UNIVERSIDAD JOSÉ ANTONIO PÁEZ

SISTEMA DE DETECCIÓN DE INTRUSO EN UNA RED LOCAL

Autor:
Julio Trigo
C.I. 27.432.292

Urb. Yuma II, calle Nº 3. Municipio San Diego
Teléfono: (0241) 8714240 (master) – Fax: (0241) 8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERIA
ESCUELA DE COMPUTACIÓN

SISTEMA DE DETECCIÓN DE INTRUSO EN UNA RED LOCAL

Proyecto del Trabajo de Grado para optar por el título de

INGENIERO EN COMPUTACIÓN

Autor:
Julio Trigo
C.I. 27.432.292
Tutora:
Dra. Milbet Rodríguez

San Diego, Noviembre 2021

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

ACTA DE APROBACIÓN

INFORME FINAL DE PASANTÍA ☐

TRABAJO DE GRADO ☒

El jurado designado por la Facultad de Ingeniería para la evaluación del **Informe Final de Pasantía o Trabajo de Grado** titulado: Sistema de Detección de Intruso en una Red Local.

Realizado por el (la) Br. Julio Trigo

C.I. Nº 27.432.292 cursante de la carrera de Computación

hace constar después de analizar su contenido y oída la exposición oral, considera que el Informe Final o Trabajo de Grado ha obtenido la calificación de:

APROBADO ☒ **NO APROBADO** ☐

El Jurado

Tutor Académico (Coordinador)
Nombre: Milbet Rodríguez
C.I.: 7.996.228

Jurado
Nombre: José Saavedra
C.I.: 15.217.919

Jurado
Nombre: José Pravda
C.I.: 10.916.149

Fecha: 03/06/2022

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
DECANATO DE INGENIERÍA

FI C 002 2022-1CR TG

Valencia, 27 de abril de 2022

Ciudadano:
TRIGO MEDINA, JULIO DAVID
27.432.292

Presente -

Cumplo con informarle que la comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **Nº 1-2022** de fecha **14/02/2022** aprobó el proyecto de grado titulado:

Sistema de detección de intruso de una red local

Presentado por usted como requisito para optar al título de Ingeniero en Computación.

Se ratifica la designación del Tutor Académico que lo asesorará en el desarrollo de este proyecto a: Lcda. Milbet Del Carmen Rodríguez Alcalá, titular de la cédula de identidad V- 7.996.228

Atentamente

Dr. Francisco Gelanzé Sevilla.
Decano de Ingeniería

c.c. Coordinación de Pasantías y Trabajo de Grado

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN COMPUTACIÓN

CONSTANCIA DE APROBACIÓN PARA LA PRESENTACIÓN DEL TRABAJO DE GRADO.

Quien suscribe, **Dra. Milbet Rodríguez** Portador del número de cédula de identidad **V-7.996.228**, en mi carácter de tutor del trabajo de grado presentado por los ciudadanos **Julio David Trigo Medina** titular de la cédula de identidad **V-27432292**, titulado **SISTEMA DE DETECCIÓN DE INTRUSOS DENTRO DE UNA RED LOCAL,** presentado como requisito parcial para optar por el título de ingenieros en computación, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a presentación pública y evaluación por parte del jurado examinador que designe.

En San Diego, a los nueve días del mes de mayo del año 2022

Dra. Milbet Rodríguez

V-7.996.228

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

ACTA DE APROBACIÓN

INFORME FINAL DE PASANTÍA ☐

TRABAJO DE GRADO ☒

El jurado designado por la Facultad de Ingeniería para la evaluación del **Informe Final de Pasantía o Trabajo de Grado** titulado: Sistema de Detección de Intruso en una Red Local.

Realizado por el (la) Br. Julio Triso

C.I. N° 27.432.292 cursante de la carrera de Computación

hace constar después de analizar su contenido y oída la exposición oral, considera que el Informe Final o Trabajo de Grado ha obtenido la calificación de:

APROBADO ☒ **NO APROBADO** ☐

El Jurado

Tutor Académico (Coordinador)
Nombre: Wilbet Rodríguez
C.I.: 7.976.228

Jurado
Nombre: José Saavedra
C.I.: 15.217.419

Jurado
Nombre: José Saavedra
C.I.:

Fecha: 03/06/2022

ÍNDICE GENERAL

Contenido

LISTA DE FIGURAS

FIGURA **Pág.**

LISTA DE TABLAS

TABLAS **Pág.**

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA EN COMPUTACIÓN

SISTEMA DE DETECCIÓN DE INTRUSOS EN UNA RED LOCAL

Autores: Trigo Medina, Julio Trigo
Tutor: Dra. Milbet Rodríguez.
Fecha: Noviembre, 2021.

RESUMEN INFORMATIVO

En la presente investigación se planteó la elaboración de un Sistema de detección de intrusos para una red local con capacidades de avisos o llamados de atención cuando ingrese algún intruso, respondiendo a la necesidad de seguridad dentro de una pequeña empresa ante los ataques informáticos. Para el logro de los objetivos planteados se hizo uso de la metodología XP. Dicho sistema se desarrolló con el lenguaje de programación Java, y se puso a prueba con el sistema operativo Kali Linux. El estudio llevado a cabo obedece a una investigación de tipo proyecto especial, descriptivo, documental y de campo. Se encuentra inmerso en la línea de investigación de Gestión de proyecto de tecnologías de información y comunicación. Es un sistema que pueda ayudar a las empresas a tener respuestas eficientes contra algún intruso además de ser capaz de dar consejos capaces de proveer una mayor seguridad y concientización. Como recomendaciones para la mejora de este programa se puede mejorar mucho el apartado grafico haciéndolo mucho más agradable y bonito de ver además de agregar elementos que permitan a los usuarios tener una mejor compresión de los elementos en pantalla

Descriptores: Ciberseguridad, Sistema, Detección de Intruso.

INTRODUCCIÓN

En la actualidad las empresas se encuentran en constante peligro debido al gran avance tecnológico que recibimos diariamente, ya que tal magnitud de posibilidades no solo ayudan al bien, sino que también abren puertas a muchos ataques y al ser estos a través de computadora nunca se puede estar seguro de cuándo sucederá.

La sociedad actual no es realmente consiente de dicha problemática lo que causa que la gran mayoría de empleados dentro de una empresa no sepa a ciencia exacta la verdadera magnitud de dicho problema provocando así no tener el suficiente cuidado necesario .Con este proyecto se quiere encontrar la manera de reducir el impacto que causa dichos ataques mientras al mismo tiempo intenta mantener informado a las personas del como sucede esto.

El propósito general de la investigación es elaborar un sistema de detección de intrusos eficiente que al mismo tiempo que este se encarga de mantener vigilado la presencia dentro de una red local, te provea de una serie de consejos específicos sobre los ataques más recientes desde su instalación.

Para la investigación se realizara una serie de pruebas dentro de una red local para buscar la mayor comodidad del uso de dicho sistema, una velocidad de respuesta útil y espacio de consejos el cual no estorbe al usuario.

El sistema estará conformado por una serie de base de datos los cuales tendrán todos los tipos de ataques conocidos hasta la fecha con una lista de consejos para disminuir la posibilidad de sufrir dicho ataque, un sistema jerárquico que permita a cierto tipo de usuarios tener una mayor manipulación de dicho sistema y así evitar alarmas y un requerimiento bastante bajo buscando el menor consumo del equipo posible.

El estudio es un trabajo de campo basado en un proyecto factible, de carácter descriptivo. La investigación consta de cuatro (04) capítulos, cuyos contenidos se presentan a continuación:

Capítulo I: El problema, formulación del problema, objetivos de la investigación, general y específicos, justificación y alcance.

Capítulo II: Comprende los antecedentes de la investigación, las bases teóricas, las bases legales y la definición de términos básicos.

Capítulo III: Es el marco metodológico, el cual está formado por; el tipo de investigación, diseño de investigación, nivel de investigación, población y muestra, técnicas e instrumentos de recolección de datos, fases del estudio y análisis de datos.

Capítulo IV: Define los resultados obtenido en cada una de las fases de la investigación y la culminación del desarrollo del proyecto

Capítulo V: Corresponde a la conclusión final después del trabajo de investigación y recomendaciones para la mejora del mismo

CAPÍTULO I

EL PROBLEMA

1.1 Planteamiento del problema

La implementación de un sistema de detención de intrusos es una extensión de la seguridad para una organización y que a su vez consiste en detectar actividades inapropiadas o incorrectas desde el exterior e interior de un sistema informático.

Con el pasar de los años la tecnología ha avanzado a pasos agigantados donde un día se utilizó un simple computador para entrar a internet y buscar información, hemos avanzado a máquinas capaces de poder tumbar todo un imperio y por muy fantasioso que sea esto, es la realidad, en la actualidad una sola persona es capaz de entrar en las computadoras de las corporaciones más prestigiosas y con un par de click poder exponer los secretos o informaciones más personales de dicha empresa y no solo exhibir todas las técnicas que poseía sino que también dañar el prestigio de dicha empresa.

A medida que las comunicaciones se globalizan, el acrecentamiento en la utilización de redes, ya sean estas Intranet o Internet, los dinámicos informáticos se ven cada vez más propensos a ataques de agentes por medio de la red.

Es conocido que en todas las empresas siempre se ha hecho uso de redes locales, ya que estas cumplen con los propósitos dentro de una empresa que es el de poder de compartir información entre varias computadoras, pudiendo prescindir del internet o “Bluetooth” ya que esta permite la conexión entre varios equipos y poder entrar en los documentos de cada equipo que este dentro de una red.

Xavier García, ingeniero de Sistemas de Symantec Iberia, para el 2006, afirmó que la gran mayoría de las compañías demandan, sobre todo, soluciones antivirus y protección del correo electrónico, "aunque se están empezando a solicitar cada vez más soluciones de protección para mensajería instantánea". Asimismo, expone que los servicios de monitorización de seguridad también están teniendo mucha aceptación. "Se trata de sistemas que monitorizan todo lo que sucede en las redes y sistemas de sus clientes y en cuanto detectan una anomalía en el sistema envían una alerta para que se inicien los procesos de respuesta más adecuados". (Redes & Telecom).

Este arquetipo de amenaza se asienta en el uso de contenido malicioso o agentes que, una vez introducidos en el computador, son capaces de ejercer por sí mismos y trascender internamente sin requerir ningún tipo de conexión con el atacante original. El formato puede ser de virus, gusano, active web content o troyano. Por ello es meritorio aplicar la seguridad informática, es uno de los principales activos de una empresa, donde la información nunca estará libre de estar en peligro o riesgo. (Peluffo, 2014).

