Fundación Universitaria
SAN MATEO

INGENIERÍA DE SISTEMAS

Diseño aplicativo móvil, enfocada en la confidencialidad y seguridad de datos personales

Trabajo de grado modalidad de opción de grado

David G. Urrego
Fundación Universitaria San Mateo
Ingeniería De Sistemas
Ingeniero William Mendoza Rodríguez
Noviembre 2020

NOTA DE SALVEDAD DE RESPONSABILIDAD INSTITUCIONAL

"La Fundación Universitaria San Mateo NO se hace responsable de los conceptos emitidos en el presente documento, el departamento de investigaciones velará por el rigor metodológico de la investigación".

Tabla de contenido

Índice De Figuras

Índice De Tablas

Dedicatoria

Dedico este proyecto de manera muy grata y con mucho cariño a mi madre Iraidys, cuyo esfuerzo a lo largo de su vida como protectora y guía, me ha permitido forjarme como una persona dedicada, responsable y luchadora; además, de convertirse para mí, en un ejemplo de persona íntegra y altruista. Ah ella le debo los logros que he tenido durante todo mi etapa educativa y personal, el ser la primera persona en creer en mí y apoyarme en los momentos de dificultad, me permitió continuar motivado. Le agradezco su tiempo y sacrificio invertido, todo enfocado para verme progresar, y ser una persona de provecho.

Mil gracias, Mamá.

A pesar de que puede sonar un poco egocéntrico, también me permito dedicarme este trabajo a mí, por continuar en los momentos difíciles, y no rendirme; el lograr una meta tan significativa, me llena de orgullo y gratitud hacia mí mismo. Todos los logros obtenidos y principalmente a las dificultades, me han hecho crecer como persona y principalmente en creer en mí.

Así mismo, desee agradecer a mi amiga Dania, cuya comprensión, apoyo incondicional, y palabras de ayuda, me llevaron al final de esta etapa, de una manera destacada; al convertirse en una confidente, donde su voz de aliento fue fundamental para llenarme de fortaleza y poder continuar, en este camino tan largo. Por enseñarme que debemos luchar, y que hay personas que están mirando nuestros pasos y debemos convertirnos en un ejemplo para ellos.

Por supuesto a mis familiares más cercanos, que me han demostraron su cariño y su preocupación por mí,

Y finalmente, pero no menos importantes a todas esas personas que fueron parte del camino de mi vida, y que, por algún motivo la vida nos separó, principalmente por

malentendidos, todas esas experiencias que me dejaron sean buenas o malas, me llevaron de algún modo a convertirme en la persona que soy y a crecer como persona.

Agradecimientos

Quiero mostrar mi gratitud a todos los que estuvieron presentes en la realización de este objetivo, de este sueño que es tan importante para mí, agradecer sus ayudas, sus palabras motivadoras, sus conocimientos, sus consejos y su dedicación para mi evolución, educación y a nivel personal.

Además, quiero agradecer a mi amiga Dania, quien de alguna manera se convirtió, en un punto fundamental en el desarrollo de este trabajo, en mis manos, las cuales me permitieron llegar de manera satisfactoria a la meta final.

Finalmente, pero no por eso menos importante agradezco especialmente a la base de todo, a mi madre, quien con sus consejos fue quien me impulsó y fue mi constante motivación, muchas gracias por su paciencia, comprensión, y sobre todo por su infinito amor.

¡Muchas gracias por todo!

Abreviaturas

Zettabytes (ZB):	Unidad de medida de almacenamiento de información, equivalente a 10^{21} bytes.
Millennials:	También conocida como generación Y, que corresponde a los nacidos entre la década de los 80´s y 2000.
USB o Pendrive:	Universal Serial Bus (Dispositivo de almacenamiento).
ISO:	International Organization for Standardization (Organización Internacional de Normalización).
Windows:	Sistema operativo desarrollado por Microsoft.
Linux:	Sistema operativo de código abierto.
MAC:	Sistema operativo de propiedad de Apple Inc.
Google Chrome:	Navegador desarrollado por Google LCC.
Microsoft Edge:	Navegador desarrollado por Microsoft.
Firefox:	Navegador de código libre.
Safari:	Navegador desarrollado por Apple Inc.
Opera:	Navegador desarrollado por Opera Software.
SO:	Sistema Operativo.
Smart Watch:	Reloj inteligente.
SGSI:	Sistema de Gestión de Seguridad de la Información.
Crackers:	Traducido como rompedor, se utiliza para referirse a personas que vulneran algún sistema de seguridad con intenciones maliciosas.
SMMLV:	Salario Mínimo Mensual Vigente.

DAFO o DOFA:	Matriz utilizada dentro de una empresa con el fin de identificar las debilidades, amenazas, fortalezas y oportunidades.
Stakeholders:	Referencia a una persona, organización o empresa, involucrados o interesados en un proyecto.
DATA:	Datos, información.
Nube:	Paradigma que permite ofrecer servicios de cómputo en la red.
SGCI:	Sistema de Gestión de Ciberseguridad Industrial.
CVSS:	Common Vulnerability Score System. Es un sistema de puntaje para estimar el impacto de las vulnerabilidades.
EPS:	Entidad promotora de salud.
Back-up:	Copia de seguridad de datos.
BA-CSIRT:	Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires (BA-CSIRT).
Malware:	Software malicioso.
CNN:	Cable News Network, canal televisivo estadounidense.
Nequi:	Aplicativo móvil (Neobanco) propietaria de Bancolombia.
SMS:	Short Message Service (servicio de mensajes cortos).
MySQL:	Gestor de base de datos desarrollada bajo licencia dual.
SQL Server:	Gestor de base de datos desarrollada por Microsoft.
Post-it:	Marca registrada de 3M Company, conocida popularmente como pequeñas hojas autoadhesivas.
App:	Del inglés application, tipo de programa informático diseñado como herramienta.

URL:	Uniform Resource Locator (localizador uniforme de recursos), dirección especifica de un recurso en la red.
E-mail:	Correo electrónico.
OAuth:	Open Authorization; estándar, abierto simple de autorizaciones.
API:	Application programming interhace; conjunto de funciones y procedimientos, que ofrece un servicio puntual para ser utilizado por otro software.
SDK:	Software development kit (kit de desarrollo de software).
IP:	Internet protocol; es un conjunto de números que identifica a un dispositivo digital dentro de una interfaz en la red.
WEP:	Wired Equivalent Privacy (privacidad equivalente a cableado).
WPA:	Wireless Protected Access (acceso Wi-Fi) protegido estándar para proteger las redes inalámbricas.
Activity:	Son las diversas interfaces que se encuentra en un aplicativa y la cual cumplen una actividad dentro de esta, de aquí su nombre.
.XML:	eXtensible Markup Language, (Lenguaje de Marcado Extensible).
Screenshot:	Captura de pantalla.
SQL:	(Structured Query Language), (lenguaje de consulta estructurada).
Check-list:	Lista de chequeo se estipulan los requerimientos, para tener un control de cumplimiento.
Fragments:	Función de Android Studio, Permite el ahorro de recursos para el funcionamiento del aplicativo.
Java:	Java es un lenguaje de programación orientado a objetos.

Kotlin:	Kotlin es un lenguaje de programación pragmático pensado para funcionar con Máquina Virtual de Java (JVM) y Android.
Flutter:	SDK de código fuente abierto de desarrollo de aplicaciones móviles creado por Google.
HTTP:	Hypertext Transfer Protocol, (Protocolo de transferencia de hipertexto).
GitHub:	Plataforma que permite alojar proyecto de software en la nube.
LAN:	Local Area Network, (Red de área local).
GSM:	Global System for Mobile communications (sistema global para las comunicaciones móviles).
GPRS:	General Packet Radio Service (servicio general de paquetes vía radio).
4G:	Cuarta generación en telecomunicaciones.
3G	Tercera generación en telecomunicaciones.
IOS:	Sistema operativo móvil desarrollado por Apple Inc.
RAM:	Random Access Memory (memoria de acceso aleatorio).
MongoDB:	Gestor de base de datos no relacional.
Cassandra:	Gestor de base de datos no relacional.
MariaDB:	Motor de base de datos relacional.
SGBD:	Sistema gestor de base datos.
SVG:	Scalable Vector Graphics (Gráficos vectoriales escalables).
MD5:	Message Digest Algorithm 5 (Algoritmo de Resumen del Mensaje 5).
SHA:	Secure Hash Algorithm (Algoritmo de Hash Seguro).
RSA:	Rivest, Shamir y Adleman.
DSA:	Digital Signature Algorithm (Algoritmo de Firma digital).

DES:	Data Encryption Standard (Estándar de cifrado de datos).
3DES:	Triple - Data Encryption Standard (Triple Estándar de cifrado de datos).
IDEA:	International Data Encryption Algorithm (Algoritmo internacional de cifrado de datos).
RC5:	Rivest Cipher (Cifrado de Rivest).
AES:	Advanced Encryption Algorithm (Estándar de cifrado avanzado).
DART:	Lenguaje de programación usado dentro del Framework Flutter.
POO:	Programación orientada a objetos.
C++:	Lenguaje de programación.
MVP:	Modelo – Vista – Presentador, arquitectura de software.
Framework:	Marco de trabajo, constituido por un grupo de herramientas.
Mockups:	Fotomontajes previos de una interfaz gráfica.
VPN:	Virtual Private Network (red privada virtual).
JSON:	JavaScript Object Notation.
HTML:	HyperText Markup Language (lenguaje de marcas de hipertexto).
JavaScript:	Lenguaje de programación.

Resumen

Palabras Clave:

En la presente investigación se realiza un análisis respecto a la viabilidad de diseñar un aplicativo móvil que otorgue la disponibilidad de administrar las contraseñas de los usuarios; por esta razón, se realizó una investigación documental permitiendo de este modo identificar los mejores métodos o herramientas respecto a la seguridad de la información para garantizar la integridad y confidencialidad; así mismo, se implementó una técnica de observación fortaleciendo de este modo los resultados obtenidos durante la primera fase.

Se explicarán las normas y leyes que están implementadas a nivel global y nacional (Colombia), respecto a la protección de datos; de este modo, certificar que los pilares de la seguridad informática se cumplan de manera general y destacada se encuentran: la norma ISO 27001, el Reglamento General de Protección de Datos (Unión Europea) y Habeas Data (Latinoamérica).

Los puntos para evaluar durante la investigación fueron generalmente los más usados en un aplicativo móvil: inicio de sesión, registro, almacenamiento. Igualmente, se indagó de manera más profunda respecto a la protección como tal de los datos, necesaria para los inicios de sesión (cifrado, autentificación, acceso remoto y generador de contraseñas).

En base en que se desea que los datos estén en la palma de la mano a través del aplicativo móvil, se logra identificar un método que permita la autentificación y acceso de manera segura eliminando drásticamente el uso de contraseña; de igual manera, se realizó la comparación de varios algoritmos de cifrado identificando el más acorde para salvaguardar los datos; de este modo, en caso de un ciberataque, dificultar el robo de la

información privada. Así mismo y como valor agregado, se identificó la factibilidad de iniciar sesión a las cuentas de usuario a través del mismo dispositivo móvil sin la necesidad de autocompletar el formulario para ingresar, dado que en muchos casos el permitirlo da hincapié a manipular la data.

No obstante, a través de la norma IEEE 830, se establecieron los requerimientos de manera general que podrán ser implementados en la etapa de desarrollo dentro del aplicativo en contexto a los resultados obtenidos durante la investigación.

