáticos de una organización, las acciones que un malware puede realizar van desde mostrar mensajes no deseados en la pantalla de una computadora, hacer que los programas trabajen de forma errática, hasta cifrar archivos exigiendo un rescate para descifrarlos o incluso destruir datos o discos duros. A continuación, se describen los diferentes tipos de malware.

7.3.7.1. Virus

Un virus informático es un código malicioso que necesita adjuntarse a un programa o software para causar daño y por lo tanto requieren de interacción

humana. Algunos virus informáticos están diseñados para dañar dispositivos o programas, eliminar archivos o formatear el disco duro. Otros simplemente se replican a sí mismos o inundan la red con tráfico, impidiendo a las organizaciones trabajar con normalidad. Incluso los virus informáticos menos dañinos pueden interrumpir significativamente el rendimiento de una computadora, agotando la memora y provocando fallas en la misma.

7.3.7.2. Gusano

Un gusano es un tipo de malware que distribuye copias de el mismo de dispositivo en dispositivo, este puede replicarse a sí mismo sin interacción humana y a diferencia de un virus no necesita adjuntarse a un programa de software para causar daño. Por ejemplo, un gusano puede enviar el mismo un correo electrónico a todos los contactos en una libreta de direcciones y luego repetir este proceso una y otra vez desde la computadora de cada usuario que infecta. Esto generara una cantidad enorme de tráfico que puede provocar una denegación de servicio muy rápidamente.

7.3.7.3. Troyanos

Los troyanos son programas que pretenden hacer una cosa, pero cuando se cargan en realidad realizan una acción maliciosa. Los troyanos obtienen su nombre del cuento épico de Homero, La Ilíada. Para derrotar a su enemigo, los griegos construyeron un caballo gigante de madera con soldados en su interior. Los griegos engañaron a los troyanos para que llevaran el gran caballo de madera dentro de la ciudad fortificada de Troya. Ya en la oscuridad de la noche, los griegos salieron del caballo de madera, abrieron la puerta y dejaron entrar a más soldados que esperaban afuera. Un software troyano se basa en el mismo concepto. El usuario piensa que el archivo es seguro de ejecutar, pero después

de que el archivo es ejecutado una actividad maliciosa es llevada a cabo. Los troyanos son muy efectivos porque típicamente se presentan como algo que el usuario quiere, como un archivo PDF, un documento de Word o una hoja de cálculo de Excel. Un troyano puede permitir al atacante acceder a un sistema de forma remota, guardar un registro de cada pulsación del teclado con el objetivo de obtener contraseñas, colocar una puerta trasera, provocar una denegación de servicio o incluso desactivar la protección antivirus o el software de firewall.

7.3.7.4. Ransomware

En los últimos años, el ransomware ha sido usado por los cibercriminales para ganar dinero cifrando información valiosa para las organizaciones y cobrando un rescate para descifrarla. Se puede propagar a sí mismo como un gusano. En muchos casos la demanda de pago del rescate viene con una fecha límite. Si la víctima no paga a tiempo, la información es eliminada o la cantidad demandada incrementa.

7.3.7.5. Spyware

El spyware es otra forma de código malicioso, este es muy similar a un troyano pues es instalado sin el consentimiento o conocimiento del usuario. El spyware se encarga de monitorear el dispositivo y el uso de internet, es configurado para ejecutarse en segundo plano cada vez que el dispositivo inicia. Uno de los usos del spyware es vigilar y determinar cuáles son nuestros hábitos de compras en Internet y reportar esta información a empresas de *marketing* con la idea de mostrarnos publicidad.

7.3.8. Honeypot

Un honeypot es básicamente una trampa para un ciber atacante, está destinado a atraer ciberataques por medio de un señuelo. Este imita el funcionamiento de un sistema real y utiliza los ataques recibidos para obtener información sobre las técnicas y forma de operación de los ciber atacantes con la idea de usar esta información para prevenir futuros ciberataques. Por ejemplo, un honeypot podría encubrirse como el servidor de correo electrónico de una empresa, este es un objetivo frecuente de ataques pues los ciber delincuentes desean encontrar información confidencial.

Una vez los ciber atacantes están dentro, su comportamiento puede ser rastreado y registrado. Los honeypots se vuelven atractivos para los atacantes al incorporar vulnerabilidades de seguridad de forma deliberada. Por ejemplo, un servidor honeypot puede tener un sistema operativo desactualizado al cual no se le han aplicado los parches de seguridad necesarios. El propósito de un honeypot no es resolver un problema puntual, como un cortafuegos. En cambio, es mecanismo que provee datos útiles que ayudan a entender las ciber amenazas existentes y prevenir ser víctimas de las ciber amenazas emergentes. Con la ciber inteligencia obtenida de esta herramienta, los esfuerzos de seguridad se pueden enfocar en lo realmente importante. Hoy en día existen distintos tipos de honeypots (What is a honeypot?, 2021).

