UNIVERSIDAD JOSÉ ANTONIO PÁEZ

SISTEMA DE SEGURIDAD PARA UNA APLICACIÓN DE MENSAJERÍA BASADO EN LA ENCRIPTACIÓN

Autor:

Deiskel Gatriel Villegas Michelena

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 INGENIERÍA
ESCUELA DE INGENIERÍA EN COMPUTACIÓN

SISTEMA DE SEGURIDAD PARA UNA APLICACIÓN DE MENSAJERÍA BASADO EN LA ENCRIPTACIÓN

Proyecto del Trabajo de Grado para optar al título de
INGENIERO EN COMPUTACIÓN

Autor:
Deiskel Villegas
C.I:26.899.744
Tutor:
Ing. Oneida Jiménez
C.I: 10.227.464

San Diego, septiembre de 2022

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 seguridad para una aplicación de mensajería basado en la encriptación.

Realizado por el (la) Br. Deiskel Villegas

C.I. Nº 26.899744 cursante de la carrera de Ingeniería en 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: 20 ptos.

APROBADO ☒ **NO APROBADO** ☐

El Jurado

Tutor Académico (Coordinador)
Nombre: Oneida Jimenez
C.I.: 10227464

Jurado
Nombre: José Saavedra
C.I.: 15217919

Jurado
Nombre: Manuel Trejo
C.I.: 14315776

Fecha: 01/03/2023

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

CONSTANCIA DE APROBACIÓN PARA LA PRESENTACIÓN PÚBLICA DEL TRABAJO DE GRADO

Quien suscribe, Ing. Oneida Jiménez, portador de la cédula de identidad N° V-10.227.464, en mi carácter de tutor del trabajo de grado presentado por el ciudadano Deiskel Villegas, portador de la cédula de identidad N° V-26.899.744, titulado **SISTEMA DE SEGURIDAD PARA UNA APLICACIÓN DE MENSAJERÍA BASADO EN LA ENCRIPTACIÓN,** presentado como requisito parcial para optar al título de Ingeniero de Computación, 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 08 días del mes de febrero del año dos mil veintitrés.

Ing. Oneida Jiménez
C.I: 10.227.464

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA

FI C 002 2022-2CR TG

Valencia, 18 de enero de 2023

Ciudadano:
VILLEGAS MICHELENA, DEISKEL GATRIEL
26.899.744
Presente -

Cumplo con informarle que la comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **N° 10-2022** de fecha **12/09/2022** aprobó el proyecto de grado titulado:

Sistema de seguridad para una aplicación de mensajería basado en la encriptación.

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:
Ing. Oneida Emilia Jiménez de Peralta, titular de la cédula de identidad V-10.227.464

Atentamente

Facultad de Ingeniería
UJAP
DECANATO

Dra. Laura Aurora Sáenz Palencia
Decana de la Facultad de Ingeniería

c.c. Coordinación de Pasantías y Trabajo de Grado de la Facultad de Ingeniería

ÍNDICE GENERAL

ANEXOS

LISTA DE CUADROS

LISTA DE GRÁFICOS

LISTA DE TABLAS

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

SISTEMA DE SEGURIDAD PARA UNA APLICACIÓN DE MENSAJERÍA WEB BASADO EN LA ENCRIPTACIÓN

Autor: Deiskel Villegas
Tutor: Ing. Oneida Jiménez
Fecha: septiembre 2022

RESUMEN INFORMATIVO

El siguiente trabajo de grado enfatiza en los problemas de seguridad en la información de los usuarios en las aplicaciones de mensajería instantánea, proponiendo el desarrollo de un sistema de seguridad basado en la encriptación de los mensajes de la aplicación antes mencionada. La investigación se denota como proyecto especial acompañada de una investigación de campo, con un nivel de investigación descriptivo, la Población corresponde a todos los consumidores de aplicaciones de mensajería instantánea, siendo la muestra 10 de estos consumidores, se elige como técnica de recolección de datos la encuesta. El proyecto será desarrollado utilizando utilizando la metodología XP y los lenguajes de programación: Go, JavaScript, HTML (Hyper Text Markup Language), CSS (Cascading StyleSheet), Nodejs, Frameworks: Reactjs y postgresSQL para la base de datos. Las líneas de investigación vinculadas al siguiente trabajo son: Desarrollo de nuevas tecnologías de la información y comunicación de la Universidad José Antonio Páez de la Facultad de Ingeniería de la Escuela de Computación.

Descriptores: Sistema de seguridad de la información, Aplicación, Interfaz gráfica.

INTRODUCCIÓN

La tecnología con el pasar del tiempo se ha hecho de uso cotidiano para la persona, hoy en día tenemos en nubes guardada toda nuestra información personal, que van desde imágenes hasta claves de cuentas bancarias. Aunque es algo bueno y no ha ayudado a facilitarnos nuestro día a día, también los ciberdelitos, que no son más que ciberdelincuentes que buscan hacerse con toda nuestra información. Las personas no se dan cuenta que a diario están exponiendo su información privada a un peligro de que alguien más se las robe y sin ellos enterarse, desde entrar a un link de dudosa procedencia, a un ataque directo hecho a nuestros equipos tecnológicos de uso diario. La seguridad de la información es un tema que todos deberíamos tener en cuenta e informarnos cuál es la mejor manera de mantener segura toda nuestra información; estamos hablando que en cualquier momento podemos ser víctimas de un ataque cibernético, por la vulnerabilidad y la falta de un buen sistema de seguridad de la información en condiciones.

Este trabajo de grado, está enfocado en la creación de un sistema de seguridad en una aplicación de mensajería instantánea, que satisfaga las necesidades del usuario y les ofrezca la completa seguridad de que toda su información transmitida por este medio, está perfectamente segura, pero, ¿por qué? hoy en día, todas las personas usamos un servicio de mensajería instantánea (véase whatsapp, telegram, etc…) pero ¿quién se para a pensar si realmente toda nuestra información está realmente segura? Pasamos este tema por alto, pero no nos damos cuenta que por este medio, desde un “buenos días” hasta la “contraseña de una cuenta” que se envía por este medio, podría ser leído por una persona externa, exponiéndose a un ataque y dejando toda nuestra información al descubierto, si no tenemos un buen sistema de seguridad. Por todo esto, en dicho proyecto se busca encriptar mediante el cifrado cualquier mensaje enviado, de manera que, si una persona externa intenta robarnos nuestra información, no tendrá la capacidad de leer nuestra información, gracias a este método de protección, dejando así al usuario con la completa seguridad de que toda su información está completamente resguardada y libre de cualquier ataque. El descrito proyecto se encuentra dispuesto de la siguiente manera:

Capítulo I, El Problema: Referido a la descripción general del problema, justificación, objetivos de la investigación, incluyendo objetivos específicos y el alcance de la investigación.

Capítulo II, Marco Teórico: Comprende el marco teórico de la investigación, los antecedentes más influyentes, las bases teóricas, las bases legales y los términos básicos que sustentan la investigación.

Capítulo III, Marco Metodológico: Contiene la descripción de la metodología que regirá el desarrollo del proyecto, además de establecer los métodos de recolección de información a emplear y las fases metodológicas.

Capítulo IV, Resultados: Describe los recursos empleados a lo largo de la investigación y desarrollo de la aplicación.

CAPÍTULO I

EL PROBLEMA

1.1 Planteamiento Del Problema

La seguridad de la información digital se ha vuelto indispensable, debido a que todo el mundo hace uso de aplicaciones web, digitales, de mensajería o redes sociales. Debido a esto, los constantes ataques cibernéticos han ido en aumento, donde se centran en robar la información de los usuarios, dejando su privacidad al descubierto, pudiendo de esta manera conseguir datos personales, que ponen en riesgo la integridad de los usuarios. Debido a la gran importancia que ha cobrado la Seguridad de la Información, los usuarios requieren de un sistema capacitado, que puedan proteger toda su información, dándole la seguridad por medio de esta aplicación, podrá estar completamente protegido de estos ciberataques.

Hoy en día las aplicaciones de mensajería de texto abundan en el mercado, pero, así como abundan, son muy pocas las que ofrecen realmente un sistema de seguridad óptimo a los usuarios, dejándolos así a merced de los ataques cibernéticos. Estos usuarios no se dan cuenta, y regularmente en las mensajerías suelen pasar información privada, ya puede ser una conversación privada, o podría ser los datos de una cuenta bancaria; al no tener un sistema de seguridad en condiciones hace muy fácil robar toda esta información, incluso hay aplicaciones que por sí mismas son las que roban este tipo de información.

Los ataques cibernéticos se clasificaron como el quinto riesgo más alto en 2021 y se convirtieron en el nuevo estándar para los sectores público y privado. Esta industria de alto riesgo seguirá creciendo en 2022, ya que se espera que los ataques cibernéticos de IoT (Internet of Things) se dupliquen para 2025. Según el fbi existen más de 400 ciberataques por día a organizaciones en Estados Unidos, esto no incluye a individuos ya que es casi imposible realizar unas estadísticas sobre estos ataques, ya que cada segundo hay una nueva víctima,

En base a lo anteriormente descrito, y con el fin de solucionar estos problemas, en este trabajo de grado, se propone la creación de un sistema de seguridad para un sistema de mensajería, capaz de encriptar todos y cada uno de los mensajes enviados, dando la seguridad a los usuarios,

de que sólo el emisor-receptor es capaz de leer estos mensajes, evitando así el robo de información mediante ciberataques.

1.2 Formulación Del Problema

¿Cómo solucionar los problemas de privacidad, seguridad y filtración de información personal de los usuarios en aplicaciones web de mensajería?

1.3 Objetivos De La Investigación

1.3.1 Objetivo general:

- Desarrollar un sistema de seguridad para una aplicación de mensajería de texto basado en la encriptación de extremo a extremo.

1.3.2 Objetivos específicos:

- Recolectar información sobre la problemática, las necesidades y el sistema actual para poder cubrir los principios básicos de la seguridad informática.
- Identificar los requerimientos funcionales y no funcionales del programa, los cuales proyectarán las necesidades reales esperadas y las características operacionales requeridas de forma que este cumpla su función de manera efectiva y eficiente.
- Diseñar el sistema de seguridad junto a la aplicación de mensajería, considerando los requerimientos de la aplicación.
- Construir la aplicación y realizar pruebas de verificación del correcto funcionamiento a través de la prueba, para corregir posibles errores.

1.4 Justificación De La Investigación

Como ya sabemos, a día de hoy, una vida sin las aplicaciones de mensajería es inimaginable; se utilizan en todo momento, para todo tipo de usos, ya sea de ponerse en contacto con una persona en específico, para hacerles llegar información o simplemente para saludarlos. Por eso, los usuarios buscan tener la mayor seguridad posible, de su privacidad y de su confidencialidad. La información es el factor primordial por el cual muchos usuarios malintencionados cometen actos ilícitos, usando métodos que muchos de nosotros no podemos ni imaginarnos.

La presente investigación surge de la necesidad de dotar de seguridad, confidencialidad e integridad de las personas al usar una aplicación de mensajería, con el propósito de mantener su información segura en todo momento, ya que la mayoría de las personas no están conscientes que siempre están a merced de un ataques cibernéticos, de hecho, muchas personas no se pueden llegar

ni a imaginar que les pueden llegar a robar información mediante estas aplicaciones, por ello con esta aplicación lo que se busca es entregar la total seguridad de todos los usuarios de su información.