Finalmente, luego de realizar una evaluación de diferentes arquitecturas y metodologías se establecieron las más acordes para efectuar la creación de la herramienta, a través de un análisis de desventajas y ventajas de cada una de ellas.

Abstract

Key Words:

In this research, an analysis is carried out on the viability of designing a mobile application that provides the availability to manage user passwords; For this reason, a documentary investigation was carried out, which made it possible to identify the best methods or tools about information security to guarantee integrity and confidentiality; Likewise, an observation technique is implemented, thus strengthening the results obtained during the first phase.

The norms and laws that are implemented worldwide and nationally (Colombia), regarding data protection will be explained; In this way, certify that the pillars of computer security are generally and prominently complied with: the ISO 27001 standard, the General Data Protection Regulation (European Union) and Habeas Data (Latin America).

The points to be evaluated during the investigation were generally those most used in a mobile application: login, registration, storage. Likewise, a more in-depth investigation was carried out regarding the protection as such of the data, necessary for the logins (encryption, authentication, remote access, and password generator).

Starting from the fact that you want the data to be in the palm of your hand through the mobile application, it is possible to identify a method that allows authentication and secure access, drastically eliminating the use of password; Likewise, a comparison of various encryption algorithms was carried out, identifying the most suitable ones to safeguard the data; therefore, in the event of a cyberattack, make it difficult to steal private information. Likewise, and as an added value, the feasibility of logging into user

accounts through the same mobile device without the need to auto-complete the login form was identified, since in many cases allowing it emphasizes the manipulation of data.

However, through the IEEE 830 standard, the requirements were established in a general way that can be implemented in the development stage within the application in context to the results obtained during the investigation.

Finally, after carrying out an evaluation of different architectures and methodologies, the most suitable ones were established to carry out the creation of the tool, through an analysis of the disadvantages and advantages of each one of them.

Introducción

La presente investigación se refiere a determinar la viabilidad de ofrecer a los usuarios un aplicativo móvil que permita gestionar las contraseñas junto con los datos (usuarios, correo electrónico y sitios web) para de esta manera evitar memorizarlas, y posteriormente realizar engorrosos procesos de recuperación de claves; por lo cual, se reducirán drásticamente los ciberataques.

La característica del aplicativo está basada bajo los pilares de la seguridad informática (confiabilidad, disponibilidad eh integridad), donde los usuarios tengan la certeza de que sus datos se encuentren de forma segura y permita un fácil acceso dado que la información estará disponible a la palma de su mano contando con los métodos de seguridad más eficientes disponibles en la actualidad. Además, determinar cómo valor agregado el inicio de sesión desde el mismo dispositivo junto con una extensión en los navegadores web; de igual manera, ofrecer la disponibilidad de visualizar las contraseñas sin necesidad de conexión alguna a una red; así mismo, otorgar un generador de password que cumpla con los estándares de seguridad (Farfán y Pérez, 2020).

Los usuarios en la red para acceder a sus cuentas generalmente optan por implementar contraseñas de baja seguridad como lo son: 12345, fechas de cumpleaños, número telefónico, número de identificación, entre otros; con el fin, de recordar fácilmente dicha información. Por este motivo es muy frecuente que el robo de información sea por medio del descifrado de contraseñas.

Existen actualmente herramientas que ofrecen un servicio similar al que se hace mención; no obstante, algunos de ellos implementan una prestación poco práctica y fiable, dificultando el ingreso dado a la baja disposición de la información y además que no cuentan con la privacidad

adecuada; del mismo modo, se han registrado casos de robo de datos en algunos de estos gestores de contraseñas de forma masiva.

El proceso de investigación se realizará por medio de la selección de diferentes fuentes de información donde se llevará a cabo una comparación de los métodos de protección enfocados al desarrollo móvil y web; igualmente, es necesario realizar la observación de las herramientas que manejan contenidos de suma importancia; de este modo, adaptamos los métodos de seguridad implementados en estas aplicaciones como base para fortalecer los sistemas de seguridad de la información.

Capítulo I

Descripción Del Proyecto

1.1. Presentación del problema de investigación

El aumento de la expansión de la internet en los últimos años a nivel mundial ha provocado que cada vez más exista un número de usuarios con acceso a esta tecnología, por consiguiente, esto ha provocado que se manejen grandes cantidades de información en diferentes sitios web, ya que si tenemos en cuanta cifras, podemos identificar que en el presente año (2020), más de la mitad de la población mundial tiene acceso a la internet, lo que equivale a un 59% de la población más específicamente a 4.540 millones de personas, a diferencia del año pasado que eran aproximadamente 4.388 millones. (Galeano, 2020).

Debido a este crecimiento la capacidad de almacenamiento de la información también ha venido en aumento, tanto así que se estima que durante el periodo 2018-2023 la capacidad de almacenamiento a nivel mundial alcance unos 11.7 zettabytes (ZB), en otras palabras, alcanzara un aumento mayor al doble actual. (Framingham, Mass;, 2019)

Por esta razón, las compañías están realizando grandes esfuerzos para poder proteger los datos de los usuarios, con el fin de evitar posibles ataques informáticos y por consiguiente el robo de información. Sin embargo, a pesar de los grandes esfuerzos, existen diferentes casos donde se han visto vulnerables los sistemas de seguridad de varias compañías, un ejemplo de esto muy conocido a nivel mundial fue el robo de datos privados de más de 75 millones de personas que poseían una cuenta de usuario dentro de la plataforma de Play Station Network (PSN), esto fue anunciado por la misma compañía SONY, donde informó que entre los datos que pudieron ser robados se encontraban desde: (números tarjetas de crédito, nombres, direcciones,

fecha de nacimiento, entre otros), el nivel de robo fue tan grande que fue considerado uno de los robos de información más grande de la historia. (BBC Mundo, Tecnología, 2011)

Para dar solución a esta dificultad, las grandes y pequeñas organizaciones, han reforzado sus protocolos de seguridad, con nuevos sistemas; aunque para los usuarios esto genera que, en ciertos métodos de recuperación de datos, se encuentren con procesos tediosos, donde en muchas ocasiones el usuario desista de continuar.

La complejidad de los usuarios en recordar sus datos de acceso a cuentas se ha incrementado debido a lo anteriormente mencionado, un mundo más digital, y un número más grande de personas con acceso a la internet; donde cada persona generalmente cuenta con más de un correo electrónico el cual, está asociado con más de un sitio web al momento de registrar una nueva cuenta de usuario. Teniendo en cuenta que para el acceso a las cuentas, se debe recordar la contraseña de acceso junto con su usuario o correo electrónico y que por ejemplo, un latinoamericano en promedio cuenta con nueve cuentas de solo redes sociales, podemos concluir que, el acceder a cada una de ellas, resulta ser un proceso en ocasiones complicado, debido a que se debe recordar diversas contraseñas para realizar la apertura de sesión; esta problemática puede venir en aumento debido a que los "Millennials" son las personas en la actualidad que poseen más cuentas en redes sociales con un promedio de 9.9 a nivel global (Coneo Rincón, 2020); esto quiere decir que las personas más jóvenes vienen con una tendencia a involucrarse más a las nuevas tecnologías.

Las medidas poco seguras que han optado los usuarios para no tener dificultades al tener acceso a sus cuentas se encuentran desde asignar contraseñas poco seguras como: (123456, 111111, número de cedula, número telefónico, fechas especiales, etc.), hasta de usar la misma contraseña en todas sus cuentas, permitiendo una vulnerabilidad más alta.

Por lo anteriormente explicado, se desea saber, ¿de qué manera se puede desarrollar una aplicación móvil, que permita a las personas tener sus datos de acceso a cuentas a la mano y que sea segura, permitiendo la implementación de un generador de contraseñas seguras?, evitando de esta manera posibles robos de información, y que el usuario tenga el poder de proteger sus datos como este lo desee.

1.2. Justificación

Una problemática muy común es la baja confidencialidad que tiene los datos más importantes y el olvido de estos por las personas; el usuario, contraseña, son información básica pero fundamental para el ingreso a un perfil personal dentro de un sitio web, pero frecuentemente descuidados; a pesar de la existencia de métodos que ayudan a esta problemática, no siempre resulta fácil el proceso de recuperación.

Por consiguiente, el hecho de que cada persona pueda tener control de estos datos, dentro de un aplicativo móvil ampliaría la seguridad, accesibilidad y aumentar la confidencialidad, además de facilitar el acceso de sus cuentas, sin engorrosos procesos de recuperación que, aunque estos procesos son altamente seguros, en ocasiones resulta tediosos.

El objetivo de querer almacenar la información personal antes mencionada dentro de un sistema Android en este caso, y más específicamente dentro de un dispositivo móvil es debido a que, los dispositivos móviles continúan con la tendencia de convertirse en un elemento fundamental para las personas, el uso de estos dispositivos varía entre diferentes aplicaciones como son: educativas, ocio, negocios, comunicación e incluso facilidades de pago de diferentes servicios, podemos notar lo enunciado previamente teniendo en cuenta que en el año 2017 existían 5.000 millones de usuarios que contaban con un dispositivo móvil, y se pronostica que para finales del año 2022 este número llegaría a 5.500 millones de usuarios, lo que equivale a un

71% de la totalidad de la población. El uso de dispositivos es tan alto, que esto ha generado que existan más terminales móviles que personas en el mundo, tanto así que para el 2022 los celulares alcanzaras un total aproximado de 12.000 millones. (Trendic, 2019)

Así mismo, una variable muy importante a tener en cuenta si gustes el alto número de páginas webs existentes dentro del ciberespacio, donde el incremento ha sido exponencial en las últimas décadas, más exactamente desde el año 2000, donde para inicios del milenio existían aproximadamente 17 millones de páginas web, a pesar de ser un número elevado, no se puede llegar a comparar con el número actual donde existen más de 1.797 millones de sitios (Núñez, 2019). En vista de lo anterior, se puede analizar que cada vez más son los datos que se deben manejar y por ende proteger, para facilitar el acceso al propietario, corroborando lo dicho en el punto anterior (Presentación del problema).

Teniendo en cuanta, que bajo la norma del *Habeas data, (Explicada más adelante),* donde toda persona, que se encuentre dentro de los países donde se rige esta acción jurisdiccional, tiene derecho a la confidencialidad de sus datos y el manejo de los mismos, como este lo crea necesario, se debe garantizar que sus datos se encuentren seguros pero a la vez sean de fácil acceso; sin embargo, existen casos donde muchas veces esta información es robada y usada sin ningún tipo de autorización; con lo explicado previamente podemos concluir que, en muchas ocasiones la información no es manejada de manera correcta, y que los nuevos sistemas de seguridad han provocado que la información sea cada vez más difícil de acceder especialmente para el propietario.

1.3. Objetivos

1.3.1. Objetivo General

Estudiar la posibilidad de diseñar un aplicativo móvil, que permita tener organizado, a la mano, y en confidencia, la información requerida para iniciar sesiones ya sea en dominios de correos electrónicos o sitios web, teniendo en cuenta almacenar los datos necesarios para ese proceso.

1.3.2. Objetivo Específicos

- Validar por medio de la investigación, la creación de la aplicación, que permita la confidencialidad de datos.
- Definir los requerimientos del sistema dependiendo de los resultados de la investigación, y la necesidad a suplir teniendo en cuenta, la definición del problema.
- Seleccionar una arquitectura, y metodología de software que más se ajuste al diseño del aplicativo móvil.

