UNIVERSIDAD JOSÉ ANTONIO PÁEZ

DESARROLLO DE UNA PLATAFORMA DE SEGURIDAD ELECTRÓNICA BASADA EN UNA INTELIGENCIA ARTIFICIAL

Autores:
Cabrera Licón, Oswaldo Manuel

Duran Martínez, Alex Daniel

Urb. Yuma II, calle No. 3. Municipio San Diego
Teléfono: (0241) 8714240 (Máster) - Fax: (0241) 87123

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JÓSE ANTONIO PÁEZ

FACULTAD DE FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN

DESARROLLO DE UNA PLATAFORMA DE SEGURIDAD ELECTRÓNICA BASADA EN UNA INTELIGENCIA ARTIFICIAL

Autores:

Cabrera Licón, Oswaldo Manuel

Duran Martínez, Alex Daniel

Tutor:

Msc. Jetro López

San Diego, octubre del 2020

ANEXO D

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO
FACULTAD DE INGENIERÍA

PLANILLA SOLICITUD: ANÁLISIS Y APROBACIÓN DE TRABAJO DE GRADO

DATOS PERSONALES		
Apellidos: Cabrera Licón	Nombres: Oswaldo Manuel	C.I: V- 26.879.752
Dirección (Cabrera): Urb. Lomas del Este; Av. Rotaria, Edificio: Residencias Claudia.		Telf.: 0414-4251202
DATOS ACADÉMICOS		
Escuela: Ingeniería en Computación	Índice Académico: 14,64	
DATOS DEL PROYECTO DE TRABAJO DE GRADO		
Autores Nombre: Oswaldo Manuel Cabrera Licón. Teléfono: 0414-4251202 Nombre: Alex Daniel Duran Martínez. Teléfono: 0414-8012222		
Título del Trabajo Plataforma de seguridad electrónica basada en una inteligencia artificial		
Breve Explicación: Plataforma electrónica que permite la encriptación de todo y cada uno de los datos que manejan los usuarios utilizando una inteligencia artificial para la encriptación de la misma, a su vez esta será de carácter escalable de manera que sea utilizable tanto como por industria como por personas naturales y permitirá enviar y recibir información de manera segura y eficiente, todo con el objetivo de la innovación en el área de la ciberseguridad		
Lugar donde se desarrollará el Proyecto: Por definir		
Tiempo de Desarrollo: 32 semanas		
Tutor Académico propuesto: Jetro López Tutor metodológico: Alicia de Pizzella 0424 4155612 correo: alipiz54@gmail.com		

APROBADO _____X_____ NO APROBADO _____

COMITÉ DE EVALUACIÓN

COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

Prof. Ana Avendaño	ACAP	13-05-2020
Nombre	Firma	Fecha

DIRECCIÓN DE ESCUELA

BELKYS ARAUJO	BELKYS ARAUJO	05-05-2020

Nombre Firma Fecha

ANEXO D

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO
FACULTAD DE INGENIERÍA

PLANILLA SOLICITUD: ANÁLISIS Y APROBACIÓN DE TRABAJO DE GRADO

DATOS PERSONALES		
Apellidos: Duran Martínez	Nombres: Alex Duran	C.I: V- 28.429.539
Dirección (Duran): San Diego sector la Esmeralda.		Telf.: 0414-8012222
DATOS ACADÉMICOS		
Escuela: Ingeniería en Computación	Índice Académico 13,64	
DATOS DEL PROYECTO DE TRABAJO DE GRADO		
Autores Nombre: Oswaldo Manuel Cabrera Licón. Teléfono: 0414-4251202 Nombre: Alex Daniel Duran Martínez. Teléfono: 0414-8012222		
Título del Trabajo Plataforma de seguridad electrónica basada en una inteligencia artificial		
Breve Explicación: Plataforma electrónica que permite la encriptación de todo y cada uno de los datos que manejan los usuarios utilizando una inteligencia artificial para la encriptación de la misma, a su vez esta será de carácter escalable de manera que sea utilizable tanto como por industria como por personas naturales y permitirá enviar y recibir información de manera segura y eficiente, todo con el objetivo de la innovación en el área de la ciberseguridad		
Lugar donde se desarrollará el Proyecto: Por definir		
Tiempo de Desarrollo: 32 semanas		
Tutor Académico propuesto: Jetro López Tutor metodológico: Alicia de Pizzella 0424 4155612 correo: alipiz54@gmail.com		

APROBADO _____X_____ NO APROBADO _____

COMITÉ DE EVALUACIÓN

COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

Prof. Ana Avendaño — ACAP — 13-05-2020

Nombre Firma Fecha

DIRECCIÓN DE ESCUELA

BELKYS ARAUJO BELKYS ARAUJO 05-05-2020

Nombre	Firma	Fecha

Materias o áreas del conocimiento del Pensum que intervienen en la realización del Proyecto (Enumérelas)

1. El I: Seguridad de red.
2. Redes de computadoras.
3. Sistema de Información I.
4. Sistema de Información II.
5. Sistemas de base de datos.
6. Lenguaje de programación.
7. Sistema de Programa.
8. Metodología de la Investigación.
9. Ingeniería de Software.
10. Interfaces con el Usuario.

Línea de Investigación:

Sistemas de información.

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JÓSE ANTONIO PÁEZ
FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA COMPUTACIÓN

APROBACIÓN DEL TUTOR

Quien suscribe, Msc. Jetro López. titular de la cédula de identidad Nº 8779723 , en mi carácter de tutor del trabajo especial de grado titulado: Desarrollo De Una Plataforma De Seguridad Electrónica Basada En Una Inteligencia Artificial presentado por los ciudadanos Alex Daniel Duran Martínez y Oswaldo Manuel Cabrera Licón, titulares de la cédula de identidad Nº 28.429.539 y Nº 26.879.752, respectivamente; presentado como requisito parcial para optar al título de ingeniero, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la Presentación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, a los 27 días del mes de Octubre del año 2020.

Jetro Lopez

Msc. Jetro López

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

San Diego, octubre de 2020

ACTA DE REVISIÓN METODOLÓGICA DEL TRABAJO DE GRADO

Quienes suscriben esta Acta, dejan constancia que el Proyecto de Trabajo de Grado **"DESARROLLO DE UNA PLATAFORMA DE SEGURIDAD ELECTRÓNICA BASADA EN UNA INTELIGENCIA ARTIFICIAL".** Ha sido revisado y, cumpliendo con los requisitos exigidos para su aprobación, recomiendan su tramitación ante el organismo académico correspondiente.

Msc. Jetro López	_____	_____
Tutor Académico	Firma	Fecha
		28-6-20
Ing. Alicia de Pizzella	_____	_____
Tutor Metodológico	Firma	Fecha

ÍNDICE

RESUMEN **10**

INTRODUCCIÓN **1**

EL PROBLEMA 3
1.1.- Planteamiento del problema 3
1.2.- Formulación del problema 7
1.3.- Objetivos de la investigación 7
1.3.1 General 7
1.3.2.- Específicos 7
1.4.- Justificación de la investigación 7
1.5.- Alcance de la investigación 8
1.6.- Limitaciones 9

MARCO TEÓRICO 9
2.1.- Antecedentes de la Investigación 11
2.2.- Bases Teóricas 13
2.2.1.- Seguridad de la información: 14
2.2.2.- Seguridad en las redes 17
2.3.- Bases Legales 18
2.4.- Definición de Términos Básicos 21

MARCO METODOLÓGICO 21
3.1.- Tipo de Investigación 23
3.2.- Diseño de la investigación 24
3.3.- Nivel de la investigación 24
3.4.- Población y muestra 24
3.5.- Técnicas e instrumentos de recolección de datos 25
3.6.- Fases de la Investigación 25

RESULTADOS 27

RECURSOS 44
5.1.- Recursos humanos 45
5.2.- Recursos Institucionales. 45
5.3.- Recursos Materiales. 45
5.4.- Tiempo. 45

REFERENCIAS BIBLIOGRÁFICAS 45

REPÚBLIC A BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JÓSE ANTONIO PÁEZ
FACULTAD DE FACULTAD DE INGENIERÍA
ESCUELA DE COMPUTACIÓN

DESARROLLO DE UNA PLATAFORMA DE SEGURIDAD ELECTRÓNICA BASADA EN UNA INTELIGENCIA ARTIFICIAL

Autor: Cabrera Licón, Oswaldo Manuel; Duran Martínez, Alex Daniel
Tutor: Msj. Jetro López.
Fecha: junio, 2020

RESUMEN

Dado a al exponencial desarrollo de la tecnología que se ha observado en la última década, ha aumentado paralelamente la necesidad y la presencia, de redes inalámbricas al punto en el que casi todo dispositivo electrónico, ya sean esto de uso personal o laboral están conectados a algún tipo de red inalámbrica; es debido a esto que se ha vuelto imperativo el desarrollo constante de nuevos medios de seguridad en redes. Es por ello que el presente trabajo especial de grado tuvo como objetivo el desarrollo de una plataforma que sea capaz de proteger los sistemas de información mediante de distintas herramientas, siendo la principal la aplicación de una inteligencia artificial. Durante el desarrollo de este proyecto se utilizó la metodología de un trabajo de tipo especial con un nivel de trabajo descriptivo y una población y muestra la cual fue delimitada una vez que se había programado la plataforma; por otra parte la recolección de datos se realizó mediante la observación de hechos, fenómenos y situaciones que evidenciaban la importación de un plataforma de esta naturaleza.

Descriptores: Redes Inalámbricas. Inteligencia Artificial. Encriptación. Seguridad

INTRODUCCIÓN

El uso de dispositivos electrónicos se ha vuelto parte vital de la vida humana en los últimos año al punto que se normalizo convertir a la tecnología en un punto de apoyo necesario para el libre desenvolvimiento, claro está, la dependencia creada se debe a que esta herramienta facilita increíblemente múltiples tareas del día a día. Es por estas razones que se percibe la tecnología como una parte fundamental en estilo de vida de una persona promedio en la actualidad, es a consecuencia de ello que eventualmente se produjo la virtualización y globalización de la mayor parte de la información que se maneja en el mundo moderno.

Lo antes descrito ha permitido el fácil acceso a cualquier tipo de información o datos sin preocupación de un límite geográfico, dicha globalización es permitida gracias al desarrollo de nuevas redes inalámbricas que permiten la conectividad global de los usuarios de una manera eficiente. En este orden de ideas, migrar tantas actividades, y conjuntos tan grandes de información al área de la tecnología causa, que evidentemente se inició una época en la cual se volvió común avistar ataques electrónicos, por distintos tipos de piratas informáticos causando incertidumbre en los usuarios por la seguridad de sus datos digitales.

En consecuencia se vio la necesidad, que se debía satisfacer, de crear softwares de seguridad electrónica que contasen con la capacidad de brindarles certeza y tranquilidad a los usuarios. Es en ese punto en el que entran en el campo las plataformas o los servicios de seguridad informática, buscando proteger y salvaguardar la integridad digital de la data almacenada de cada persona, empresa, institución, en fin, de cualquier usuario que así lo viere necesario. El trabajo de investigación a desarrollar comprende la importancia de la seguridad informática y de la protección de redes inalámbricas en una sociedad moderna, es por esto que el propósito de la plataforma planteada en el presente es la protección de los datos informáticos manejados a través de los dispositivos que a su vez puedan depender de la privacidad de estas redes.

Además aplicando una inteligencia artificial para que la protección de los datos sea altamente eficaz y se fundamente en principios de progresión y protección automática. Por estos motivos, se plantea la siguiente estructura que abarca todo el proceso de desarrollo, la cual se distribuye de la siguiente manera:

Capítulo I, El problema, donde se hace referencia a la realidad del estado actual de la seguridad informática, haciendo énfasis en la importancia del uso de una inteligencia artificial, englobando las ventajas y justificando la elaboración de la plataforma.