1.5 Alcance

La aplicación abarca el área pertinente a una aplicación de mensajería, enfocándose más en el sistema de seguridad de todos los datos personales, dándole la seguridad al usuario de que cada uno de sus mensajes serán cifrados de extremo a extremo, manteniendo su privacidad segura. La interfaz es simple de comprender para cualquier persona, desde niños hasta personas mayores.

1.6 Limitaciones

Este sistema web será desarrollado en la Universidad José Antonio Páez y podrá ser implementado en cualquier empresa en general, el tiempo de desarrollo se ajustará a lo estipulado en el cronograma de actividades abarcando el noveno y décimo semestre. El proyecto se limitará únicamente a la fase de construcción y de prueba.

CAPÍTULO II

MARCO TEÓRICO

En este capítulo, se detallan, describen y dan a conocer los aspectos teóricos y antecedentes relacionados con la investigación, con el objetivo de proporcionar una base fundamentada, esperando que su estructura lógica y consistencia interna permita el análisis de los hechos conocidos, así como orientar la búsqueda de otros datos relevantes.

En este sentido, Palella y Martins (2012), afirman que el marco teórico es el soporte principal del estudio, en el que se amplía la descripción del problema, pues permite integrar la teoría con la investigación y establecer su interrelación. Representa un sistema coordinado, coherente de conceptos y propósitos para abordar el problema (p.55).

2.1 Antecedentes De La Investigación

Existen experiencias de investigación mundial con documentación que se relaciona específicamente en los temas de seguridad de algoritmos de encriptación. Luego de revisar diferentes teorías y documentos que indican los riesgos y amenazas que representan los ataques realizados por los intrusos, delincuentes cibernéticos, vulgarmente conocidos como “hackers”; se revisaron diferentes documentos relacionados con la seguridad de la información, con el fin de tomar los aspectos más resaltantes que presentaban estas y que contribuyeron a la realización de esta investigación. A continuación, hablaremos de los antecedentes que se relaciona con lo que se ha investigado:

Keyly Ortiz (2022) En su investigación "**Seguridad en el uso de aplicaciones de mensajería instantánea de comunicación interna**" se orienta en los peligros existentes de las instrucciones en la red, en la seguridad del sistema y de las personas. La gran motivación de esta investigación es ayudar a la minimización de los riesgos a los ataques de los recursos de una red de ordenadores cuyo objetivo principal de esta tesis fue desarrollar las mejoras a un sistema en la seguridad de la información y se basaba especialmente en el modelado de los mensajes que permiten intercambiar por medio de un protocolo de comunicaciones.

Se denomina a este sistema como SSM (del inglés, Structural Stochastic Model),utiliza el modelo de Markov, representa las cargas más útiles que permiten asociarlas a los protocolos que

se basan en el paso de los mensajes. El cual relatan que fue un éxito en la detección de los ataques que se basan en la web, esta información se obtuvo por los resultados por este sistema que el investigador se motivó en la indagación de potenciales modificaciones que se orientan a mejorar sus prestaciones para operar en espacios tales como los servicios de la web en explotación.

Las muchas propuestas mostradas son eficazmente evaluadas y los resultados son cotejados con los que se logran mediante el sistema SSM original, verificando una mejora en las prestaciones del sistema de descubrimiento de intrusos.

Moya, (2015) En su tesis doctoral en la Pontificia Universidad Católica del Ecuador, para optar por el título de ing. en sistemas. "**Proceso una aplicación para la encriptación de los datos en la transmisión de la información de un aplicativo de mensajes en la web"** Cuyo objetivo principal fue desarrollar una aplicación para la encriptación de la información en la web. En esta investigación el escritor en mención ha aplicado las herramientas en su totalidad durante el trabajo desarrollado, utilizó la metodología SCRUM, pues con este método todos los entregables son más pequeños, pudiéndose revisar habitualmente y permitiendo más efectividad en la identificación de los errores y los cambios. El método Scrum se direcciona específicamente en la transmisión de productos en menor cantidad en la calidad del código Xtreme Programming (XP); esta metodología no parte de cero, sino que se va adaptando a nuestras preferencias, se utiliza también herramientas existentes de ser necesario. En esta investigación se probó múltiples herramientas como ya es conocido el Dreamweaver, HyperText Markup Language, es decir, Lenguaje de Marcas de Hipertexto (HTML), Hypertext Pre-Processor que significa Lenguaje de Programación Interpretado (PHP), Active Server Pages (ASP), NET, Visual Studio y los gestores de bases de datos como son: Microsoft Lenguaje Estructurado de Consultas (SQL) Server, MySQL, Postgre SQL, que permitió la realización de los cambios, al finallograron su objetivo.

En esta indagación podemos visualizar un claro ejemplo de la vulnerabilidad de los datos en estos tiempos. Esto ha permitido que hoy en día tengan mayor auge en la investigación e implementación de muchos modelos de encriptación de datos, cuya finalidad es asegurar la privacidad cuando se intercambia la información. Esta averiguación aborda la protección de datos y a la vez proporciona información sobre el trabajo de encriptación de algunos algoritmos.

Ing. Simón Cifre (2020) En su tesis en la Universidad Tecnológica Nacional para optar por la maestría. **"Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas".** Cuyo objetivo principal fue la realización de un estudio comparativo de soluciones de

encriptación a la seguridad de los datos con la finalidad de ser utilizada en los métodos de Auditaje Organizacional. Aquí el investigador ha realizado una comparación de soluciones de encriptación a la seguridad de los datos, para que se entienda de una manera más clara esta investigación lo que permite es resguardar los datos utilizando diferentes formas de encriptación que se tiene para cifrar los datos, sobre todo la contraseña del usuario lo que nos permite proteger los equipos, asimismo se realizó esta investigación para que las personas que tengan la intención en este tema experimenten la forma simple y rápida a valorar la importancia que son los datos, tanto para las pequeñas como para las grandes empresas y sobre todo tener en cuenta los procedimientos de seguridad que permitan alejar las visitas de los hackers. Es muy fácil la encriptación de nuestras contraseñas, para ello se utiliza softwares gratuitos que se encuentran en internet y debemos tener conocimiento que estas herramientas no son eficaces en la seguridad de los datos.

En este estudio de indagación se aprecia una investigación comparativa de diferentes tipos de algoritmos de encriptación y a la vez se puede determinar cuál es el más eficaz, así poder utilizar en las pequeñas o grandes empresas, se plantea el cifrado con mayor confiabilidad para dar seguridad a los datos de la organización.

En esta indagación podemos visualizar un claro ejemplo de la vulnerabilidad de los datos en estos tiempos. Esto ha permitido que hoy en día tengan mayor auge en la investigación e implementación de muchos modelos de encriptación de datos, cuya finalidad es asegurar la privacidad cuando se intercambia la información. Esta averiguación aborda la protección de datos y a la vez proporciona información sobre el trabajo de encriptación de algunos algoritmos.

2.2 Bases teóricas

Las bases teóricas corresponden a los fundamentos del trabajo de investigación, debido a que sobre estas es construido dicho trabajo. Así, con la finalidad de cumplir los objetivos planteados, es necesario conocer previamente algunos aspectos teóricos relacionados con las variables de estudio.

A continuación, se desarrollan los fundamentos teóricos de la investigación, según Arias (2016), “Las bases teóricas se refieren al desarrollo de los aspectos generales del tema, comprende un conjunto de conceptos y proposiciones que constituyen un punto de vista y enfoque determinado, dirigido a explicar el fenómeno o problema planteado”. Por lo tanto, se presentarán las bases teóricas que formaron parte del desarrollo de la investigación:

2.2.1 Seguridad de los datos

La seguridad de los datos es definida por Sharon Shea (2022) como: Es la práctica de salvaguardar la información digital del acceso no autorizado, la pérdida accidental, la divulgación y la modificación, la manipulación o la corrupción a lo largo de todo su ciclo de vida, desde la creación hasta la destrucción.

Esta práctica es clave para mantener la confidencialidad, integridad y disponibilidad de los datos de una organización. La confidencialidad se refiere a mantener los datos privados, la integridad para garantizar que los datos sean completos y confiables, y la disponibilidad para proporcionar acceso a entidades autorizadas.

Conocida colectivamente como la tríada de la CIA, si alguno de los tres componentes se ve comprometido, las empresas pueden enfrentar daños financieros y de reputación. La tríada de la CIA es la base sobre la que se construye una estrategia de seguridad de datos. Dicha estrategia debe abarcar políticas, tecnologías, controles y procedimientos que protejan los datos creados, recopilados, almacenados, recibidos y transmitidos por una empresa.

2.2.2 Encriptación

Según la misma Sharon Shea (2022) El cifrado "es el proceso de convertir texto plano legible en texto cifrado ilegible utilizando un algoritmo de cifrado o cifrado. Si se interceptan datos cifrados, es inútil, ya que no pueden ser leídos o descifrados por nadie que no tenga la clave de cifrado asociada."

En relación a lo previamente mencionado, podemos observar que es posible usar el proceso de encriptación, para encontrar una manera de asegurar que cualquier dato sea ilegible, haciendo posible mantener de una manera segura cualquier tipo de datos al que se le aplique este método; ya que al estar cada uno de los datos cifrados, es irrelevante si estos logran ser robados, no podrán ser leídos por ellos si no se hacen en su poder con la clave de cifrado.

2.2.3 Cifrado

Habiendo definido previamente lo que es la encriptación y la seguridad de datos, es posible ahondar más en el cifrado, ya que esto es lo que brinda la protección de los datos. Este proceso funciona mediante la traducción de un texto legible a una serie de caracteres sin una lógica aparente, conocido como ciphertext; al realizar el cifrado se entrega una clave especial para poder descifrar dicho texto, sin esta clave es imposible poder leer los datos que fueron cifrados anteriormente. La empresa multinacional IBM afirma:

> "Hay cantidades masivas de información confidencial administrada y almacenada en línea en la nube o en servidores conectados. El cifrado utiliza la ciberseguridad para defenderse de la fuerza bruta y los ciberataques, incluidos el malware y el ransomware. El cifrado de datos funciona asegurando los datos digitales transmitidos en la nube y los sistemas informáticos."

2.2.4 Sistemas de Información.

Vinculado al concepto, Montilva, (1999), describe lo siguiente; "un sistema de información es un sistema hombre máquina que procesa datos a fin de registrar los detalles originados por las transacciones que ocurren y las entidades que forman una 21 organización; y proporcionar información que facilite la ejecución de actividades, operaciones y funciones de una organización". (p.35).

2.2.4 Lenguaje de Programación

Es un lenguaje formal que, mediante una serie de instrucciones, le permite aun programador escribir un conjunto de órdenes, acciones consecutivas, datos y algoritmos para, de esa forma, crear programas que controlen el comportamiento físico y lógico de una máquina.

Mediante este lenguaje se comunican el programador y la máquina, permitiendo especificar, de forma precisa, aspectos como:

- Cuáles datos debe operar un software específico
- Cómo deben ser almacenados o transmitidos esos datos
- Las acciones que debe tomar el software depende de las circunstancias variables.