7.3.8.1. Trampas de correo electrónico

Los robots de spam recorren internet, recopila direcciones de correo electrónico y les envían spam. Obteniendo ingresos monetarios por la venta de esas direcciones de correo electrónico a otros spammers. Rápidamente, cualquier correo electrónico publicado en Internet recibirá cientos de mensajes

de correo no deseado todos los días. Las trampas de correo electrónico consisten en direcciones de correo electrónico configuradas específicamente para atrapar a los spammer en acción. La mayoría son trampas con cuentas de correo inactivas a las que ninguna persona en circunstancias normales enviaría un correo electrónico legítimo, el hecho de estar recibiendo correos electrónicos indica claramente que estos provienen de un spammer. De esta forma podemos identificar patrones, palabras claves y direcciones IPs y bloquearlas en los servidores de correo.

7.3.8.2. Bases de datos señuelo

Una base de datos señuelo se usa para atraer ataques específicos de bases de datos, como inyecciones SQL, muchas veces estos ataques son indetectables por los cortafuegos. De esta forma es posible desviar a los atacantes de los objetivos reales y obtener información útil para proteger las bases de datos.

7.3.8.3. Honeypot de malware

Un honeypot de malware es un señuelo que atrae ataques de malware. Los profesionales de la ciberseguridad pueden usar los datos de dichos honeypots para desarrollar software antivirus avanzados para los sistemas operativos más comunes. También pueden estudiar los patrones de ataques de malware para mejorar la tecnología de detección de malware.

8. PROPUESTA DE ÍNDICE DE CONTENIDOS

4.2.2.5. Red Hat Ansible Automation Platform

4.2.3. Herramientas para el versionado de código

4.2.3.1. Git

4.2.3.2. CVS

4.2.3.3. Apache Subversión (SVN)

4.2.3.4. Mercurial

4.2.3.5. Monotone

4.3. Fundamentos de ciberseguridad

4.3.1. Amenaza

4.3.2. Vulnerabilidad

4.3.2.1. Vulnerabilidades en aplicaciones

4.3.2.2. Vulnerabilidades en sistemas operativos

4.3.2.3. Vulnerabilidades debidas a configuraciones erróneas

4.3.3. Exploit

4.3.4. Riesgo

4.3.4.1. Desastres naturales

4.3.4.2. Ciberataques

4.3.4.3. Virus y malware

4.3.4.4. Divulgación de información confidencial

4.3.4.5. Ataques de denegación de servicio o denegación de servicio distribuido

4.3.5. Actores de amenaza

4.3.5.1. Script kiddies

4.3.5.2. Grupos de delincuencia organizada

4.3.5.3. *Hackers* patrocinados por el Estado

4.3.5.4. Hacktivistas

4.3.5.5. Grupos terroristas

5.7.2. Encuestas

6. TÉCNICAS DE ANÁLISIS DE INFORMACIÓN

CONCLUSIONES

RECOMENDACIONES

REFERENCIAS

APÉNDICES

ANEXOS

9. METODOLOGÍA DE LA INVESTIGACIÓN

En este capítulo se desarrollan los aspectos metodológicos y el proceso de investigación del presente estudio. También se dan detalles de la perspectiva desde la cual se aborda la investigación. Se muestra las estrategias y técnicas utilizadas para la compilación de la información.

9.1. Diseño de la investigación

Para el presente estudio el tipo de diseño de investigación que mejor lo describe es el experimental, debido a que el principal objetivo es reunir, analizar y publicar información fácilmente digerible, que luego se transforme en acciones que puedan ser implementadas por empresas guatemaltecas para protegerse de ataques cibernéticos.

El diseño experimental es una técnica de investigación con un enfoque científico, donde algunas variables se mantienen inmutables, mientras que otras se miden como objetivo del experimento.

La metodología utilizada es puramente experimental ya que se utilizarán los conocimientos adquiridos durante los cursos de esta maestría, se desarrollará un sistema de información y se aplicarán conceptos de ciberseguridad para resolver un problema.

Una verdadera investigación experimental se considera exitosa sólo cuando el investigador confirma que un cambio en la variable dependiente se debe a la manipulación de la variable independiente. Es importante para una investigación experimental establecer la causa y el efecto de un fenómeno, lo que significa que debe ser claro que los efectos observados en un experimento se deben a la causa.