Capítulo II, Marco Teórico, que hace referencia la a las investigaciones previas que son útiles para la elaboración del proyecto, además, se documentan los conocimientos necesarios para el desarrollo de este trabajo, se da soporte de las decisiones para la elaboración del mismo.

Capítulo III, que corresponde al Marco Metodológico, se describen los aspectos formales para el trabajo de investigación en la que se define: el tipo de investigación, el diseño y el nivel de la misma, lo que se considera como la población y muestra para el desarrollo del sistema, las técnicas utilizadas, la metodología y sus fases.

Capítulo IV, en el cual se señalan los recursos que se emplean para la investigación y desarrollo de la plataforma planteada.

CAPÍTULO I
EL PROBLEMA

1.1.- Planteamiento del problema

La Tecnología y la informática son pilares fundamentales en la evolución humana, de hecho, hoy en día se puede llegar a considerar que los avances que se alcancen en casi cualquier área o rama del saber, o de la vida de los seres humanos se debe, en gran parte, a las mencionadas instituciones. Es por ello que Jiménez, C (2013) plantea que: “La tecnología es el resultado del saber que permite producir artefactos o procesos, modifica el medio, incluyendo las plantas y animales, para generar bienestar y satisfacer las necesidades humanas”, dejando en claro que es el escalón necesario para alcanzar el progreso.

Por su parte, la informática no se queda atrás, esta es definida por La Real Academia Española como: “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores”, de esta manera es de fácil comprensión que las dos áreas del conocimiento se entrelazan, pues una, provee los equipos que cubren las necesidades y la otra aplica estos equipos para manejar la información en las distintas escalas.

Siguiendo en este razonamiento conceptual es fácil comprender que la sociedad se encuentra en una realidad global, la cual es la sociedad del conocimiento, sencillamente los distintos ámbitos, es decir, político, laboral, social, económico, y otros; aplican constante y conscientemente las tecnologías de la información y la comunicación en vísperas de hallar un constante progreso. Ahora bien, el hecho de que exista la mencionada sociedad del conocimiento, genera, en consecuencia, un llamado a la protección de toda la data que se maneje en esta, la cual, lógicamente, es masiva.

En este orden de ideas, es de importancia resaltar el hecho de que el progreso por medio de la tecnología debe ir de la mano con redes de seguridad que puedan mantener

en un alto estatus a la seguridad jurídica institucional y social, ello en vista de que los hackers cada vez atacan con mayor frecuencia a las instituciones que cuentan con respaldos electrónicos de información, lógicamente, en la actualidad son casi todas las que cuentan con estos respaldos. Para ejemplo de lo previamente plasmado se encuentra Estonia, una nación sumamente avanzada tecnológicamente hablando, la cual, a pesar de que se independizó el 3 de marzo de 1991, tuvo que dar grandes pasos en el progreso tecnológico, y ciertamente no fue por gusto, más bien fue por una necesidad latente

En efecto, uno de los pioneros Linnar Viik, (2018) en todo este avance planteo lo siguiente: “En realidad, nosotros no quisimos crear un Estado digital. Era una cuestión de supervivencia. Enseguida nos dimos cuenta de que la Administración Pública y la burocracia gubernamental eran muy caras” (p. 3). En consecuencia, Estonia, se levanta de un régimen y surge tomada de la mano con las tecnologías de la comunicación y de la información, convirtiéndose en una maravilla mundial. De esta manera, en 2005 se percatan de que el progreso tecnológico no puede surgir adecuadamente sin avances en seguridad cibernética, esto debido a que sufren el primer ciberataque, no fue altamente preocupante o peligroso, pero genero un escrutinio público.

Posteriormente, en 2007 se ven comprometidos los datos de la población puesto que hubo un ciberataque que subió de escala y afecto las redes informáticas del estado. Fue en ese momento en el cual el gobierno de Estonia Toma la decisión de desarrollar un fuerte sistema de Ciberseguridad orientado a la protección de los datos de la población, en un principio, y posteriormente a todo lo referente al estado mismo. La previa reseña se realizó con la intención de demostrar la importancia de la creación de una red segura de información, en principio siempre será para la protección de los datos de los particulares, y es notorio que (en este caso) se involucran secretos de estado, estrategias militares y demás elementos de suma importancia para el correcto funcionamiento de una nación.

Evidentemente Estonia tuvo que vivir una violación a su información para poder atacar esa situación, lo cual no descarta que cualquier otra nación que quiera evolucionar e inmiscuirse más en la globalización, en el progreso y los avances tecnológicos se vea en el riesgo de sufrir ataques electrónicos, situación que no niega la posibilidad de protegerse ante dichos ataques. El ejemplo antes desarrollado demuestra, a gran escala por tratarse de una nación, el por qué se debe contar con una red segura de datos. Esto lleva al punto clave, se requiere de innovación, es cierto que las redes de seguridad son elementales en ciertos lugares del mundo, lo cual no quiere decir que estén preparadas para responder de manera certera y veloz a una amenaza.

Ahora bien, al visualizar la frecuencia con la monitoreada con la que empresas y los particulares se ven atacadas por hackers, la cual ha ido aumentado de manera exponencial a medida que la tecnología avanza, se llega a entender el porqué de la solicitud tacita del mercado en esta área, pues los estudios realizados por la Security Magazine indica que se da un ataque electrónico aproximadamente cada 39 segundos. La idea anteriormente planteada es reforzada por el hecho de que si se analizan los mayores ataques electrónicos en 2019 se encuentran que, al menos, 7.9 billones de registros, incluidos números de tarjetas de crédito, domicilios, números de teléfono y otra información altamente confidencial han sido expuestas a través de ataques cibernéticos.

Es por ello que cualquier sistema de información electrónica debe estar protegido, a pesar de que claramente un sistema de uso particular, por ejemplo, no debe contar con las capas de seguridad que requiere una nación completa, pero no por ello debe descuidarse la privacidad y la integridad de los datos de usuarios de pequeños sistemas. Así pues, para brindar dicha seguridad y confidencialidad se fusionaran la un inteligencia artificial con las redes de seguridad, al hacer esto existe la posibilidad de que a través del aprendizaje profundo los sistemas puedan determinar y reconocer a las distintas amenazas que se encuentren de manera instantánea, basándose en los parámetros previamente pautados por el programador y los datos que hayan podido

recuperar por medio de la experiencia que pueda recopilar el software en su tiempo de vida.

Finalmente, la intención de aplicar la inteligencia artificial en las redes seguras no es más que dar un paso hacia el futuro, llevarle la delantera a todos aquellos que busquen acceso a información de manera indebida y lograr, eventualmente, brindar distintas garantías a los particulares que busquen contratar con alguna institución.

1.2.- Formulación del problema

De la problemática antes descrita, surge la siguiente pregunta:

¿Cómo se puede garantizar la seguridad y confidencialidad de la información en las redes con la constante evolución tecnológica?

1.3.- Objetivos de la investigación

1.3.1 General

Desarrollar una plataforma de seguridad electrónica basada en una inteligencia artificial con la finalidad del mejoramiento de la seguridad

1.3.2.- Específicos

1. Determinar los requerimientos funcionales y no funcionales necesarios para la plataforma de seguridad.
2. Diseñar una plataforma de seguridad electrónica basada en los requerimientos funcionales y no funcionales del sistema, siguiendo la metodología de desarrollo XP.
3. Construir una plataforma de seguridad que garantice la protección de la información en las redes.

1.4.- Justificación de la investigación

Para sustentar la idea presentada sobre un sistema de seguridad electrónica basado en una inteligencia artificial primero se debe expresar la importancia de la seguridad electrónica en la actualidad. Debido a los datos presentados anteriormente, se comprende porque hay una preocupación colectiva por parte de grandes y pequeñas empresas por ataques electrónicos, lo cual se ve reflejado en el reporte de 2019 del

World Economic Forum sobre los riesgos más grandes de la actualidad coloca a los "ciberataques de larga escala" como número cinco por encima de "Daño y desastre ambientales hechos por el hombre".

A su vez por la por la creciente conciencia en la sociedad con respecto a la seguridad virtual se da la necesidad de mecanismos de protección digital escalables los cuales puedan ser usados tanto a nivel empresarial como personal, es decir, que sin importar el volumen de información estos mecanismo deben mantener su eficiencia, confiabilidad, seguridad y accesibilidad. Al entender la verdadera importancia que posee la protección de los datos sociales e institucionales, mediante el resguardo de todos y cada uno de los caracteres de información que manipula una institución, solo es necesario analizar una problemática que permita mejorar el estado de la seguridad electrónica actual.

Si se continúan estudiando las estadísticas presentadas por distintos profesionales se encuentran los distintos estudios en los cuales se ha utilizado la colaboración de hackers, entre los cuales está el publicado a través de la página Thycotic.com en la cual se concluye que "el 73% de los hackers de sombrero negro dijeron que la seguridad tradicional de firewall y antivirus es irrelevante u obsoleta".

Por todo lo previamente expresado podemos concluir que en la sociedad actual toda la información se maneja de manera electrónica, en todos los niveles sociales, y que en vista de ello el desarrollo de mecanismos de protección digital se encuentra en un auge de demanda. Tener la capacidad de innovar en el área de seguridad informática y a su vez lograr crear una convergencia con una inteligencia artificial es parte de un futuro tangible y necesario, pues esa, justamente, es la premisa del presente proyecto.

1.5.- Alcance de la investigación

Pues bien, al haber entendido lo ya desarrollado, se plantea que el alcance de la presente investigación tiende a ser indefinido por naturaleza, pues su finalidad es proteger los datos informáticos, en vista de ello tiene un alcance bastante amplio, el cual se limitará en principio a computadores, no trabajará con equipos móviles.

1.6.- Limitaciones

El presente trabajo especial de grado se encuentra limitado por las siguientes situaciones:

• Tiempo de desarrollo y equipo de trabajo, evidentemente desarrollar una red de seguridad con el uso de una inteligencia artificial requiere de un equipo de trabajo amplio, y adicionalmente un periodo de tiempo extenso.

• Desarrollar un sistema de esta naturaleza requiere de una aplicación en el campo, cuestión que es delicada porque requiere el acceso a la información del establecimiento que se preste para ello.

CAPÍTULO II
MARCO TEÓRICO

2.1.- Antecedentes de la Investigación

En principio se plantea la investigación realizada por Torres y Ferreira (2019) desarrollaron un proyecto titulado: **“Encriptación simétrica de señales usando arquitecturas neuronales”** como trabajo especial de grado para optar al título de ingeniería electrónica en la Universidad Distrital Francisco José de Caldas. Proyecto en el cual se plantearon dos modelos de cifrados para la encriptación de la data, el primero de ellos utilizando una inteligencia artificial de tipo caóticas y el segundo utilizando emulación del algoritmo DES (Data Encryption Standard), por medio de la aplicación de una red neuronal de tipo feedforward.

En este se desarrolla uno de los fundamentos de la plataforma de seguridad a desarrollar, siendo este el cifrado de la data aplicando las una inteligencia artificial, brindando

dos variantes que serán evaluadas para escoger la que mejor se adapte a los requerimientos que el proyecto presente.

Así mismo antecede el trabajo de final de grado realizado por Payá (2015) titulado: **“Redes neuronales. Un modelo de clasificación para la detección de dominios DNS maliciosos”.** En el cual desarrolló una herramienta que lograba lo que el título plantea, detectar DNS maliciosas, de tal manera que consiguió clasificar la información que contienen los dominios y de esa manera pasarla por un proceso de normalización para que posteriormente pudiese ser procesada por una red neuronal la cual propiamente realiza el dictamen del carácter malicioso o no, de la DNS.

Ciertamente El ingreso y acceso a múltiples DNS es una amenaza hoy día y es por ello que del ya señalado proyecto se toma en un importante factor de seguridad y validación de seguridad, señalando que dominios pueden ser perjudiciales para el usuario, carácter que al agregarlo a la plataforma de seguridad crea un complemento que lo vuelve sumamente atractivo.