Esta problemática se presente en las grandes y pequeñas empresas (como cyber, tiendas, ferreterías, entre otros) apoyado en observaciones y conversaciones personales de algunos cyber, todo esto se presenta ya que no es algo controlable, más allá del error humano también está la malicia de personas que no tiene otro propósito más que el de dañar y desprestigiar compañías poderosas y reconocidas y todo desde un simple computador.

Con el fin de gestionar el riesgo asociado a la exhibición a estas amenazas, es inevitable establecer controles aptos que se enfoquen en la necesidad de responder la ciberseguridad, especialmente la integridad de la información que se distribuye por estas redes críticas. Por esta razón, este trabajo presentará un mecanismo de protección a través de un sistema de detección de intrusos dentro de una red local que conseguirá dar más protección a la información procesada en éstas.

1.2 Formulación del Problema

¿Cuenta cualquier pequeña empresa (Cyber, entre otros) de un Sistema de Detección de Intrusos en su red local que detecte la presencia de intrusos y ayude a disminuir las intrusiones internas y externas que comprometen la seguridad de la información?

1.3. Objetivos de la Investigación

1.3.1 Objetivo General

- Desarrollar un sistema de detección de intrusos dentro de una red local que informe a los usuarios la razón de la vulnerabilidad

1.3.2 Objetivos Específicos

- Diagnosticar la situación en relación a la detección de un intruso en una red local
- Identificar los requerimientos funcionales y no funcionales del programa, los cuales proyectaran las necesidades reales esperadas
- Diseñar la aplicación haciendo uso de la metodología de desarrollo de Programación Expresa XP.
- Realizar pruebas funcionales para verificar el correcto funcionamiento e identificar errores

1.4. Justificación de la Investigación

Las redes locales desde su creación ha sido de las mejores herramientas que existen en un área de trabajo en la cual almacenar y compartir información entre computadoras o equipos, pero a pesar de dichas ventajas no se puede dejar de lado el hecho de que existe una delincuencia virtual, donde las redes locales suelen ser uno de los principales objetivos, y no es para menos ya que dichas redes posee mucha información privada e importante. El propósito de dicha investigación es la creación de un sistema que permita alertar de un ataque a la red ya que con dicho programa tendrían la seguridad de tener un aviso que les permita reaccionar de manera más eficiente ante dichos ataques.

En la actualidad, observamos que las empresas tienen cada vez un mayor nivel de concienciación sobre la importancia de la Seguridad de la Información. Para amortiguar los peligros de integridad de la información es importante tener funcionalmente un sistema de prevención de intrusos (IPS) que vaya de la mano con el sistema de detección de intrusos (IDS), siendo el primero sustancial para identificar cualquier proceder sospechoso o extraño para que el IDS tome la acción de bloquear o alertar a su administrador sobre este comportamiento

El sistema se enfoca en ayudar a cualquier instalación que dependa del uso de una red local ya sean empresas, institutos, hospitales, bancos, cybers, entre otros. A poder detectar dichos ataques, ofreciendo una cultura empresarial con la ciberseguridad. Por ello, es necesario dar un mayor apoyo a las áreas técnicas en la toma de decisiones durante una situación de crisis.

1.5 Alcance

Para el desarrollo de este sistema se va buscar informar sobre diferentes tipos de sistemas e identificar qué cosas los hace especiales y diferentes del resto, además de poder investigar sistemas que hayan fallado y lograr identificar cuáles fueron sus razones, esto con el fin de resolver esas problemáticas con mi proyecto. También se investigará sistemas con funciones similares para poder tomar referencia de sus funciones de las funciones más resaltantes y los cuales sean mejor para poder realizar un sistema el cual sea capaz de ofrecer seguridad Se enfocará principalmente en pequeñas empresas y se desarrollará su capacidad de modo que trabaje de manera eficiente en un ambiente indefinido de equipos.

CAPÍTULO II

MARCO TEÓRICO

En esta etapa de la investigación se busca un sistema coordinado y coherente de conceptos y proposiciones que permiten abordar el problema en su contexto teórico a fin de situarlo dentro de un conjunto de conocimientos, orientado a la búsqueda y ofrezca una conceptualización adecuada de los términos que se utilizaran en el trabajo. En apoyo a estos argumentos, Sabino (2002) señala que:

> "El Marco Teórico, tiene un propósito: dar a la investigación un sistema coordinado y coherente de conceptos y proposiciones que permitan abordar el problema, es decir, se trata de integrar el problema dentro de un ámbito donde éste cobre sentido, incorporando los conocimientos previos referentes al mismo y ordenándolos de modo tal que resulten útiles en nuestra tarea (p. 47)."

2.1 Antecedentes

Los antecedentes de la investigación son indagaciones previas que sustentan el estudio sobre el mismo problema o se relacionan con otros, sirviendo de guía al investigador, teniendo ideas y comparaciones sobre cómo se trató el problema en esa oportunidad, teniendo un acertamiento a los temas que centran la atención de los investigadores del área y detectar la existencia de algunas líneas de investigación comunes.

En la búsqueda y recolección de información sobre investigaciones que hayan sido realizadas con anterioridad y relacionados con el tema de estudio, se ubicaron algunos que serán detalladas a continuación, que sirven de apoyo para el desarrollo de la investigación. Así mismo, Plata (2006), señala que los antecedentes de una

investigación:

> Se refieren a los estudios previos y tesis de grado relacionadas con el problema planteado, es decir, investigaciones realizadas anteriormente y que guardan alguna vinculación con el problema en estudio. En este punto se deben señalar, además de los autores y el año en que se realizaron los estudios, los objetivos y principales hallazgos de los mismos (p. 43).

Cedeño & Bermúdez (2021), en su trabajo titulado: **"metodología para la investigación forense en dispositivos móviles con sistema operativo android¨.** La presente se realizó en la universidad simón bolívar, con el cual va a optar al título de Ingeniero en Telecomunicación. El propósito de esta investigación fue enfocarse en el rastreo de teléfonos celulares Android para responder a posibles hackers los cuales ataquen desde este medio, los cuales tienen como objetivo proponer una metodología que permita investigar de manera apropiada los datos contenidos en dispositivos móviles equipados con sistema operativo Android. Esta se considera como una investigación experimental con investigación de campo. El aporte más significativo de este trabajo consistió en que ofrece una fundamentación teórica y metodológica sobre herramientas y formas de la investigación de datos dentro de la posibilidad de ciberataques desde un dispositivo móvil Android.

También esta Vargas Henry (2020) En su trabajo de grado titulado: **"defensa contra intrusos en redes de dispositivos iot usando técnicas de blockchain y machine learning"** este fue realizado en la Universidad de los Andes, para optar al título Magister en Seguridad de la Información. Proponen el uso de técnicas de Blockchain y Machine Learning como defensas anti intrusos en redes. Su objetivo es crear un mecanismo de protección integral para las redes de dispositivos IoT(Internet of Things), que permitiera identificar amenazas y activar mecanismos seguros de transferencia de información. Dicho proyecto se considera una investigación experimental. La aportación para importante para mi investigación es el sistema de mecanismo automatizado que utilizaran al momento de detección de cualquier ataque

para buscar utilizar dentro del sistema de consejos además de que el mismo sistema de detección también es una buena aportación.

Así mismo, Noguera Aaron. (2019) En su trabajo de grado titulado: ¨**implementación de un sistema de detección de intrusos para venezolana del vidrio c.a¨.** Este fue Realizado en la Universidad Central de Venezuela en Caracas, para optar al título Especialista en Telecomunicaciones Digitales. Proponen el diseño e implementación de un sistema de detección de intrusos en la empresa "Venezolana del vidrio C.A". Esta es considerada como una investigación tipo documental y de campo. El aporte de esta investigación al presente estudio, son los resultados obtenidos, entre ellos se tiene la información del de la seguridad implantada, proveedores, dispositivos, software, y acceso a la red empresarial.

Por otro lado Bernal y Dueñas (2019). En su trabajo de investigación **"implementación de un sistema de protección de intrusos en la vlan de servidores de la empresa sonda de Colombia s. a.".** Universidad piloto de Colombia especialización en seguridad informática Bogotá DC, para optar al título de especialización en seguridad informática. Propone la realización e implementación de un sistema de protección de intrusos dentro de una empresa en la cual se monitoreara el tráfico y se evitara fallas de seguridad conocidas en la red interna donde plantean el evitar dichos ataques con modificación de reglas.

Este trabajo posee una investigación de tipo documental y de campo. Su aporte a mi investigación es la metodología empleada en el proceso de realización de dicho sistema en donde buscan no solo crear dicho sistema funcional sino que también se harán prueba invitando a atacar para comprobar de qué manera sucede pudiendo aportar dichos resultados.

Por último, Álvarez C. César M. (2018) En su investigación: **la gerencia y el problema de la seguridad de la información en las organizaciones modernas.** Relacionado al "Caso Gandalf Comunicaciones C.A" en este trabajo se muestra la importancia de la seguridad informática dentro de una empresa haciendo uso de un caso real del cual se busca obtener respuestas las cuales permitan explicar de forma

más concisa los problemas que se suelen presentar en cada una de las empresas para ser más capaces de la identificación de amenazas potenciales teniendo en consideración la confiabilidad e integridad de la información. Se considera como una investigación de campo. El aporte de esta investigación al presente estudio son los problemas de seguridad presentados en la empresa investigada.

2.2 Bases Teóricas

Las bases teóricas son el punto importante de la investigación, mediante su elaboración se realiza un análisis de todos los puntos que afectan el estudio, es decir, los aspectos generales del tema, comprendiendo un conjunto de conceptos y proposiciones que constituyen un punto de vista o enfoque determinado, dirigido a explicar el fenómeno o problema planteado y a su vez sustentan la investigación con los aportes de distintos autores para una sustentación a nivel científico.

En toda investigación es necesario una fundamentación teórica o documental, es por ello que se llega a este punto de la estructura metodológica para darle credibilidad a dicho estudio, de allí pues que Tamayo y Tamayo, M (2004), describe las bases teóricas como "la parte de la investigación que amplía la descripción del problema, integrada la teoría con la investigación y sus relaciones mutuas ". (p.96).

Cuando se hace énfasis en un tema determinado es necesario tener una base que sustente dicho tema, los conceptos explican en detalle a lo que se refiere un investigador. Según Arias, F (2012), "Las bases teóricas implican un desarrollo amplio de los conceptos y proposiciones que conforman el punto de vista o enfoque adoptado, para sustentar o explicar el problema planteado" (p.107).