Capítulo 2

Marco Teórico

En el presente capítulo se describe diferentes conceptos que están vinculados con la seguridad de la informática en general, pero principalmente se puede conocer los esfuerzos que se están realizando para poder suplir la necesitad o problemática explicada previamente; igualmente se conoce que normas y leyes se han creado ya sea a nivel global y nacional, donde la principal entre todas ellas es conocida como la Norma ISO 27001.

2.1. Antecedentes de la investigación

Varias herramientas se han creado a lo largo de los últimos años con el objetivo de proporcionar accesibilidad de manera sencilla los datos a los usuarios, principalmente las contraseñas, una de las primeras organizaciones con esta idea la realizo la compañía LogMein donde con la herramienta LastPass brindó este servicio, su objetivo es que las personas puedan olvidarse de las contraseñas definitivamente, y todo sea accesible gracias a una contraseña maestra. En la actualidad luego de 12 años, esta herramienta cuenta con más de 25 millones de usuarios en todo el mundo. (LogMein, 2020). Actualmente, LastPass no solamente ofrece servicios de gestión de contraseñas, sino además, tal como especifican es la página oficial, cuenta igualmente con gestión y almacenamiento de datos mucho más personales como los son: (pasaporte, tarjeta de crédito, seguridad social, etc.) la manera de almacenar esta información es por medio de notas, así mismo, tiene la opción de autocompletar formularios reduciendo de esta manera tiempos de inicios de sesión o al momento de realizar alguna compra de manera virtual; el compartir las mismas contraseñas con otras personas igualmente es posible, finalmente, si lo desea el usuario la herramienta cuenta con un generador de contraseñas que cumple con los lineamientos de seguridad para este tipo de dato. LastPass se encuentra para su uso en un número

importante de plataformas, ya sean dispositivos móviles o de escritorio; para dispositivos móviles ya se pueden encontrar versiones de su app en dispositivos Android o IPhone; para terminales de escritorio puede ser instalada en diferentes sistemas operativos (Windows, Mac, Linux) así mismo, en un número variado de navegadores web (Google Chrome, Microsoft Edge, Firefox, Safari, Opera), Incluso cuenta con una versión universal para cada SO mencionado previamente; y por último una versión para smartwatch. (LogMein, s.f.)

LastPass cuenta con diferentes versiones ya sean gratuitas, de paga en incluso profesional. Entre los más de 25 millones de usuarios se encuentran alrededor de 61.000 empresas que usan los servicios de la herramienta.

Algunas características con las que cuenta LogMein en su herramienta y por lo que se hacen denominar "líderes en materia de seguridad", es que cuentan con un algoritmo de cifrado potente (tal como lo definen ellos) para la protección de los datos en la nube, el algoritmo es (AES de 256 bits con PBKDF2 SHA-256); el proceso de cifrado y descifrado de los datos, se realiza netamente dentro del dispositivo ya sea móvil o de escritorio, y por último, dentro de su página web destaca la autentificación multi - factor, fortaleciendo las medidas de seguridad. (LogMein, s.f.)

Otra de las compañías que ha hecho esfuerzos para brindar a los usuarios de la internet una opción para poder gestionar sus contraseñas, es la misma compañía Google, donde por medio de su navegador (Google Chrome) pero principalmente por medio de una cuenta de correo Gmail, la compañía da la opción a los usuarios de poder almacenar los datos generados posteriormente a la creación de una cuenta de usuario: (Sitio web, usuario o correo electrónico y contraseña) dentro del mismo dominio de correo de Gmail; esto ha proporcionado a los usuarios un fácil acceso de inicio de sesión en las cuantas de usuario. Sin embargo, el hecho de que el

almacenamiento se asocie a la cuenta de Gmail ha generado que esta función esté disponible únicamente para usuarios que cuenten con una cuenta de correo proporcionada por Google; además de que, para tener acceso a la información en un dispositivo provisional, es necesario iniciar sesión dentro del mismo navegador, lo que puede generar que la información sea de fácil acceso para terceros, en caso de que el usuario olvide cerrar la sesión.

A nivel Colombia, Bex Technology con más de 10 años de experiencia, ha creado una herramienta denominada BSR Bext-SelfReset cuyo fin en este caso es proporcionar una solución respecto a la gestión de contraseña a nivel empresarial, la compañía define a su herramienta BSR Bext-SelfReset como "una aplicación web que permite la autogestión y el cambio de contraseñas a cada usuario activo aumentando la productividad, reduciendo el costo de implementación y facilitando su uso sin usar una mesa de ayuda." (Bex Technology, s.f.)

Lo que incentivó la creación, fue que, día a día un gran número de usuario de Windows olvidan la contraseña de acceso, esto provoca que, la persona tenga que iniciar el proceso de recuperación de contraseña por medio de una compañía externa, principalmente en lo que se denomina "mesa de ayuda"; el proceso inicia cuando la persona envía una petición por medio de un ticket, donde un agente verifica esta petición, debido a que este proceso se realiza de forma manual, esto provoca una pérdida de tiempo por parte del usuario y del mismo agente; estudios realizados por la misma compañía, han logrado identificar que los tiempos de operación dentro de las mesas de ayuda para realizar el proceso anteriormente mencionado, equivalen a un 20% en el mejor de los casos, en casos muchos más complicados estos tiempos pueden llegar a un 40% de carga de trabajo, tiempo que obviamente puede ser usado para otras actividades.

Principalmente BSR Bext-SelfReset está siendo usada dentro del gobierno y educación, además de esto, algunas otras compañías que han decidido usar la herramienta dentro de su

organización han sido: Alpina, Universidad de la sabana y otra muy conocida, la Universidad del rosario. (Munoz, 2016)

El tema de seguridad informática se ha convertido en un punto vital dentro de las organizaciones, el proteger los datos de posibles robos o afectar la integridad de los mismos ha sido un tema complejo: en una escala muy pequeña, prácticamente se puede decir que, el objetivo se encontraba en que la información no pueda ser sustraída dentro de los establecimientos de cada organización, debido principalmente a que muchos de los datos que se manejaban no se encontraban de forma digital, sino por medio físicos. No obstante, con la llegada de la internet y la digitalización del mundo y esencialmente de los datos, las organizaciones debieron fortalecer sus medidas de protección para garantizar que su información se mantenga segura. Dado que las compañías, no solamente deben proteger sus propios datos, sino igualmente información de suma importancia e incluso muy personal de sus clientes, como lo pueden ser: (Nombre, dirección, teléfono, e incluso datos como tarjetas de crédito o cuentas bancarias); los sistemas de seguridad debieron fortalecerse.

Tanto así que, el realizar investigaciones respecto al tema, se ha convertido en un tema interesante y fundamental para la industria de la informática, uno de los libros más completos, con información muy precisa y actual, cuyo nombre es (Introducción a la seguridad informática y el análisis de las vulnerabilidades), escrito por un grupo de ocho profesionales con alta experiencia y grandes títulos enfocado al tema de la seguridad, que van desde ingenieros hasta magister en información empresarial, cuya investigación realizada por estos profesionales y plasmada dentro del documento permite evaluar lo extenso del tema, (Romero Castro, y otros, 2018)

Así mismo, la investigación realizada por Gabriel Baca Urbina, plasmado en el libro (Introducción a la seguridad informática), se puede evidenciar principalmente un análisis de riesgos que se pueden presentar en los sistemas de información, tal como lo exalta en su documento, los riesgos pueden traer daños relevantes, donde explica que las empresas constantemente están en riesgo de pérdida de información, sin embargo, la probabilidad de que esto suceda, depende de los medios de protección que use cada organización, y reducir el número de vulnerabilidades que pueda tener algún sistema de información. (Gabriel, 2016)

Colombia al ser una de las naciones de Latinoamérica que, dentro de su constitución política, tiene como derecho fundamental la protección de los datos de las personas, ha establecido unas normas cuyo fin es la de reducir los posibles robos de información. Dentro del documento Manual de seguridad Versión 2, publicado por el ministerio de educación podemos ver con claridad las normas mencionadas anteriormente, que van desde protección a nivel de software a físicas. Además de las normas, dentro del documento encontramos varias recomendaciones de seguridad, desde creación de contraseñas seguras, control de accesos y algunas vulnerabilidades.

2.2. Bases Teóricas o fundamentos de concepto

2.2.1. Seguridad Informática

Si se desea brindar a las personas una herramienta, el cual les permita tener sus datos de correos electrónicos junto con sus contraseñas dentro de la palma de su mano, favoreciendo de esta manera la accesibilidad de los mismos, debemos analizar una variable fundamental, el cual es la seguridad, en este caso la seguridad informática, los datos que se desean manejar son de alta importancia, por ende, es fundamental que la herramienta cuente con un sistema de seguridad robusto, pero a la vez de fácil acceso, por este motivo, el definir de que se trata con exactitud la

seguridad informática es esencial. Para Gabriel Baca Urbina, autor del libro introducción a la seguridad, menciona que la seguridad informática es.

> La disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta (Baca Urbina, 2016).

Principalmente se determina que la definición de seguridad informática consiste en proteger y mantener la integridad de la información de posibles daños o robos, que se puede encontrar principalmente en el medio informático. Cabe destacar que, esta definición está muy enfocada a los lineamientos de seguridad dentro de la compañía; recordemos que, dentro de las compañías se manejan diferentes reglamentes de seguridad, algunas normas que generalmente se usan van desde prohibir el uso de correos electrónicos que no sean del dominio de la misma compañía, manejar contraseñas en cada dispositivo de la organización, etc. Esto hablando de métodos de protección a nivel de software, sin embargo, también se manejan métodos de protección a nivel físico, como lo pueden ser, deshabilitar los puertos USB, rigurosos controles a la entrada de la organización, con el fin de hallar dispositivos de almacenamiento, prohibir el uso de celulares en los puestos de trabajo etc.

En complemento a la definición anterior Leonardo Camargo se permite definir a la seguridad informática: “como cualquier acción que impida la ejecución de operaciones no autorizadas sobre un sistema informático o red de computación” (Camargo Cardona, 2019), lo que podemos concluir con esta definición, es que la seguridad informática es un conjunto de acciones que se deben realizar dentro de un SGSI, por parte de las compañías, principalmente previniendo vulnerabilidades, el objetivo principalmente para la creación de estas medidas, son

proteger o administrar de forma sobresaliente los tres pilares de la seguridad informática, los cuales se especificaran más adelante; además de lo anterior, Leonardo menciona que la seguridad informática es más un proceso que un producto, esto debido a que es necesario realizar periódicamente procesos de controles de supervisión, donde se desea determinar si las medidas establecidas para mitigar los riegos funcionan correctamente, de lo contrario, es fundamental realizar cambios en los métodos de protección. Cabe destacar que las medidas son principalmente para evitar que una vulnerabilidad suceda, mas no corregirlo, sin embargo, el proceso de mantenimiento correctivo no queda descartado; el motivo de que el la seguridad informática priorice el evitar los riegos, es debido a que en cualquier ataque sufrido en alguna vulnerabilidad puede provocar pérdida o robo de información, y es precisamente este tipo de acciones lo que quiere evitar la seguridad informática y claro está, cualquier organización que maneje cualquier tipo de información de suma importancia.