Ahora bien, Novas (2018), desarrolló un trabajo denominado: **“Redes neuronales aplicadas al criptoanálisis del Advanced Encryption Standard”,** presentado en la Universidad Abierta de Cataluña en el cual el autor realiza un estudio proponiendo entrenar una red neuronal con distintos ejemplos de textos en plano y sus correspondientes cifrados, para intentar descifrarlo, demostrando que los cifrados que se realizan a través de las redes neuronales vuelven ineficaz el criptoanálisis desarrollado ante el algoritmo que ponen a prueba. Brindando así certeza de los cifrados efectivamente pueden ser altamente eficientes ante ataques de este tipo.

Finalmente Riofrío y Jarrín (2019) desarrollan el trabajo comparativo titulado : **“Estudio comparativo entre modelos de aprendizaje profundo, desarrollados a partir de redes neuronales recurrentes a redes neuronales convolucionales, para la detección de intrusos en la red”** el cual tiene por finalidad comparar los dos modelos de aprendizaje profundo para determinar el trafico benigno o maligno en una red, estos se validados mediante técnicas de validación cruzada, obteniendo una precisión de sobre el 97%. Demostrando que ambos son sumamente eficaces y que lo

que realmente distingue a uno de otro es el tiempo de entrenamiento de cada uno, puesto que las redes neuronales convolucionales demostraron entrenarse más rápido que las recurrentes.

Craig Mead (2017), desarrolló una patente denominada: **“Modelo De Encriptación De Inteligencia Artificial (Aiem) Con Autorización De Dispositivo Y Detección De Ataques (Daaad)”,** en donde describen como un usuario de un dispositivo cliente establece una conexión segura a un servidor (u otro) dispositivo sin usar claves públicas o certificación de terceros ingresando solo un subconjunto de caracteres en un nombre de usuario asociado con el usuario y una contraseña de uso único en el dispositivo del cliente; una aplicación en el dispositivo cliente recopila información sobre el hardware, software o información de red relacionada con el dispositivo cliente o información biométrica relacionada con el usuario. Los datos enviados entre el cliente y el servidor se cifran (y luego se transmiten) utilizando el subconjunto de caracteres, la contraseña de un solo uso y la información recopilada.

Blackledge, Bezobrazov y Tobin (2015) publicaron un trabajo llamado: **“Criptografía utilizando inteligencia artificial”**, publicado en la Conferencia conjunta internacional sobre redes neuronales (IJCNN) de 2015, este trabajo presenta y analiza un método para generar algoritmos de cifrado utilizando redes neuronales y computación evolutiva. Se basaron en la aplicación de fuentes de ruido natural obtenidas a partir de datos que pueden incluir ruido atmosférico (generado por emisiones de radio debidas a rayos, por ejemplo), desintegración radiactiva, ruido electrónico, etc., "enseñaron" a un sistema a aproximar el ruido de entrada con el objetivo de generar una función de salida no lineal.

2.2.- Bases Teóricas

Señala Bavaresco (2006), que las bases teóricas tienen que ver con las teorías que brindan al investigador el apoyo inicial dentro del conocimiento del objeto de estudio, es decir, cada problema posee algún referente teórico, lo que indica, que el

investigador no puede hacer abstracción por el desconocimiento, salvo que sus estudios se soporten en investigaciones pura o bien exploratorias, teniendo esto en cuenta, a continuación se tienen las tareas que se consideran llevar a cabo en esta investigación.

2.2.1.- Seguridad de la información:

Bien es señalado por Alexander (2007), que el 80% de los valores intelectuales de las organizaciones se encuentran en medios electrónicos, en vista de ellos los interesados en resguardarlos deben encargarse de interponer las mayores y más eficaces acciones para evitar los riesgos de fuga o modificación de la información, como una situación altamente perjudicial, o, por su parte, que simplemente la información almacenada no se encuentre disponible en un momento de necesidad de la misma. En cualquiera de las situaciones previamente señaladas se coloca a una situación desfavorable al sujeto poseedor del sistema de información afectado, motivo por el cual contar con una red de seguridad es un carácter imprescindible.

Seguridad de la información

Según la norma ISO 27002 (2005), la seguridad de la información es “la preservación de la confidencialidad, integridad y disponibilidad”, evidentemente refiriéndose a la preservación de la información propia de un sistema determinado. La cuestión con la protección de la información es que a medida que la tecnología avance también lo harán las fallas, y es por ello que los programadores deben darse la tarea de buscar una manera de encontrarle soluciones tangibles y eficaces a dichas fallas. En este orden de ideas, es comprensible que la seguridad absoluta sea inalcanzable, pero no es esto lo que se busca como finalidad, puesto que los ideales utópicos escasas veces pueden concluir en su materialización.

Para ello plantea Kendall (2005) que para alcanzar dicha seguridad se encuentran tres aspectos fundamentales, los cuales son: la seguridad física, la seguridad lógica y la seguridad conductual. En primer lugar, la seguridad física se refiere a los propios equipos, tanto el acceso controlado a la sala en la cual se encuentren, como la seguridad medioambiental, es decir, temperatura, humedad, flujo eléctrico, entre otros factores. En segundo lugar la seguridad lógica, que se encarga de controles lógicos de software y de transporte de datos por las distintas redes de computadoras; estos constan de distintos mecanismos de verificación de seguridad y a su vez de softwares de encriptación para el contenido almacenado y el contenido transportado.

Finalmente, la seguridad conductual podría ser la estelar, a pesar de que las previamente desarrolladas juegan un papel fundamental, estas no son suficientes para proporcionar la seguridad deseada, para ello se requieren distintos niveles de adiestramiento y concientización de los operadores, convirtiendo en una necesidad vital el hecho de supervisar el comportamiento de los mismos para evitar desviaciones que contribuyan a los fallos.

Necesidad de la seguridad de la información

Todos estos revolucionarios sistemas cuentan con un factor determinantemente favorecedor para aquellas personas que tengan interés en incurrir en actos delictivos o

vandálicos, el cual no es más que el carácter impersonal que puede asumir el mismo atacante, esto se debe a que no requiere la presencia, físicamente hablando, y tampoco necesita del contacto físico con la persona o institución que sea figura del ataque. Solo con manejar y manipular ciertos caracteres técnicos se logra acceder a la información desprotegida. De este modo, se vuelve impredecible para reducir los riesgos de filtración o manipulación de información, lo cual puede ser crítico para el ente afectado. La seguridad de la información cuenta con un papel fundamental para garantizar la continuidad en el tiempo de cualquier organización, y es por ello que se debe tomar en cuenta en las estrategias organizacionales

Principios de seguridad

Chirilo (2005), en sus investigaciones de seguridad informática ha llegado a señalar que la misma se fundamenta en tres aspectos que pueden ser considerados pilares indispensables e indiscutibles de la seguridad de redes, estos son: la confiabilidad, la disponibilidad y la integridad. En principio la confiabilidad, aprecia Chirilo (2005), significa que la información debe estar disponible únicamente para aquellas personas que se encuentren autorizadas para acceder a esta, es decir, lograr mantener el conjunto de datos que conformen la información en secreto, e incluso cifrada, de manera tal que si el atacante llegase a tener acceso a la información no tuviese la capacidad de entenderla.

En segundo lugar, la integridad es la posibilidad que tiene el ente poseedor de la información de brindar certeza de que la información se encuentra intacta, sin ningún tipo de modificación desautorizada durante su almacenamiento o durante el desarrollo. En tercer lugar la disponibilidad, a pesar de parecer evidente, la disponibilidad es uno de los principios de seguridad más importante, esto debido a que no sirve de nada contar con un conjunto de datos secretos y legítimos que no se encuentren disponibles para la finalidad de dichos dato; siendo así los ataques a la disponibilidad son denominados interrupciones.

2.2.2.- Seguridad en las redes

En principio es necesario tener presente que las redes es un conjunto de computadores que se interconectan para permitir el traspaso de información y recursos, esto eventualmente conformaría un sistema de comunicación de datos que tiene capacidad de expansión, ya sea por medio de redes LAN, MAN, WAN o en su defecto redes inalámbricas.

Dicha expansión de redes es inevitable, a medida que las sociedades crecen también los hacen ellas, es parte de la globalización, y es justamente ese el motivo por el cual se convierte en una necesidad primaria trabajar en la seguridad digital, lógicamente como producto de ese crecimiento, de esa expansión global, se generan distintas amenazas para la conectividad desarrollada, como lo pueden ser los distintos tipos de virus, los hackers o incluso fraudes electrónicos.

Todo lo antes expuesto es prueba de la latente necesidad de la seguridad de redes, pero no es el único motivo por el cual se convierte en un enfoque fundamental, también lo hace porque a medida que se generan más ataques se compromete la calidad del servicio, de modo que se encuentra un reto en lograr un transporte eficaz de la información que se encuentre en la red.

Continuando con este orden de ideas, a la transmisión de información entre redes se le denomina enrutamiento, y esta, según Mishar (2008) cuenta con siete (7) principios o propiedades que se deben considerar para que la seguridad sea óptima, siendo los siguientes:

Puntualidad: Marca de tiempo.

Orden: Número secuenciador.

Autenticidad: Contraseñas, certificados.

Autorización: credenciales.

Integridad: Firma digital.

Confidencialidad: Encriptación.

No repudio: Encadenamiento de la firma digital.

Ahora bien estos elementos se deben supervisar mediante un sistema de gestión de red, en vista de que en el momento en el que falle alguno de ellos se pueda atacar al instante, y así reforzar el aspecto lo más rápido posible.

2.3.- Bases Legales

Las bases legales se encuentran por un conjunto de leyes, normas y reglamentos que se consideran primordiales en la investigación, es por ello que son bien definidas por el diccionario jurídico OPUS como "Sinónimo de Fundamento Jurídico. Dícese de la Norma Jurídica en la cual se apoya determinada reclamación, argumentación o decisión". Es por ello, que esta particular parte de la investigación constituye un difícil desafío, es sumamente amplio, y beneficiaría múltiples áreas, pero, ciertamente, no por ello tiene bases legales en todos los rubros del derecho a los que beneficiara. En vista de la planteada situación, la primera base legal pertinente es el artículo 110 de la Constitución de la República Bolivariana de Venezuela, el cual establece:

> El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía (Constitución de la República Bolivariana de Venezuela, Art 110).

Entendiendo de ello que es de exacerbada claridad la importancia que le dio el legislador al área de la ciencia, tecnología y más áreas señaladas en el artículo, y eso no se debe a una decisión aleatoria, es como muy bien lo planteo, es por ser "…fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y la soberanía nacional…", fue desarrollado de una manera tan correcta y adecuada que realmente pareciera no poder extenderse ni mejorarse el texto legal en ese aspecto. A continuación se citan artículos del Decreto con Rango y Fuerza de Ley Orgánica de Ciencia, Tecnología e Innovación, del año 2001; siendo estos los siguientes:

> **Artículo 2°.** Las actividades científicas, tecnológicas y de innovación son de interés público y de interés general.

> **Artículo 19.** El Ministerio de Ciencia y Tecnología es el órgano rector en materia de ciencia y tecnología y actuará como coordinador y articulador del Sistema Nacional de Ciencia, Tecnología e Innovación, en las acciones de desarrollo científico y tecnológico, con los organismos de la Administración Pública Nacional. Los mecanismos de comunicación y participación del Sistema Nacional de Ciencia, Tecnología e Innovación serán definidos en el reglamento de este Decreto-Ley.

Evidentemente se refuerza la importancia que se le otorga a la tecnología, el legislador, sabiamente, consideró que la tecnología era parte vital del progreso de la nación, cabe destacar que fue en el año 2001, año en el cual la tecnología realmente no era tan revolucionaria como hoy en día, y mucho menos tan fundamental y esencial.