2.2.1 Java

Java es un lenguaje de programación y una plataforma informática que fue comercializada por primera vez en 1995 por Sun Microsystems. Hay muchas aplicaciones y sitios web que no funcionarán, probablemente, a menos que tengan Java instalado, y cada día se crean más. Java es rápido, seguro y fiable.

“El significado de java, tal y como se le conoce en la actualidad, es el lenguaje de programación y un entorno de ejecución de programas escritos en java. Al contrario de los compiladores tradicionales , que convierten el código fuente en instrucciones a nivel de máquina, el compilador java traduce el código fuente java en instrucciones que son interpretadas por la maquina virtual de java (JVM, Java Virtual Machine). A diferencia de C y C++ en los que está inspirado. Java es un lenguaje interpretado.

Aunque hoy en día java es por excelencia el lenguaje de programación para Internet y la World Wide Web en particular, java no comenzó como proyecto Internet y por las circunstancias es idóneo para las tareas de programación de propósito general y, de hecho muchas de las herramientas java están escritas en java.” (Cruz Francisco, 2018)

2.2.2 TCP/IP

TCP/IP define cuidadosamente cómo se mueve la información desde el remitente hasta el destinatario. En primer lugar, los programas de aplicación envían mensajes o corrientes de datos a uno de los protocolos de la capa de transporte de Internet, UDP (User Datagram Protocol) o TCP (Transmission Control Protocolo).

“TCP/IP es una denominación que permite identificar al grupo de protocolos de red que respaldan a Internet y que hacen posible la transferencia de datos entre redes de ordenadores. En concreto, puede decirse que TCP/IP hace referencia a los dos protocolos más trascendentes de este grupo: el conocido como Protocolo de Control de Transmisión (o TCP) y el llamado Protocolo de Internet (presentado con la sigla IP).” (Porto Julian y Merino María, 2008)

2.2.3 Ataques pasivos

Estos son los de escucha sin autorización o de monitoreo de tráfico. Los objetivos de estos ataques consisten en obtener la mayor cantidad de información del mensaje transmitido y del oponente.

“Los ataques pasivos están orientados exclusivamente a obtener información que puede ser suficiente en sí misma o ser empleada para posteriores ataques activos,

es por esto, que identificar un ataque pasivo puede poner en alerta al usuario respecto a uno activo" (Introducción a la seguridad informática y el análisis de vulnerabilidades, 2018)

2.2.5 Ataques activos

Los ataques activos involucran y comprometen los pilares básicos de las prácticas de seguridad: la confidencialidad, la integridad y la disponibilidad (CIA Confidentiality, Integrity and Availability).

"Dependen de quiénes los están realizando y pueden ser personas internas o externas dependiendo de lo que se quiere realizar, un ataque interno es realizado por una persona dentro de la organización que tiene el conocimiento para poder ingresar información confidencial quienes pueden desde dañar hasta robar información importante del sistema."(Alvear Francisco, 2019)

2.2.6 Phishing

Es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial. Aprenda cómo funciona para que pueda detectar y bloquear las estafas de phishing y mantener así sus datos a salvo de atacantes.

"el Smishing se caracteriza por tener dos clasificaciones o dos vectores de ataque. El primero es cuando el atacante envía un mensaje de texto SMS con información de una compra, cambios, rembolsos o cancelaciones. El usuario se alarma por esta transacción y se deja engañar, el mensaje incluye un número de teléfono del atacante. El teléfono Smart permite la llamada a este número, comunicándose con el atacante quien solicita información personal del usuario o códigos necesarios para un micro pago en línea. Esta forma de ataque se resume al robo de información mediante una conversación telefónica entre la víctima y el atacante. La segunda forma es a través del envió de un mensaje de texto SMS, este incluye una dirección URL que, al ser visitada por el usuario, un malware es instalado en su teléfono. Después replica toda la

información del usuario almacenada en el teléfono al servidor del atacante.” (Anna Kang, 2014)

2.2.7 Spyware

“Un Spyware es un software espía que trabajan con o sin conexión a Internet, estos se encargan de recopilar información del equipo infectado y enviarla hacia el atacante, la información que este puede recolectar es muy amplia, todo depende de la cantidad de información que cuente el equipo infectado, para lo más común que se utiliza los spyware es la obtención de las pulsaciones de teclado que el usuario pulsa cuando inicia sesión en sitios web, tiendas online y bancos, utilizando un Keylogger” (Bettany y Halsey)

2.2.8 Ransomware

“Es un tipo de malware que, una vez instalado en la computadora, despliega un mensaje de alguna agencia federal (como el FBI o la policía federal) señalando una violación a la ley, por lo que el equipo quedará bloqueado a menos que se pague una multa; o quizá muestra un pop-up indicando que los archivos se encriptarán permanentemente si no se paga algún rescate por ellos.” (Vélez Martínez, 2017)

2.2.9 Kali Linux

“Kali Linux es una distribución la cual contiene su propia colección de cientos de herramientas de software, especialmente hechas a medida para los usuarios; como profesionales en pruebas de penetración y otros profesionales de seguridad. También viene con un programa de instalación para completamente configurar Kali Linux como el sistema operativo principal en cualquier computadora.

Es muy parecido a todas las otras distribuciones Linux existentes, pero existen otras características las cuales diferencian a Kali Linux, muchas de las cuales se adaptan a necesidades específicas de los profesionales en pruebas de penetración. A continuación se exponen algunas de estas.” (Caballero Alonso, 2019)

2.2.10 Malware

"El malware en muchos casos se instala en nuestro ordenador sin nuestro conocimiento, generalmente a través de descargas o enlaces de carácter engañoso que simulan ser contenido en el que podríamos estar interesados. Una vez que el malware se ha instalado en el ordenador, las personas que tienen el control en muchas ocasiones pueden intentar acceder a nuestra información personal" (Universidad Jaén, 2018)

2.3 Bases Legales

La tecnología ha tenido y sigue teniendo un gran impacto en la sociedad, pues el fácil acceso a la información y el crecimiento de nuevas economías han marcado de manera radical el mundo tal cómo se conocía.

El uso de Internet y de dispositivos tecnológicos no sólo trajo beneficios para la sociedad moderna, sino que también ha desencadenado una ola de nuevos delitos de tipo informático. Es por ello que nace la necesidad de un marco legislativo y reglamentario que permita trabajar en el campo de las TIC bajo lineamientos jurídicos que regulen la vida en la sociedad digital.

Es por esto que los organismos reguladores nacionales e internacionales se han visto en la obligación de crear un conjunto de leyes, regulaciones y estandarizaciones que permitan que la justicia intervenga de alguna manera en las actividades informáticas.

Todo proceso de peritaje informático debe apegarse a regulaciones nacionales e internacionales. Es de suma importancia que cualquier proceso de peritaje tenga en vigor el marco legal y a pesar de que el perito no necesariamente sea un experto en el área legal, éste debe conocer y tener presente la legislación.

En Venezuela, para realizar un proceso de peritaje informático (recolección de datos, informes, dictámenes y análisis), es importante que éste se encuentre siempre apegado a la legislación venezolana.

Es indispensable tener en vigor el marco legal vigente y aunque el entendimiento de los textos legales para los inexpertos en el área pueda resultar complicado y

ambiguo, es necesario tenerlos presente y tratar de clasificarlos lo mejor posible.

A continuación, se citan los artículos relevantes de las regulaciones vigentes en Venezuela en materia de seguridad de la información.

2.3.1 Articulo 60 de la Constitución de la República Bolivariana de Venezuela

"Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación."

"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos." Con este artículo permite, la protección de información de la población destacando de esta manera, si alguien llega a extraer información sin consentimiento de una persona, dicha persona puede tomar acciones legales

2.3.2 Ley contra delitos informáticos del 2001 – Gaceta oficial No. 37.313

TÍTULO I - DISPOSICIONES GENERALES

Artículo 1 - Objeto de la Ley.

"La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley." El primer artículo de dicha ley aclara que se dara protección legal a todos los equipos y sistemas que recaben información de personas siempre que no sobrepase el limite de la información personal sin consentimiento, y se le aplicara sancion los mismos equipos y sistemas que hayan sobrepasado el mismo limite

TÍTULO II - DE LOS DELITOS

- Capítulo I - De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información.
- Artículo 7 - Sabotaje o daño a sistemas.

"Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de

información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias" En conexión con la ley anterior con respecto a la protección de los sistemas, entra en dicho contexto la alteración de los mismos buscando evitar los sabotajes internos

- Artículo 11 - Espionaje informático.

"Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas (300) a seiscientas (600) unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado." El artículo 11 revela que no solo la obtención de información privada es ilegal, si no que la divulgación de la misma tambien sera penada. Sumandole a esto tambien en caso de hacer dichos ataque por beneficio propio, el castigo aplicable sera mucho mayor al ya mencionado, y en caso de que la información perjudique al estado o alguna persona de carácter jurídico, sera aun mayor la condena

2.3.3 Ley de Infogobierno del 2013 – Gaceta oficial No. 40.274

Ley de Infogobierno publicada en conformidad con lo previsto en el artículo 213 de la Constitución de la República Bolivariana de Venezuela el 10 de octubre del 2013.

- Artículo 1 - Objeto de la ley

“Esta Ley tiene por objeto establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, para mejorar la gestión pública y los servicios que se prestan a las personas; impulsando la transparencia del sector público; la participación y el ejercicio pleno del derecho de soberanía; así como, promover el desarrollo de las tecnologías de información libres en el Estado; garantizar la independencia tecnológica; la apropiación social del conocimiento; así como la seguridad y defensa de la Nación.” El primer artículo se enfoca en que su objetivo como ley es la de ser lo más transparentes posibles con sus sistemas de seguridad enfocando que serán de uso exclusivo para la protección del publico

- Artículo 23 - Principio de seguridad

  “En las actuaciones electrónicas que realicen el Poder Público y el Poder Popular se debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, documentos y comunicaciones electrónicas, en cumplimiento a las normas y medidas que dicte el órgano con competencia en materia de seguridad de la información.” Con esta ley obliga a todos los sistemas no solo a garantizar la seguridad del pueblo, si no que al mismo tiempo obliga a que todo tipo de información recabada sea de disponibilidad publica, además de tener que ser 100% veridica

- Artículo 54 - De la Superintendencia de Servicios de Certificación Electrónica

  “La Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) es el órgano competente en materia de seguridad informática, y es responsable del desarrollo, implementación, ejecución y seguimiento al Sistema Nacional de Seguridad Informática, a fin de resguardar la autenticidad, integridad, inviolabilidad y confiabilidad de los datos, información y documentos electrónicos obtenidos y generados por el Poder Público y por el Poder Popular, así como la generación de contenidos en la red.” El artículo 54 garantiza de manera legal que el sistema de seguridad nacional será de carácter confiable y auténtica”

- Artículo 57 - Subsistemas que integran el Sistema Nacional de Protección y

Seguridad Informática.