9.2. Enfoque de la investigación

El enfoque del presente trabajo es cuantitativo, ya que se usará recolección de datos para probar hipótesis con base en la medición numérica y análisis estadístico para establecer patrones de comportamiento.

El enfoque cuantitativo utiliza la recolección y el análisis de datos para contestar una o varias preguntas de investigación y probar las hipótesis establecidas previamente. Se basa en la medición numérica, el conteo y la mayoría de las veces en la estadística para determinar con exactitud, patrones de comportamiento en una población. Se basa en un esquema deductivo y lógico, es reduccionista y pretende generalizar los resultados de sus estudios mediante muestras representativas. Luego de tener la pregunta de investigación se derivan una o varias hipótesis y se desarrolla una estrategia para probarla o refutarla.

9.3. Población de estudio

La población de estudio serán empresas medianas y pequeñas guatemaltecas con una infraestructura de tecnologías de la información con la capacidad de aplicar las recomendaciones publicadas como resultado de esta investigación.

9.4. Tipo de muestreo

Se tomarán los valores aleatoriamente por lo que el tipo de muestra del estudio es probabilístico.

9.5. Tamaño de la muestra

Para el tamaño de la muestra usaremos la ecuación:

$$n = \frac{Z_{\propto}^2 Npq}{e^2(N-1) + Z_{\propto}^2 pq}$$

Se escogerá un nivel de confianza de mínimo 80 % por lo que $Z_{\propto} = 1.28$ y la proporción de individuos se hará simétrica por lo tanto $p = q = 0.5$.

El tamaño de la población es de $N = 400$ individuos. El error muestral será de $e = 5\ \%$.

Por lo que al sustituir los datos.

$$n = \frac{(1.28)^2 * 200 * 0.5 * 0.5}{(0.05)^2(200-1) + (1.28)^2 * 0.5 * .5} = 90.31 \cong 90$$

Por lo que el tamaño de la muestra a usar será de 90 empresas guatemaltecas.

9.6. Técnicas de investigación

Se utilizarán la documentación, encuentras y entrevistas como técnicas de investigación.

9.6.1. Investigaciones previas y entrevistas

Se sacará provecho de la documentación existente para configurar y automatizar la implementación del *honeypot*, luego de esto se obtendrá la información y será publicada para su fácil acceso.

Se harán encuestas en la red social Linkedin, la cual es una red social profesional que nos permitirá tener acceso al personal está a cargo de la ciberseguridad de varias empresas guatemaltecas. Gracias a estas encuestas obtendremos la opinión de los profesionales de la ciberseguridad en Guatemala, así como su retroalimentación de las publicaciones realizadas.

El proceso de recopilación de datos tiene dos pasos fundamentales: identificar las fuentes de información y recopilar datos. Este trabajo de investigación tiene como objetivo apoyar a empresas medianas y grandes guatemaltecas por lo que se deben generar las encuestas y ser dirigidas específicamente a esta población, luego la recolección de datos se hará enviando las respuestas a hojas de Excel para posteriormente será analizada y publicada.

9.7. Instrumentos de recolección de datos

A continuación, se mencionan muestran los instrumentos elegidos para la recolección de datos.

9.7.1. Documentos

La primera parte de la recolección de datos se basa en la documentación existente, esto con la idea de buscar la forma ideal de la implementación. En esta parte se decidirá qué tipo de servicios serán implementados en el honeypot, en que plataforma de virtualización será nos basaremos y el tipo de topología que mejor se adapte a las necesidades.

9.7.2. Encuestas

Hoy en día es muy fácil llegar a un grupo objetivo de personas gracias a las redes sociales, la red social Linkedin es una red principalmente orientada a la búsqueda de empleos, pero también en ella podemos a encontrar a muchos profesionales que día a día comparten sus experiencias diarias de trabajo y están dispuestos a ayudar a otros profesionales. Por medio de esta red se pretende llegar a los profesionales de la ciberseguridad para plantearles distintivos tipos de encuestas y poder obtener la información necesaria antes de iniciar la implementación del proyecto.