En complemento con lo anterior, se menciona que a pesar de que los mecanismos preventivos son un de los puntos más importantes dentro de la seguridad informática, son generalmente vistos como algo poco útil, o en otras palabras, un proceso de alto costo pero poco necesario, un ejemplo puede ser una persona que requiera de un seguro de autos, el cual cubre algún tipo de choque o accidente, recordemos que para que este tipo de seguros tenga valides y se encuentre vigente, es necesario un pago mensual y constante (Rodríguez et al., 2019); sin embargo, para algunos esto puede llegar a ser una "perdida" de dinero, debido a que muchas personas que acceden a este tipo de seguros puede que nunca tengan algún accidente, por ende, nunca hicieron uso de este seguro; en muchos de los casos los procesos de la seguridad informática funcionan de la misma manera, donde las organizaciones deben realizar grandes inversiones de dinero y tiempo, más sin embargo, pueda que nunca sufran algún tipo de ataque,

es por este motivo que generalmente este proceso sea tan poco valorado y muchas veces no implementado. Entre los métodos preventivos se mencionan los siguientes:

- Respaldo de información: donde se busca que toda información que se maneje dentro de una organización tenga una respectiva copia; a este proceso en palabras más técnicas se define como un Back-up, el fin de realizar este proceso es tener una copia de respaldo de la información en caso de una perdida de datos, ya sea por robo o daño físicos del dispositivo de almacenamiento.
- Horario de respaldo: es importante igualmente, seleccionar un horario correcto donde se pueda realizar el Back-up, un punto muy importante a tener en cuenta es la disponibilidad de la información, ya sea para los usuarios o para los empleados de las organizaciones, esto dependo mucho del tipo de data que se maneje, generalmente los horarios para realizar este respaldo son establecidos dentro de los tiempos de menos concurrencia.
- Control de respaldos: como su nombre lo indica es esencial la existencia de controles para los respaldos creados, por el hecho de que sean una copia de la información no indica que tiene menos importancia, sino todo lo contrario, es igualmente significativo realizar controles que certifiquen que los datos, no puedan ser accesibles para un tercero no autorizado.
- Compresión de data: una de las ventajas de las copias de seguridad es que estos datos pueden entrar en procesos de compresión; el proceso consiste en que la data tenga un tamaño menor que el dato original, sin embargo, los datos serán más difícil de acceder; no obstante, esta acción se permite dado que es una copia. Cabe mencionar

que se debe realizar un análisis previo de los datos, para identificar con claridad qué tipo de información es apta para este proceso.

Así mismo, y como se mencionó previamente el proceso de mantenimiento correctivo no queda descartado, es por este motivo que igualmente se deben realizar métodos correctivos, entre los puntos diferenciales en comparación con los métodos preventivos es el costo y tiempo; en este caso los precios para la corrección de los daños y posteriormente suplir la vulnerabilidad son muy altos, además, el hecho de que se entre en proceso de corrección, indica que el SGSI ha sufrido inmediatamente un daño, o accesibilidad ilegal de terceros. Por ende, se deben realizar acciones de manera prioritaria, que solucione el problema detectado y en un corto periodo de tiempo; a diferencia de los métodos de prevención, donde el tiempo no necesariamente, en un gran número de casos es prioridad.

Finalmente, en complemento con los procesos o métodos anteriores, existen los métodos de detección o mecanismos detectivos, donde a través de diversos mecanismos se busca la detección de vulnerabilidades, ya sean físicos o lógicos, es prioritario que el proceso de análisis lo realice personal capacitado y con altos conocimientos técnicos respecto a la seguridad informática, donde posteriormente se deberá realizar una clasificación de riegos o vulnerabilidades, para luego, determinar la manera de abarcarlas con el objetivo de mitigar los riegos (Romero Castro, y otros, Introducción a la seguridad informática., 2018).

En conclusión, se debe destacar que básicamente la seguridad informática más que un producto es un proceso, el cual debe ser implementado por las compañías, sin importar la cantidad, ni el tipo de datos, esto justifica las diversas normas y leyes, creadas para la protección de la información, ya sea la norma ISO 27001, el RGPD o el Habeas data hablando de temas penales, las cuales serán explicadas más adelante.

2.2.2. Pilares de la seguridad informática

Como se explicó en el punto anterior, el tema de la seguridad informática es fundamental para la implementación de un SGSI seguro, para esto, la seguridad informática debe priorizar tres puntos esenciales para gestionar cualquier tipo de información almacenado en cualquier SGSI, conocidos principalmente como los pilares de la seguridad, los cuales son: Confidencialidad, Disponibilidad e Integridad; sin embargo, en algunas organizaciones implementan como pilares otros factores, cabe mencionar que, esto depende de las compañías, donde luego de una evaluación de sus sistemas de seguridad, optaron por adicionar otros pilares; sin embargo, los tres pilares de seguridad básicos, son los mencionados anteriormente, y que serán explicados a continuación.

2.2.2.1. Confidencialidad

La confidencialidad de datos es uno de los tres pilares que conforman la seguridad de la información, dado que la protección de los datos que se manejan dentro de alguna organización se basa en estos pilares, igualmente es un tema sumamente importante que se encuentra muy arraigado con la protección de datos, una definición dada por Leonardo Camargo Cardona, donde en su investigación (Regulación en Colombia de los delitos informáticos) es: "La confidencialidad hace alusión a la garantía de que cada mensaje transmitido por las redes de comunicaciones o almacenado en un sistema informático pueda ser leído por su legítimo destinatario, garantizando las medidas de seguridad apropiadas para ese objetivo". (Camargo Cardona, 2019).

Podemos analizar, teniendo en cuenta esta definición que, cada persona tiene derecho a que la información que fue precisamente enviada a su persona, solo pueda ser leída por sí misma, no obstante, esta definición está muy enfocada principalmente a casos de la recepción de mensajes

personales; considerando que, la problemática definida previamente, es esencialmente encaminada al posible robo de datos personales y al mal manejo de estos, la definición dada por Leonardo Camargo, no se ajusta con exactitud, mientras que, la definición que plasma el ministerio de educación de Colombia a través de su manual de seguridad versión 2, encontramos que definen la confidencialidad como: "La garantía que tiene una persona para que acceder exclusivamente a su información". (MINEDUCACIÓN , 2018).

Esto nos da a entender que, a pesar de que cada definición no se asemeja, el concepto en general es igual, demostrar que cada persona puede manejar sus datos como este lo desee, y que este tiene derecho a que solo el propietario de estos sea quien tenga acceso.

2.2.2.2. Disponibilidad

A pesar de que es primordial de que los datos tengan un alto nivel de confidencialidad, es igualmente importante que los datos estén disponibles de manera sencilla, ya que como se ha mencionado reiteradamente, las personas tienen el derecho de administrar sus datos, tal como él lo desee, así lo afirma Cristina Useche Samudio dentro de su proyecto de grado, donde textualmente menciona que la disponibilidad:

> Consiste en que la información siempre este accesible cuando se necesite los usuarios, teniendo en cuenta los niveles de seguridad y los usuarios. La disponibilidad, puede en ocasiones chocar frontalmente con la confidencialidad, ya que un cifrado complejo o un sistema de archivado más estricto puede convertir la información en algo poco accesible, por lo que no se trata en absoluto de un punto menor y marca en gran medida el buen hacer del responsable de la seguridad de la información de la empresa u organización (Useche Samudio, 2016).

No obstante, si se realiza un análisis de los controles de seguridad de los SGSI de diversas compañías, y además, teniendo en cuanta la experiencia de diferentes usuario, podemos preguntar ¿Realmente la información está totalmente disponible en todo momento para los usuarios?, esta interrogante es debido a los difíciles y tediosos procesos de recuperación de contraseña con la que cuentan las organizaciones, donde debido a esto, la data no siempre está disponible; así lo mencionan Grace Liliana Figueroa Morán, Galo Roberto Parrales Azules y los demás escritores de introducción a la seguridad informática y el análisis de vulnerabilidades, donde afirman que:

> Para poder considerar que se dispone de una seguridad mínima en lo que a la información respecta, se tiene a la disponibilidad, de nada sirve que solo el usuario acceda a la información y que sea incorruptible, si el acceso a la misma es tedioso o imposible, la información para resultar útil y valiosa debe estar disponible para quien la necesita (Romero Castro, y otros, 2018).

Es aquí, donde teniendo en cuanta lo anterior, debemos enfatizar los esfuerzos, para que, así como se garantiza la confidencialidad de la data, también se garantice la disponibilidad de esta.

2.2.2.3. Integridad

Finalizando la descripción de los pilares de la seguridad informática, encontramos la integridad, donde el objetivo en este punto es establecer medidas de seguridad y control, con el fin de que los datos se mantengan intactos, en otras palabras, que no sufran ningún tipo de daño, ya sea un daño lógico o físico, así lo afirma Leonardo Camargo Cardona, donde explica que la integridad "está relacionada con la garantía de que los contenidos de un documento no hayan sido alterados desde su creación" (Camargo Cardona, 2019); es obvio que una persona desea que sus datos no sufran ningún tipo de alteración, un ejemplo de esto, puede ser algún profesional que esté

realizando un trabajo de gran importancia en la nube, durante un tiempo ya importante, efectuando avances periódicamente, donde un día cualquiera por alguna razón, su trabajo sufre algún tipo de daño, provocando una pérdida de tiempo, y lo más lamentable la pérdida de su información.

Igualmente, la integridad trabaja muy de la mano con la confidencialidad, debido a que los datos no solamente deben estar protegidos de posibles fallos, sino también, deben estar seguros a posibles accesos de terceras personas que puedan modificar algún dato en específico; pongamos en contexto, a una persona que por alguna razón tuvo que realizarse un examen médico y cuyo resultado se almacenara dentro de la base de datos de la EPS, pero por el acceso ilegal de un tercero, los resultados fueron modificados, esto potencialmente puede provocar una mala medicación por parte del médico lo que puede generar que la salud del paciente puede verse afectado; por esta razón se debe garantizar que los datos se mantengan tal cual fueron creado y posteriormente almacenados; Cristina Useche menciona algo respecto a la integridad y más específicamente al punto de no modificabilidad de data, básicamente.

> Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina (Useche Samudio, 2016).

En general, por lo explicado previamente es de suma importancia que la información se mantenga segura e intacta, cualquier daño que reciba la data conducirá a posibles daños hacia alguna persona, no solamente físicos sino también dependiendo del tipo de dato, problemas legales.