> **Artículo 12.** La actividad de la Administración Pública se desarrollará con base en los principios de economía, celeridad, simplicidad administrativa, eficacia, objetividad, imparcialidad,

> honestidad, transparencia, buena fe y confianza. Asimismo, se efectuará dentro de parámetros de racionalidad técnica y jurídica.
> La simplificación de los trámites administrativos será tarea permanente de los órganos y entes de la Administración Pública, así como la supresión de los que fueren innecesarios, todo de conformidad con los principios y normas que establezca la ley correspondiente.
> A fin de dar cumplimiento a los principios establecidos en esta Ley, los órganos y entes de la Administración Pública deberán utilizar las nuevas tecnologías que desarrolle la ciencia, tales como los medios electrónicos, informáticos y telemáticos, para su organización, funcionamiento y relación con las personas. En tal sentido, cada órgano y ente de la Administración Pública deberá establecer y mantener una página en la internet, que contendrá, entre otra información que se considere relevante, los datos correspondientes a su misión, organización, procedimientos, normativa que lo regula, servicios que presta, documentos de interés para las personas, así como un mecanismo de comunicación electrónica con dichos órganos y entes disponible para todas las personas vía internet.

Por otra parte, uno de los fundamentos más pronunciados de las bases legales es el **Decreto 3.390** del 23 de diciembre de 2004 sobre el software libre, en este se plantea que la Administración Pública Nacional empleara prioritariamente un particular tipo de Software denominado “Software Libre”, su finalidad es que todos los órganos y entes que sean parte de la Administración Pública inicien procesos de migración gradual o progresiva hacia el software libre desarrollado con estándares abiertos, figura definida en el mismo decreto como:

> Programa de computación cuya licencia garantiza al usuario acceso al código fuente del programa y lo autoriza a ejecutarlo con cualquier propósito, modificarlo y redistribuir tanto el programa original como sus modificaciones en las mismas condiciones de licenciamiento acordadas al programa original, sin tener que pagar regalías a los desarrolladores previos.

Y en este mismo orden de ideas, podría incluirse la Ley Especial Contra los Delitos Informáticos (2001). La cual 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.

2.4.- Definición de Términos Básicos

Entrenamiento (Inteligencia artificial): Método de ingreso manual de variables para generar parámetros iniciales para que el módulo de inteligencia artificial tenga un punto de partida para sus análisis.

Inteligencia Artificial: Se conoce como inteligencia artificial a aquella exhibida por las máquinas, que les permite realizar tomas de decisiones basados en sus propios análisis del entorno, basados en parámetros “aprendidos” a través del ingreso manual de parámetros por parte de los creadores de dichas máquinas.

Machine Learning: Es una disciplina científica del ámbito de la Inteligencia Artificial que crea sistemas que aprenden automáticamente. Aprender en este contexto quiere decir identificar patrones complejos en millones de datos.

Malware: es un término general para referirse a cualquier tipo de “malicious software” (software malicioso) diseñado para infiltrarse en los dispositivos electrónicos sin el conocimiento de los usuarios.

Sistema de información: son un conjunto de elementos interrelacionados que procesan, almacenan y distribuyen la data ingresada en ellos.

CAPÍTULO III
MARCO METODOLÓGICO

La metodología en un trabajo de investigación constituye propiamente los procesos de la misma, por lo cual Nava (2008) concibe al marco metodológico como "El núcleo, el eje de la planificación de la investigación, está constituido por una serie de elementos y fases ordenadas, que deben seguirse para lograr obtener lo significativo de los hechos y objetos estudiados" (p. 227). En vista de ello, a continuación se enmarca la metodología aplicada en el trabajo especial de grado.

3.1.- Tipo de Investigación

El presente trabajo especial de grado se enmarca dentro del tipo de proyecto especial, definido por la Universidad Pedagógica Experimental Libertador (UPEL) como "el desarrollo de software, prototipos y productos tecnológicos en general". También definido por la Mijares y García en la normativa de la Universidad José Antonio Páez (2007), señala que el proyecto especial:

> Consistirá en las creaciones tangibles, susceptibles de ser realizadas a problemas demostrados, o que respondan a necesidades o intereses de tipo cultural. Se incluyen en esta categoría los trabajos de elaboración de libros de texto y de materiales de apoyo educativo, el desarrollo de software y hardware, prototipos y productos tecnológicos en general. (P. 5).

Los mismos son conformados por actividades que requieren del uso de materiales y/o financieros; requieren de metas y problemáticas delimitadas a un plazo específico. Así pues, para el desarrollo del software se empleo la metodología de Extreme Programing (XP, Programación Extrema). Pressman, 2010 establece "La programación extrema usa un enfoque orientado a objetos como paradigma preferido de desarrollo, y engloba un conjunto de reglas y prácticas que ocurren en el contexto de cuatro actividades estructurales: planeación, diseño, codificación y pruebas" (p.61). Siendo esta la más indicada para la finalidad del proyecto.

3.2.- Diseño de la investigación

Este según Palella y Martins (2012):

> Se fundamenta en la revisión sistemática, rigurosa y profunda del material documental de cualquier clase. Se procura el análisis de los fenómenos o el establecimiento de la relación entre dos o más variables. Cuando opta por este tipo de estudio, el investigador utiliza documentos, los recolecta, selecciona, analiza y presenta resultados coherentes. (pa.87)

Motivo por el cual se considera que la presente cuenta con un diseño de campo.

3.3.- Nivel de la investigación

Tamayo y Tamayo (2009), lo define como la "descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o procesos de los fenómenos". (p. 52). Así pues, se consideró un nivel descriptivo.

3.4.- Población y muestra

De acuerdo con el criterio de Hernández, Fernández, Baptista (2010), la población es: "el conjunto de todos los casos que concuerdan con una serie de especificaciones". (p. 238).

A su vez Arias, F (2012) define como "(…) conjunto finito o infinito de elementos con características comunes, para los cuales serán extensivas las conclusiones de la investigación. Esta queda limitada por el problema y por los objetivos de estudio", (p. 81).

Por su parte la muestra, según Arias, F. (2012), es: "un subconjunto representativo y definitivo que se extrae de la población accesible" (p. 83).

En vista de que se busca desarrollar un sistema de seguridad con distintas posibles aplicaciones, genérico, por así llamarlo, puesto que podrá ser utilizado por distintas instituciones.

Así pues, la población en principio son todos aquellos que manejen información en sus computadores, pero en vísperas de la delimitación se toma como población a un grupo de estudiantes en un semestre regular en la Universidad José Antonio Páez que es de alrededor de 250 estudiantes. Tomando a su vez a la muestra a un conjunto de 50 estudiantes, los cuales se entrevistaron a través de la herramienta online encuesta.com.

3.5.- Técnicas e instrumentos de recolección de datos

Arias, F. (2012) define que "las técnicas de recolección de datos son el procedimiento o formas particulares de obtener la información" (p.111). Por su parte Hernández, Fernández y Baptista (2010) definen como," recolectar los datos implica elaborar un plan detallado de procedimientos que nos conduzcan a reunir datos con un propósito específico" (p. 198).

Así pues, la técnica de recolección de datos fue la observación, mientras que la técnica definida por Arias, F (2012), como: "las técnicas de recolección de datos son las distintas formas o maneras de obtener la información". (p. 53). En el caso del trabajo desarrollado se utilizó la encuesta, la cual, según Tamayo y Tamayo (2008) es "aquella que permite dar respuestas a problemas en términos descriptivos como de relación de variables, tras la recogida sistemática de información según un diseño previamente establecido que asegure el rigor de la información obtenida"

3.6.- Fases de la Investigación

Fase I: Determinar los requerimientos funcionales y no funcionales necesarios para el sistema de seguridad. En este punto de la investigación se recopilaron los datos que establecerán el esquema de funcionamiento del sistema de seguridad, de manera al que se establecerán los requisitos y el alcance del mismo.

Fase II: Diseñar un sistema de seguridad basándose en los requerimientos funcionales y no funcionales del sistema, siguiendo la metodología de desarrollo XP. Tomando en cuenta los requisitos obtenidos una vez desarrollada

la fase previa se creará un prototipo no funcional del sistema de seguridad de red siguiendo las distintas etapas de desarrollo de la metodología XP.

Fase III: Construir un sistema de seguridad que garantice la protección de la información en las redes. Finalmente se tomarán todos los avances desarrollados en la fase previa para crear el prototipo funcional del sistema de seguridad, considerando los tiempos de trabajo que establece la metodología a seguir.

CAPÍTULO IV

RESULTADOS

Para el desarrollo del presente capítulo se siguió el patrón de desarrollo de la metodología XP, tal y como se planteó previamente, pues está al brindar una estrategia de desarrollo ágil con un ciclo de vida dinámico, le permite a los programadores una organización puntual e iterativa para aquellos proyectos que cuenten con un corto periodo de entrega, lo cual, por motivos lógicos, es ideal para el presente desarrollo. Dicha planificación se divide en cuatro fases. Diagnóstico (planificación), diseño, desarrollo y pruebas, lo cual brinda un conjunto de etapas organizadas, al final de las cuales se encuentra como producto un desarrollo óptimo.

Fase I: Diagnóstico.

Para completar esta etapa, se implementó el instrumento de recolección de datos, es decir la encuesta, la cual se conformó por cinco (5) preguntas cerradas las cuales se reflejaran a continuación:

Pregunta 1: ¿Maneja usted frecuentemente Información de importancia en su Computadora?

Al estudiar las respuestas de los encuestados a estas preguntas se puede corroborar que la mayor parte de ellos suelen manejar información de alta importancia en sus computadores, tal y como se verifico con los siguientes datos: 82% (41 entrevistados) **SI;** 18% (9 entrevistados) **NO.**

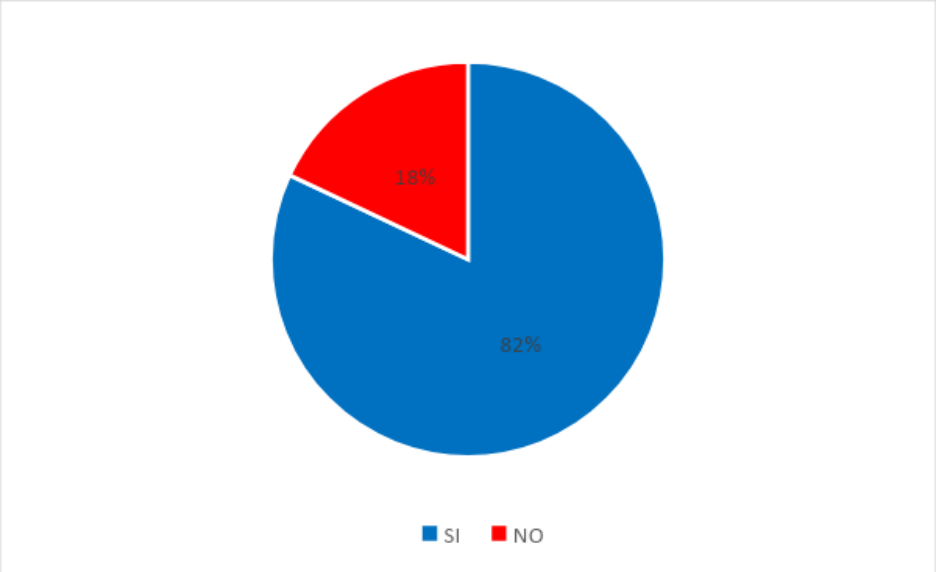

Figura Nº 1: Item Nº 1 Fuente: Cabrera y Duran (2020).

Pregunta 2: ¿Considera usted que la información que maneja por medio de las computadoras se protege adecuadamente?