2.2.5 Tecnología de desarrollo

Python, es un lenguaje de programación interpretado cuya filosofía hace hincapié en una sintaxis que favorezca un código legible. Y define este como un lenguaje multiparadigma, debido a que soporta orientación a objetos, programación imperativa y en menor medida programación funcional. Es interpretado de tipo dinámico y multiplataforma.

Go, es un lenguaje de programación concurrente y compilado, desarrollado por los ingenieros de Google. Go vio la luz en el año 2009, esto hace a Go un lenguaje relativamente nuevo, pero que esto no nos engañe, Go es un lenguaje maduro, con el cual se han desarrollado miles de proyectos alrededor del mundo.

JavaScript, lenguaje ligero e interpretado, orientado a objetos con funciones de primera clase, más conocido como el lenguaje de script para páginas web, pero también usado en muchos

entornos sin navegador. Es un lenguaje script 27 multiparadigma, basado en prototipos, dinámico, soporta estilos de programación funcional, orientada a objetos e imperativa. (Mozilla Developer Network, 2015) El estándar de JavaScript es ECMAScript. Desde el 2012, todos los navegadores modernos soportan completamente ECMAScript 5.1. Los navegadores más antiguos soportan por lo menos ECMAScript 3.

Typescript, es un superset de JavaScript. Decimos que una tecnología es un superset de un lenguaje de programación, cuando puede ejecutar programas de la tecnología, Typescript en este caso, y del lenguaje del que es el superset, JavaScript en este mismo ejemplo. En resumen, esto significa que los programas de JavaScript son programas válidos de TypeScript, a pesar de que TypeScript sea otro lenguaje de programación.

2.2.6 Base de Datos

Una base de datos es definida como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

Características de una Base de Datos

- Independencia lógica y física de los datos.
- Redundancia mínima.
- Acceso concurrente por múltiples usuarios.
- Integridad de datos.
- Consultas complejas optimizadas.
- Seguridad de acceso y auditoría.
- Respaldo y recuperación.
- Acceso a través de lenguajes de programación estándar.

2.2.7 Framework

Framework sirve para escribir código o desarrollar una aplicación de manera más sencilla. Es algo que permite una mejor organización y control de todo el código elaborado, así como una posible reutilización en el futuro. Debido a esto, garantiza una mayor productividad que los métodos más convencionales y una minimización del coste al agilizar las horas de trabajo volcadas en el desarrollo. Este sistema plantea varias ventajas para los programadores, ya que automatiza muchos procesos y además facilita el conjunto de la programación. Es útil, por ejemplo, para evitar el tener que repetir código para realizar funciones habituales en un rango de herramientas, como

puede ser el acceder a bases de datos o realizar llamadas a Internet. Todas estas tareas son las que se realizan de forma mucho más fácil cuando se trabaja dentro de un framework.

2.2.8 Metodología XP

Según Sutherland, J y Ken, S (2013) indican que el Extreme Programming es una de varios populares procesos ágiles. Ya se ha demostrado ser muy exitoso en muchas empresas de todos los tamaños y sectores a nivel mundial. Extreme Programming es exitoso porque hace hincapié en la satisfacción del cliente. En vez de entregar todo lo que pueda desear en una fecha lejana en el futuro este proceso proporciona el software que necesita cuando lo necesite. Extreme Programming permite a los desarrolladores responder con seguridad a las cambiantes necesidades de los clientes, incluso tarde en el ciclo de vida.

Las fases de la metodología XP son:

- **Primera Fase**: Planificación del Proyecto.
- **Segunda Fase**: Diseño.
- **Tercera Fase:** Codificación.
- **Cuarta Fase:** Pruebas.

2.3 Bases Legales

Las bases legales de esta investigación se encuentran representadas, en primer lugar, en la **Constitución de la República Bolivariana de Venezuela (1999)**, en los artículos 98, 103, 108, 110. Seguidamente, en la **Ley Orgánica de Ciencia, Tecnología e Innovación (2014)**, artículos 2 y 21. **Ley especial contra los delitos informáticos.** Gaceta Oficial N° 37.313 del 30 de octubre de 2001, artículo 1. Además, en la **Ley sobre el derecho de autor.** Gaceta Oficial N° 4.638 Extraordinario de fecha 1 de octubre de 1993, Sección Primera de las obras del ingeniero, artículos 1, 2, 3 y 17. Luego, en la sección quinta de los programas informáticos artículo 17. Finalmente, en la **Ley sobre mensajes de datos y firmas electrónicas,** artículos 1, 4, 9, 16.

2.4 Definiciones de Términos Básicos

Automatización: Es el conjunto de elementos o procesos informáticos, mecánicos y electromecánicos que operan con mínima o nula intervención del ser humano. Estos normalmente se utilizan para optimizar y mejorar el funcionamiento de una planta industrial, pero igualmente puede utilizarse la automatización en un estadio, una granja o hasta en la propia infraestructura de las ciudades.

Información: Es un recurso que otorga significado o sentido a la realidad, ya que, mediante códigos y conjuntos de datos, da origen a los modelos de pensamiento humano.

Interfaces: Se utilizan para nombrar a la conexión física y funcional entre dos sistemas o dispositivos de cualquier tipo dado una comunicación entre distintos niveles.

Programa informático: Es una secuencia de instrucciones escritas para realizar una tarea específica en una computadora. Este dispositivo requiere programas para funcionar, por lo general, ejecutando las instrucciones del programa en un procesador central.

Procesos: Conjunto de actividades mutuamente relacionadas o que al interactuar transforman elementos de entradas y los conviertes en resultados.

Software: Es el soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Usuario: Es una persona que utiliza una computadora o un servicio de red. Los usuarios de sistemas informáticos y productos de software generalmente carecen de la experiencia técnica necesaria para comprender completamente cómo funcionan.

Aplicación de mensajería: La **mensajería instantánea** es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados ya sea a una red como *Internet*, o datos móviles sin importar la distancia que exista entre los dos dispositivos conectados.

CAPÍTULO III

MARCO METODOLÓGICO

De acuerdo a, Palella & Martins (2012, pág. 79), el marco metodológico es "una guía procedimental, producto de la reflexión, que provee pautas lógicas generales pertinentes para desarrollar y coordinar operaciones destinadas a la consecución de objetivos intelectuales". De esta forma, en el presente capítulo se procederá a desarrollar el tipo de la investigación, la descripción del diseño de estudio en detalle, además de la población y muestra de estudio, las técnicas e instrumentos para la recolección de datos y análisis de resultados.

3.1 Tipo de Investigación

En relación al problema planteado y a los objetivos a alcanzar, la investigación en cuestión es de tipo especial. Según el Manual de Normas de Trabajo de Grado de la Universidad José Antonio Páez, un proyecto especial es definido como "Son trabajos que conllevan a la creación de objetos tangibles, para ser usados como solución a problemas, intereses o necesidades demostradas". La presente investigación busca solucionar la problemática diagnosticada a través del desarrollo e implementación de un sistema de seguridad para la protección de los datos de los usuarios de una aplicación de mensajería, para ello se dispondrá de las variables involucradas en esta actividad.

3.2 Diseño de la investigación

El diseño de la investigación presentado en este trabajo es uno híbrido entre campo y documental. Según Arias (2016) define una investigación de campo como: "Aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental." También el mismo Arias (2006) define que la que investigación documental como: "la investigación documental es un proceso basado en la búsqueda, recuperación, análisis, críticas e interpretación de datos secundarios, es decir los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas". Por su parte, Cazares (2000), "La investigación documental depende fundamentalmente de la información que se recoge o

consulta en documentos, entendiéndose este término, como todo material de índole permanente, es decir, al que puede acudir como fuente o referencia en cualquier momento o lugar.

Después de revisar las distintas posturas metodológicas de varios autores, se llegó a la conclusión de que lo mejor para esta investigación sería una combinación de la investigación de campo y la investigación documental, debido a la necesidad constante de recolectar datos constantes de la problemática, pero también se hará basada en la documentación relacionada con esta misma.

3.3 Nivel de la investigación

El nivel de investigación se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio. La presente investigación es de tipo descriptivo, ya que es necesario desarrollar la descripción, registro y análisis de todos los individuos y hechos con el fin de entender la estructura de su comportamiento, Arias (2016) indica que:

> "La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere." (pág.24).

Este tipo de investigación está relacionado con la presente investigación debido a que está basada en las condiciones reales del manejo de los sistemas de seguridad de la información.

3.4 Población y Muestra

3.4.1 Población

Palella y Martins (2012), definen la población de la siguiente manera: "es el conjunto de unidades de las que se desea obtener información y sobre las que se van a generar conclusiones. (p.105)". De acuerdo a esto, la población de la presente investigación de campo corresponde a todos los individuos, que se encarguen de la creación y mantenimiento de los sistemas de seguridad, especialmente, los especialistas, así como los usuarios que hagan uso del sistema de seguridad planteado en este trabajo de investigación.

3.4.2 Muestra

Como destaca Arias (2016), la muestra "es un subconjunto representativo y finito que se extrae de la población accesible". Para fines concretos de esta investigación, la muestra corresponde al área de la seguridad informática, con distintos ingenieros en esta misma área, así como los usuarios que hagan uso del sistema de seguridad previamente nombrado.

3.5 Técnicas e instrumentos de recolección de datos

Arias (2016) define un instrumento de recolección de datos como: “Cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información.” En cuanto a la técnica, Según Zapata (2006), las técnicas de observación “son procedimientos que utiliza el investigador para presenciar directamente el fenómeno que estudia sin actuar sobre él, esto es, sin modificar o realizar cualquier tipo de operación que permita manipular”. En concordancia Balestrini (2002) considera que la técnica de observación documental es como un “punto de partida en el análisis de las fuentes documentales, mediante una lectura general de los textos, se iniciará la búsqueda y observación de los hechos presentes en los materiales escritos consultados que son de interés para la investigación.

En la presente investigación, con el fin de recolectar la información necesaria para cumplir con el desarrollo de la misma, serán empleadas las siguientes técnicas e instrumentos de recolección de datos: Cuestionario estructurado, observación directa y el análisis documental, puesto que los datos recolectados serán mediante documentos, páginas webs, trabajos de investigación, etc. haciendo un análisis documental de cada uno de ellos.

3.5.1 Observación directa

En relación a lo antes mencionado, la observación directa es definida por Arias (2016) como:

> “La observación es una técnica que consiste en visualizar o captar mediante la vista, en forma sistemática, cualquier hecho, fenómeno o situación que se produzca en la naturaleza o en la sociedad, en función de unos objetivos de investigación preestablecidos. " (pág.69).

3.5.2 Análisis documental

Con el fin de obtener una base de conocimiento respecto a la información a recolectar se emplea la revisión documental, definida por Hurtado (2010) como:

> “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” (pág. 427)

3.5.3 Encuesta estructurada

Se utilizará la técnica de la encuesta para recabar la información de manera estructurada y dicotómica de forma cerrada, para su óptimo procesamiento, definida por Según Tamayo y Tamayo (2008) como:

> "la encuesta "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". (p. 24)

3.6 Técnicas de análisis de resultados

Posteriormente a la recolección de datos realizada a través de las técnicas e instrumentos mencionados, se procederá a la digitalización de los mismos con la finalidad de organizarlos en función de los objetivos de la investigación. De esta forma, junto con el cumplimiento de las fases metodológicas establecidas, efectuar los pasos necesarios para cumplir con los requisitos funcionales y no funcionales del sistema. Los resultados obtenidos se presentarán mediante gráficos donde será posible, visualizando las interfaces y código de la aplicación, corroborar la satisfacción de los requisitos planteados en la presente investigación.