2.2.3. Seguridad de la información

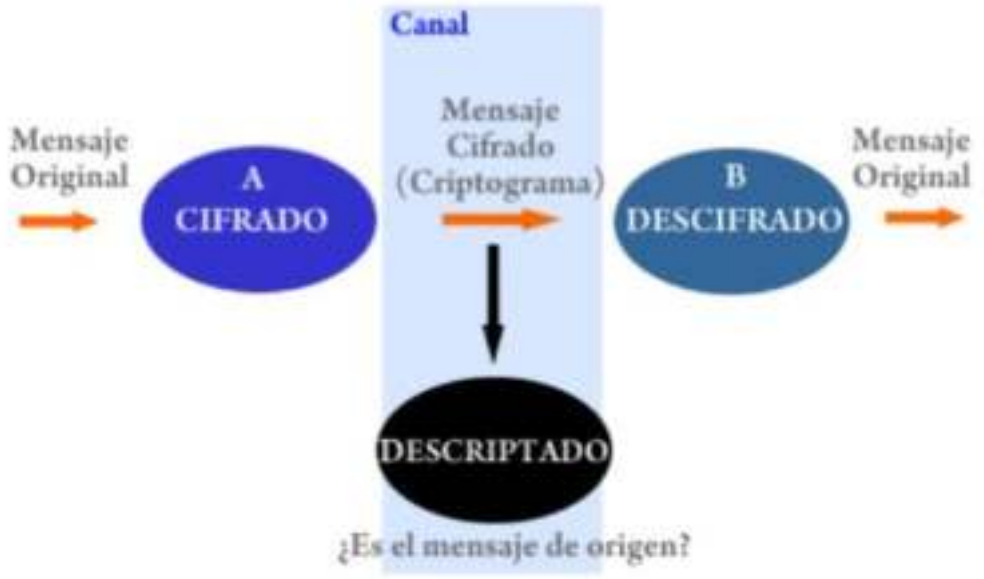
En muchos casos se suele confundir los conceptos de seguridad informática y la seguridad de la información, donde el objetivo podría ser proteger de manera general la información, sin embargo para que sea más claro, la diferencia principal es que la seguridad informática no solamente está orientado al medio informático, sino tal como su nombre lo indica, a todo lo que contenga información o data, tal como se explica en el libro de (La introducción a la seguridad informática y el análisis de vulnerabilidades). (Romero Castro, y otros, 2018) Es aquí principalmente, que es de gran importancia la implementación de la norma 27001, es esencial que las empresas protejan la información, y como se explicó previamente esta norma esta creada esencialmente para que esto se cumpla, igualmente, dependiendo de la ubicación geográfica de la empresa, también se debe implementar el RGPD, el cual se explicara su importancia más adelante.

Generalmente dentro de una organización es importante para la seguridad de la información tener personal enfocado a este tema puntual, el cual será el encargado de llevar rigurosos métodos de control y detección de vulnerabilidades; su cargo dentro de la empresa será definido como el oficial de seguridad de la información, así lo estipula el Ministerio de educación de Colombia, por medio del manual de seguridad informática; donde especifica que las responsabilidades de este rol son las de vigilar que se cumplan las medidas de protección emitidas posteriormente al análisis de riegos, y claramente este proceso debe estar respectivamente documentado. (MINEDUCACIÓN , 2018)

Así mismo, este proceso no solamente está enfocado dentro de Colombia, sino también, cualquier empresa que tenga o desee implementar la norma ISO 27001, donde es fundamental la implementación de este rol dentro de la compañía.

Figura 1

Esquema de Cifrado



Fuente: (Sanjuan, Universidad del Norte)

Donde se puede identificar qué, se inicia con un mensaje o texto original que se desea proteger, por este motivo el siguiente paso es transformar este mensaje por un proceso de cifrado, a través de un algoritmo (dentro de la informática), es en este punto donde se puede considerar que los datos se encuentran cifrados, posteriormente se usa un canal, ya sea para enviar o almacenar este mensaje; el siguiente paso de este proceso es descifrar el mensaje para que finalmente el receptor al cual fue enviado el mensaje originalmente, pueda acceder al mensaje.

Los propósitos principales por los cuales es recomendable el uso de la criptográfica, se pueden contar en 3, tal como lo explica Leudis Sanjuan dentro de su presentación criptografía 1, donde menciona qué, como primer propósito del uso de cifrado es que permite mantener la **(confidencialidad)** de los mensajes, tal como se mencionó previamente se busca que los datos solo sean accesibles por la persona receptora; el segundo propósito menciona que se busca

garantizar la identidad del destinatario y así mismo la del receptor, promoviendo de esta forma la **(disponibilidad)** de la información; finalmente permite que el mensaje no sea corrompido durante su envió, y pueda ser accedido tal cual como fue creado, asegurando la **(integridad)**. (Sanjuan, Universidad del Norte)

Además, como se menciona en el documento introducción a la seguridad informática y el análisis de vulnerabilidades, existen diferentes métodos de criptografía, que van desde protección a nivel local, remota e igualmente métodos de cifrado vía inalámbrica, la implementación de cualquiera de estos métodos depende del uso o tipo de información que se desea proteger. Entre los algoritmos o métodos más destacados se encuentran: (Romero Castro, y otros, 2018)

- MD5,
- SHA,
- Firma digital,
- WEP,
- WPA.

Así mismo, Juan Pablo Vargas en su trabajo de tesis, realiza una comparación muy completa entre diferentes algoritmos de cifrado teniendo en cuanta variable muy importante como lo son el tiempo de cifrado, tamaño, objetivos de cada uno de los algoritmos. Algunos de los algoritmos que son usados para realizar la comparación se encuentran varios de los más usados y conocidos los cuales son: (Vargas Salvador, 2019)

- DES,
- AES,
- RSA.

En conclusión, dentro de los métodos de seguridad fundamentales se encuentra el cifrado, y existe un número muy variado de algoritmos; recordando que se desea determinar por parte de la investigación, la viabilidad de crear una herramienta que maneje datos de alto grado de importancia, este punto es fundamental, los datos deberán contar con esta estructura segura para proteger la información, se debe realizar una evaluación y comparación de los diferentes algoritmos existentes, para de esta manera seleccionar el más acorde a la necesidad.

2.2.4. Vulnerabilidades

En un tema tan importante como es el de gestionar las contraseñas, correos electrónicos y además datos para el acceso a cuentas de usuario en los sitios web, es necesario crear métodos de control que permitan que esta información no sea vulnerada y mucho menos robada, claro está que para crear métodos de control que mitiguen los riesgos, es necesario determinar qué es lo que se desea controlar, en otras palabras, analizar y evaluar las vulnerabilidades que puedan atacar a los SGSI. Primero debemos identificar que es una vulnerabilidad, Gabriel Vaca Urbina menciona que una vulnerabilidad se constituye como "un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza" (Baca Urbina, 2016). Analizando esta definición se puede identificar que, las vulnerabilidades existen en el momento que no se han formulado de forma sobresaliente medidas de protección, de esta manera, se pueden crear riesgos y ataques que concluyan con robos o pérdidas de data.

Además de lo anterior, el ministerio de educación de Colombia dentro de las diferentes medidas de protección recomendadas en el manual de seguridad informática, menciona una lista de objetivos específicos del por qué es necesario implementar estas medidas al momento de la detección de vulnerabilidades dentro de un SGSI, algunas de las más destacadas son:

- Permite identificar los puntos vulnerables,
- Implementación de controles, cuyo objetivo es mitigar los riesgos,
- Seguimiento de monitoreo periódico que permite identificar si los controles se están llevando correctamente; entre otros.

Igualmente, dentro del mismo documento un punto muy importante mencionado es que, nos brinda información muy valiosa respecto a la gestión de vulnerabilidades, cuyo tema está dividido en varias secciones, como los son; la caracterización de gestión de vulnerabilidades, fase de gestión de vulnerabilidades, etc. Dentro de la caracterización de gestión, el ministerio proporciona una categorización de vulnerabilidades, de la siguiente manera:

Tabla 1

Ponderación De Fuentes De Riesgos

Fuentes	Puntuación (CVSS)
Categoría I	15
Categoría II	10
Categoría III	5
Servidores	15
Equipos perimetrales	15
Networking	10
Estaciones de Trabajo	5

Fuente: Tomado de (MINEDUCACIÓN, 2018).

Este tipo de información es muy útil al momento de implementar las medidas dadas dentro del mismo documento e incluso, las medidas dentro de la misma Norma ISO 27001; en

complemento con esto, también provee una calificación de riesgos, que van desde un rango de riego bajos hasta uno crítico (MINEDUCACIÓN, 2018), de esta manera:

Tabla 2

Matriz de Caracterización de Riesgos

Puntaje	Rango del Riesgo	Descripción
20	Critico	Estas vulnerabilidades incluyen riesgos que podrían comprometer los equipos e inclusive interrumpir el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.
15	Alto	Estas vulnerabilidades incluyen riesgos que podrían comprometer los equipos con degradación en el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.
10	Medio	Estas vulnerabilidades incluyen riesgos que podrían comprometer los equipos con degradación en el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.
5	Bajo	Estas vulnerabilidades incluyen riesgos que podrían comprometer los equipos con degradación en el servicio de las aplicaciones Categoría I, Categoría II y Categoría III.

Fuente: Tomado de (MINEDUCACIÓN , 2018)

Igualmente, el gran grupo de profesionales en el ámbito informático y autores del libro introducción a la seguridad informática y el análisis de vulnerabilidades mencionan la existencia de dos tipos de vulnerabilidades de manera general que pueden tener un SGSI, las vulnerabilidades lógicas y físicas, además de manera más profunda explican otros tipos de vulnerabilidades, desde errores en la web, errores de configuración y demás. (Romero Castro, y otros, Introducción al análisis de vulnerabilidades, 2018) Finalmente, la explicación de metodologías para la detección de vulnerabilidades y el proceso a llevar a cabo; es esencial realizar un proceso de detección de vulnerabilidades dentro de todo sistema de información, la

importancia en este caso de los datos es muy alta, y alguna vulnerabilidad que no sea detectada puede generar algún robo de información.

2.2.5. Ciberataques

La necesidad de realizar un profundo análisis de vulnerabilidades en los sistemas de seguridad es debido a la existencia de los ataques informáticos, también conocidos como ciberataques; generalmente los ciberataques se pueden definir como operaciones ilegales con el objetivo de realizar daños o robos de información, ya sea en niveles bajos como pueden ser computadores personales, o en grandes magnitudes como lo puede ser dentro de las organizaciones.

Complementando esta definición, el Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires (BACSIRT) menciona que los "ciberataques son acciones llevadas a cabo por personas u organizaciones, cuya intención principal es la de realizar algún tipo de daño a los sistemas de seguridad; sin importar la magnitud, cada acción de ciberataque provoca algún tipo de daño". (BACSIRT Vamos Buenos Aires, Centro de Seguridad, 2018)

En niveles bajos se puede mencionar como un ciberataque a la creación de un malware informático por parte de una persona, donde posteriormente será distribuido por diferentes medios, el cual posteriormente será ejecutado en las computadoras personales, lo que causara daños a los archivos personales o en el peor de los casos daños en el mismo sistema operativo o hardware; este tipo de casos es muy común, se puede decir que una gran número de personas han sido víctimas de este tipo de ataque, tanto así que, ¿Quién no ha sufrido algún tipo de virus en las computadoras o en algún dispositivo de almacenamiento móvil como lo puede ser un pendrive?. No obstante, también existen ciberataques de grandes magnitudes, que están enfocadas a las grandes organizaciones y han generado grandes daños o robos de información, así como el

ciberataque que sufrió Sony el cual fue explicado inicialmente, y que fue considerado como uno de los ataques informáticos más grandes de la historia; este tipo de ciberataques puede generar daños irreparables y generar grandes pérdidas en las organizaciones, ya sean de dinero o de data.