"El Sistema Nacional de Protección y Seguridad Informática tiene como objeto proteger, resguardar, mitigar, y mejorar la capacidad de respuesta del Poder Público y del Poder Popular frente a riesgos y amenazas derivados del desarrollo de los sistemas de información." Esta ley explica y obliga al mismo sistema nacional de protección de seguridad informática a proteger la información del público y a mejorar su capacidad de respuesta ante las diferentes amenazas.

2.4 Definición de Términos

Ciberseguridad: Se puede definir como un revestimiento de protección para los archivos de información, a partir de ella, se realizan diferentes trabajos para evitar todo tipo de amenazas, las cuales ponen en riesgo que la información que es procesada, transportada y almacenada en cualquier dispositivo sea corrompida, o extraída. La ciberseguridad trata de trabajar en sistemas que sean capaces de actuar antes, durante y después de los incidentes, no sirve únicamente para prevenir, sino también para dar confianza a los clientes y al mercado, pudiendo asi reducir el riesgo de exposición del usuario y de los sistemas.

Firewall: Un firewall o cortafuegos son un dispositivo o sistema de seguridad de la red que controla el tráfico entrante y saliente y decide si permite o bloquea, además de cifrar o decodificar el tráfico especifico en función de un conjunto definido de reglas de seguridad.

- **Firewall de hardware:** Este cortafuegos, normalmente, se encuentra instalado en el router que se emplea para acceder a Internet o como un dispositivo físico extra dentro de nuestra topología, y por tanto, sirve para proteger a todos los ordenadores de una red
- **Firewall de software:** Se trata del firewall que viene con el sistema operativo del ordenador, y por tanto, en este caso tan solo protege un equipo y no todos ´ los que integran una red. Se ocupa de rastrear el tráfico para bloquear aquí el que no está autorizado. También existen firewalls por software más especializado en esta tarea que permiten analizar todo el tráfico de la red tal como pfSense.

IDS (Sistema de detección de Intrusos): Es un software que monitorea el tráfico de la red para detectar actividades ´ inusuales o sospechosas. La detección de actividad anómala e informar al administrador de la red es la función principal, sin embargo, algunas herramientas de IDS pueden actuar de acuerdo a las reglas configuradas cuando se detecta actividad maliciosa, por ejemplo, bloqueando cierto tráfico. "El Sistema de Detección de Intrusos (IDS) aporta a la red un grado de seguridad de tipo preventivo ante cualquier actividad sospechosa. El sistema IDS consigue este objetivo a través de alertas anticipadas dirigidas a los administradores de sistemas."

Detección de intrusión basada la red (NIDS): la mayor parte de los sistemas de detección de intrusos están basados en red. Estos IDSs detectan ataques capturando y analizando paquetes de la red. Escuchando en un segmento, un NIDS puede monitorear el tráfico que afecta a múltiples hosts que están conectados a ese segmento de red, protegiéndolos. Los IDSs basados en red a menudo están formados por un conjunto de sensores localizados en varios puntos de la red. Estos sensores monitorean el tráfico realizando análisis local e informando de los ataques que se producen a la consola de gestión. Como los sensores están limitados a ejecutar el software de detección, pueden ser más fácilmente asegurados ante ataques. Muchos de estos sensores son diseñados para correr en modo oculto, de tal forma que sea más difícil para un atacante determinar su presencia y localización.

Detección de intrusión basada en Host (HIDS): los HIDS fueron el primer tipo de IDSs desarrollados e implementados. Operan sobre la información recogida desde dentro de una computadora, como pueden ser ´ los archivos de auditoria del sistema operativo. Esto permite que el IDS analice las actividades que se producen con una gran precisión, determinando exactamente ´ que procesos y usuarios están involucrados en un ataque particular dentro del sistema operativo. A diferencia de los NIDSs, los HIDSs puede ver el resultado de un intento de ataque, al igual que pueden acceder directamente y monitorear los archivos de datos y procesos del sistema atacado.

Intrusión: Se puede definir como un incidente de seguridad en el que un intruso o usuario no autorizado obtiene, o intenta obtener, acceso a un sistema o recurso del sistema sin tener aprobación para hacerlo, también se puede especificar como "cualquier" acción que atente y comprometa la integridad, confidencialidad o disponibilidad de un recurso.

Servidor proxy: "Un servidor proxy es un sistema informático que se encuentra entre el cliente que solicita un documento web y el servidor de destino (otro sistema informático) que sirve el documento. En su forma más simple, un servidor proxy facilita la comunicación entre el cliente y el servidor de destino sin modificar peticiones o res puestas. Cuando iniciamos una solicitud de un recurso desde el servidor de destino, el servidor proxy secuestra nuestra conexión y se representa a sı mismo como un cliente para el servidor de destino, Solicitando el recurso en nuestro nombre. Si se recibe una respuesta, el servidor proxy nos la devuelve. Dando una sensación de que nos hemos comunicado con el servidor de destino

Software: Es un conjunto de instrucciones de programas de cómputo que incluye datos, procedimientos y rutinas que permiten realizar distintas tareas en un sistema informático. Teniendo esto en cuenta se puede decir que el software es "la parte inmaterial o lógica de un sistema informático. Son los datos y los programas necesarios para que la parte física de un ordenador hardware (Hw) funcione y produzca resultados

Industria 4.0: Al hablar de industria 4.0, es importante destacar que es un concepto que se ha venido desarrollando a partir de la constante evolución de las tecnologías de la información y de la capacidad de análisis de grandes bases de datos (Big Data, Data Science, Data Mining, etc.), y de la forma en que estás están impactando en la economía, incluida las formas de producción, generando nuevos desafíos para los países, las empresas, y los sistemas educativos.

Big Data: Se ha dicho que la analítica es un proceso relacionado con la exploración de datos con el fin de obtener nueva información que facilite la toma de decisiones.

CAPÍTULO III

MARCO METODOLÓGICO

Balestrini (2006) define el marco metodológico como: La instancia referida a los métodos, las diversas reglas, registros, técnicas y protocolos con los cuales una teoría y su método calculan las magnitudes de lo real. De allí que se deberán plantear el conjunto de operaciones técnicas que se incorporan en el despliegue de la investigación en el proceso de la obtención de los datos. El fin esencial del marco metodológico es el de situar en el lenguaje de investigación los métodos e instrumentos que se emplearan en el trabajo planteado, desde la ubicación acerca del tipo de estudio y el diseño de investigación, su universo o población, su muestra, los instrumentos y técnicas de recolección de datos, la medición, hasta la codificación, análisis y presentación de los datos. De esta manera se proporcionará al lector una información detallada sobre cómo se realizará la investigación. (pp. 114)

En el marco metodológico de la presente investigación, se especifica el procedimiento de cómo se solucionará el problema propuesto; de principio a fin. De esta forma se describe la metodología, el procedimiento y los tipos de muestras empleados para recaudar y disponer los datos indispensables para la culminación del trabajo de grado.

3.1. Tipo de Investigación

Desde el punto de vista del tipo de investigación, la misma se rige bajo los parámetros de un proyecto especial, debido a que el enfoque del proyecto está basado en una propuesta utilitaria con interés cultural y real.

Según la definición de Meverell Loker y Vosti (1993) precisan que “el concepto de proyecto especial está relacionado con la existencia de una unidad técnico-

administrativa llamada a cumplir funciones de desarrollo integral en un área determinada". En este caso la propuesta es el desarrollo de un sistema de detección de intrusos para una red local, respondiendo a la creación de un sistema real y cumpliendo con la utilidad que permita mantener informado a la empresa de cualquier intrusión.

3.2 Diseño de la Investigación

Este trabajo es catalogado como **un diseño de campo**, atendiendo a lo planteado por Fidias G. Arias (2012). "La investigación de campo es aquella que consiste en la recolección de todos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variables alguna, es decir, el investigador obtiene la información pero no altera las condiciones existentes".

Además, está enmarcado dentro de una investigación de tipo documental, aportando una profundización del conocimiento mediante el estudio de nuevas tecnologías y avances sobre problema en cuestión, con información parcialmente obtenida por trabajos de investigación anteriores, sucesos u actualizaciones en la actualidad y el marco normativo legal relacionado.

Con la finalidad de manejar la totalidad de los conceptos en esta etapa del marco metodológico La investigación documental según Arias (2012), "es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos" (p.27).

3.3 Nivel de Investigación

El presente trabajo se enmarca dentro de una metodología de investigación de tipo descriptivo, Arias (2012 p.24) afirma que "consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento".

Conociendo el nivel de investigación bajo el cual se rige este trabajo, es importante destacar este sistema explicara el porqué de cada una de las vulnerabilidades, con la finalidad de explicar y concientizar a los trabajadores sobre las amenazas que llegasen a vivir.

3.4 Población y Muestra

Población

Según Arias (2012) se entiende por población “Un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el problema y por los objetivos del estudio." (p. 81). El mismo autor agrega que la población finita es la “Agrupación en la que se conoce la cantidad de unidades que la integran.” (p. 82). Por lo que, la población estará conformada por los sistemas de redes ya sean locales o inalámbricos tomando en cuenta su tipo de funcionamiento.

Muestra

Arias (2012). La muestra es "aquella que por su tamaño y características similares a las del conjunto, permite hacer inferencias o generalizar los resultados al resto de la población con un margen de error conocido." (p 83). Con esta definición la causa relacionada con este trabajo será los sistemas de redes locales de dos (2) cyber, ubicados en Naguanagua – Paseo la granja

3.5 Técnicas e Instrumentos de Recolección de Datos

Según Tamayo y Tamayo (2012), “la recolección de los datos depende en gran parte del tipo de investigación y del problema planteado para la misma”. (p.98). Adicionalmente, debe distinguirse el concepto de técnicas de recolección de datos de los instrumentos de recolección de datos.

3.5.1 Técnicas de Recolección de Datos

Las técnicas de recolección de datos son definidas por Arias (2016 p.53) como las distintas formas o maneras de obtener información como se mencionó, el mismo

autor señala que los instrumentos son medios materiales que se emplean para recoger y almacenar datos.

Para lograr los objetivos de la investigación se debe elegir la técnica y el instrumento de recolección de datos. Conscientes de esto, para efecto de esta investigación, las técnicas de recolección de datos utilizadas serán: La Observación directa, Observación Participante y la Revisión documental.