Analizando los resultados se demuestra que la información de importancia, tal y como se demostró en la pregunta anterior, no se encuentra adecuadamente protegida, lo cual genera una necesidad de salvaguardar dichos datos de una manera rápida, sencilla, eficaz e intuitiva. Los entrevistados demostraron, en su mayoría, que consideran que los datos no son protegidos adecuadamente como se pudo verificar con los siguientes resultados: 30% (15 entrevistados) **SI;** 70% (35 entrevistados) **NO.**

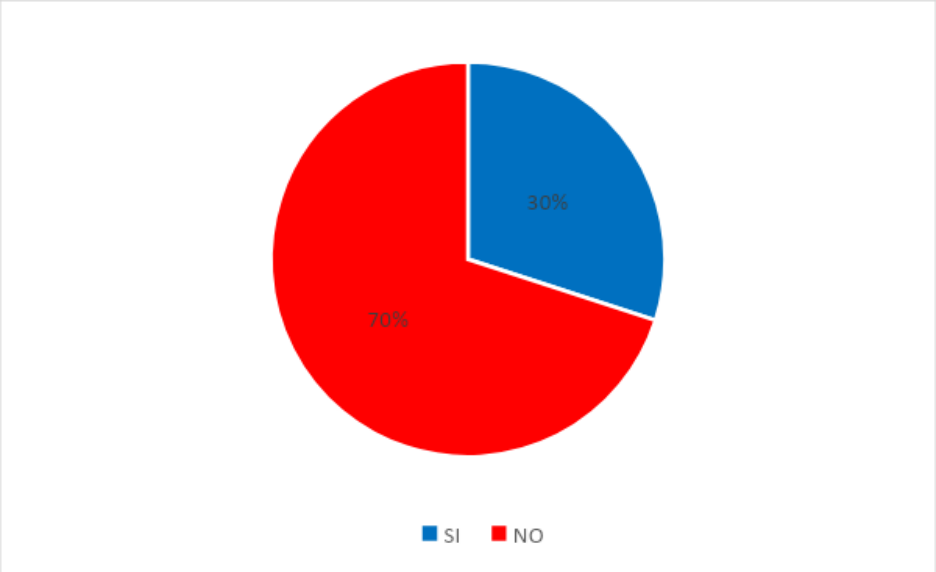

Figura Nº 2: Item Nº 2 Fuente: Cabrera y Duran (2020).

Pregunta 3: En su opinión, ¿Todos los que manejen datos electrónicos por medio de computadoras deberían contar con la posibilidad de asegurarlos para proteger la información que contenga?

De esta manera se demuestra que hay mercado para la plataforma de seguridad electrónica, en vista de que las encuestas arrojaron los siguientes resultados: 82% (41 entrevistados) **SI;** 18% (9 entrevistados) **NO.**

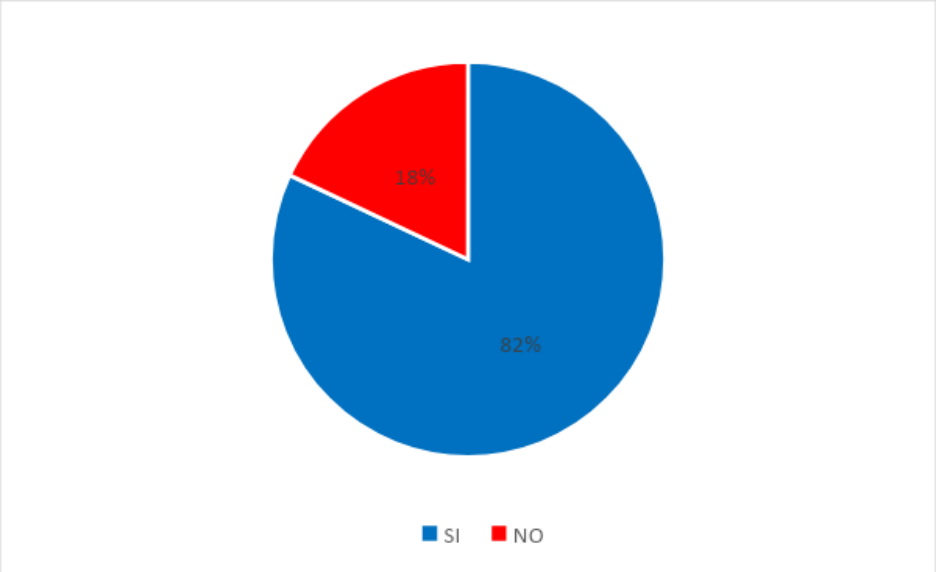

Figura Nº 3: Item Nº 3 Fuente: Cabrera y Duran (2020).

Pregunta 4: ¿Conoce usted mecanismos de seguridad electrónica para computadoras?

Los resultados a esta pregunta demuestran que la ignorancia sobre temas de seguridad electrónica causa que los usuarios sean propensos a tener violaciones en sus datos informáticos, puesto que las respuestas arrojaron los siguientes porcentajes: 30% (15 entrevistados) **SI;** 70% (35 entrevistados) **NO.**

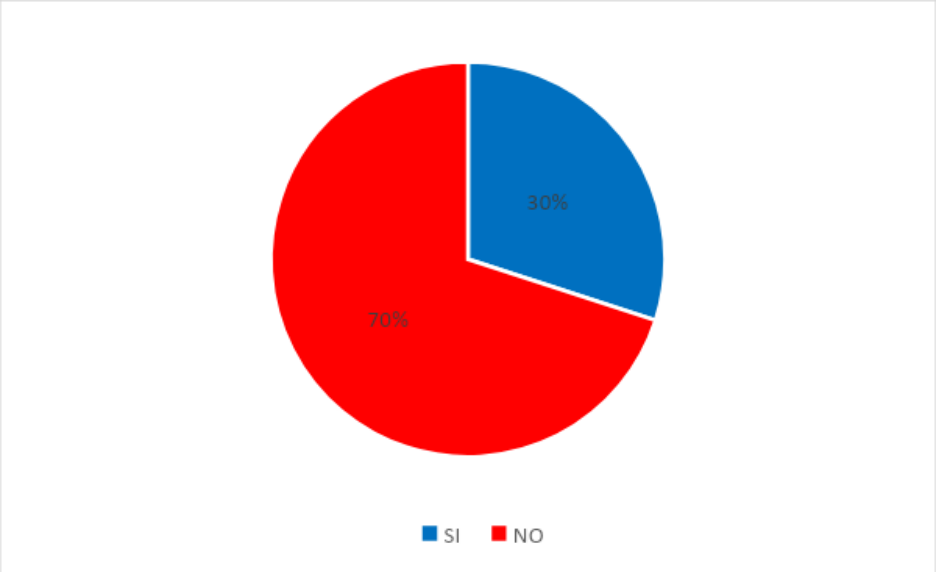

Figura Nº 4: Item Nº 4 Fuente: Cabrera y Duran (2020).

Pregunta 5: ¿Estaría dispuesto a utilizar en su computadora una plataforma de seguridad electrónica que le brinde seguridad a sus datos y que sea intuitiva?

Y finalmente, por medio de la última pregunta, se corroboro que el mayor porcentaje de entrevistados está dispuesto a utilizar una plataforma que los ayuden a proteger sus datos. Siendo los porcentajes de respuestas obtenidos los siguientes: 96% (48 entrevistados) **SI;** 4% (2 entrevistados) **NO.**

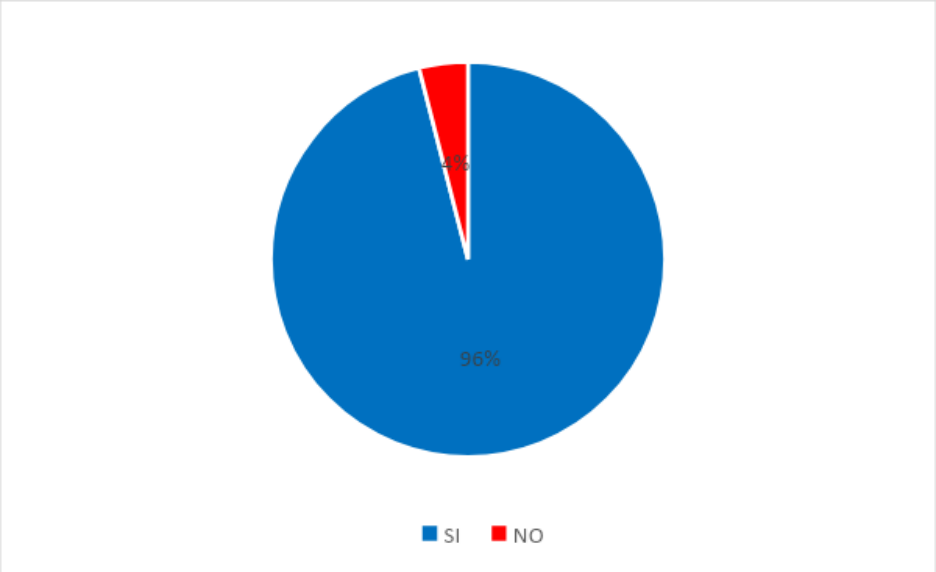

Figura Nº 5: Item Nº 5 Fuente: Cabrera y Duran (2020).

En vista de los resultados obtenidos se llega a la conclusión que efectivamente es necesario crear una plataforma de uso intuitivo para que los usuarios puedan proteger los datos que manejan a través de sus computadoras. Por lo cual, luego de un análisis se delimitaron los siguientes requerimientos funcionales y no funcionales

Requerimientos Funcionales:

La aplicación debe ser capaz de los siguientes procesos: encriptación, desencriptar y generar llaves, tanto públicas como privadas.

La aplicación dará la opción para seleccionar el lugar dentro de la máquina donde serán guardados los archivos generados dentro de la aplicación

La aplicación debe ser ejecutable tanto en windows como en macOS

Proceso de Encriptación

El usuario debe ser capaz de elegir cualquier archivo en su computador

Se implementa un algoritmo de encriptación simétrico al archivo, y se genera una nueva llave simétrica

La llave simétrica será encriptada con un algoritmo asimétrico utilizando la llave pública provista por el usuario

La llave simétrica encriptada asimétricamente y el archivo encriptado simétricamente serán combinados en un solo archivo

Proceso de Desencriptación

El usuario debe ser capaz de elegir cualquier archivo en su computador

El programa debe ser capaz de separar la llave simétrica encriptada de el archivo encriptado de manera asimétrica

El programa primero desencripta la llave encriptada utilizando la llave privada provista por el usuario, y después utilizando la llave resultante desencripta el archivo

Proceso para Generar llaves

El usuario debe ser capaz de asignar un nombre al par de llaves

La llaves deberán ser generadas en un formato .pem

Requerimientos No funcionales:

Eficiencia:

El proceso para generar llaves debe ser menor a 20 segundos

Seguridad lógica y de datos

Todos los archivos deben ser par de llaves específicas

Los archivos encriptados con una llave pública sólo pueden ser desencriptados por llave privada gemela

La inteligencia artificial debe cambiar el patrón de seguridad lo suficiente para que en caso de que se comprometa un archivo esto no comprometa ni afecte el nivel de seguridad de los demás archivos

Usabilidad:

La interfaz debe ser intuitiva

Debe ser fácil identificar cómo se inicia cualquiera de los procesos dentro de la aplicación

Fase II: Diseño.

La fase de diseño en la metodología empleada es aquella en la que se desarrolla un bosquejo conceptual sobre el proyecto, teniendo presente que serán diseños sencillos pues en ellos se plantean los diseños imprescindibles para que el software funcione, y de esa forma, posteriormente en la fase III: desarrollo, se complementa el prototipo desarrollado, teniendo presente que deben ser desarrollados con la intención de que la interacción con los usuarios finales sea lo más intuitiva posible.

En principio es importante recalcar que el modelo de cifrado bajo el cual se trabajara es un modelo asimétrico, el cual consta de una llave pública y una llave privada, estas para brindar una mayor seguridad en la criptografía de los archivos. Los usuarios tendrán la posibilidad de seleccionar si el archivo será cifrado solo una vez o dos veces, aplicando una sola llave pública y una sola privada o dos públicas y dos privadas, respectivamente.