3.7 Validación de instrumento

Según Pérez y Martines (2008). "En la investigación con enfoque cuantitativo, el instrumento se constituye en un elemento para la recolección de información, este, permite medir las variables las cuales surgen de los objetivos y el marco teórico. Para lograr lo anterior, estadísticamente se recomienda que las preguntas y, en general, el instrumento deba contar con validez de constructo, de confiabilidad y de contenido. Lo anterior, garantiza que los instrumentos empleados en investigaciones con enfoque cuantitativo cuenten con validez, de tal forma que la información obtenida, realmente sea veraz y coherente con lo medido".

Para este proyecto, que, por medio de una encuesta se cuantificó cada una de las respuestas en un valor porcentual que permitirá ayudar a medir las variables a tomar en cuenta, validar la información de la problemática planteada y el cual fueron validadas por un total de tres expertos en el área de la ingeniería, ya que, debido que existen múltiples factores difíciles de controlar que pueden influir la fiabilidad de una pregunta, se necesitará una correcta validación del instrumento.

3.8 Confiabilidad del instrumento

Para Hernández, Fernández y Baptista (2003). “La confiabilidad de un instrumento de medición es medida a través de diferentes técnicas que buscan la aplicación repetida al mismo objeto buscando resultados similares, con la finalidad de verificar si la información obtenida es confiable para obtener los objetivos planteados en la investigación”.

Para el trabajo de investigación que se presentará, se desarrolló la identificación del problema, a través, de una encuesta cuyas preguntas eran de aplicación repetidas o con un conjunto de sinónimos para tener el mismo resultado esperado y que la validez tenga coherencia para que genere el grado de confiabilidad necesario. A continuación, se presenta la fórmula para calcular la confiabilidad del instrumento por medio del coeficiente Kuder-Richardson.

Coeficiente de Kuder-Richardson:

$$r_{kr20} = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum pq}{\sigma^2}\right)$$

Donde:

K = Número de Ítems del instrumento

p= Porcentaje de personas que responde correctamente cada ítem.

q= Porcentaje de personas que responde incorrectamente cada ítem.

σ^2 = Varianza total del instrumento

Rangos para interpretar el coeficiente de confiabilidad de Kuder-Richardson

KR-20	*Interpretación*
0,9 - 1	*EXCELENTE*
0,8 - 0,9	*BUENA*
0,7 - 0,8	*ACEPTABLE*
0,6 - 0,7	*DEBIL*
0,5 - 0,6	*POBRE*
< 0,5	*INACEPTABLE*

Fuente: Villegas. (2023)

3.9 Fases metodológicas

El desarrollo de la aplicación se llevará a cabo a través del uso de la metodología de desarrollo de software Extreme Programming (XP). Como lo indican Sutherland y Ken (2013) "En XP se realiza el software que el cliente solicita y necesita, en el momento que lo precisa, alentando a los programadores a responder a los requerimientos cambiantes que plantea el cliente en cualquier momento". Esta metodología brinda las herramientas necesarias para llevar a cabo proyectos que necesiten de una buena interacción del equipo de desarrollo y el cliente, haciendo énfasis en la retroalimentación., siendo esta la principal razón por la cual será empleada.

- **FASE I: Recolección de información sobre la problemática, las necesidades y el sistema actual para poder cubrir los principios básicos de la seguridad informática.**

  Con el fin de diagnosticar las necesidad y problemas de almacenamiento y manejo de datos, se propone la aplicación de las técnicas e instrumentos de recolección de datos, siendo estas la observación directa y encuesta estructurada.

- **FASE II: Identificación de los requerimientos funcionales y no funcionales del sistema a desarrollar.**

  Posteriormente al desarrollo de la fase anterior, se procede a la identificación de los requerimientos funcionales y no funcionales del sistema con la información provista por los especialistas.

- **FASE III: Diseño de la aplicación haciendo uso de la metodología de desarrollo de software Programación Extrema.**

  En esta fase se procede al diseño inicial de la aplicación haciendo uso de los procedimientos establecidos en la metodología de desarrollo de software seleccionada.

- **FASE IV: Construcción de la aplicación y realización de las pruebas de usuario y seguridad.**

  Finalmente, con el fin de completar esta fase, se iniciará el proceso de creación del código el cual conformará la aplicación, a través de los lenguajes de programación denominados. Posteriormente, serán efectuadas las pruebas de funcionamiento conjuntamente con los especialistas, haciendo énfasis en la seguridad de la información privada almacenada en la aplicación.

CAPÍTULO IV

RESULTADOS

En el presente capítulo de la investigación, es necesario presentar operaciones en la fase de análisis e interpretación de los resultados, con el fin de obtener algún significado de los datos recolectados, con la intención de organizarlos y pretender dar respuesta al objetivo general trazado en este estudio, como lo señalan Hernández, Fernández y Batista (2009), “el propósito del análisis e interpretación de los resultados, es resumir las observaciones llevadas a cabo de forma que proporcionen respuestas a las interrogantes de la investigación”(p. 180).

Esta fase conformará los resultados obtenidos una vez aplicada y desarrollada la investigación, está contemplada por 5 fases las cuales explicarán detalladamente cada paso que se hizo para lograr el objetivo.

4.1 FASE I: Recolección de información sobre la problemática.

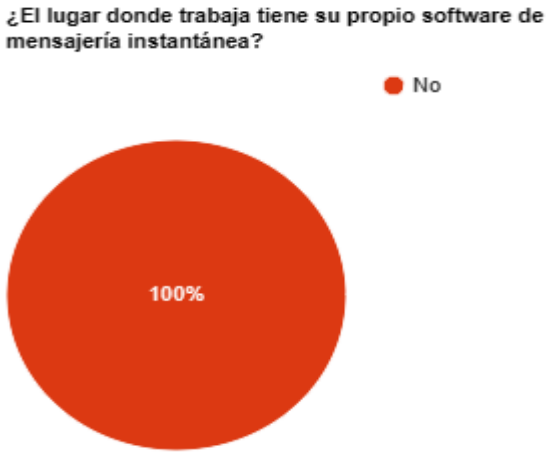
Con el fin de diagnosticar las necesidad y problemas de almacenamiento y manejo de datos, se propone la aplicación de las técnicas e instrumentos de recolección de datos, siendo estas la observación directa y encuesta estructurada a 10 personas.

Cuadro 1: Instrumento de recolección de datos pregunta 1.

Fuente: Villegas (2023).

Los resultados obtenidos en esta pregunta demostraron que el 100 por ciento de las personas encuestadas, hacen uso de aplicaciones de mensajería instantánea. Esto significa que tienen alguna experiencia previa o información respecto al tema, lo que indica que el personal antes descrito podrá utilizar el sistema de información con mayor facilidad.

Cuadro 2: Instrumento de recolección de datos pregunta 2.



Fuente: Villegas (2023).

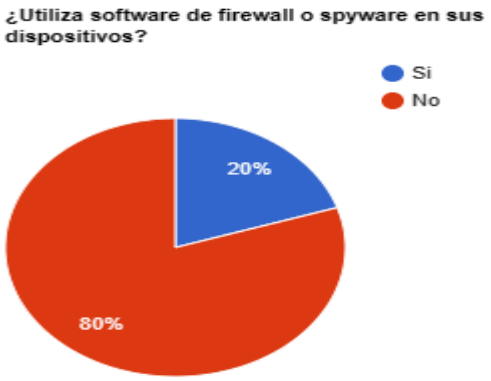
Con estos resultados obtenidos podemos evidenciar como la mayoría de personas y o empresas usan estas aplicaciones de externos, lo que nos deja en claro que es de baja probabilidad encontrar un entorno de trabajo donde creen su propia aplicación.

Cuadro 3: Instrumento de recolección de datos pregunta 3.

Fuente: Villegas (2023).

A pesar de que la mayoría de personas usa estas aplicaciones, al presentar esta pregunta podemos notar como un porcentaje alto no se asegura antes de darle uso a estas aplicaciones, si poseen un sistema de seguridad que sea capaz de proteger toda su información. Lo cual nos demuestra que hay un desconocimiento muy grande del peligro al que exponen toda su información privada a diario sin darse cuenta.

Cuadro 4: Instrumento de recolección de datos pregunta 4.



Fuente: Villegas (2023).

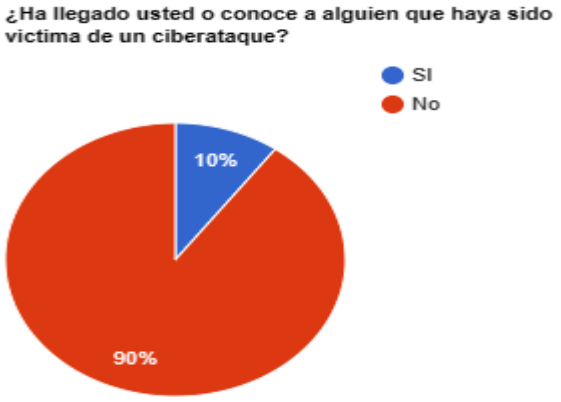
Con los resultados obtenidos lo que podemos notar, ya no es sólo que no se aseguran de que las aplicaciones que usan tengan un sistema de seguridad de seguridad, sino que tampoco se utilizan software de seguridad en los dispositivos que tienen, que permita proteger su información, en todo caso las aplicaciones no tengan el suyo propio.

Cuadro 5: Instrumento de recolección de datos pregunta 5.

Fuente: Villegas (2023).

La mayoría de las personas encuestadas no conocen lo que es el cifrado de la información ni la importancia que este tiene para proteger toda su información en estas aplicaciones de mensajería instantánea. No sólo en estas aplicaciones, en general podemos notar un poco o casi nulo conocimiento sobre el peligro que corren de ser víctimas de un ciberataque.

Cuadro 6: Instrumento de recolección de datos pregunta 6.



Fuente: Villegas (2023).

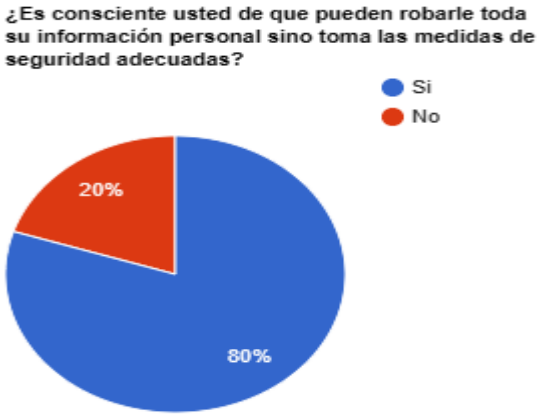
Acá lo que podemos notar, es que la mayoría de los encuestados hasta donde saben no han sido víctimas de un ciberataque, solo uno de los encuestados se dio cuenta en su momento que su información estaba siendo robada por una aplicación, por lo que podemos notar que el resto de personas si han sido víctimas de estos ciberataques no se percataron de ello.