3.5.1.1 Observación Participante

Según Kawulich (2005) "Es el proceso que faculta a los investigadores a aprender acerca de las actividades de las personas en estudio en el escenario natural a través de la observación y participando en sus actividades".

3.5.1.2 Revisión Documental

Según Hurtado (2008, p 427) La Revisión Documental Es una técnica en la cual se recurre a información escrita, ya sea bajo la toma de datos que pueden haber sido producto de mediciones hechas por otros o como texto que en sí mismo constituyen los eventos de estudio.

Para esta investigación se aplicó la técnica de revisión documental, consultando textos asociados a la información, con el fin de obtener una base de conocimiento.

3.5.1.3 Observación Directa

Según Heinemann (2003) Se tiene un contacto directo con los elementos o caracteres en los cuales se presenta el fenómeno que se pretende investigar, y los resultados obtenidos se consideran datos estadísticos originales.

3.5.2 Instrumentos de Recolección de Datos

Para Hurtado (2008, p.153), representa la herramienta con la cual se va a recoger, filtrar y codificar la información, es decir el con qué. Los instrumentos pueden estar ya elaborados e incluso normalizados.

3.5.2.1 Cuaderno de notas

Según Finol y Camacho (2006, p.77) es un documento similar al diario. En él se registran la información de los hechos, eventos o acontecimientos en el propio terreno; ayudarían a analizar la situación al momento de recoger material.

3.5.2.2 Encuestas

Según Naresh K. Malhotra (2004) "Las encuestas son entrevistas con un gran número de personas utilizando un cuestionario prediseñado, dicho cuestionario está diseñado para obtener información específica." El uso de este método es por la razón de que me permite informarme de forma directa todos los tipos de descuidos que suelen tomar los negocios que hacen uso de una red local, además de poder entender cuáles son las principales preocupaciones de las personas a las que busco como objetivo para el sistema

3.6 Técnicas de Análisis de Datos

Con respecto al procesamiento de los datos, los cuales son de gran importancia para la integración, pues le indica al investigador que hacer una vez que se haya copiado toda la información. Según Tamayo y Tamayo (2012) En otras palabras, las técnicas de análisis de datos son técnicas que se realizan después de que los investigadores recopilan, procesan y organizan los datos y luego interpretan los resultados obtenidos. En el orden de esta idea se utilizará la matriz FODA, acrónimo que hace referencia a las debilidades, oportunidades, fortalezas y amenazas de la investigación.

Según García (2009): "Es un instrumento metodológico que sirve para identificar acciones viables mediante el cruce de variables, en el supuesto de que las acciones estratégicas deben ser ante todo acciones posibles y que la factibilidad se debe encontrar en la realidad misma del sistema. Es decir, por ejemplo, la posibilidad de superar las debilidades que obstaculizan el logro de una meta solo se puede dar dejando que existan sus ventajas y oportunidades". Para la construcción de la matriz, debemos tratar de determinar la estructura organizacional, finanzas, políticas nacionales, lineamientos comerciales, factores ambientales, logística, mercadeo, inventarios,

investigación, relaciones comunitarias, sindicatos relevantes y otros aspectos relacionados. No se pueden crear oportunidades o problemas, y deben ser previstos con anticipación y preparados para ello.

3.7. Metodología seleccionada

La metodología elegida y utilizada para el desarrollo del sistema es la metodología XP. La programación Extrema XP surge como una metodología ágil para el desarrollo de cualquier software, que, en comparación con las metodologías tradicionales, reduce el costo de implementación del sistema en todas las etapas de su ciclo de vida al agregar funcionalidades y características que habilitan los requisitos necesarios. Esto hace que el usuario se convierta en el mismo miembro del equipo para promover la disciplina del cambio y el trabajo en equipo. XP, al ser una metodología de desarrollo ágil, se ocupa de las buenas prácticas de desarrollo de software que involucran a todo el grupo de trabajo, los procesos y el propio cliente, estos principios conllevan a las siguientes características:

a) **Planificación incremental:** Se basa en el análisis de las necesidades pasadas del cliente, de manera que a medida que avanza el desarrollo del sistema se negociará la parte funcional principal del sistema, esto incluirá la distribución de avances parciales, primero será entregado desde la parte inicial hasta llegar a la parte final de los ciclos que incluirán todas las funciones de la plataforma, pasando por la planificación, desarrollo, pruebas, entrega y evaluación del sistema.
b) **Diseño simple:** el diseño del sistema se basará únicamente en los requisitos actuales y no incluirá los requisitos de planificación futuros.
c) **Programación en pareja:** esta es una de las características fundamentales, ya que el trabajo en equipo conduce a la satisfacción del cliente, ya que se encuentran mejores soluciones de diseño y se proporciona un trabajo de mejor calidad.
d) **Propiedades colectivas:** la información, desarrollo y diseño del proyecto son conocidos por todo el grupo de trabajo, de manera que cada desarrollador conoce el código y estructura del proyecto para que todos puedan sugerir mejoras y optimización del sistema.

e) **Ritmo sustentable:** una de las características que se considera fundamental es que el equipo no trabaja más de 40 horas semanales, esto se debe a que se reducirá la calidad del código y por ende la calidad del sistema.
f) **Cliente presente:** En esta metodología, uno de los miembros del grupo de trabajo es el usuario o el cliente de tiempo completo, esto se debe a que a medida que avanza el desarrollo del sistema, el usuario da avisos y forma las condiciones requeridas para que el sistema funcionar con eficacia.

Durante el desarrollo del proyecto, surgirán problemas que provocarán cambios en el código y como resultado, surgirán nuevos requisitos que conducirán a cambios en los modelos y reglas de negocio. Por esta razón, hay algunos valores en esta metodología que abordarán aún más estos problemas eficazmente, y el grupo de trabajo debería estar constituido de la siguiente manera:

a) **Comunicación:** todos los tipos de cambios en el proyecto deben ser conocidos por todos los miembros del equipo.
b) **Simplicidad:** El desarrollo del sistema debe comenzar con la parte más simple y luego comenzar a cubrir todo el complejo a medida que aumenta la complejidad.
c) **Respuesta:** Para cada fase o ciclo del sistema, se deben realizar las pruebas funcionales correspondientes para conocer su confiabilidad y viabilidad.

3.8 Fases Metodológicas

Para alcanzar el objetivo principal de la investigación planteada, el cual es Elaborar el sistema de detección de intrusos para una red local, para su implementación en empresas, dirigida principalmente a la protección de la información y al explicación de las amenazas ocurridas dentro del uso de dicho sistema, se deben tomar en cuenta 3 aspectos importantes para llevar a cabo la metodología, que a su vez definen cada fase de la misma y serán descritas a continuación:

Fase I: Diagnosticar la situación en relación a la detección de un intruso en una red local

Se utilizará la observación participante por parte del investigador para diagnosticar y describir la situación actual en cuanto a la localización de los ataques en las computadoras en los cybers, en este se describe los procesos dependiendo de los ataques en el cual requiere trabajo humano para la presentación del trabajo, como también las necesidades del nuevo sistema. Por tal motivo, se puede manifestar que esta es la fase más importante de la metodología para el usuario.

Fase II: Identificar los requerimientos funcionales y no funcionales del programa, los cuales proyectaran las necesidades reales esperadas

Esta fase se estableció los requerimientos funcionales y no funcionales para red locales que automatiza la lectura de datos para que no cometa errores, basados en conjunto de algoritmos de aprendizaje automático que intenta prevenir y avisar las razones de los ataques.

Fase III: Diseñar la aplicación haciendo uso de la metodología de desarrollo de Programación Expresa XP

En esta fase se procede a la realización de pruebas unitarias para lograr tener una capacitación de lo que se quiere llegar. Esta fase es en donde se desarrolla la funcionalidad del sistema, como la elaboración y el proceso de codificación de las bases de datos a través de las fases de la Programación Expresa XP, usando herramientas computacionales.

Fase IV: Realizar pruebas funcionales para verificar el correcto funcionamiento e identificar errores

Por último, en esta fase, se realizarán las distintas pruebas al sistema para determinar el funcionamiento óptimo y planificando del mismo, evaluando la funcionalidad de los módulos tanto individualmente como en conjunto para detectar posibles fallas.

CAPÍTULO IV

RESULTADOS

En este capítulo se expondrán todos los resultados obtenidos en cada fase

4.1 Fase I: Diagnosticar la situación en relación a la detección de un intruso en una red local

En el desarrollo de esta fase, se investigó la preocupación de algunas empresas ante la posibilidad de la invasión de un intruso dentro de su red, para lo que se entrevistó personalmente a algunas personas encargadas donde se dividió entre empresas con red local al público y otras con red local más privadas.

Para esta pregunta no se tenían preguntas preconcebidas pero entre las preguntas hechas se puede hacer un total de 5 items dentro de las preguntas para generalizar la información obtenidas de estas

Tabla N°1 Preguntas

Items	Red local publica	Red local privada
1# ¿Cuánta importancia le das a tu red local?	Algunos si revisan su red, pero no tanto como deberían, siempre dejan	Todos le dan bastante más importancia debido a la información importante que hay en ella, alguna

	que sus programas borren todo lo descargado. Uno si lo revisa más a menudo pero es porque no usa esa herramienta	intenta hacer que sus empleados sean conscientes del peligro
2# ¿Tienes alguien que pruebe tu seguridad?	Ninguno tiene alguien que pruebe su seguridad	De las 3 empresas con red local privada 2 no tienen un personal en esa área debido al presupuesto pero la otra empresa que tiene más personal tiene un par encargados en esa área
3# ¿Alguna vez te han intentado hackear?	2 de las 3 empresas respondieron que no, pero la otra empresa que dijo que si, menciono que no estaba seguro, que creía que sí y tuvo que bloquear y reiniciar el equipo por si acaso	Las empresas que no tienen personal en ciberseguridad ambas mencionaron que afortunadamente no han pasado nada así, en cambio la 3ra empresa menciono que si experimentaron un ciberataque
4# ¿Alguna vez ha aparecido una maquina desconocida en tu red local?	1 empresa respondió que si hubo una vez que aparecido una pero se logró solucionar	Las 3 empresas respondieron que ninguna vez le había solucionado nada similar

	rápidamente, en otra respondió que una vez se estaba intentando pero se sacó a la persona que estaba haciendo eso y otra empresa respondió que nunca le paso algo similar	
5# ¿Usas herramientas/programas para cuidar tu red local?	Las 2 empresas usan distintas herramientas tanto para controlar la cantidad de máquinas como para eliminar cualquier archivo sospechoso, la otra empresa sí que no usa	2 Empresas si utilizan algunas herramientas distintas, una más que otra, y la 3ra empresa sí que no utiliza debido a que cree que no es necesario de momento

Fuente: Trigo (2022)

Con estos resultados pude darme cuenta que si hay cierto grado de conciencia a la posibilidad del hurto de la información, pero al mismo tiempo se podía observar que hay bastante dependencia de los programas y herramientas para la protección de la seguridad lo que no es del todo correcto debido a que siempre puede existir algunos tipos de script para burlar dicha seguridad.