Para cumplir adecuadamente con el diseño es necesario plantear casos de uso, de esta forma se presenta de forma más clara para el programador al momento de adaptar el sistema a los requerimientos. Hay dos tipos de usuarios que encuadran en los casos de usos: Emisor y Receptor, a continuación se desarrollan los casos:

En principio el emisor quien tiene el archivo original, por denominarlo de alguna forma, tendrá la posibilidad y la necesidad de generar sus llaves, es decir, la llave pública y la llave privada. Así mismo, una vez generadas tendrá la posibilidad de adjuntar los archivos desde su equipo y cifrarlos utilizando las llaves. Posteriormente el sistema realizaría el procedimiento de encapsulamiento de los archivos y el usuario podrá guardarlo una vez encriptado para poder enviarlo.

En segundo lugar, el receptor, al igual que el emisor, tiene la posibilidad de generar sus claves, en caso de utilizar un doble encriptado, podrá adjuntar el archivo recibido por el emisor y que de esa manera el sistema pueda ejecutar el algoritmo para

desencapsular y luego desencriptar el archivo. Finalmente podrá guardar el archivo para su utilización.

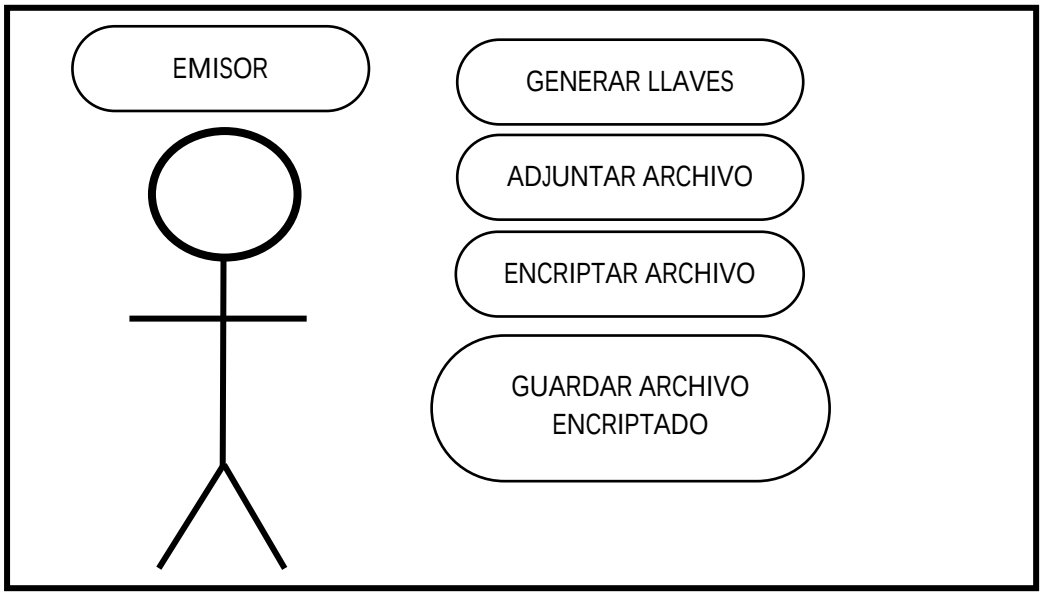

Figura Nº 6: Item Nº 6 Fuente: Cabrera y Duran (2020).

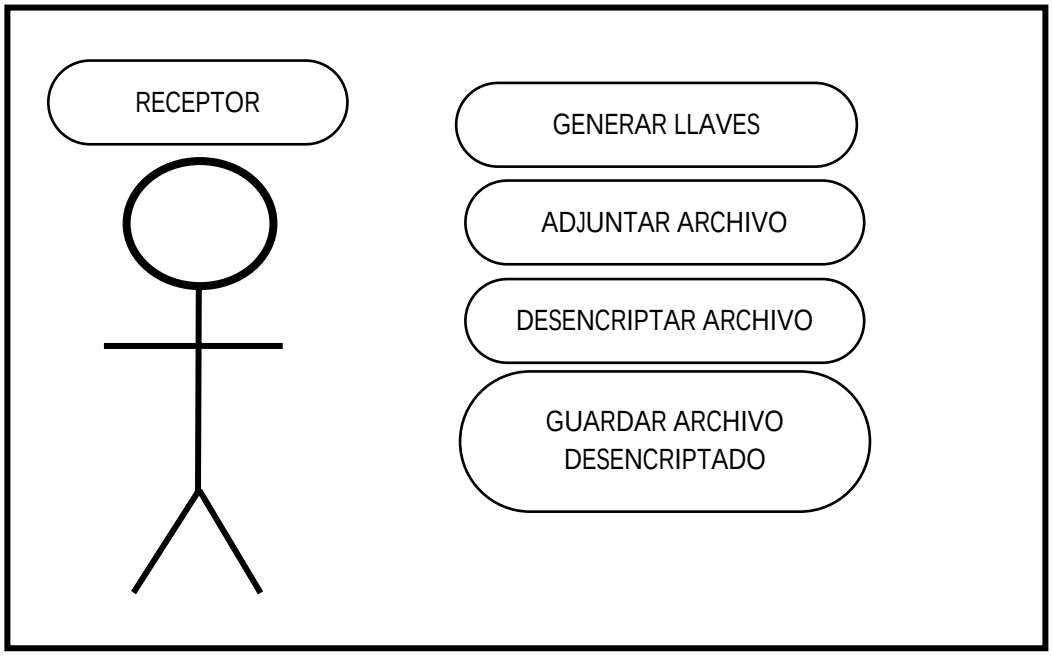

Figura Nº 7: Item Nº 7 Fuente: Cabrera y Duran (2020).

Ahora bien, para el proceso de encriptación se implementará un sistema de encriptación “híbrido”. FERNET y RSA fueron los algoritmos simétricos y asimétricos, respectivamente, que se utilizaran para el desarrollo del sistema híbrido, es necesario recalcar que este modelo se utiliza porque de esa manera se encuentran beneficios que aumentan la calidad del cifrado, como por ejemplo, el sistema simétrico es inseguro y el asimétrico es lento, pero al emplear el híbrido se toma la velocidad del primero y la seguridad del segundo. Por su parte el asimétrico presenta una limitación de cifrado a archivos de 2mb, limitación que se evade implementando el híbrido.

Por otra parte se implementará un formato de encapsulamiento denominado PEM, lo cual permite agregarle un nivel más de seguridad a la data encapsulada, la cual, en este caso, es cada llave generada. El algoritmo de encapsulamiento se corre de forma automática, y sin previa solicitud del usuario, es un algoritmo ejecutado por la inteligencia artificial.

Apropósito de la inteligencia artificial, es importante señalar que no todo lo que es inteligencia artificial hace referencia al “Machine Learning”, la AI hace referencia a cualquier tipo de sistema con inteligencia, lo que no quiere decir que este deba ser consciente completamente de las decisiones que toma, o que deba estar basado en la inteligencia humana, sencillamente significa que será capaz de resolver un problema en específico, o de reaccionar a ciertos estímulos en base a una serie de datos previamente proporcionados por el programador.

Es por ello que es importante señalar que el machine learning ciertamente es uno de los tipos de inteligencia artificial, uno de los que retiene la mayor parte de la atención, pero no por ello es el único. En el presente desarrollo se planteó una mecanismo de inteligencia artificial sencillo, que facilita el desarrollo del procedimiento de cifrado y unifica las fracciones y acciones del algoritmo desarrollado.

Fase III: Desarrollo.

Diseño de interfaces

Primeramente se estableció la paleta de colores utilizada alrededor de toda aplicación, la cual es representada primordialmente por azules oscuros, ya que desde un punto vista psicológico color azul transmite confianza y estabilidad como significados dominantes, a su vez dentro de la industria de la tecnología este representa inteligencia, sabiduría y entendimiento; es por esto que su interpretación contemporánea se asocia con el racionalismo y, más concretamente, con la ciencia, la tecnología y la innovación. En el mundo del marketing se emplea en muchas marcas debido a su vinculación con credibilidad, confianza, verdad y poder. Es un color elegante y corporativo, uno de los más usados por las empresas. Y principalmente por su asociación con la credibilidad y la confianza que se eligió este color, dado que esta dos características son primordiales para una aplicación de seguridad electrónica como es la presentada en este trabajo especial de grado.

A continuación se enlista todas las vista dentro programa:

Inicio de sesión

Este es el primer formulario que se debe rellenar para ingresar en la aplicación. De no estar registrado se deberá proceder a rellenar el formulario de registro.

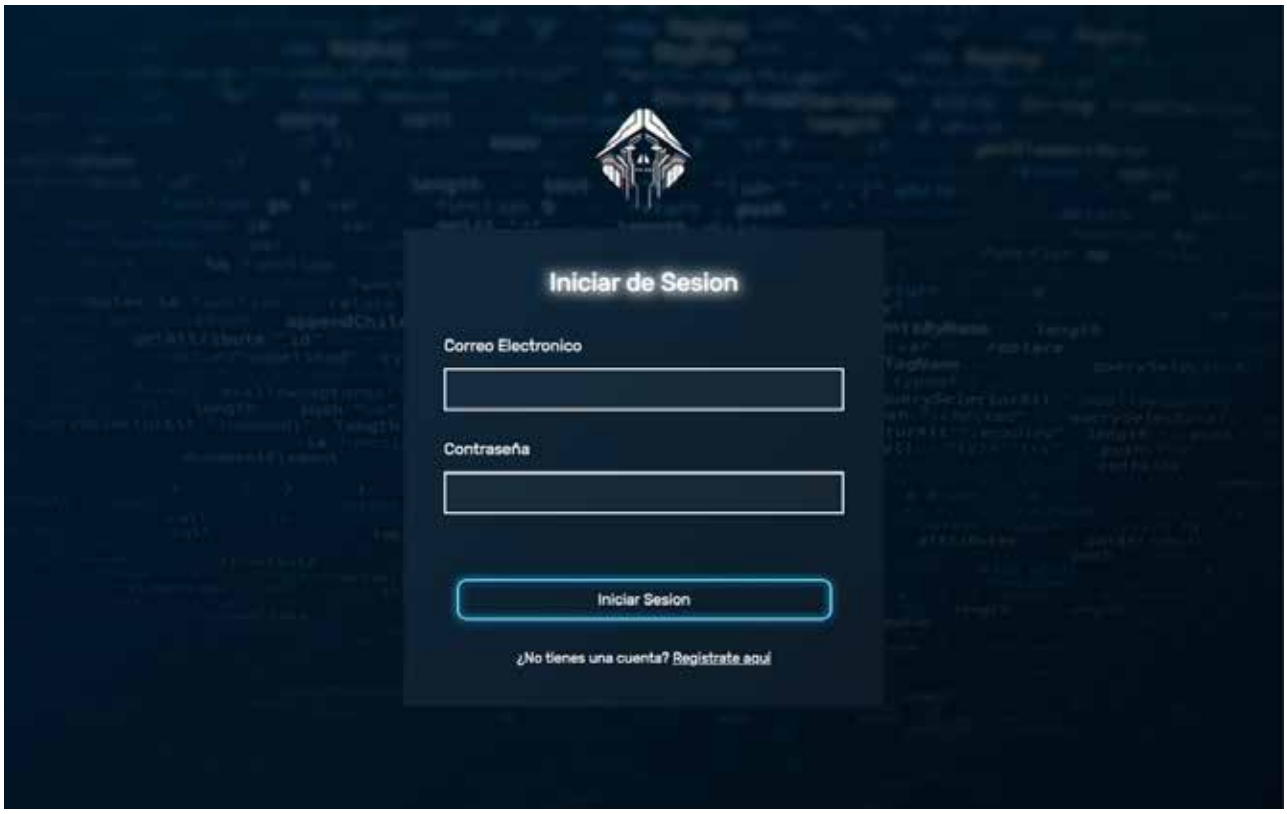

Figura Nº 8: Item Nº 8 Fuente: Cabrera y Duran (2020).

Registro de usuario

Es el segundo formulario de la aplicación, deberán rellenarlos todos los usuarios nuevos, en este se solicita nombre, apellido, correo electrónico y contraseña.