Además, enfocándonos en el tema de la gestión de contraseñas, y principalmente en la herramienta LastPass podemos mencionar el ciberataque que sufrió esta aplicación en el año 2015, donde hasta la misma CNN dio difusión al respecto, mencionando que la herramienta había sufrido un ciberataque donde datos como el correo electrónico, contraseña e inclusive la contraseña maestra de varios usuarios habían sido robadas, no obstante LogMein (creadores de la herramienta), anunciaron que el robo afortunadamente fueron en los datos de texto sin formato, justificando de esta manera la importancia del cifrado de información; los usuarios con más probabilidad de que sus datos personales fueran robados eran principalmente los que contaban con contraseñas maestras de baja seguridad, debido a este problema la misma compañía recomendó a los usuarios realizar el proceso de cambio de contraseña maestra, dificultando de esta manera el acceso a los crackers (CNNMoney, 2015). Ahora bien, analizando el ciberataque sufrido por LastPass, podemos identificar que una de las vulnerabilidades encontradas consiste en la baja seguridad que muchos usuarios establecen como contraseña maestra; recordando que, entre los objetivos de un gestor de contraseña, es permitir que los usuarios de alguna manera puedan olvidarse de memorizar un gran número de contraseñas. Sin embargo, darles la necesidad a los usuarios de recordar y asignar una contraseña maestra, puede provocar precisamente que los usuarios fijen contraseñas de baja seguridad, para reducir de esta manera la probabilidad de olvidar la clave, generando de esta manera, en caso de un ataque, que la información se acceda de manera más sencilla.

Existen diferentes tipos de ciberataques que puedan poner en riesgo los SGSI, que como se mencionó previamente pueden causar diferentes tipos de consecuencias o daños; a continuación, se mencionaran una lista de algunos de los ataques:

- Hoax,
- Phishing,
- Spoofing.

Cada uno de estos tipos de ataque tiene una modalidad diferente de acción o modus operandi, que van desde él envió de mensajes a través de los dispositivos móviles, en el caso de un ciberataque tipo Hoax, hasta la suplantación de identidad en el caso de los Spoofing. En los ciberataques de tipo Haox generalmente el atacante realiza una distribución aleatoria de mensajes por medio de la plataforma WhatsApp o mensajes de textos, brindando de forma engañosa algún tipo de ayuda a la potencial víctima, como por ejemplo alguna ayuda humanitaria con la idea de generar interés; el mensaje viene acompañado con un link o enlace que, al ser seleccionado, la victima será direccionado a un formulario, donde se le solicitarán datos altamente personales; de manera muy similar, funciona el ciberataque tipo phishing, donde la diferencia principal está en que el contacto con el usuario se maneja por medio de correo electrónico. Cómo se puede ver en esta breve explicación, el modus operandi de estos tipos de ataque se caracteriza por el hecho de que el atacante no tiene ningún tipo de contacto con la víctima. En total disimilitud funciona el Spoofing donde el atacante, busca por medio de una llamada telefónica y la suplantación de identidad, obtener información del afectado; un ejemplo de esto, es cuando la suplantación se realiza por medio de un supuesto asesor bancario, que desea realizar una “actualización” de información de un cliente bancario, donde necesariamente se debe realizar contacto con la víctima. (Gutiérrez Pinzón, 2016)

De manera general podemos darnos cuenta de que los ciberataques mencionados se encuentran enfocados al robo de información, pero se destaca principalmente, en que es necesario tener algún tipo de contacto con el posible afectado. No obstante, también existen otros tipos de ataques que funcionan por medio totalmente diferentes, entre las más comunes se encuentran las denominadas como infecciones por malware o virus, donde por medio de un software malicioso (malware) se realiza el daño a los sistemas de seguridad, los malware más populares son:

- Virus,
- Worms también conocidos como gusanos,
- Troyanos,
- Keyloggers,
- Adware,
- Ransonware.

Cada uno de estos virus, coloquialmente hablando, trabaja de una manera diferente, algunos de ellos buscaran infectar archivos extendiéndose con el objetivo de propagarse, mientras que otros pueden ir desde, la detección de pulsaciones realizadas dentro de un ordenador como lo realizan los keyloggers, hasta del cifrado de archivos, restringiendo todo acceso a ellos, y la única manera de poder acceder a esta información es por medio de realizar un pago al creador del malware, convirtiéndose en una modalidad de extorsión. (BACSIRT Vamos Buenos Aires, Centro de Seguridad, 2018) Algo que tiene en común este tipo de software, es que generalmente son archivos o programas "camuflados" que tienden a mostrarse como software totalmente confiable, el objetivo de esto es que, para iniciar su funcionamiento, el malware

necesita ser ejecutado como la mayoría de programas, es por este motivo que los usuarios con pocos conocimientos informáticos sean las principales víctimas.

2.2.6. Bases Legales De La Investigación

Para fortalecer la seguridad en los sistemas de seguridad se han creado diferentes normas a nivel internacional y nacional, incluso se han creado leyes con el fin de penalizar con cárcel el acto de robos de información. A continuación, se explicará algunas normas que se deben tener en cuanta, e incluso algunas leyes penales, donde en conjunto se minimicen los riegos de robos de información.

2.2.6.1. Norma ISO 27001

Internacionalmente se han realizado esfuerzos muy grandes para reducir ataques informáticos dentro los sistemas de información, tanto así que, La International Organization for Standardization (ISO), ha creado la normal 27001, la cual tiene como nombre (El sistema de Gestión de seguridad de la información (SGSI)); el fin de la creación de esta norma es para tener estándares de seguridad definidos las cuales se deben implementar dentro de las compañías, de este modo fortalecer la seguridad de la información. Los objetivos de estos estándares son la de evaluar los riesgos y amenazas, así mismo, la norma permite definir controles y estrategias.

La norma establece un proceso de 9 fases, los cuales, una compañía debe llevar a cabo, para de este modo reducir en un alto porcentaje, posibles fragilidades que pueda tener su SGSI. A continuación, se explicará de forma muy breve, que puntos se evaluaran durante el tiempo que dure estas fases.

Primeramente, un punto a evaluar y que aconseja esta norma, consiste en la identificación de las amenazas, esto se puede denominar como la base de un SGSI seguro, dentro de este análisis no solo debe estar enfocado a posibles riesgos a nivel de la internet o en otras palabras a riesgos

digitales, sino igualmente a riesgos físicos, tales como eventos naturales, fallas técnicas, o incluso posibles robos de información por parte de un empleado de la misma organización; este tipo de análisis se debe realizar evaluando la probabilidad de ocurrencia en un hecho que pueda poner en riesgo la integridad, confiabilidad y disponibilidad de los datos, además de lo anterior es de suma importancia identificar o evaluar las consecuencias de estos hechos, que pueden ser, desde un robo de información dentro de la misma compañía, hasta la del robo de datos de terceros y en el peor de los casos, la destrucción total del dispositivo de almacenamiento (Servidor), esto hablando de información digital.

Luego de la detección de las amenazas y como segunda fase, es necesario realizar implementaciones de controles, dentro de esta fase se busca por medio de puntos de control, que los riesgos puedan entran en un proceso de auditoria.

En la siguiente fase (3) se realiza un plan de tratamiento, cuyo fin de este proceso, consiste identificar las formas en cómo se afrontarán estos riesgos que fueron hallados en la primera fase, ya sean eliminarlos, mitigarlos o en algunos casos, trasladarlos, lo cual consiste por ejemplo, en contratar algún tipo de seguro que, de forma monetaria intente de alguna forma compensar el daño producido a la información; eso depende por supuesto del tipo de riego que se haya detectado en fases posteriores.

Posteriormente, es de suma importancia determinar el alcance del SGSI, dado que no todas las organizaciones son iguales, se pueden manejar diferentes implementaciones dentro del sistema, ya que algunas de ellas manejan un número mayor de empleados, o manejan un flujo superior de información, e inclusive varias sedes.

Después, la ISO 27001 aconseja analizar el contexto de la organización, un método o esquema utilizado para esto, es el uso de la matriz DAFO o también conocida como DOFA, donde por

medio de esta matriz identificaremos con gran exactitud y claridad, las Debilidades, Oportunidades, Fortalezas y Amenazas.

En complemento con lo anterior, en la siguiente fase, es necesario identificar las partes interesadas en la organización, en palabras más técnicas, este grupo de interesados son llamados como “stakeholders”, esto igualmente nos permitirá a desmenuzar o hallar con más profundidad algunos riegos.

Ya en la fase 7, es de gran relevancia establecer dentro de la organización, objetivos que permitan gestionar los riesgos, estos objetivos deben ser establecidos con el objetivo de reconocer la importancia de lo que se está manejando, y por ende estos objetivos deben ser dados a conocer a los empleados de la compañía; es fundamental que tengan una evaluación constante, por este motivo, la norma, sugiere el uso de indicadores, que permitan esta evaluación y una comparación de resultados.

Nada de lo anteriormente explicado tendría ningún sentido, si estos procesos no tuvieran su respectiva documentación, en este punto la norma es tan estricta, que de no llevarse a cabo de forma correcta este proceso, la acreditación de la norma, no sería otorgada. Sin embargo, a pesar de lo estricto de este proceso, la International Organization for Standardization permite realizar este proceso en diversos tipos de formato, que van desde documentación en físico, hasta archivos de video o de sonido, esto lo puede determinar la misma compañía.

Para llevar un control de los riegos dentro de un SGSI, las organizaciones que deseen obtener la acreditación deberán realizar cada cierto tiempo auditorias, cuyo objetivo, es la de comprobar que los riesgos hallados y controles establecidos previamente se hayan identificado e implementado de manera correcta y cumplan con el objetivo de proteger la información. (International Organization for Standardization, 2013)

Luego de la breve explicación de las fases con las que debe optar una organización para obtener la acreditación de la norma; se puede identificar que es un proceso muy minucioso que conlleva gran trabajo y transparencia, sin embargo, se debe tener en cuenta la importancia del bien que se está manejando, y debido a que, actualmente el mundo se está digitalizando, son más los datos que se debe manejar y por ende proteger. Por este motivo es que era necesario la implementación de normativas a nivel global que, al momento de ser efectuadas, contribuyera a la protección de la información.

2.2.6.2. Norma ISO 27002

En complemento con la norma ISO 27001, la International Organization for Standardization creó la norma ISO 27002, donde el objetivo dentro de una organización es que, por medio de estándares explicados dentro de la norma, puedan identificar con exactitud los activos que posee, de esta manera, la detección de riesgos puede ser más fácil y con más exactitud. Claro está, que al momento de hablar de activos debemos tener en cuenta que hablamos de activos a nivel informático, como lo pueden ser computadoras, dispositivos móviles, servidores, software, sistemas operativos, periféricos, bases de datos, servicios de internet, entre otros.

Dentro de las actividades de control que se deben realizar se requiere que los activos hallados, deber ser justificados y además de esto, deberán contar con un responsable de estos, cuyo objetivo principal es la de velar por la protección y rotundamente la implementación de controles. Así mismo, dentro de las funciones del "propietario" de los activos, está la de realzar periódicamente, el correspondiente proceso de inventariado.

La ISO 27002 recomienda, que los activos estén clasificados dependiendo de diferentes variables, entre las más importantes se encuentran la sensibilidad de la información, y nivel de riesgos; esto ayudaría que al momento de querer implementar las fases de la norma 27001 y más

específicamente los métodos de control, se obtengan resultados más exactos. Igualmente, es aconsejable que la selección de variables de clasificación no sea muy alta, debido a que, puede que el proceso de selección de métodos de control resulte muy complejo y poco satisfactorio. De la misma manera es necesario la clasificación de la información, donde se deberá evaluar el nivel de protección que deberá tener.

Complementando las actividades de control, se deben mencionar igualmente que es importante realizar una regulación para el uso adecuado de estos activos de información, la cual debe estar documentada, y dada a conocer, es de suma importancia que los activos sean usados de una manera correcta. (ISOTools Ex, 2019)

Por si sola la norma ISO 27002, no proporciona estándares de seguridad muy altos a lo que respecta el robo de información o identificación de vulnerabilidades de los SGSI, debido a que está muy enfocada a detección de los activos dentro de la empresa, no obstante, en conjunto con la norma ISO 27001, puede convertirse en una parte vital que lleve a una implementación mucha más acertada de los posibles fallos o riesgos que puede tener la información, por ende, prevenirlos o eliminarlos.