Cuadro 7: Instrumento de recolección de datos pregunta 7.

Fuente: Villegas (2023).

Como podemos notar en esta pregunta, sólo la mitad de los encuestados son capaces de detectar un virus/malware en sus dispositivos, por lo cual serían incapaces de saber si su información está siendo robada, esta falta de conocimientos que hoy a día es esencial es lo que hace que tanta información sea tan fácil de robar por los ciberdelincuentes, ya que las personas no poseen el conocimiento general de cómo protegerse.

Cuadro 8: Instrumento de recolección de datos pregunta 8.



Fuente: Villegas (2023).

En esta pregunta se nota que la mayoría de las personas son conscientes de que su información puede ser robada, pero no buscan los medios para impedirlo, ni se aseguran de que estén usando un software que posea un sistema de seguridad capaz de proteger su información, uniéndose con las preguntas anteriormente propuestas.

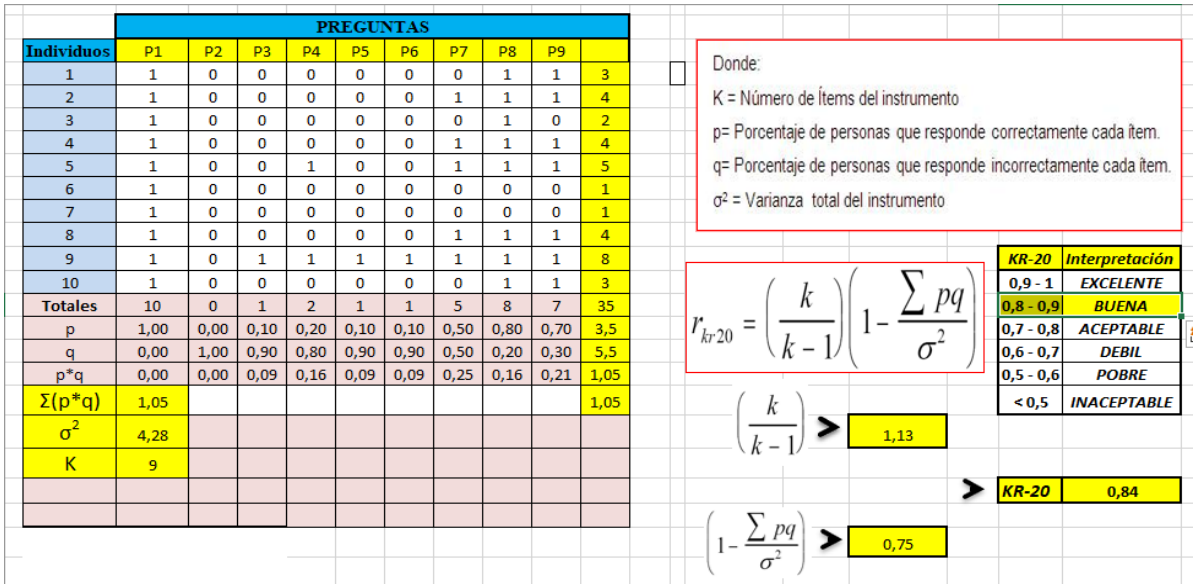
Cuadro 9: Instrumento de recolección de datos pregunta 9.

Fuente: Villegas (2023).

4.1.2. Coeficiente de Kuder-Richardson

En base a los resultados obtenidos mediante el instrumento de recolección de datos del tipo cuestionario de preguntas cerradas. Se obtuvo el siguiente coeficiente de Kuder-Richarsdon.

Gráfico 1: Coeficiente de Kuder-Richardson



	PREGUNTAS									
Individuos	P1	P2	P3	P4	P5	P6	P7	P8	P9	
1	1	0	0	0	0	0	0	1	1	3
2	1	0	0	0	0	0	1	1	1	4
3	1	0	0	0	0	0	0	1	0	2
4	1	0	0	0	0	0	1	1	1	4
5	1	0	0	1	0	0	1	1	1	5
6	1	0	0	0	0	0	0	0	0	1
7	1	0	0	0	0	0	0	0	0	1
8	1	0	0	0	0	0	1	1	1	4
9	1	0	1	1	1	1	1	1	1	8
10	1	0	0	0	0	0	0	1	1	3
Totales	10	0	1	2	1	1	5	8	7	35
p	1,00	0,00	0,10	0,20	0,10	0,10	0,50	0,80	0,70	3,5
q	0,00	1,00	0,90	0,80	0,90	0,90	0,50	0,20	0,30	5,5
p*q	0,00	0,00	0,09	0,16	0,09	0,09	0,25	0,16	0,21	1,05
Σ(p*q)	1,05									1,05
σ^2	4,28									
K	9									

Fuente: Villegas (2023).

4.2 Fase II: Determinación de los requerimientos funcionales y no funcionales del software.

4.2.1 Requerimientos

Se procedió a establecer los requerimientos funcionales y no funcionales del sistema, con el fin de obtener la funcionalidad ideal y una óptima experiencia de usuario.

4.2.1.1 Requerimientos funcionales

- **Registro:** se mostrará al usuario una pantalla de registro donde debe ser registrado proporcionando su información personal.
- **Iniciar sesión:** Los usuarios tendrán una sesión privada en la cual podrán realizar sus interacciones de manera segura.
- **Contactos:** El usuario podrá agregar, eliminar o ver una lista de sus contactos, y seleccionar aquel con el que quiere comenzar una conversación.
- **Conversaciones:** se podrá acceder a una lista de todas sus conversaciones, o borrarlas a elección del usuario.

- **Mensajes**: El sistema almacenará todos los mensajes de forma permanente hasta que el usuario decida eliminarlos.

4.2.1.2 Requerimientos no funcionales

- **Prueba de carga:** Se procede a testear el sistema con un flujo de datos estándard para evaluar su desempeño y estabilidad.
- **Estabilidad:** Se intenta llevar el sistema a punto de quiebre, realizando pruebas con un volumen de datos elevado para encontrar posibles mejoras de rendimiento.
- **Usabilidad:** Conjunto de pruebas controladas, para medir la curva de aprendizaje para utilizar el sistema.
- **Seguridad:** Se establecen los requerimientos de seguridad necesarios para el buen uso, como cifrado de datos y autenticación de inicio de sesión.
- **Escalabilidad:** Se definen los elementos que se pueden ir mejorando con el pasar del tiempo además de su nivel de complejidad, el sistema debe ser sencillo de actualizar y de soportar nuevas funcionalidades
- **Mantenibilidad:** Se establecen los plazos y tiempos de mantenimiento y soporte del sistema.
- **Respaldo de Datos:** Efectuar todas las validaciones necesarias y realizar copias de archivos para la preservación de la base de datos del sistema

4.3 **Fase III: Diseño de las bases del sistema de información administrativo mediante la metodología XP.**

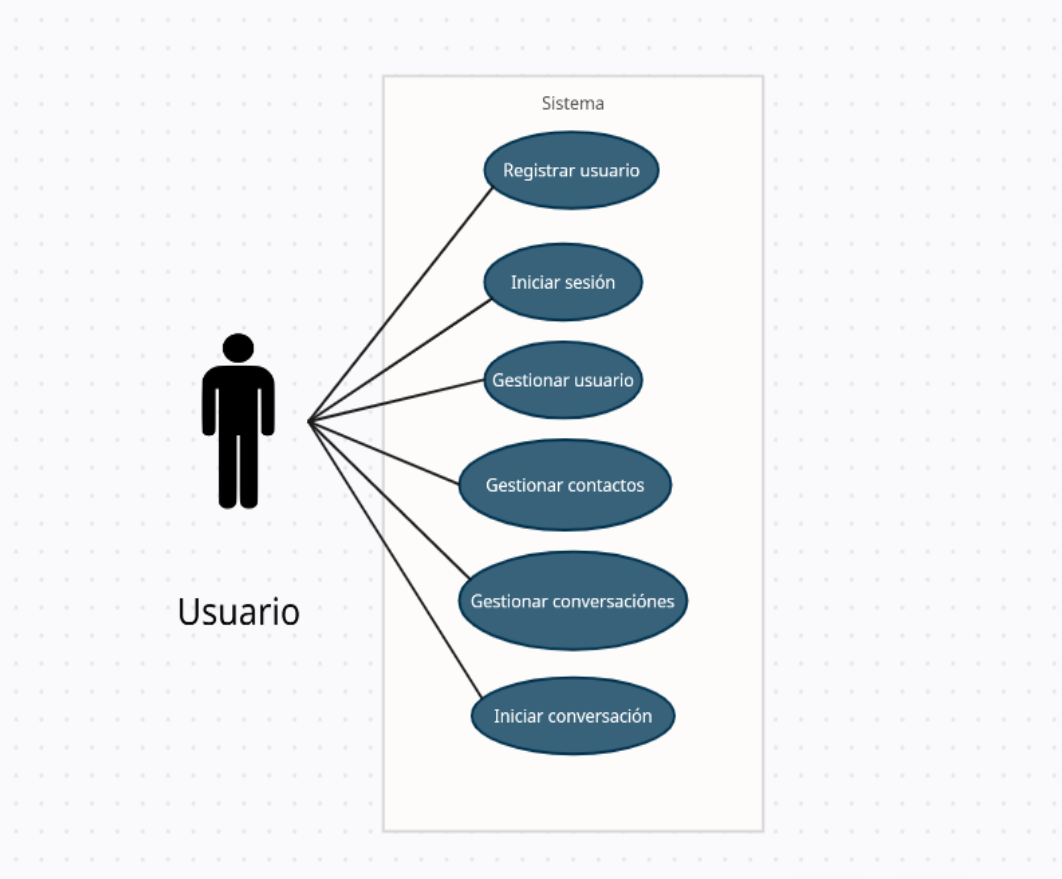
Con los datos obtenidos mediante la encuesta, la previa documentación y los requerimientos funcionales y no funcionales se procedió a establecer mediante diagramas las funciones y procedimientos que se realizan, haciendo uso de distintos métodos y herramientas que se utilizan para dar una referencia visual sobre cada caso de uso existente en la aplicación, así como también una estructura general que incluye también el modelado de la base de datos de tipo no relacional.

4.3.1 Diagrama de casos de uso

Esta herramienta se utilizará para definir los actores dentro de la aplicación, de igual manera las acciones o roles que tendrán dentro del sistema, además de la relación entre ellos. Cada caso de uso indica un objetivo sencillo y funcionalidades con las que el usuario va a interactuar.

4.3.1.1 Diagrama de caso de uso

Gráfico 1. Caso de uso usuario



Fuente: Villegas (2023).

El usuario es capaz de usar todas las operaciones disponibles de la plataforma, como gestionar su propio usuario, agregar o eliminar contactos, iniciar o eliminar conversaciones con sus contactos.