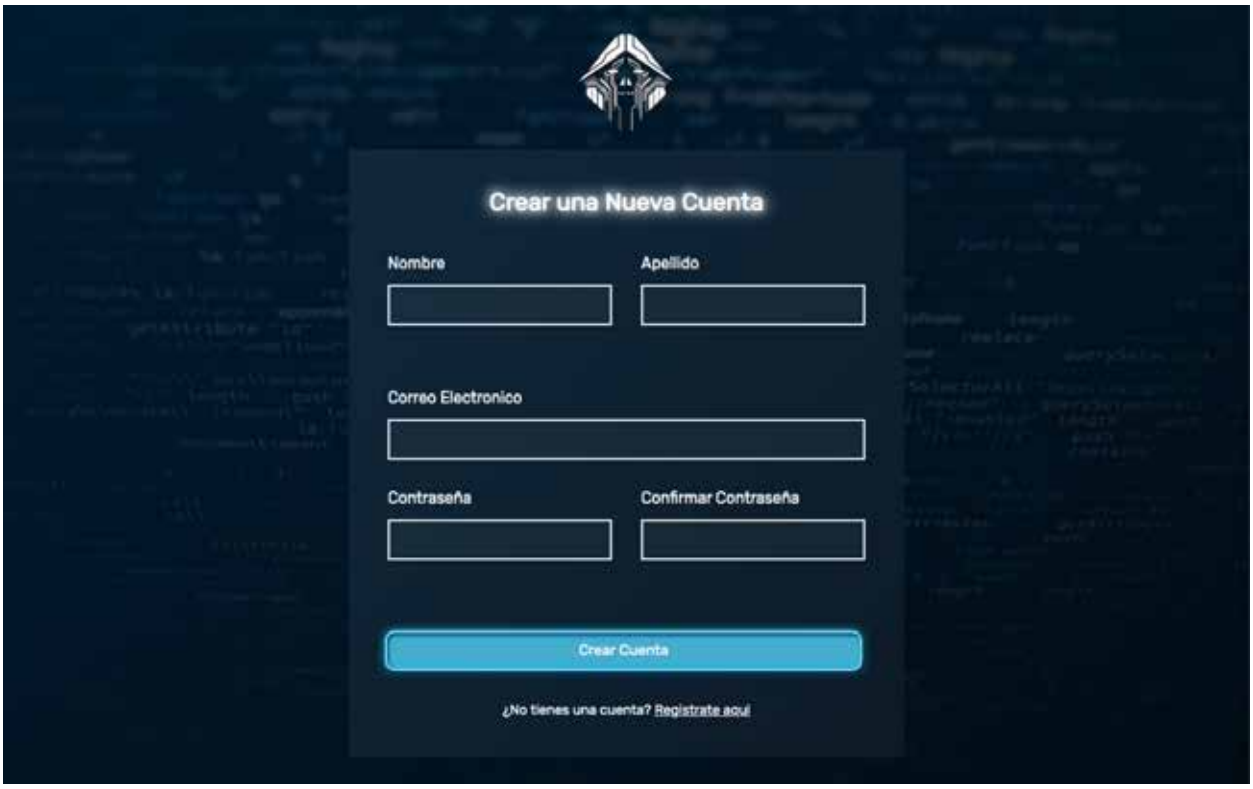

Figura Nº 9: Item Nº 9 Fuente: Cabrera y Duran (2020).

Inicio

En esta pantalla se presentan las opciones principales del sistema en el centro, encriptar y desencriptar. Y al lado Izquierdo en un panel se encuentra la opción de generar llavero, en caso de que sea un usuario primerizo que desee encriptar un archivo y no cuente con llave pública ni privada.

Figura Nº 10: Item Nº 10 Fuente: Cabrera y Duran (2020).

Encriptar archivo

En esta pantalla se ingresa el archivo a encriptar y la llave correspondiente para el proceso.

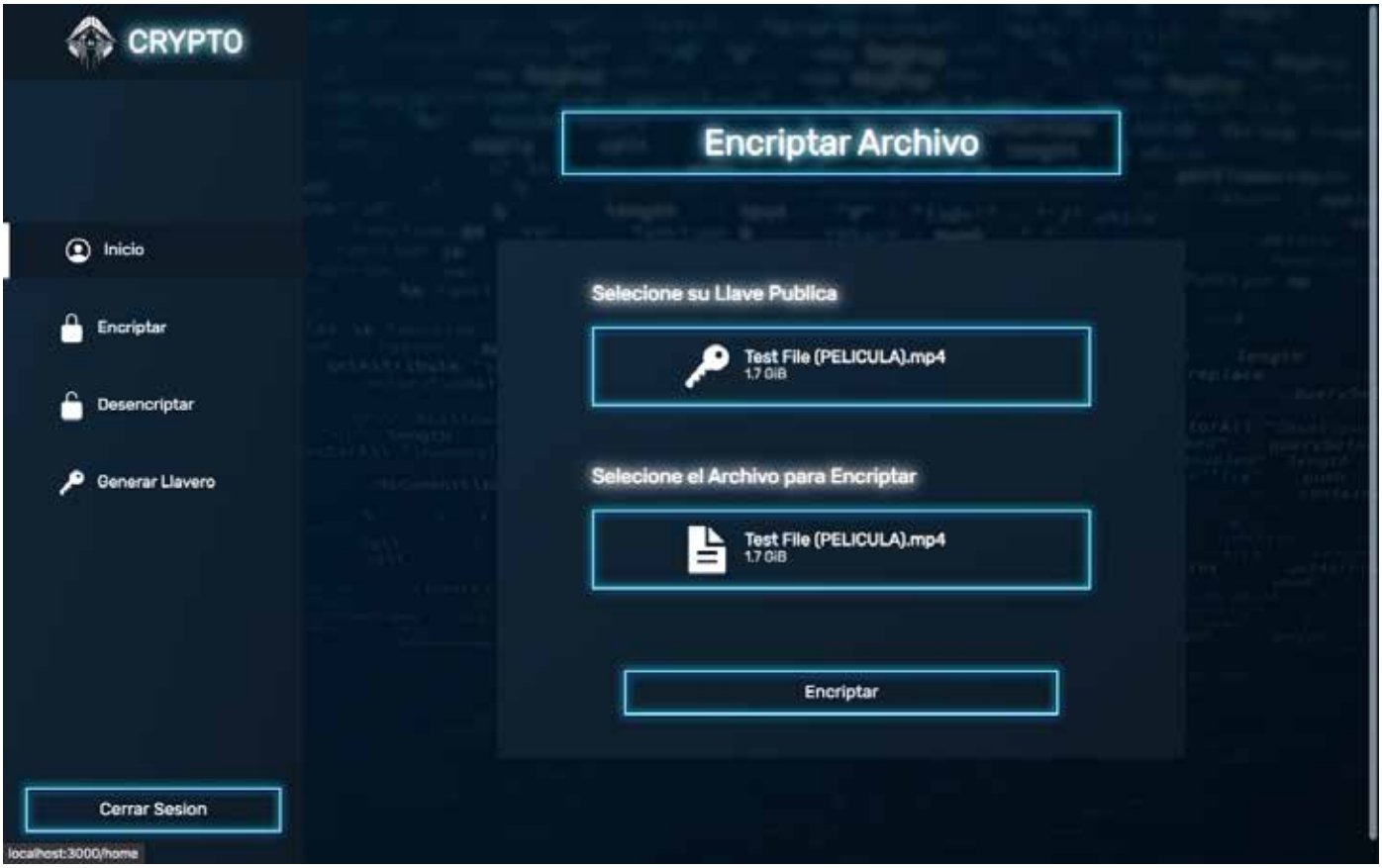

Figura Nº 11: Item Nº 11 Fuente: Cabrera y Duran (2020).

Desencriptar archivo

En esta pantalla se ingresa el archivo a desencriptar y la llave correspondiente para el proceso.

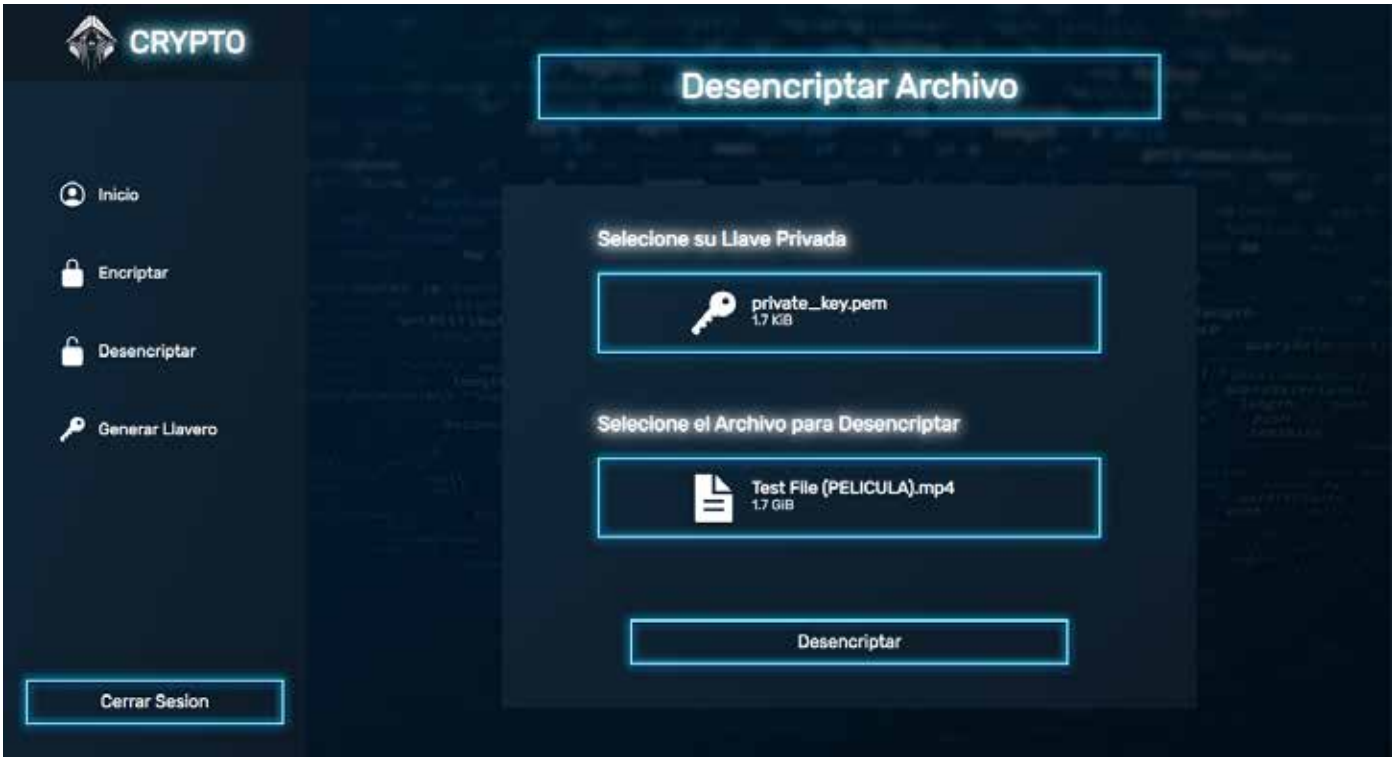

Figura Nº 12: Item Nº 12 Fuente: Cabrera y Duran (2020).

Generar llavero

En esta pantalla se gestiona la generación de claves públicas y privadas, el usuario tendrá la posibilidad de generar llaves tantas veces como lo vea necesario, pero estas funcionan por pares. No pueden mezclarse las llaves de dos llaveros distintos, pues no funcionará el sistema de encriptación.