Para lo siguiente se decidió hacer unas preguntas extras para las empresas de red local privada.

Tabla N°2 Preguntas

Items	Respuestas

#6 ¿Alguna vez ha sido vulnerado debido a un error de un empleado?	Las 2 empresas pequeñas respondieron que afortunadamente no han vivido una situación similar pero la empresa grande respondió que si paso una situación así
#7 ¿Ha tenido que explicar causas de hackeos por errores humanos?	Como la empresa grande fue la única que respondió que si a la pregunta anterior pues fue a la única que se le hizo esta pregunta a lo que sí tuvieron que explicar la causa debido al desconocimiento
#8 ¿Alguna vez algún empleado ha cometido más de 1 vez el mismo error?	Aquí volvemos al mismo caso que la pregunta anterior pero en este caso la empresa grande afortunadamente no ocurrió

Fuente: Trigo (2022)

4.2 Fase II: Identificar los requerimientos funcionales y no funcionales del programa, los cuales proyectaran las necesidades reales esperadas

4.2.1 Requerimientos Funcionales:

- Cuidado y vigilancia de la red local
- Adoctrinamiento para disminución de errores humanos
- Funcionamiento en segundo plano
- Eficiencia en el reconocimiento de la vulnerabilidad
- Eficiencia en el aviso del intruso

4.2.2 Requerimientos No Funcionales:

- Uso de herramientas externas para su cuidado
- Disposición de personal para el mantenimiento
- El programa se realizó en el lenguaje de Java

- Se usó lenguaje SQL para la creación de una base de datos para las ip de seguridad, y una librería para la detección de las vulnerabilidades y mensajes para los empleados
- Uso del sistema operativo Kali Linux para la prueba de las vulnerabilidades

4.3 Fase III: Diseño la aplicación haciendo uso de la metodología de desarrollo de Programación Expresa XP

Entonces, en base a los resultados obtenidos en la fase I, se procedió a realizar un estudio de las características del sistema para así realizar un diseño adaptado a los requerimientos determinados en la fase anterior, iniciando así con la descripción de los actores y consecuente, los diagramas de casos de uso, los diagramas de clases, el modelado de los datos y además dejando clara las principales funciones que el sistema debe cumplir.

Tabla N° 3: Descripción de los actores Usuario

Actor	Descripción
Maquinas	Este actor es el usuario básico del programa. Este usuario representa todas las maquinas conectadas a la red local.

Fuente: Trigo (2022)

Tabla N° 4: Descripción de los actores Administrador

Actor	Descripción
Servidor	El actor Administrador que en este caso es el servido, este tiene la tarea de comunicar y/o permitir la conexión entre las demás máquinas, conectar con la base de dato, gestionar la base de

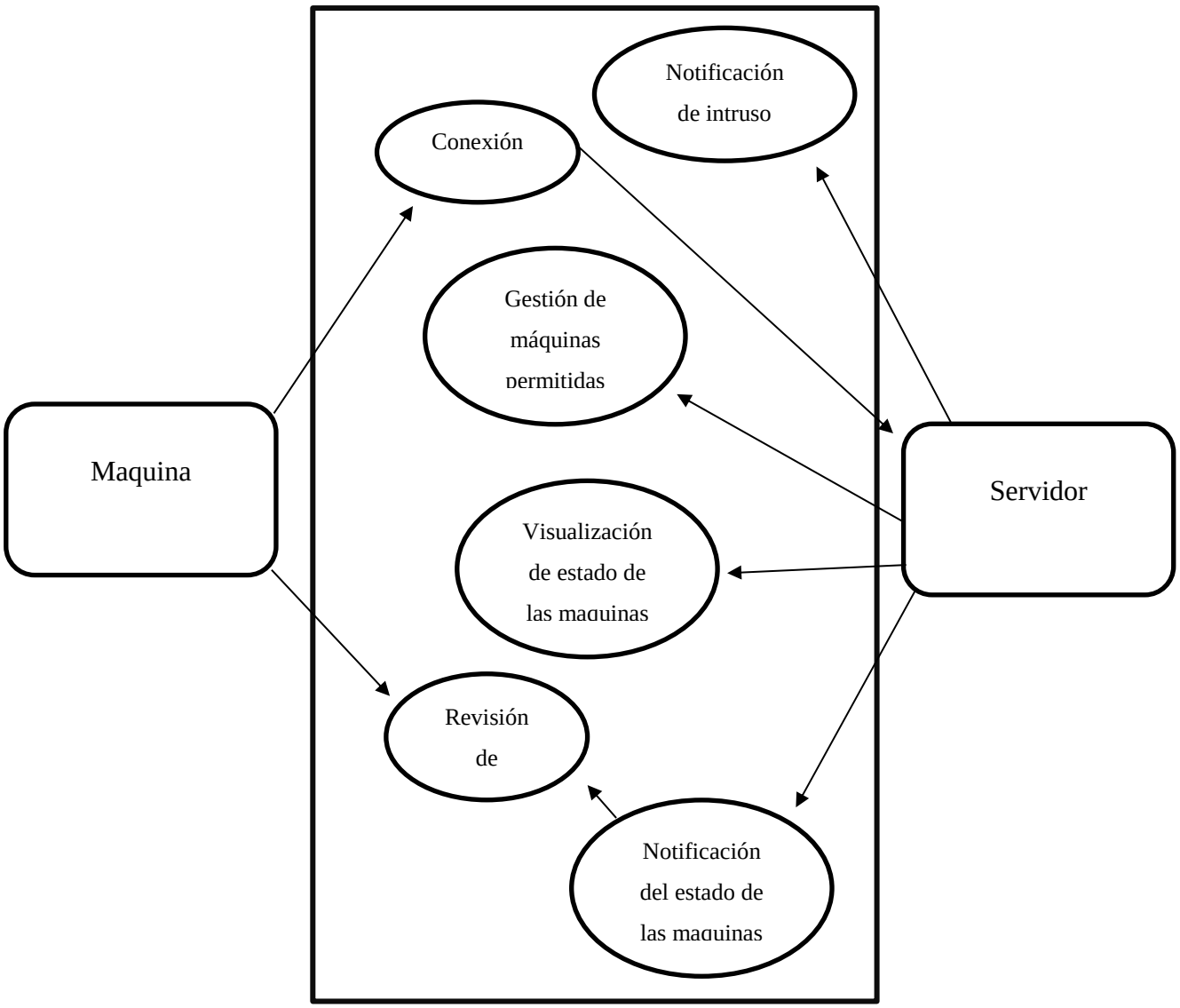
	datos, y comunicarse con las demás máquinas.

Fuente: Trigo (2022)

4.3.1 Casos de uso

Según Sommerville (2011), los casos de uso identifican las interacciones individuales entre el sistema y sus usuarios y otros sistemas. En su forma más sencilla, un caso de uno identifica a los actores implicados en una interacción y nombra el tipo de interacción. (p. 107) Entonces, los casos de uso tienen como función mostrar las diferentes acciones que tienen los actores dentro del sistema. Seguidamente se muestra algunos de los casos de uso

Figura N°1 Diagrama de casos de uso



Fuente: Trigo (2022)

Tabla N°5: Definición de caso de Conexión

Definición del caso de uso	
Nombre del caso de uso	Conexión
Actor principal	Maquina

Actor secundario	Servidor
Objetivo en contexto	La máquina en cuestión envía una señal con la ip hacia el servidor para a de una lista se verifique si se puede conectar o no
Precondiciones	Debe existir la ip en la lista de permisos, el puerto tiene que estar libre
Disparador	El programa tiene que abrirse
Condición de termino	La ip tiene que estar registrada
Condición de termino fallido	La ip no está registrada
Prioridad	Alta

Fuente: Trigo (2022)

4.3.2 Diagrama de clases

Los diagramas de clase nos permiten modelar las clases de un sistema en una visión estática en cual se mostrarán los atributos, operaciones y relaciones que ejecutan las mismas