4.3.2 Descripción de los casos de uso

Tabla 1. Registro

Usuario: Registrarse
Actor: Usuario
Descripción: Registrarse en el sistema
Precondición: Haber ingresado a la vista principal del sistema

Flujo normal:	**Flujo alterno:**
1. Ingresar en el formulario 2. Rellenarlo con los datos solicitados 3. Hacer click en el botón registrar	1. Equivocarse al rellenar un dato 2. Tener un nombre de usuario que este previamente registrado

Fuente: Villegas (2023).

Tabla 2. Iniciar sesión

Usuario: Iniciar sesión	
Actor: Usuario	
Descripción: Iniciar sesión en el programa	
Precondición: Haberse registrado	
Flujo normal: 1. Ingresar en el formulario 2. Rellenarlo con los datos solicitados 3 Hacer click en el botón entrar	**Flujo alterno:** 1. Equivocarse al rellenar un dato. 2 No estar registrado 3 No se da acceso a la plataforma, hasta ingresar las credenciales correctas.

Fuente: Villegas (2023).

Tabla 3. Agregar contacto

Usuario: Agregar contacto	
Actor: Usuario	
Descripción: Agregar un contacto dentro del sistema	
Precondición: Haber ingresado a la vista principal del sistema	
Flujo normal: 1. Ingresar en el formulario	**Flujo alterno:** 1. Equivocarse al rellenar un dato

2. Rellenarlo con los datos solicitados 3. Hacer click en el botón agregar	2. Tener un nombre de usuario que no esté registrado

Fuente: Villegas (2023).

Tabla 4. Buscar contacto

Usuario: Buscar contacto	
Actor: Usuario	
Descripción: Buscar un contacto dentro del sistema	
Precondición: Haber agregado a un contacto anteriormente	
Flujo normal: 1. Ingresar en el formulario 2. Rellenarlo con los datos solicitados 3. Hacer clic en el botón buscar	**Flujo alterno:** 1. Equivocarse al rellenar un dato 2. Tener un nombre de usuario que no tengas agregado

Fuente: Villegas (2023).

Tabla 5. Iniciar conversación

Usuario: Iniciar conversación	
Actor: Usuario	
Descripción: Iniciar una conversación dentro del sistema	
Precondición: Haber buscado a un contacto anteriormente	
Flujo normal: 1. Hacer click en el contacto con el que iniciar la conversación 2. Enviar un mensaje	**Flujo alterno:** 1. No tener agregado ningún contacto

Fuente: Villegas (2023).

Tabla 6. Enviar mensaje

Usuario: Enviar mensaje	
Actor: Usuario	
Descripción: Enviar un mensaje en una conversación iniciada	
Precondición: Haber iniciado una conversación anteriormente	
Flujo normal: 1. Ingresar en la conversación 2. Rellenar con el mensaje a enviar 3. Hacer clic en el botón enviar	**Flujo alterno:** 1. No iniciar la conversación

Fuente: Villegas (2023).

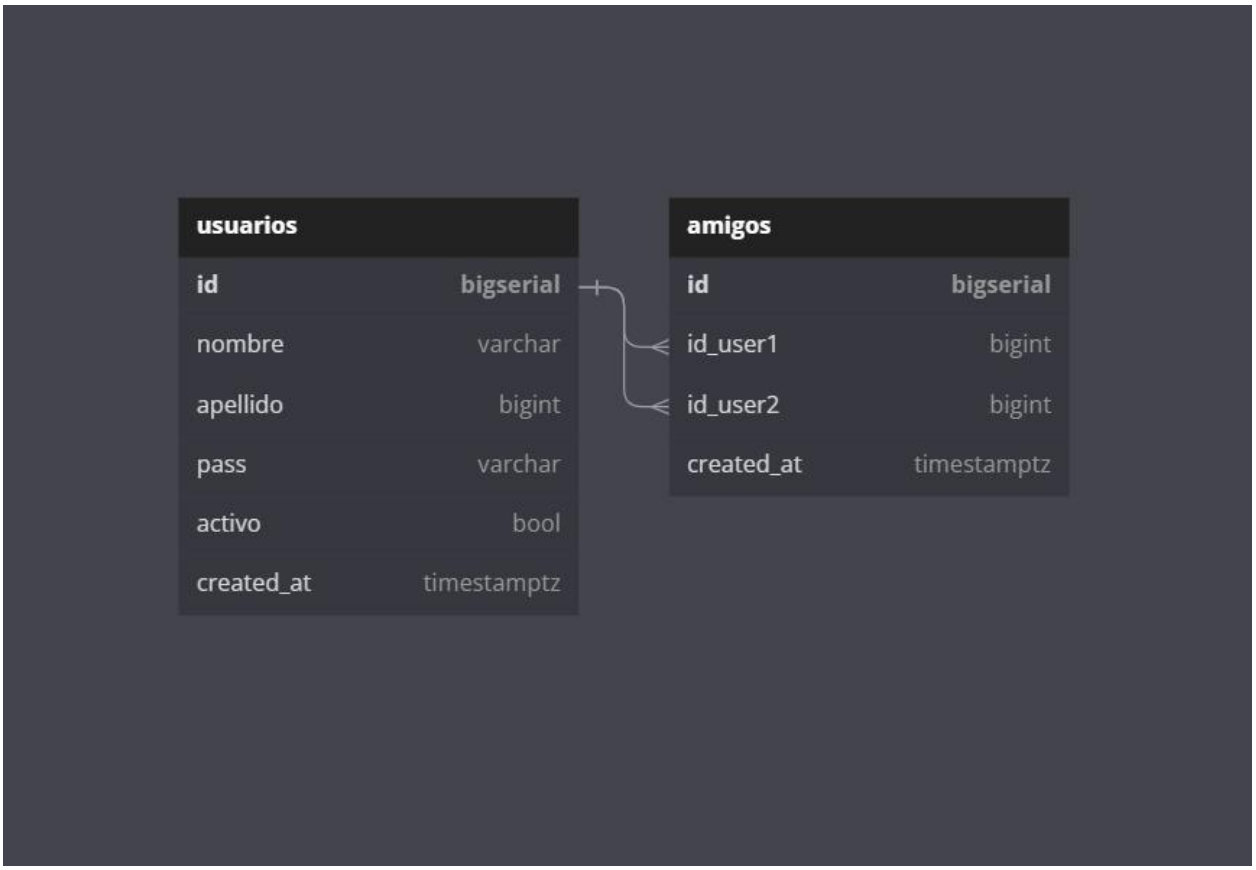
Tabla 7. Enviar imagen

Usuario: Enviar imagen	
Actor: Usuario	
Descripción: Enviar una imagen en una conversación iniciada	
Precondición: Haber iniciado una conversación anteriormente	
Flujo normal: 1. Ingresar en la conversación 2. Hacer click en el botón seleccionar imagen 3. Hacer clic en el botón enviar	**Flujo alterno:** 1. No iniciar la conversación 2. No escoger una imagen

Fuente: Villegas (2023).

4.3.3 Modelo de base de datos.

Gráfico 3: Diagrama de base de datos

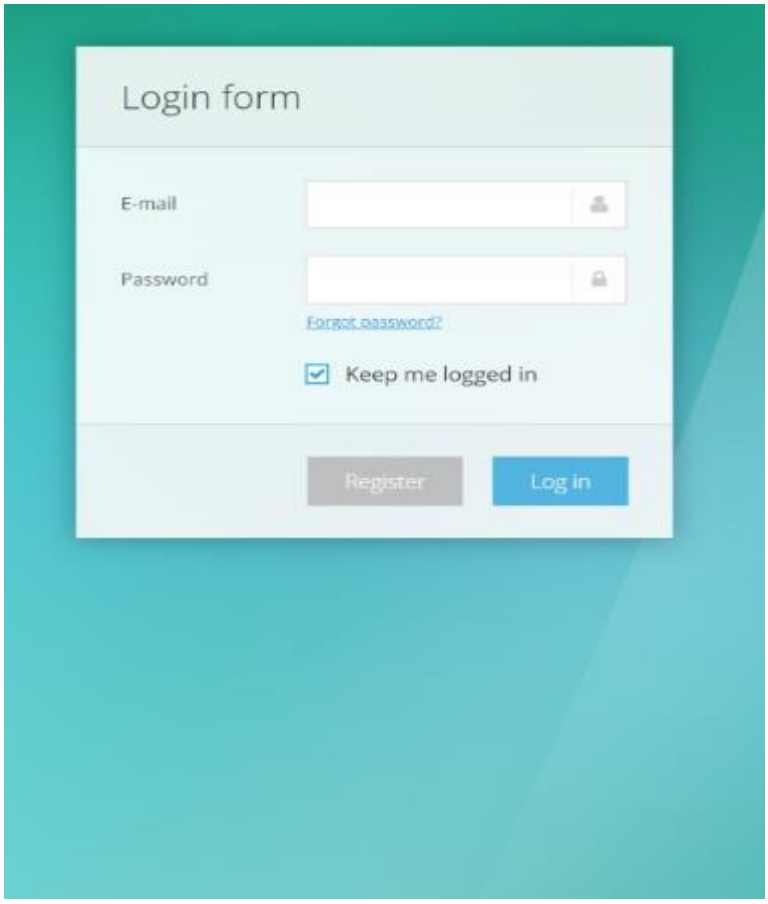


Fuente: Villegas (2023).

4.3.4 Diseño de interfaz y experiencia de usuario

Para el diseño de las interfaces se tuvo como objetivo ser una aplicación que visualmente sea cómoda de seguir. A continuación, se procedió a diseñar las vistas de la interfaz de usuario utilizando el lenguaje de marcas de hipertexto HTML, y el lenguaje de hojas de estilo en cascada CSS:

Gráfico 4. Formulario de inicio de sesión



Fuente: Villegas (2023).

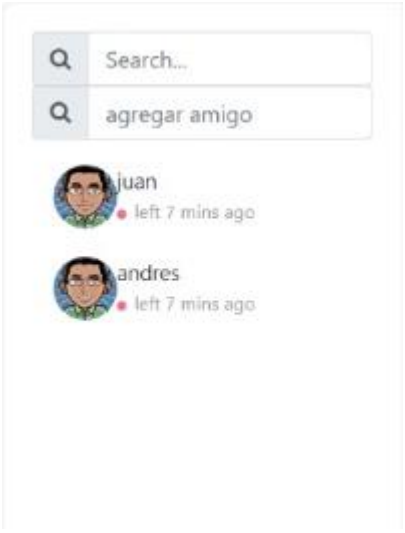
Los usuarios podrán entrar a sus perfiles individuales mediante este formulario, si un usuario está bloqueado le saldrá una alerta rechazando su acceso.

Gráfico 5. Registro

Fuente: Villegas (2023).

El presente formulario tiene como objetivo registrar a los nuevos usuarios que vayan a usar el sistema, todos los campos de registro son obligatorios.