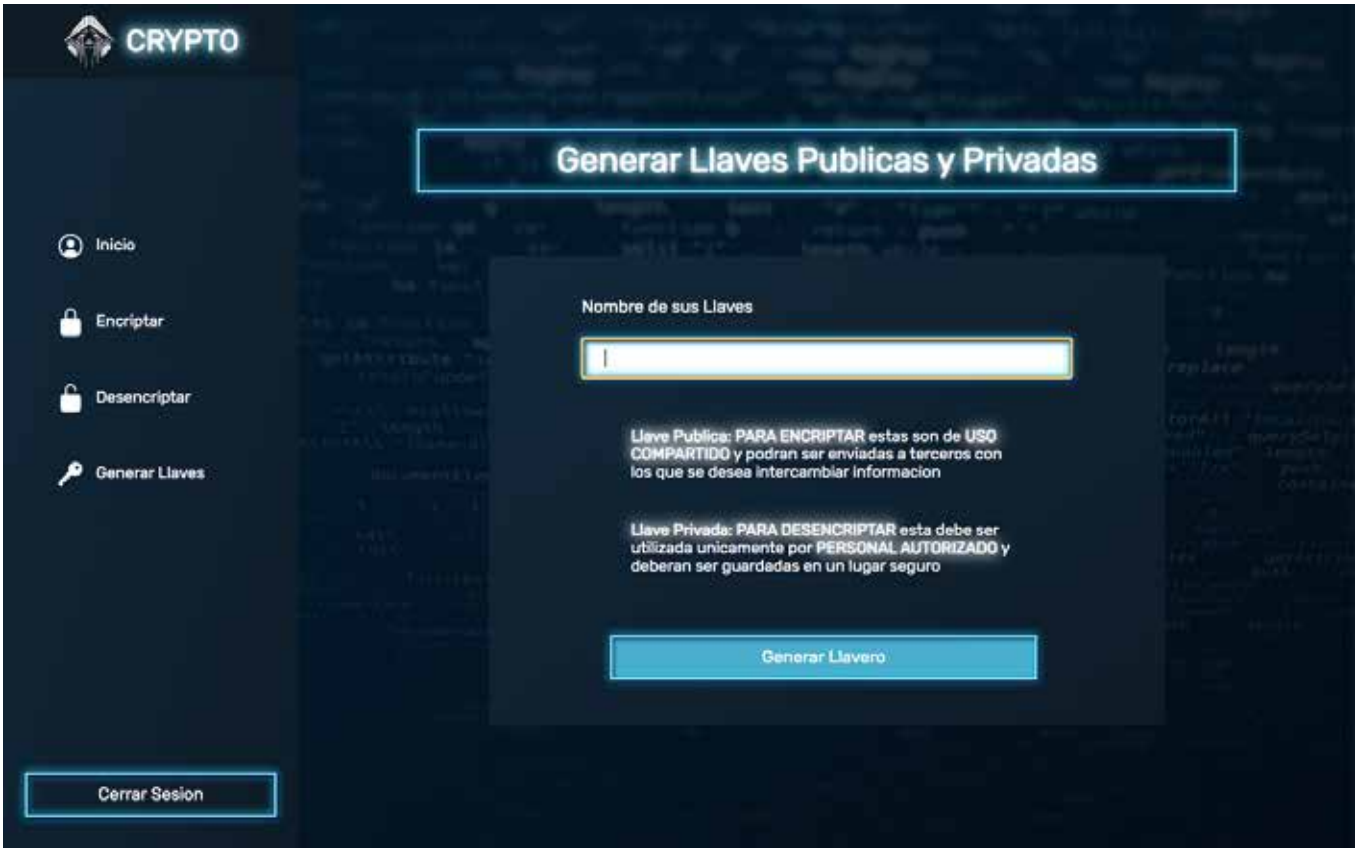

Figura Nº 13: Ítem Nº 13 Fuente: Cabrera y Duran (2020).

Fase IV: Pruebas.

Pruebas de caja blanca.

DI	Caso de prueba	Descripción	Funcionalidad	Resultado
CB0	**Generación de llaves**	**Se probó que el sistema crea un llavero que se conforma por una llave pública y una privada, y que estas se adecuan a las metodologías de cifrado implementadas**	**Generar llaves**	**Efectivo**
CB1	**Encriptación**	**Se corroboró que la información que se ingresó al sistema pasó satisfactoriamente a través del algoritmo y arrojó la data cifrada.**	**Encriptar**	**Efectivo**
CB2	**Encapsulamiento**	**Se demostró que una vez generadas las llaves estas se encapsulan para protegerse**	**Encapsular**	**Efectivo**
CB3	**Desencriptación**	**El procedimiento inverso a la encriptación, en este se corre el algoritmo para descifrar los archivos, este se realizó de forma efectiva.**	**Desencriptar**	**Efectivo**
CB4	**Desencapsulamiento**	**Correspondientemente sería el proceso inverso al encapsulamiento, este se utiliza cada vez que deban implementarse las llaves, ya sea para cifrar o descifrar**	**Desencapsular**	**Efectivo**

Pruebas de caja negra.

D1	Caso de prueba	Descripción	Funcionalidad	Resultado
CN0	**Generación de llaves**	**El usuario puede generar un llavero cada vez que lo desee en la ventana de generar llaves. Cada llavero generado deberá nombrarlo para distinguirlo y se guardarán en una carpeta.**	**Generar llaves**	**Efectivo**
CN1	**Encriptación**	**Una vez que el usuario haya decidido que archivo desea encriptar, podrá ingresarlo en el sistema en conjunto con las llaves para que se**	**Encriptar**	**Efectivo**

		proceda al proceso de cifrado y posteriormente se guarde en el equipo el nuevo archivo cifrado.		
CN2	**Desencriptación**	**El usuario final, quien desencripte el archivo, debe recibir de un remitente el archivo cifrado en conjunto con la llave correspondiente al proceso que realizará, y una vez tenga lo necesario lo ingresa en el sistema para poder habilitar el archivo al descifrarlo.**	**Desencriptar**	**Efectivo**

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1.- Conclusiones.

Una vez desarrollada la plataforma de seguridad electrónica con la implementación de inteligencia artificial, se alcanzaron las siguientes conclusiones:

En primer lugar, al analizar los resultados de las investigaciones se visualizó que en materia de seguridad informática hay una gran falta de conocimiento la cual se refleja en la falta de protección voluntaria de los archivos.

Adicionalmente se concluye que los usuarios de equipos electrónicos realmente se preocupan por la seguridad de la información que manejan y que están dispuestos a implementar mecanismos de seguridad.

Que el uso de un software intuitivo y funcional permitirá una mayor aceptación en el mercado

5.2.- Recomendaciones.

De la misma manera, una vez concluido el trabajo final de grado se realizan las siguientes recomendaciones:

Utilizar Crypto como módulo de seguridad complementario en ámbitos en donde se maneje información confidencial.

Contratar un servidor externo y expandir la capacidad de verificación de usuarios del sistema para alcanzar un mayor grado de automatización.

Implementar este sistema en distintos mecanismos de evaluación en los sistemas educativos para mantener el carácter personalísimo y confidencial de las evaluaciones.

REFERENCIAS BIBLIOGRÁFICAS

Arias F. (2012) El Proyecto de Investigación. Guía para su elaboración. 3era Edición. Caracas. Editorial Episteme.

Alexander, A. (2007). Diseño de un sistema de seguridad de la información. Bogota. Alafomega Colombiana S.A.

Bavaresco, A. (2006). Proceso metodológico en la investigación: Cómo hacer un Diseño de Investigación. Maracaibo, Venezuela. Recuperado de http://biblioteca.bcv.org.ve/cgi-win/be_alex.exe?Autor=Bavaresco+de+Prieto,+Aura&Nombrebd=bcv_internet

Belic, I (2019) Malware. Recuperado de: https://www.avast.com/es-es/c-malware

Chirilo, J. y Dalielyan, E. (2005) Introducción a la teoría general de la administración. (7ª Ed). México. Study guide. New York. McGraw- Hill.

El Zabayar, N (2013). Bases legales de la informática en el contexto Venezolano. Slideshare. Recuperado de https://es.slideshare.net/elzabayarshevchenko/bases-legales-de-la-informtica-en-el-contexto-venezolano

E-Justice Europa. (2017). Sistema judicial de Estonia. E-Justice Europa. Recuperado de https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-ee-es.do?member=1

Fernández, R. (1990) Estonia se independizará de la URSS paso a paso. Diario el país. Recuperado de https://elpais.com/diario/1990/03/31/internacional/638834402_850215.html

Hernández, R; Fernández, C; Baptista, P. (2010) Metodología de la investigación (5ª Ed). México. McGraw- Hill.

Jaspe, H. (2011) Diseño de un sistema de seguridad para redes de datos del ministerio del poder popular para la educación. Recuperado de: http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAS2281.pdf

Jiménez, C. (2013) El concepto de tecnología. Recuperado de https://www.gestiopolis.com/concepto-tecnologia/

Kendall, K y Kendall, J. (2005). Analisis y diseño de sistemas. (6ª Ed). Mexico. McGraw Hill.

Laudon, K y Laudon, J (2008) Sistemas de información gerencial. Recuperado de https://juanantonioleonlopez.files.wordpress.com/2017/08/sistemas-de-informacic3b3n-gerencial-12va-edicic3b3n-kenneth-c-laudon.pdf

Mishra, A. (2008) Security and Quality of service in ad hoc Wireless networks. New York. Cambridge University Press.

Merchán (2018) Aplicación de Técnicas De Machine Learning a La Seguridad. Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81110/1/jmerchanmTFM0618.pdf

Mijares, H y Garcia, L. (2007) Normas para la elaboración y presentación de los anteproyectos, proyectos y trabajos de grado.

Montana, M. Bases legales de la informática educativa en Venezuela. Blogspot. Recuperado de https://mariamontanadotblog.wordpress.com/bases-legales-de-la-informatica-educativa-en-venezuela/

Nava, Hortensia (2008). La Investigación Jurídica. Elaboración y Presentación Formal del Proyecto. (3ª. ed.). Maracaibo, Venezuela.

Novas, P (2018) Redes Neuronales Aplicadas Al Criptoanálisis del Advanced Encryption Standard. Recuperado de http://hdl.handle.net/10609/81610

Palella, S y Martins, P (2012) Metodología de la investigación cuantitativa. (3ª Ed). Fedupel. Caracas, Venezuela.

Payá, J. (2015) Redes neuronales. Un modelo de clasificación para la detección de dominios DNS maliciosos. Recuperado de http://repositori.uji.es/xmlui/bitstream/handle/10234/152846/TFG_2014_JuanPay%c3%a1Y.pdf?sequence=1&isAllowed=y

Pondal-Kleber, J.C. Legislación Informática de Venezuela. Informática Jurídica. Recuperado de http://www.informatica-juridica.com/legislacion/venezuela/

Real Academia Española: Diccionario de la lengua española (23ª Ed), [versión 23.3 en línea]. <https://dle.rae.es>

Riofrío, D y Jarrín, D (2019). Estudio comparativo entre modelos de aprendizaje profundo, desarrollados a partir de redes neuronales recurrentes a redes neuronales convolucionales, para la detección de intrusos de red. Recuperado de https://repositorio.uisek.edu.ec/bitstream/123456789/3532/1/Tesis_DAVID_JARRIN_VERSION_FINAL.pdf

Tamayo y Tamaño, Mario (2009). El Proceso de la Investigación Científica. (5ª. ed.). México: Grupo Noriega Editores.

Tecnologías información (2008). Evolución de los sistemas de información. Recuperado de https://www.tecnologias-informacion.com/evolucionsistemas.html

Torres y Ferreira. (2019) Encriptación simétrica de señales usando arquitecturas neuronales. Recuperado de http://repository.udistrital.edu.co/handle/11349/23178

Universidad Pedagógica Experimental Libertador

Viik, L (2018). Estonia, el primer país digital del mundo. Diario el país. Recuperado de https://elpais.com/elpais/2018/04/05/eps/1522927807_984041.html

Yanes, K. (2016). Lista completa de conectores para la tesis. Nerd Universitaria. Recuperado de https://nerduniversitaria.com/2016/05/09/lista-conectores-tesis/