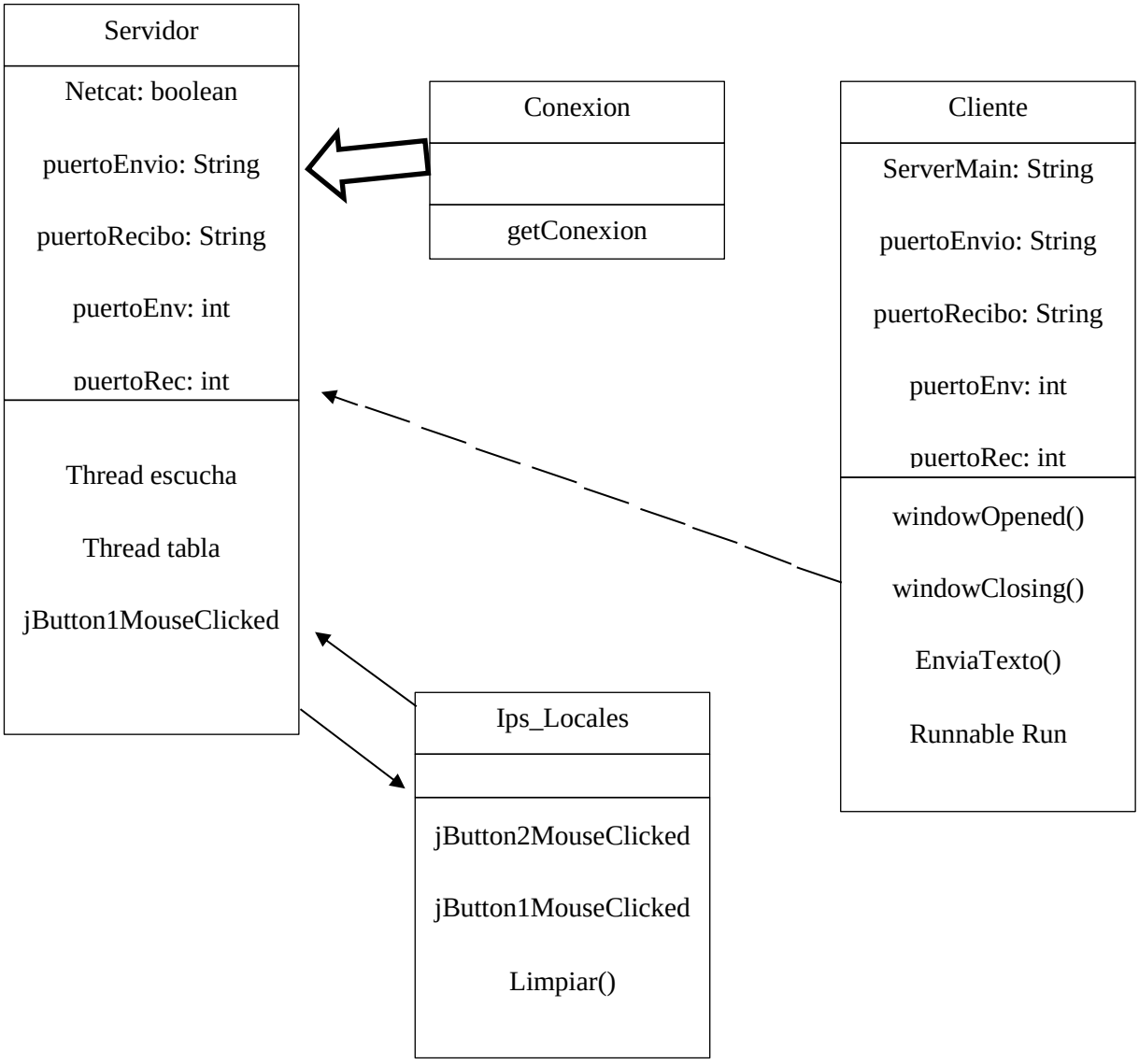


Figura N° 2: Diagrama de clases

Fuente: Trigo (2022)

4.3.3 Esquema de Base de Datos

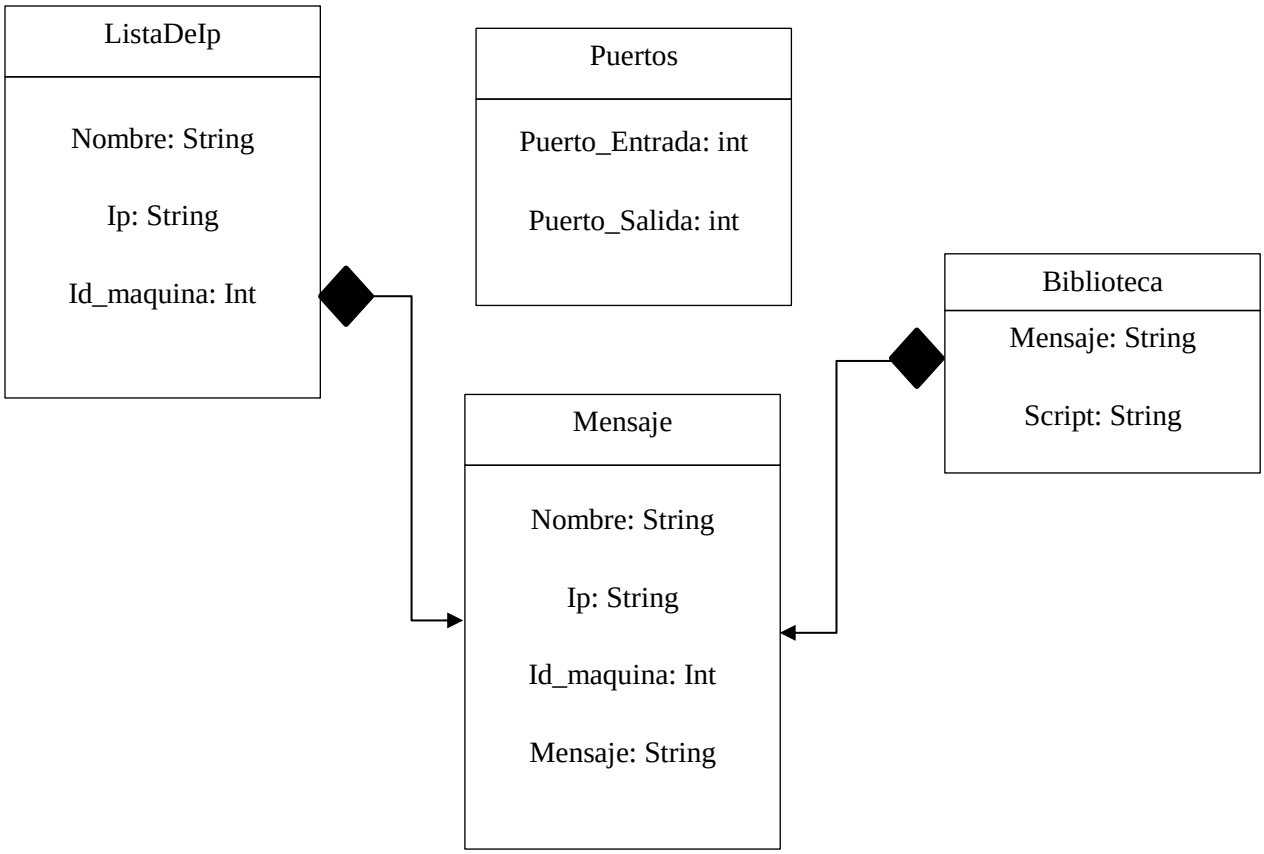


Figura N°3 Esquema de base de datos

Fuente: Trigo (2022)

4.3.4 Diseño

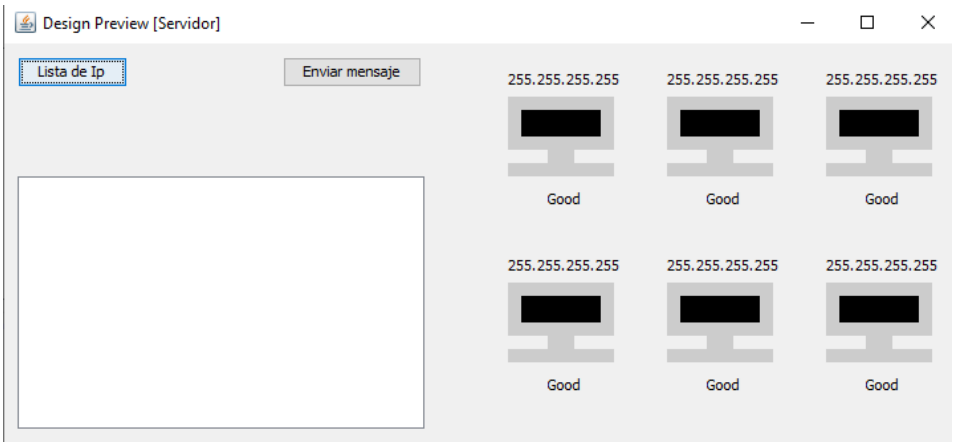


Figura N°4 Pantalla servidor

Fuente: Trigo (2022)

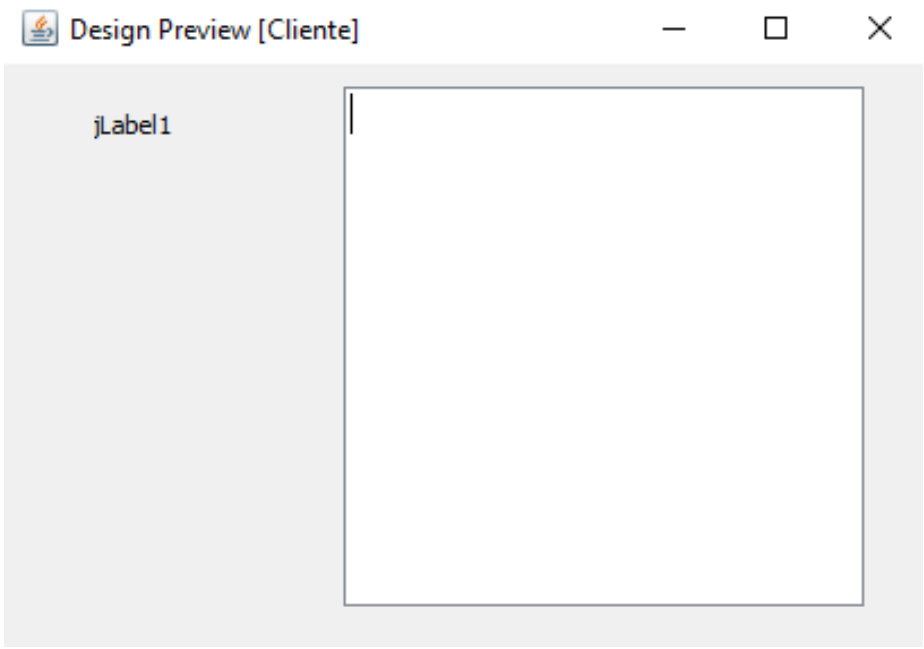


Figura N°5 Pantalla cliente

Fuente: Trigo (2022)

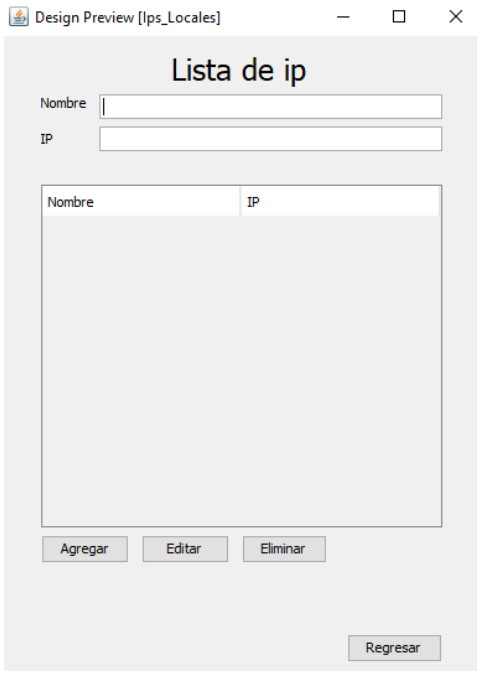


Figura N°6 Lista de las Ip (servidor)

Fuente: Trigo (2022)

4.4 Fase IV: Realización de pruebas funcionales para verificar el correcto funcionamiento e identificar errores

Esta es la última fase completada de la metodología XP en la misma se llevaron a cabo las pruebas correspondientes para garantizar la efectividad del sistema, estas pruebas se aplicaron a los diferentes módulos del sistema