10. TÉCNICAS DE ANÁLISIS DE INFORMACIÓN

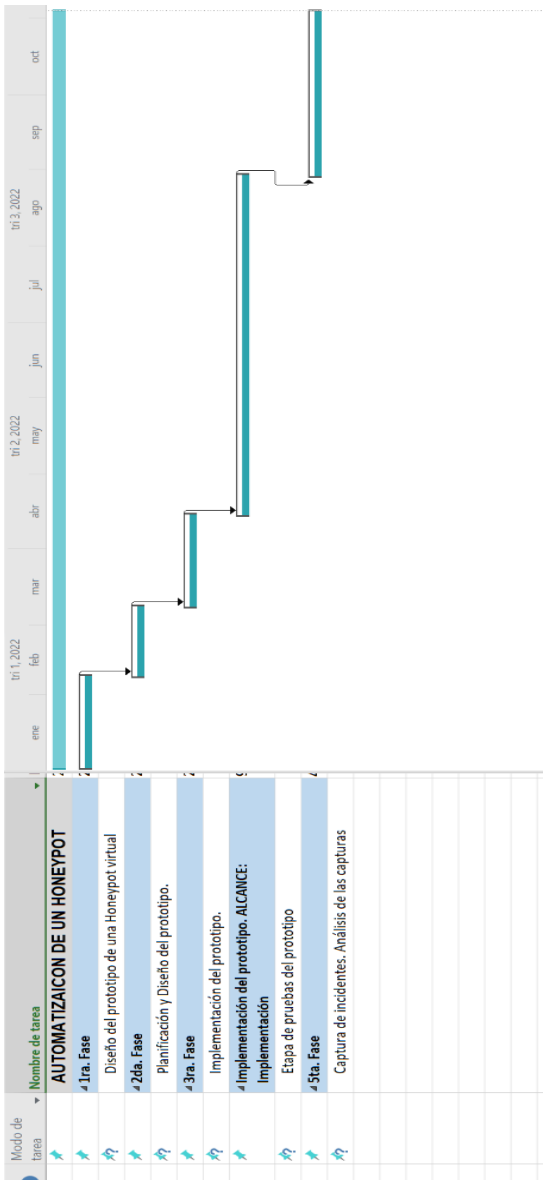
La estadística será la herramienta en la que nos basaremos para analizar la información obtenida cuando el proyecto ya se encuentre en funcionamiento, basado en los resultados, también podemos encontrar puntos y mejora y optimización del proyecto.

Dentro del *honeypot* serán desplegados varios servicios, cada uno de estos nos proporcionara datos útiles que posteriormente serán analizados para comprobar su veracidad y se buscara la mejor forma de publicarlos para que sean fácilmente entendibles por cualquier persona que se dedique a las tecnologías de la información.

Herramientas básicas de la estadística descriptiva como la frecuencia, promedios, medias, desviación serán las utilizadas para el análisis de datos obtenidos, gracias a esto obtendremos datos como plataformas que más reciben ciber ataques diariamente, desde que países se producen estos, IPs de origen de estos, vulnerabilidades más explotadas, entre otros.

11. CRONOGRAMA

Figura 2. **Cronograma de actividades**



Fuente: elaboración propia, utilizando Microsoft Project 2019.

12. FACTIBILIDAD DEL ESTUDIO

En esta parte definiremos el orden cronológico en los que serán desarrolladas todas etapas de esta investigación. Se tiene contemplado un total de 36 semanas para el diseño, implementación y finalización del proyecto.

En la primera fase se pretende recopila información y diseñar el proyecto. En esta definiremos los componentes físicos y virtuales necesarios para el buen funcionamiento del servidor honeypot.

En la segunda etapa se hará la implementación del honeypot. En esta etapa se mostrará las técnicas utilizadas para la automatización, configuraciones y recursos utilizados. Cuando se haya finalizado la implantación se correrán una serie de pruebas para garantizar el buen funcionamiento de todas las herramientas y evitar errores en el futuro que pueda causar atrasos en la finalización del proyecto.

En la tercera etapa se recolectarán los datos de los ciberataques observados y estos serán analizados. Esta etapa será perpetua, es decir, constantemente se estará recibiendo datos y al mismo tiempo serán analizados para su posterior publicación y difusión.

La cuarta y última etapa corresponde a la publicación de la información. Cabe destacar que las dos últimas etapas será ejecutada una y otra vez hasta la finalización del proyecto.

REFERENCIAS

1. Amazon. (octubre, 2021). AWS CloudFormation. [Mensaje en un blog]. Recuperado de https://aws.amazon.com/cloudformation/.

2. Arenas, P. A. (2018). *Redes inalámbricas*. Perú: Monografía.

3. Baca, B. (octubre, 2017). *Community Networks in Latin American, Challenges, Regulations and Solutions. America Latina: Redes por la Diversidad, Equidad y Sustentabilidad A.C*. Uruguay: Internet Society.

4. Chef-Io. (1 de octubre, 2021). *Chef Infra*. [Mensaje de un blog]. Recuperado de https://www.chef.io/products/chef-infra.