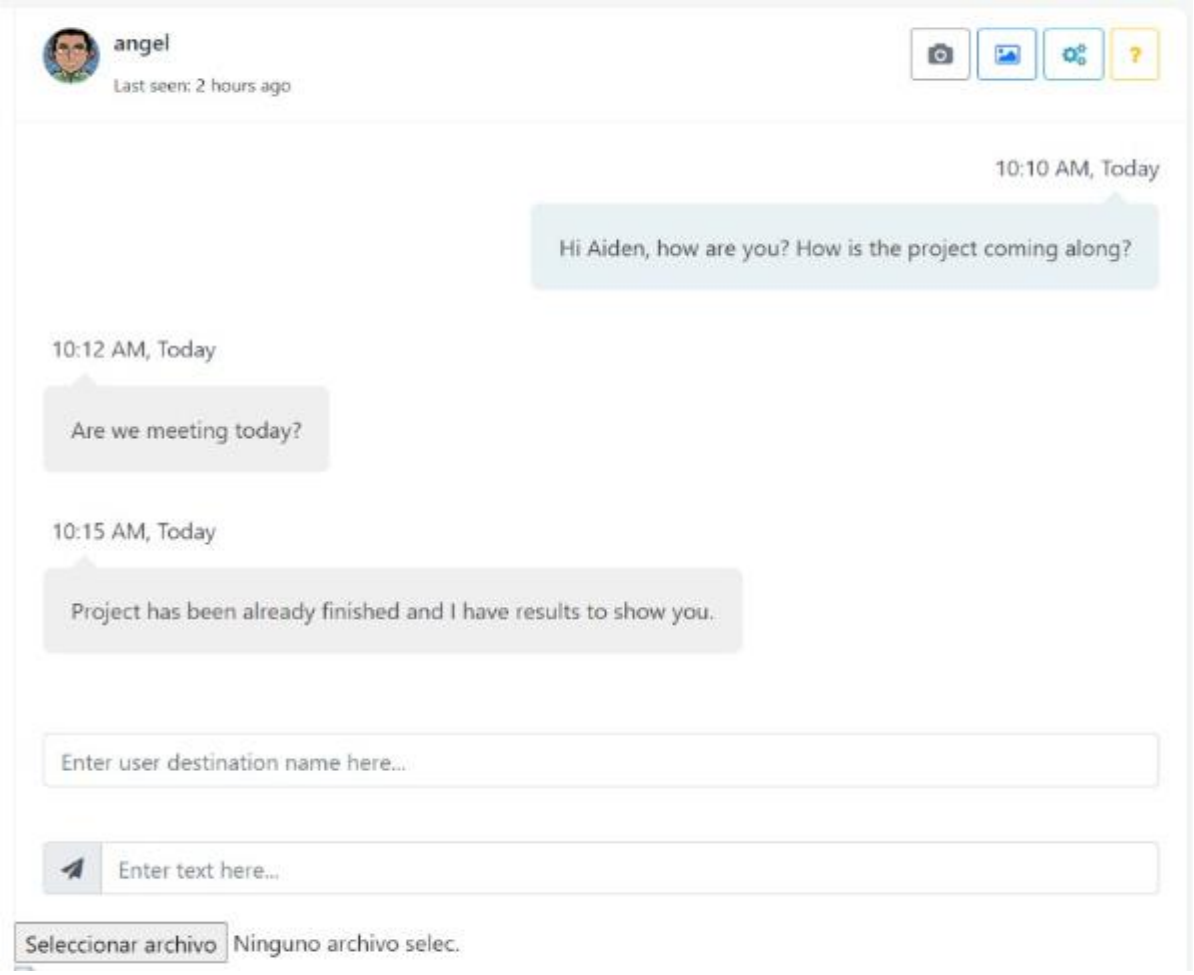
Gráfico 6. Agregar y buscar contactos



Fuente: Villegas. (2023)

En esta sección del sistema tenemos para agregar un usuario y buscar los que ya tengamos agregados para poder iniciar una conversación.

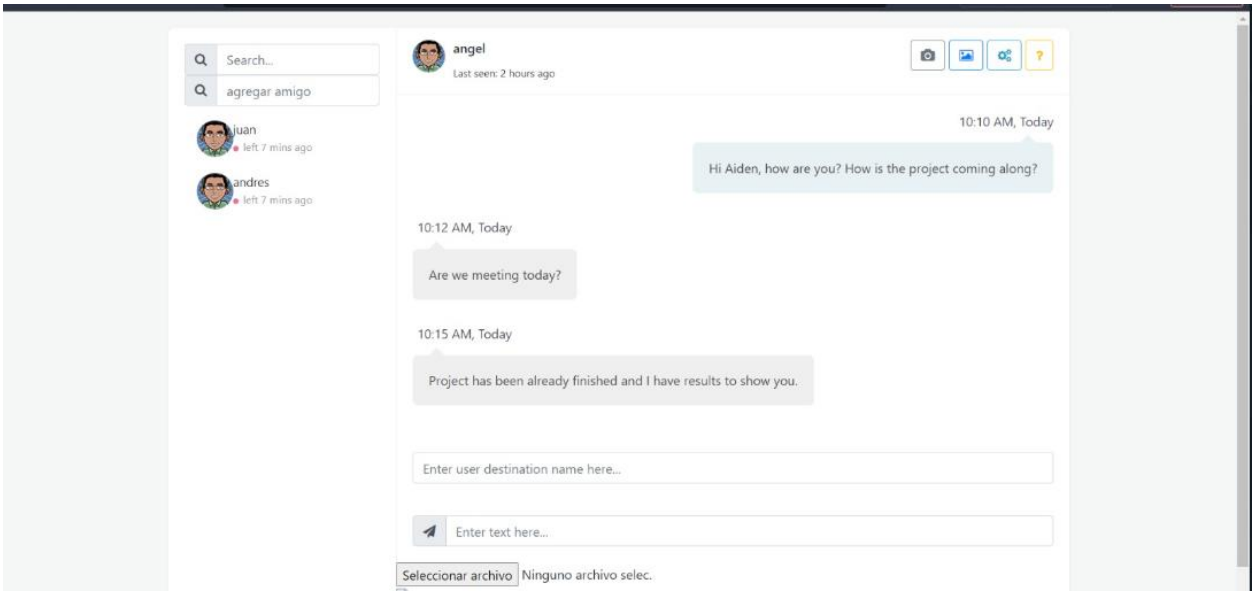
Gráfico 7. Conversación



Fuente: Villegas. (2023)

En este apartado podemos encontrar las conversaciones y todas sus funciones dentro de esta.

Gráfico 8. Vista principal del sistema



Fuente: Villegas. (2023)

Esta sería la vista principal completa del sistema, donde podemos encontrar todas las secciones mostradas anteriormente.

FASE IV: Construcción del sistema.

Se procedió a desarrollar la funcionalidad de cada uno de los diseños involucrados utilizando el lenguaje de uso general GO. Adicionalmente, para la base de datos se hizo uso del lenguaje de consulta estructurada SQL y para las interfaces de usuario se realizó mediante Node.js usando el framework de diseño de interfaces con el usuario React, además de Bootstrap junto con JavaScript.

Es importante mencionar que se realizó un trabajo en paralelo, es decir, que se desarrolló en conjunto de manera eficiente, pudiendo así escribir, modificar y probar en simultáneo, lo que es una gran ventaja para los tiempos tan cortos para la realización del proyecto, todo esto acorde a los modelos y requerimientos de cada etapa.

FASE V: Verificación de funcionalidad.

En esta última fase se realizaron pruebas de funcionamiento durante y después de culminado el software, esto con la finalidad de cerciorarse que tenga un eficaz funcionamiento tomando en consideración las observaciones y funcionalidades antes propuestas.

4.5.1 Pruebas de caja negra

Las pruebas de caja negra, se enfocan en los requerimientos funcionales del software, centrándose en lo que se espera de un módulo, es decir, intentan encontrar casos en que el módulo no se ajusta a su especificación. Por ello solo se limita a ingresar datos como entradas y estudiar las salidas, sin tomar en cuenta la estructura interna.

Tabla 8. Registro

Tabla 8. Registro y login de usuario

CASO DE PRUEBA		
Número de prueba **4**	**Caso de Uso**	Registro y login de usuario
	Estrategia	Prueba de caja negra
Descripción	Lograr registrarse e ingresar al sistema sin ningún tipo de conocimiento técnico del sistema	
Entradas	Rellenar el formulario de registro para luego entrar en el sistema	
Resultados Esperado	Se registró exitosamente y sus datos fueron indexados en la base de datos	
Resultado	Exitoso	
Observación	No se presentó ninguna dificultad en el registro y se logró acceder de manera satisfactoria en el sistema	

Fuente: Villegas. (2023)

Tabla 9. Agregar contacto

CASO DE PRUEBA		
	Caso de Uso	Agregar contacto para conversar

Número de prueba 4	**Estrategia**	Prueba de caja negra
Descripción	Lograr agregar un contacto exitosamente para poder iniciar una conversación	
Entradas	Rellenar el formulario de registro para luego entrar en el sistema	
Resultados Esperado	Se agregó el contacto exitosamente y sus datos fueron indexados en la base de datos	
Resultado	Exitoso	
Observación	No se presentó ninguna dificultad en agregar un contacto y se logró acceder a las conversaciones	

Fuente: Villegas. (2023)

Tabla 10. Iniciar conversación

CASO DE PRUEBA		
Número de prueba 4	**Caso de Uso**	Iniciar conversación con otro usuario
	Estrategia	Prueba de caja negra
Descripción	Lograr iniciar una conversación con otro usuario después de haberlo agregado	
Entradas	Iniciar la conversación para luego enviar un mensaje	
Resultados Esperado	Se logró iniciar exitosamente la conversación con otro usuario	

Resultado	Exitoso
Observación	No se presentó ninguna dificultad a la hora de iniciar la conversación y enviar un mensaje a otro usuario

Fuente: Villegas. (2023)

4.5.2 Pruebas de caja blanca.

Esta prueba se basa en analizar la estructura interna del código, analizando detalles que hacen énfasis a datos de entrada o salida, para probar la lógica del programa desde el punto de vista algorítmico.

Tabla 11. Iniciar conversación

CASO DE PRUEBA		
Número de prueba **4**	**Caso de Uso**	Registro y login de usuario
	Estrategia	Prueba de caja blanca
Descripción	El usuario desea registrarse en el sistema y verificar su correcta indexación en la base de datos.	
Entradas	Datos requeridos por el formulario de registro	
Resultados Esperado	Se registró exitosamente y sus datos fueron indexados en la base de datos	
Resultado	Exitoso	
Observación	Se comprueba la correcta integración de la interfaz de usuario con la base de datos	

Fuente: Villegas. (2023)

Tabla 12. Vulneración de login

CASO DE PRUEBA		
Numero de prueba 4	**Caso de Uso**	Intento de vulnerar el login
	Estrategia	Prueba de caja blanca
Descripción	El usuario desea ingresar al sistema sin los datos correspondientes	
Entradas	Datos de ingresos incorrectos, múltiples intentos de acceder al sistema	
Resultados Esperado	Se deniega el acceso al usuario y se muestra un mensaje en pantalla	
Resultado	Exitoso	
Observación	Se observa que el sistema cumple con los requerimientos de seguridad adecuados	

Fuente: Villegas. (2023)

Tabla 13. Buscador de contactos

CASO DE PRUEBA		
Número de prueba 4	**Caso de Uso**	Buscar contactos
	Estrategia	Prueba de caja blanca
Descripción	El usuario desea consultar los contactos agregados.	

Entradas	Nombre del contacto agregado.
Resultados **Esperado**	Muestra en pantalla el contacto consultado.
Resultado	Exitoso
Observación	Al ingresar el nombre de la consulta, se muestra la salida en menos de 1 segundo.