Tabla N°6 Caso de prueba 1

Conexión entre cliente – servidor	
Numero 1	Nombre: Caja Negra
Descripción: Comprobar los parámetros de la conexión	
Condición de ejecución: Misma red	

Entrada: Puertos
Salida: Conexión
Evaluación de prueba: Conectan correctamente
Decisión: Permitir al usuario la selección del puerto para un correcto funcionamiento

Fuente: Trigo (2022)

Tabla N°7 Caso de prueba 2

Conexión con la base de datos	
Numero 2	Nombre: Caja Negra
Descripción: Comprobar que haya conexión con la base de datos	
Condición de ejecución: Clase exclusiva para la conexión	
Entrada: Comandos de solicitud	
Salida: Valores guardados en la tabla	
Evaluación de prueba: La conexión fue fallida	
Decisión: Detectar el problema con la certificación SSL	

Fuente: Trigo (2022)

Tabla N°8 Caso de prueba 3

Detección de inicio y cerrado de sesión de una maquina	
Numero 3	Nombre: Caja Negra
Descripción: Comprobar el envío de la señal al abrir y cerrar el programa "Cliente"	
Condición de ejecución: Haber concebido la conexión	
Entrada: Envío de la señal	
Salida: Respuesta del servidor	
Evaluación de prueba: La detección funciona exitosamente	
Decisión: Limitar la cantidad de máquinas hasta 6 temporalmente por diseño	

Fuente: Trigo (2022)

Tabla N°9 Caso de prueba 4

Detección de una maquina desconocida conectada	
Numero 4	Nombre: Caja Negra
Descripción: Establecer un parámetro que verifique la ip de la maquina conectando con una lista de ip de seguridad	
Condición de ejecución: Haber creado la lista de ip	
Entrada: Señal de una maquina	
Salida: Mensaje de alerta	
Evaluación de prueba: La detección funciona exitosamente	
Decisión: Se mostrara un mensaje en pantalla del intruso mas no se guardara dicho mensaje por cuestión de espacio	

Fuente: Trigo (2022)

Tabla N°10 Caso de prueba 5

Respuesta del servidor	
Numero 5	Nombre: Caja Blanca
Descripción: Comprobar que se pueda imprimir en pantalla mensajes provenientes del servidor	
Condición de ejecución: Haber abierto el programa	
Entrada: Mensaje de conexión al servidor	
Salida: Mensaje de “Conectado” proveniente del servidor	
Evaluación de prueba: El mensaje se imprime en pantalla exitosamente	
Decisión: Deshabilitar la capacidad del cliente de escribir encima del “jTextArea”	

Fuente: Trigo (2022)

Tabla N°11 Caso de prueba 6

Visualizar la conexión de un equipo	
Numero 6	Nombre: Caja Blanca
Descripción: Observar la conexión y desconexión de un equipo a la red	
Condición de ejecución: Tener abierto previamente el servidor	
Entrada: Conexión y Desconexión	
Salida: Cambio de color en el "dibujo" de la computadora del equipo correspondiente	
Evaluación de prueba: Cambia el color exitosamente	
Decisión: Se hará que aparezca cada "dibujo" cada vez que se agregue una maquina	

Fuente: Trigo (2022)

Tabla N°12 Caso de prueba 7

Modificación de la lista de seguridad	
Numero 7	Nombre: Caja Blanca
Descripción: Permitir al operador del servidor cambiar a gusto las maquinas permitidas en la red	
Condición de ejecución: Conectar con la base de datos	
Entrada: Nombre e Ip	
Salida: Lista de seguridad	
Evaluación de prueba: Funciona a medias, los comandos de seguridad funciona mas no se ha logrado conectar con la base de datos	
Decisión: Detectar el problema con la certificación SSL	

Fuente: Trigo (2022)

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Una vez concluido con toda la investigación, haber realizado el programa de detección con sus pruebas se ha llegado a las siguientes conclusiones:

- En el proceso de la creación del programa, se fue desarrollando mejores opciones a la hora de gestionar toda la configuración tanto de los puertos como la de la lista de seguridad de tal manera que se haga cómodo para los usuarios
- Se pudo comprender un poco mejor el pensamiento y los métodos de ataque más acertados dentro de este tipo de programas gracias a la arquitectura del mismo
- Gracias a las entrevistas se pudo tener una mejor visión de las necesidades de los operadores de dicho programa para una mejor manipulación
- En el desarrollo del programa se pudo conocer más a fondo la gran importancia que tienen las redes locales en un entorno y la gran versatilidad que estas ofrecen

5.2 Recomendaciones

A continuación, se ofrecerán las siguientes recomendaciones para que sean desarrolladas posteriormente, debido a que no se trató dentro de los objetivos iniciales de la investigación:

- Mejorar la interfaz de tal manera que esta sea más agradable visualmente para los usuarios
- Elaborar una sección de guías o consejos para los usuarios para una mejor comprensión del funcionamiento de la red
- Mejorar la distribución de los elementos en pantalla del servidor para ofrecer una mayor capacidad de computadoras conectadas

REFERENCIA

Alberto H. (2016). “Implementación De Un Sistema De Detección De Intrusos Para La Red Local De La Ferretería Corintios En Santa Marta”. [Documento Línea]. Disponible: https://repository.unad.edu.co/bitstream/handle/10596/17400/7604297.pdf?sequence=1&isAllowed=y

Alfaro, J.M. (s/a). “Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia”, Rediris.es, 2019. [Online]. Disponible: http://rediris.es/cert/doc/pdf/ids-uv.pdf.

Alvear Francisco (2019) ANÁLISIS Y DISEÑO DE UNA PROPUESTA PARA MITIGAR ATAQUES CIBERNÉTICOS A CORREOS ELECTRÓNICOS UTILIZANDO TÉCNICAS DE HACKING ÉTICO documento en línea disponible: https://dspace.ups.edu.ec/bitstream/123456789/17035/1/UPS-ST004012.pdf

Arias, F. (2012). El proyecto de investigación. Introducción a la metodología científica 6ta edición [Documento en Línea]. Disponible: https://www.researchgate.net/publication/301894369_EL_PROYECTO_DE_INVESTIGACION_6a_EDICION

Balestrini, M. (2005). Elaboración de un proyecto de grado. 6ta edición. [Documento en Línea]. Disponible: https://drive.google.com/file/d/0B1sTcIvKGVSyT1FFa0JYMXFEejg/view?resourcekey=0-q-4eI4j8N4MSEkr7B1O9Vg

Bernal C. y Dueñas J. (2019) “Implementación De Un Sistema De Prevención De Intrusos En La Vlan De Servidores De La Empresa Sonda De Colombia S.A.” [Documento en Línea]. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6265/00005169.pdf?sequence=1&isAllowed=y

Britos, J., Detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico. Tesis de Maestría en Redes de Datos. Buenos Aires.

Universidad Nacional de la Plata. 2010. 34 p. disponible en http://sedici.unlp.edu.ar/b.

Cedeño M. y Bermúdez S. (2021) Metodología Para La Investigación Forense En Dispositivos Móviles Con Sistema Operativo Android [Documento en Línea]. Disponible: http://mendillo.info/seguridad/tesis/Cedeno-Bermudez.pdf

Criminalística | Ciencias Forenses. (2021). Consultado el 14 de junio de 2020 en, http://criminalistica.mp.gob.ve/division-de-ciencias-forenses/

Documento institucional de Welivesecurity. Consultado el 20 de mayo de 2020. Disponible en, https://www.welivesecurity.com/la-es/2017/12/06/conveniobudapest-beneficios-implicaciones-seguridad-informatica/

Finol y Camacho (2006). El proceso de investigación científica 2da edición. p.77.

Heinemann (2003) Introducción a la Metodología de la Investigación Empírica: El Ejemplo de Las Ciencias Del Deporte [Documento en línea] Disponible: https://seminariodemetodologiadelainvestigacion.files.wordpress.com/2011/06/introduccion-a-la-metodologia-de-la-investigacion-empirica-en-las-ciencias-del-deporte.pdf

Hernández, S. (2006). Metodología de la investigación 4ta edición [Documento en Línea].Disponible:http://187.191.86.244/rceis/registro/Metodolog%C3%ADa%20de%20la%20Investigaci%C3%B3n%20SAMPIERI.pdf

Hurtado (2008). Revisión Documental [Documento en línea]. Disponible: http://virtual.urbe.edu/tesispub/0093381/cap03.pdf

IACC. (2021). *Habilidades para el aprendizaje en la modalidad online.* Desarrollo de Habilidades para el Aprendizaje. Semana 1

Internet Security Glossary, Network Working Group The Internet Society Std. RFC 2828, 2000.

Kawulich (2005) Observación Participante. [Documento en línea]. Disponible: https://www.buenastareas.com/ensayos/Observaci%C3%B3nParticipante/848775.html

Malhorta K. Naresh (2004) Investigación de mercados. Documento en línea disponible: http://www.elmayorportaldegerencia.com/Libros/Mercadeo/%5BPD%5D%20Libros%20-%20Investigacion%20de%20Mercados.pdf

Noguera, A. (2019) “Implementación de un sistema de detección de intrusos para venezolana del vidrio c.a”. [Documento en Línea]. Disponible: http://mendillo.info/seguridad/tesis/Noguera.pdf

Peluffo, I. &. (2014). Machine Learning aplicado en Sistemas de Deteccióon de Intrusos. 1-2.

Plata (2006) Investigaciones como estudios Previos. 2da Edición. México.

Robayo, E.L. (s/a). “Deteccion De Intrusos En Redes De Telecomunicaciones Ip Usando Modelos Ocultos De Markov.”, Bdigital.unal.edu.co, 2019. [Online]. Disponible: http://bdigital.unal.edu.co/2409/1/299726.2009.pdf. [Accedido: 30-Jul2019].

Sabino (2002) La investigación como sistema coordinado. Editorial Angelus. 4ta Edición. Caracas [Documento en Linea]. Disponible: http://paginas.ufm.edu/sabino/ingles/book/proceso_investigacion.pdf

Tamayo y Tamayo, M. (2004) El proceso de la Investigación Científica. 4ta Edición [Documento en Línea]. Disponible: https://www.academia.edu/17470765/EL_PROCESO_DE_INVESTIGACION_CIENTIFICA_MARIO_TAMAYO_Y_TAMAYO_1?auto=download

UPEL (2010) Manual de Trabajo de Grados de especialización y Maestría y Tesis Doctorales. Documento en línea. Disponible: http://tesisdeinvestig.blogspot.com/2011/07/proyectos-factibles-manual-upel.html