2.2.6.3. RGPD

EL Reglamento general de protección de protección de datos (RGPD) o en sus siglas en ingles GDPD, es un Reglamento creado con el fin de proteger los datos personales, los cuales deben ser aplicados principalmente por las organizaciones, fundamentalmente a lo que respecta a la información o actividad online; el proceso para determinar el cumplimiento del reglamento se realiza a través de una lista de requisitos. Este reglamento está constituido esencialmente para su uso dentro de los estados que conforman la Unión Europea (UE). Cabe mencionar, que las empresas que incumplan o no sigan este reglamento a cabalidad, podrán tener sanciones, desde la

prohibición de su actividad económica dentro de la UE, hasta sanciones económicas. Un punto muy importante es que, si una organización no tiene su sede principal dentro de este grupo de estados, pero igualmente parte de tu actividad sí, esta compañía debe cumplir con este reglamente a cabalidad, de lo contrario, también podría recibir algún tipo de sanción. (SAGE , 2018)

El reglamento, de manera muy similar a la norma ISO 27001, busca básicamente que las organizaciones detecten los riesgos, para posteriormente realizar un análisis de estos, de este modo se podrá analizar de qué manera se podrá prevenir o en el mejor de los casos eliminarlo. (Bauzá Martorell, 2019)

Entre los diferentes artículos que están estipulados en el RGPD, podemos encontrar normas muy claras que permiten un control dentro de las empresas, a lo que respecta al manejo de la información; entre los más destacados, se encuentra el proceso de notificaciones donde la compañía luego de algún tipo de "violación" dentro del SGSI, está obligado a notificar al o a los entes de control dentro de las primeras 72 horas. (Bauzá Martorell, 2019)

Este es uno de los reglamentos más grande a nivel mundial, ya que en otras naciones a nivel global existen otras normas o reglamentos, creados con el mismo objetivo, proteger la información de las personas. Este es uno de los más importantes tanto así que, ha servido como fuente para la creación de nuevas leyes en otras naciones.

2.2.6.4. Norma ISO 27701

La ISO 27701 es una de las normas creadas más recientes (año 2019) y es definida como una extensión de la norma ISO 27001 e ISO 27002; ¿el porqué de su creación?, fue debido a que, el gran número de exigencia demandadas por el RGPD y la ISO 27001 genera una difícil implementación dentro de las compañías, incluso, hay un gran porcentaje de empresas que han

aceptado que no cumplen con este reglamento, lo que puede provocar que las medidas implementadas no sean lo suficientemente fuertes, tanto así que, ya se han conocido casos de violaciones de los sistemas de seguridad donde una gran cantidad de datos han estado en riesgo. El objetivo de la 27701 es la de detallar requisitos y brindas una orientación para la implementación del RGPD o la ISO 27001 dentro de los sistemas de seguridad; cabe destacar que, los estándares dados por la ISO 27701 se basan en la norma 27001, sin embargo, no es necesario para la implementación y una posible certificación de la ISO 27001, no obstante, es de gran ayuda debido a que incluye un conjunto de requisitos, controles y un nuevo conjunto de objetivos de control, cuyo fin es la de conseguir la certificación SGIC. (NQA)

Podemos considerar una herramienta u opción muy importante la implementación de esta norma, debido a que la implementación de los reglamentos o normas de seguridad no siempre es una tarea sencilla, y teniendo en cuanta las sanciones o penalidades tan fuertes que pueden enfrentar las organizaciones dentro de la EU, se ve con buenos ojos por parte de ellas tener una guía, para de este modo fortalecer sus sistemas de seguridad de la información.

2.2.6.5. Norma ISO 27017

Enfocado en la protección de datos en la nube la International Organization for Standardization creo una lista de controles que se deben considerar dentro de una organización, la cual se denomina norma ISO 27017, debemos tener en cuenta que actualmente mucha información se está manejando por medio de la nube, ya que de esta manera se le ha ofrecido al público, una manera más simple de poder acceder a sus datos, en diversos dispositivos, y en diferentes partes del mundo, por este motivo, se deben igualmente tener controles de seguridad para prevenir daños a la data. Y es aquí donde la ISO 27017 cumple una labor importante, donde por medio de 44 controles exigidos, donde establece buenas prácticas de seguridad, de este modo, se

fortalecerán las medidas de seguridad. La norma no solamente está enfocada hacia los clientes en sí, sino también de los proveedores del servicio de la nube. (ISO International Organization for Standardization, 2017)

Es importante aludir esta norma, debido a la gran importancia que está tomando los almacenamientos de data por este medio; un gran número de compañías, está obligada a esta forma de almacenamiento, por el tipo de servicio que ofrecen; Facebook, Twitter, Instagram, son algunos de los ejemplos de esto, dado a la gran cantidad de datos, un gran número de usuarios y, además, el tipo de información que maneja. Facebook especialmente es una red social que maneja información muy delicada, desde nombres, números telefónicos, fechas de nacimiento, entre otros. Por obvias razones, es fundamental tener protocolos que aporten a la seguridad de datos en la nube.

2.2.6.6. Norma ISO 27018

Igualmente, la ISO 27018 está enfocada a la protección de datos en la nube, sin embargo, está norma esencialmente está focalizada a la protección de los datos personales, lo que lo diferencia a la 27017 que protege los datos en genera; debemos mencionar que a pesar de que la norma 27001 está enfocada en este aspecto, muchas organizaciones manejan un gran número de información por medio de la nube y buscan certificarse igualmente con esta norma, de esta manera manifestar su compromiso con la protección de la información a través de este medio.

La misma Organización Internacional de Normalización en su página web menciona que de manera muy similar que la ISO 27001, el objetivo de la norma 27018 busca implementar un conjunto de buenas prácticas o normas y de controles, con el fin de certificar la protección de los datos, pero específicamente garantizar las obligaciones legales respecto al manejo de la información personales.

Así mismo menciona que entre las medidas más destacadas que conforman la norma y que son necesarias para su implementación, se encuentran que los proveedores deberán proporcionar las herramientas para el cumplimiento de la seguridad y protección, a la par deberá velar por el cumplimiento del tratamiento de la data.

Un punto importante a mencionar es que, fue la primera norma internacional creada con el fin de lograr la reserva en la nube y sin duda alguna la de la información (ISO, 2017).

Cabe destacar, que a pesar de que la ISO 27017 igualmente es creada para la protección de los datos en la nube, no es necesariamente la implementación de las dos normas en la misma organización; no obstante, la ejecución en conjunto de estas normas puede generar que las buenas prácticas y controles implementados sean más seguros y cumplan con más eficiencia.

2.2.6.7. Habeas Data

A nivel latinoamericano, se encuentra la ley Habeas Data, sin embargo, varias naciones no tienen en vigor esta ley constitucional, ni ninguna para la protección de datos personales. Como se ha explicado previamente el objetivo de esta ley es darles un derecho a las personas de administrar sus datos personales como ellos lo consideren e igualmente las organizaciones a proteger los datos proporcionados por sus usuarios. En Colombia, la ley Habeas Data, también conocida como la ley 1266 hasta el año 2012, donde posteriormente fue nombrada como la ley 1581, está basada bajo el Articulo 15 de la constitución política colombiana dentro del capítulo 1 (De los derechos fundamentales) la cual menciona que.

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y

> circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables (Constitución Política de Colombia, 2016).

La ley Habeas data consisten en una regulación de datos que este almacenada en bancos de datos, principalmente los datos a proteger serían los que se encuentran previstos para fines comerciales, financieras o crediticias. El objetivo principal de esta ley consiste en legitimar que, los datos personales de toda persona con nacionalidad colombiana tengan la facultad de administrar sus datos tal cual lo crea conveniente, los cuales pueden estar dentro de diferentes bancos de datos o también llamados bases de datos, certificando de esta manera el cumplimiento del artículo 15.

Es importante mencionar que, sin importar el tipo de compañía, ya sea pública o privada, estas deberán de realizar acciones para que se pueda cumplir con el propósito de la ley, en un gran número de casos las organizaciones para reducir posibles fallos en los sistemas de seguridad y así evitar robos de datos, realizan el proceso de la implementación de la norma ISO 27001 pero esencialmente la certificación. Es fundamental aclarar que, la única excepción para que los datos no sean confidentes, será cuando el Departamento Administrativo de Seguridad más conocido como el DAS o la fuerzas publica, a través de una orden requieran la accesibilidad de los datos. Las organizaciones u operadores tiene una lista de deberes para certificar que la ley se cumpla, entre las más destacadas se pueden mencionar que, es obligación llevar un manual de políticas de seguridad, enfocada a la consulta y reclamos de los usuarios hacia sus datos, igualmente deben periódicamente realizar la actualización, rectificación y una de las más importantes, es que el acceso sea concedido al titular de los datos. (El congreso de la República, 2008)

2.2.6.8. Ley 1279 Del 2009

En Colombia, a pesar de la existencia de la ley habeas data, también existe la ley 1279, la cual esta se denomina "De la protección de la información y de los datos", por medio de esta ley el congreso de Colombia busca sancionar penalmente cualquier acto de intento o robo de información; dentro de esta ley, se encuentran un número importante de artículos, cada uno de ellas identifica puntualmente un acto ilegal posible de robo de información, así mismo, la respectiva pena que puede afrontar una persona.

El artículo en general que está establecido dentro de esta ley, es el articulo 269 el cual esta desmenuzado en varios "sub-artículos" que esta definidos desde el artículo 269A hasta el articulo 269J. Entre los actos ilegales que están estipulados entre los diferentes artículos, se mencionan (Accesos abusivos a un sistema informático, Obstaculización ilegitima del sistema, Interceptación de datos, uso de software malicioso, suplantación de sitios web, hurtos, transferencias ilegales, entre otros.), las penas económicas o de cárcel establecidas dependen del acto ilícito, las cuales van de 100 a 1000 SMMLV (pena económica) y de 36 a 120 meses de precios (REPÚBLICA DE COLOMBIA - GOBIERNO NACIONAL, 2009).

Existen varias leyes, que han sido aplicadas o creadas por el congreso de Republica de Colombia, enfocada a la protección de datos personales, muchas de estas medidas se han creado dadas a las diversas vulnerabilidades que pueden tener los sistemas de seguridad.

Capítulo III

Diseño Metodológico

3.1. Tipo De Investigación

Iniciando desde la idea de que el objetivo principal de la investigación es la identificar la viabilidad de una aplicación, cuyo objetivo final es que permita almacenar y mantener de manera confidente información delicada y personal de una persona, manteniendo una accesibilidad alta de estos datos por parte del propietario, se llegó a la conclusión de implementar el tipo de investigación exploratoria.

3.1.1. Propósito

El propósito de esta selección es debido a que el objetivo principal de este tipo de investigación es encontrar mecanismos o estrategias que permitan lograr un objetivo concreto, en otras palabras, este permite solucionar problemas específicos, en este caso, la mejor manera de crear un aplicativo móvil que cumpla con el fin de proteger los datos.