Fuente: Villegas. (2023)

CONCLUSIONES Y RECOMENDACIONES

Conclusiones.

Al examinar los resultados obtenidos en cada una de las fases descritas previamente, se llegó a una serie de desenlaces relacionados a los objetivos definidos en la presente investigación.

Primera fase: Análisis de la situación

Los resultados obtenidos expresan la necesidad de un sistema de seguridad para la información del usuario, pues con la totalidad de los encuestados, se llegó a la conclusión de que la mayoría no tienen idea de cómo proteger su información debidamente, y aún más grave, ni siquiera están conscientes del peligro que corre toda su información en internet.

Segunda fase: Determinación de requerimientos funcionales, no funcionales y diseño del sistema.

Se especificaron los requerimientos del sistema, tanto funcionales como no funcionales. Se trató de escoger los requerimientos funcionales que más se adaptaran a las necesidades de los usuarios, en los no funcionales se hizo mucho énfasis que el sistema fuese intuitivo, seguro y fácil de usar con el fin de lograr una buena receptividad en los usuarios.

Tercera fase: Diseño de las bases del sistema de información administrativo mediante la metodología XP

En esta fase se diseñó el sistema de información, bajo el enfoque de la metodología XP. Mediante el cual se elaboraron todos los diagramas y tablas requeridas por las bases fundamentales en la ingeniería de software entre los cuales destacan el diagrama de base de datos, la representación y especificación de los casos de usos por roles de usuario y la arquitectura del sistema; por otra parte, se plantean y maquetan las bases del diseño que se implementó en la plataforma.

Cuarta fase: Construcción del sistema

Se implementó una interfaz llamativa estructurada con Node.js usando su framework React, estilizada con JavaScript y el funcionamiento necesario de los módulos de la aplicación, todo esto interconectado a una base de datos bajo el servidor y el manejador de base de datos MySQL, para así poder manejar la información de una forma segura y cumplir con los requerimientos mencionados. También se debe codificar un código back-end robusto y validado. Se escogió el lenguaje de GO porque permite integrar un código fuente limpio y seguro.

Quinta fase: Verificación de funcionalidad

Es esencial realizar pruebas a un sistema informático antes de su lanzamiento para verificar su funcionalidad y estabilidad, por lo tanto, se procedió a realizar los dos tipos de pruebas más comunes en el mundo del desarrollo de software que son las pruebas de caja blanca y caja negra. Se obtuvieron resultados positivos durante la fase de pruebas, finalizando en un sistema confiable y robusto.

Recomendación

Las aplicaciones de mensajería instantánea abundan hoy en día, por lo cual cualquier usuario podrá usar este software sin dificultades, la problemática es que la mayoría de usuarios al usar estas aplicaciones no realizan una breve investigación de si estos sistemas protegen su información correctamente, por eso se buscó ofrecer un buen sistema de seguridad donde el usuario pueda estar completamente seguro de que toda su información será protegida adecuadamente.

En este contexto, en vista de que los sistemas de software están en constante evolución, y los ciberdelincuentes también lo están, siempre buscando nuevas maneras de vulnerar los sistemas de seguridad, se deberían realizar actualizaciones y modificaciones al sistema de seguridad acorde a la evolución y a nuevas mejoras que salgan de estos sistemas.

REFERENCIAS

Aguirre, J. (2006). Seguridad Informàtica y criptografìa. [Sitio en internet.] Disponible en: http://www.criptored.upm.es/crypt4you/temas/criptografiaclasica/leccion1.html

Aidong, F., & Zhiwei , Z. (2018). Research on Parallel Dynamic Encryption Transmission Algorithm on VoIP . China: University, Suzhou. [Sitio en internet.]

Arias F (2016). **El Proyecto de Investigación.** [Sitio en internet]. Disponible en: https://idoc.pub/documents/el-proyecto-de-investigacion-fidias-arias-7ma-edic-2016pdf-klzzm8k2r7lg

Constitución de la República Bolivariana de Venezuela (1999). [Sitio en internet]. Disponible en: http://www.minci.gob.ve/wp-content/uploads/2011/04/CONSTITUCION.pdf

ESET Security Report. (2018). Cifrado de la información. [Sitio en internet.] Disponible en: http://www. esetla.com/centro-amenazas/descarga/Latinoamerica- 2018/

Fernández, M. (2009). Mensajería Instantánea en Internet. Argentina: Creative Commons. [Sitio en internet.]

Garcia, J. (2011). Tipos de ataques informáticos. [Sitio en internet.] Disponible en: http://www.delitosinformaticos.com/seguridad/clasificacion.shtml

Giner De La Fuente F (2004). **Los Sistemas de Información en la Sociedad del Conocimiento**. [Sitio en internet]. Disponible en: https://books.google.com.pe/books?id=94sv48wCJAMC&printsec=frontcover&dq=%20giner,&hl=es419&sa=X&ei=i4hhVdvkEsTZgTnICYAQ&ved=0CBwQ6AEwAA#v=onepage&q=giner%2C&f=true

Hurtado J (2010). **Metodología de la Investigación.** [Sitio en internet.] Disponible en: http://emarketingandresearch.com/wp-content/uploads/2020/09/kupdf.com_j-hurtado-de-barrera-metodologia-de-investigacioacuten-completo-1.pdf

Moya, J. (2015). ECB Cifrado. Desarrollo de una aplicación para encriptar infromación en la transmisión de datos en un aplicativo web. Quito, Pichincha, Ecuador: PUCE. [Sitio en internet.]

Sharon Shea (2022). What is data security? The ultimate guide. [Sitio en internet.] Disponible **en: What is Data Security? The Ultimate Guide (techtarget.com)**

Simón Cifre (2020). **"Modelo de seguridad para la gestión de vulnerabilidades de servidores en Nubes privadas"** [Sitio en internet.] Disponible en: Tesis de Maestría - Cifre Simón.pdf (utn.edu.ar)

Sutherland J, Ken S (2013). **Extreme Programming: A Gentle Introduction.** [Sitio en internet]. Disponible en: http://www.extremeprogramming.org

Universidad José Antonio Páez (2020). **Manual para la elaboración y presentación de los anteproyectos, proyectos de grado, trabajos de grado, tesis doctorales e informe de pasantía y extramuros de la Universidad José Antonio Páez.** Carabobo-Venezuela.

Universidad José Antonio Páez (2020). **Manual para la elaboración y presentación de los anteproyectos, proyectos de grado, trabajos de grado, tesis doctorales e informe de pasantía y extramuros de la Universidad José Antonio Páez.** Carabobo-Venezuela.

ANEXOS

ANEXO A: INSTRUMENTO DE VALIDACIÓN

ÍTEM	Congruencia		Claridad		Redacción		Observaciones
	SI	NO	SI	NO	SI	NO	
1	X		X		X		
2	X		X		X		
3	X		X		X		
4	X		X		X		
5	X		X		X		
6	X		X		X		
7	X		X		X		
8	X		X		X		
9	X		X		X		
10							
11							

Nro.	Aspectos Generales	SI	NO	Observaciones
1	El instrumento posee instrucciones a seguir por la persona consultada	X		
2	Los ítems permiten el logro de los objetivos relacionados con la investigación.	X		
3	Los ítems están presentados en una forma lógica secuencial.	X		
4	El número de ítems utilizados es suficiente para recoger la información.	X		

VALIDADO POR:
Nombre y Apellido del Experto: Ramon Ortega
Institución donde labora: Universidad José Antonio Páez
Nivel Académico: Magister Contable
Fecha de Validación: 09/2/23
Firma:

Condición de la Validación	
Aplicable	X
Aplicable atendiendo a las observaciones	
No aplicable	

ANEXO B: INSTRUMENTO DE VALIDACIÓN

ÍTEM	Congruencia		Claridad		Redacción		Observaciones
	SI	NO	SI	NO	SI	NO	
1	X		X		X		
2	X		X		X		
3	X		X		X		
4	X		X		X		
5	X		X		X		
6	X		X		X		
7	X		X		X		
8	X		X		X		
9	X		X		X		
10							
11							

Nro.	Aspectos Generales	SI	NO	Observaciones
1	El instrumento posee instrucciones a seguir por la persona consultada	X		
2	Los ítems permiten el logro de los objetivos relacionados con la investigación.	X		
3	Los ítems están presentados en una forma lógica secuencial.	X		
4	El número de ítems utilizados es suficiente para recoger la información.	X		

VALIDADO POR:
Nombre y Apellido del Experto: Christopher Asp.
Institución donde labora: UNAP
Nivel Académico: Ing en Informatica
Fecha de Validación: 07/02/23
Firma:

Condición de la Validación	
Aplicable	X
Aplicable atendiendo a las observaciones	
No aplicable	

ANEXO C: INSTRUMENTO DE VALIDACIÓN

ITEM	Congruencia		Claridad		Redacción		Observaciones
	SI	NO	SI	NO	SI	NO	
1	X		X		X		
2	X		X		X		
3	X		X		X		
4	X		X		X		
5	X		X		X		
6	X		X		X		
7	X		X		X		
8							
9							
10							
11							

Nro.	Aspectos Generales	SI	NO	Observaciones
1	El instrumento posee instrucciones a seguir por la persona consultada	X		
2	Los ítems permiten el logro de los objetivos relacionados con la investigación.	X		
3	Los ítems están presentados en una forma lógica secuencial.	X		
4	El número de ítems utilizados es suficiente para recoger la información.	X		

VALIDADO POR:
Nombre y Apellido del Experto: José Saavedra
Institución donde labora: UAP
Nivel Académico: Ing. Computación
Fecha de Validación: 08/01/23 **Firma:**

Condición de la Validación	
Aplicable	X
Aplicable atendiendo a las observaciones	
No aplicable	

ANEXO D

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN COMPUTACIÓN

INSTRUMENTO DE RECOLECCIÓN DE DATOS

Instrucciones:

- Lea cuidadosamente cada pregunta antes de responder.
- Según sus consideraciones, responda cada pregunta con la mayor objetividad
- Seleccione sólo una respuesta para cada pregunta, (SI-NO).
- Para cada pregunta, marque con una **X** el recuadro que corresponda con su opinión.
- No existen respuestas buenas o malas, por lo cual agradecemos no dejar ninguna pregunta sin contestar.

N.º	Ítems	Alternativas	
		Si	No
1	**¿Ha usado o usa alguna aplicación de mensajería instantánea? (WhatsApp, Telegram, etc.)**		
2	**¿El lugar donde trabaja tiene su propio software de mensajería instantánea?**		
3	**¿Antes de usar una aplicación se asegura de que esta posea un sistema de seguridad informático?**		
4	**¿Utiliza software de firewall o spyware en sus dispositivos?**		
5	**¿Conoce usted en que consiste el cifrado de la información?**		
6	**¿Ha llegado usted o conoce a alguien que haya sido víctima de un ciberataque?**		
7	**¿Es capaz de reconocer un virus/malware en sus dispositivos?**		
8	**¿Es consciente usted de que pueden robarle toda su información personal si no toma las medidas de seguridad adecuadas?**		
9	**¿Conoce la importancia que tiene el que una aplicación posea un buen sistema de seguridad informática?**		