5. Cheswick, B. (marzo, 1992). An Evening with Berferd in which a cracker is Lured, Endured, and Studied. *En B. Cheswick, An Evening with Berferd in which a cracker is Lured, Endured, and Studied*, 2(1), 163–174).

6. Ciberseguridad. (3 de octubre, 2021). Guatemala experimenta un crecimiento en ciberataques en 2020. [Mensaje en un blog]. Recuperado de https://revistamyt.com/guatemala-experimenta-un-crecimiento-en-ciberataques-en-2020/.

7. CISCO, N. A. (2 de mayo, 2014). *C. N. Academy, Editor*. [Mensaje de un blog]. Recuperado de https://www.cisco.com/.

8. Comer, D. (1996). *Redes globales de información con Iternet y TCP/IP: principios básicos, protocolos y Arquitectura*. Mexico: Prentice-Hall Hispanoamerica.

9. Creative Commons Attribution. (2013). *Redes Inalámbricas en los Países en Desarrollo*. Dinamarca: WNDW.

10. Dulong, M.; y Tréguer, F. (2019). *Telecommunications Reclaimed*. USA: CNRS, Union Europea.

11. Git. (1 de octubre, 2021). *Git.* [Mensaje de un blog]. Recuperado de https://git-scm.com/about.

12. Google. (1 de octubre, 2021). *Cloud Deployment Manager*. [Mensaje de un blog]. Recuperado de https://cloud.google.com/deployment-manager/docs.

13. Hernández, R. (1998). *Metodología de la Investigación*. México: McGraw-Hill.

14. Hubert, Z. (abril, 1980). OSI Reference Model – The ISO Model of Arquitecture for Open Systems Interconnection. *EEE Transactions on Communications,* 28(4), 425-432. Recuperado de https://web.archive.org/web/20050309080952/http://www.comsoc.org/livepubs/50_journals/pdf/RightsManagement_eid=136833.pdf.

15. IRM. (2 de octubre, 2021). Institute of Risk Management. [Mensaje en un blog]. Recuperado de https://www.theirm.org/media/4709/arms_2002_irm.pdf.

16. Kaspersky. (3 de octubre, 2021). *What is a honeypot?* [Mensaje en un blog]. Recuperado de https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot.

17. Mercurial. (1 de octubre, 2021). *Mercurial*. [Mensaje en un blog]. Recuperado de https://www.mercurial-scm.org/.

18. Microwave-link. (2 de mayo, 2018). *Microwave Link*. [Mensaje en un blog]. Recuperado de https://www.microwave-link.com/.

19. Monotone. (1 de octubre, 2021). *Monotone*. [Mensaje en un blog]. Recuperado de https://www.monotone.ca/.

20. Morris, K. (2016). *Infrastructure as Code: Managing Servers in the Cloud*. Estados Unidos: O'Reilly Media.

21. NIST. (2 de octubre, 2021). *Nist terms*. [Mensaje en un blog]. Recuperado de https://csrc.nist.gov/glossary/term/threat.

22. NongNu. (1 de octubre de 2021). *CVS - Concurrent Version System*. [Mensaje en un blog]. Recuperado de https://www.nongnu.org/cvs/.

23. QuestionPro. (04 de octubre, 2021). *¿Qué es la investigación experimental?* [Mensaje en un blog]. Recuperado de https://www.questionpro.com/blog/es/investigacion-experimental/.

24. Red Hat. (1 de octubre, 2021). *Ansible Automation Platform*. [Mensaje en un blog]. Recuperado de https://www.redhat.com/en/technologies/management/ansible.

25. Seifert, C. (2006). *Taxonomy of Honeypots*. (Tesis de licenciatura). Universidad Politécnica de Madrid, España.

26. Spitzner, L. (2002). *Honeypots: Tracking Hackers*. Estados Unidos: Addison Wesley.

27. Stoll, C. (agosto 1988). Stalking the Wily Hacker. *Unix & Bell Laboratories*, *31*(5), 1-17.

28. Subversion. (1 de octubre, 2021). *Subversion*. [Mensaje en un blog]. Recuperado de https://subversion.apache.org/.

29. Terraform. (1 de octubre, 2021). Terraform. [Mensaje de un blog]. Recuperado de https://www.terraform.io/.

30. Vega Malagón, G. Á.-M.-M.-C.-S.-A. (2021). *En Paradigmas en la investigación. Enfoque cuantitativo y cualitativo*. España: European Scientific Journal.

31. Wikipedia. (5 de septiembre, 2021). *Modelo TCP/IP*. [Mensaje en un blog]. Recuperado de https://es.wikipedia.org/wiki/Modelo_TCP/IP.