Es importante realizar una investigación que permita determinar las mejores prácticas o funciones a implementar, para la creación de la herramienta, ya sea a nivel de seguridad, como lo pueden ser métodos de verificación, en el que la mayoría de aplicativos realizan este tipo de proceso al momento de crear una nueva cuenta de usuario, donde teniendo en cuenta la experiencia propia como todo usuario, se puede constatar de manera básica que existen diferentes métodos de verificación como:

- Envió de un código al correo electrónico, para posteriormente ser digitado en la aplicación,
- Creación de cuentas a través de cuentas externas, como lo pueden ser Gmail o Facebook

- Recibir un mensaje de texto SMS al mismo celular donde se desea crear la nueva cuenta, tal como lo realiza WhatsApp
- Y en casos más extremos, verificación por medio de una fotografía de la misma cedula del usuario, una aplicación muy conocida, que realiza este proceso es Nequi, donde es necesario, además, una fotografía del propietario de la cedula.

Además de lo anterior, determinar los métodos de acceso, que deberá usar el usuario para ingresar a sus datos, es aún más importante que el punto anterior, ya que si recordamos se desea que los datos sean de fácil acceso, evitando engorrosos procesos de inicio de sesión y de recuperación de contraseñas, pero que igualmente sean seguros y solo sean accedidos por el propietario; para esto, podemos partir como guía el ciberataque, mencionado con anterioridad, que sufrió la compañía LogMein y más específicamente su herramienta LastPass, donde básicamente las claves maestras de acceso de cuentas fueron robadas.

Entre los otros puntos a evaluar para posteriormente implementar, reside en el método de protección de la información, concretamente algoritmo de cifrado, ya que como se constató anteriormente, la información debe prioritariamente contar con un sistema de cifrado, ayudando de esta manera que, en caso de robo, los datos no se encuentren de forma legible.

De esta manera, basándonos en estos puntos podemos cumplir con el propósito del primer objetivo específico, el cual, en pocas palabras, consiste en determinar la viabilidad de la creación de la aplicación; posteriormente y luego de fijar los parámetros que lleguen a cumplir con el intención, el propósito más adelante de la investigación pasara a la etapa de selección de requerimientos, la información plasmada en este apartado dependerá en gran parte por la información obtenida previamente; además de esto, la selección de la arquitectura apropiada para el fin, y la metodología más apropiada para la creación.

Para realizar este proceso debemos tener en cuenta primeramente que el tipo de investigación cuenta con tres fases que son las siguiente:

Figura 2

Etapas Investigación Aplicada.

Fuente: Tomado de (CRAI, s.f.).

Analizando esta última ilustración, podemos comprobar que, en este punto de la investigación, nos encontramos en la fase de ideación y conceptualización, más específicamente en el punto de (Diseño de metodología), donde ya previamente se ha identificado la selección del tema, el planteamiento del problema, se realizaron igualmente los antecedentes junto con las bases legales.

El enfoque de la investigación, por el contexto que se desea manejar, será de tipo mixto (Cuantitativo, Cualitativo), debido a que gran parte de la información se determinara por medio de datos tipos cualitativos, donde se determinara los mejores métodos a implementar a nivel

general, también debemos plasmar por medio de datos cuantitativos ciertos datos como lo pueden ser, características sobre los algoritmos de cifrado, costos, etc.

Cabe mencionar, que los puntos explicados previamente son básicos y generalmente usados en la mayoría de las aplicaciones móviles, por ende, es muy probable que, en el transcurso de las investigaciones se encuentren otros puntos necesarios para la creación de la herramienta.

3.2. Lugar

Complementando el punto anterior, es importante identificar de qué manera se realizará la investigación, partiendo de que en este punto se tiene la posibilidad de seleccionar tres tipos de investigación, debemos primero identificar qué procedimiento de investigación se debe realizar en cada una de ellas, para que de esta manera se pueda realizar una selección adecuada.

3.2.1.1. investigación documental

Podemos primeramente definir qué, la investigación documental básicamente consiste una búsqueda y recopilación de información por diversos medios de fuentes, que pueden ser libros, revistas, documentales, videos entre otros; sobre un tema ya existente, generalmente se busca realizar una comparación de las diversas fuentes en un tema específico, con el objetivo de llegar a una conclusión.

Entre sus rasgos principales podemos encontrar que, los resultados de este tipo de investigación generalmente son de tipo cualitativo. Además, en vista de lo anterior, se puede mencionar que la aplicación de la investigación documental no está restringa por ningún tema, por ende, puede ser utilizada en cualquier campo; lo cual generara que al final de la investigación se creen nuevos conocimientos sobre el tema investigado. (Restrepo García)

Así mismo, la investigación documental está dividida en diferentes tipos, puntalmente en dos, la exploratoria y la informativa. Donde la investigación exploratoria consiste en comprobar la veracidad respecto a un tema específico a través de una evaluación de los diferentes resultados; mientras que la investigación informativa, busca resaltar los puntos más importantes sobre un tema, sin la necesidad de realizar el consentimiento de la información.

- En complemento, las ventajas que nos proporciona este tipo de investigación son:
- Ahorro de tiempo y dinero,
- Fácil accesibilidad de la información y en grandes cantidades,
- Se puede realizar una verificación de las conclusiones. (QuestionPro)

3.2.1.2. investigación experimental

Según el profesor Atenea Alonso Serrano y otros estudiantes de la Universidad Nacional Enrique Guzmán, afirman que una investigación experimental es donde.

> El investigador manipula una o más variables de estudio, para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas. Dicho de otra forma, un experimento consiste en hacer un cambio en el valor de una variable (variable independiente) y observar su efecto en otra variable (variable dependiente)" (Alonso Serrano, y otros).

En palabras más simples, podemos precisar que tal como su nombre lo indica, este tipo de investigación consiste en un proceso de experimentación sobre un tema o variable en particular, donde generalmente los resultados no están definidos, más sin embargo pueden estar vaticinados, también se puede mencionar que es un proceso de prueba y error que se manejan en el gran número de los resultados datos tipo cuantitativos; usando de ejemplo la difícil situación sanitaria por la que pasa el planeta, debido al SARS-CoV-2, más conocido como el Covid 19, donde

diversos laboratorios a nivel global enfocaron sus esfuerzos en la creación de una vacuna. Ya varias de estas investigaciones han entrado a etapa experimental, donde el objetivo es determinar la efectividad de la vacuna; el proceso en muchos casos se realizó a través de diferentes voluntarios los cuales entrarían a una fase de seguimiento y control, donde los investigadores previamente ya tienen estipulados algunos de las posibles reacciones que puedan presentar estos voluntarios. Dentro del territorio Colombia el día 7 de octubre del presente año se han escogido un total de 17 personas para realizar un ensayo experimental de la vacuna desarrollada por el conocido laboratorio Johnson & Johnson; las personas voluntarias ingresaron a una fase de control que está determinado por un periodo de dos años desde la aplicación. (PORTAFOLIO, 2020)

Luego de la definición de la investigación experimental, es importante conocer las características que la conforman, se pueden identificar principalmente seis.

Luego de la definición de la investigación experimental, es importante conocer las características que la conforman, se pueden identificar principalmente seis.

1. En primer lugar, y como se aclaró en el ejemplo anterior el uso de sujetos de experimentación es un punto clave en este tipo de investigación, generalmente estos sujetos de prueba se dividen en varios grupos, los cuales entran en un proceso de análisis; el tiempo no está claramente definido, esto depende de la investigación y del equipo de científicos.
2. Posteriormente, luego del proceso de control y de obtener los resultados de los grupos de experimentación es necesario realizar una comparación de estos resultados, con el objetivo de identificar cual se acerca más al resultado u objetivo final planteado inicialmente por el grupo de investigación.

3. Teniendo en cuenta la definición dada por Javier Murillo al inicio de este punto, las investigaciones experimentales son muy similares a las funciones matemáticas las cuales cuentan con variables, (Dependientes e independientes), donde el resultado de la investigación depende de los resultados de los controles realizados los cuales pueden ser llamados variables independientes
4. Se deberá realizar una medición de las variables dependientes, para esto, las variables independientes serán analizadas, posteriormente el resultado dado por la variable dependiente. Es primordial que el resultado de estos datos o funciones sean de tipo cuantitativo, de lo contrario no se ajustaría con la definición de una investigación experimental. (Alonso Serrano, y otros).

3.2.1.3. investigación De Campo

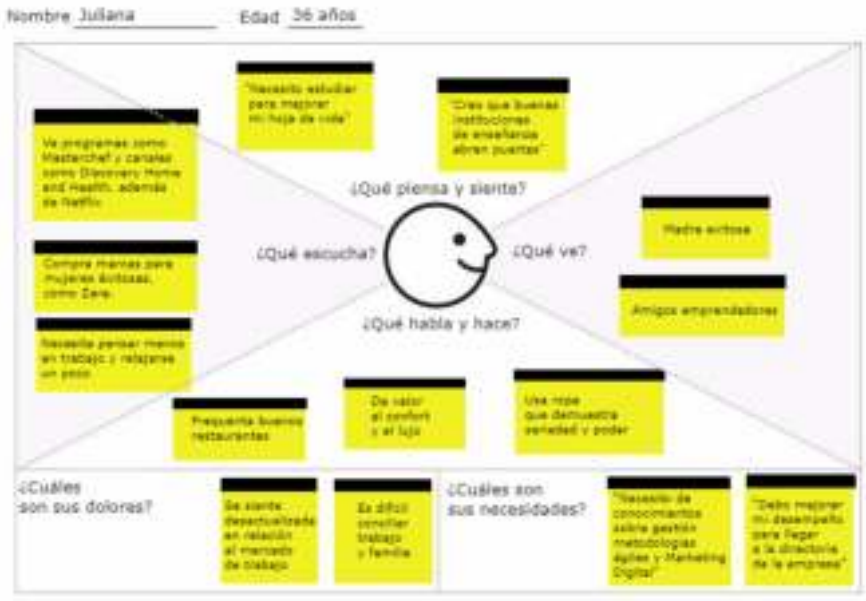
De manera similar como los anteriores tipos de investigaciones, el objetivo de la investigación de campo, es obtener información de un tema específico, sin embargo, lo que la diferencia de las demás y la caracteriza es que, es necesario que el investigador o equipo de investigación se trasladen al lugar de los sucesos y desde el mismo lugar realizar los procesos de investigación obteniendo resultados.

Entre las dificultades o desventajas se encuentran que es necesario un alto consumo de tiempo e igualmente altos costos, debido al traslado del equipo de investigación. Cabe mencionar que, los resultados suelen ser mucho más precisos, dado a que los datos recolectados son tomados por los mismos investigadores, sin necesidad de fuentes de información externos. No obstante, dependiendo de la investigación a realizar, en algunos casos se efectuarán indagaciones o encuestas a personas que estén relacionadas con el tema investigado.

Un ejemplo de lo anterior y que es muy común, son las encuestas que realizan algunas organizaciones previamente a lanzar un nuevo producto al mercado, donde a un grupo de personas previamente clasificado, se les realizaran un numero de preguntas respecto a este producto, para posteriormente analizar los resultados obtenidos y crear un plan de marketing. (Cajal, 2020) Sin embargo, con el pasar del tiempo este método de recolección de datos, se ha ido descartando debido a que, generalmente es un proceso cansino para los encuestados, lo que genera que los datos no brinden información precisa; por esta razón, un método muy usado para determinar el tipo de cliente al cual está enfocado algún producto o servicio, es la matriz de la empatía.

Figura 3

Ejemplo Matriz de la Empatía



Fuente: Tomado de (Custódio, 2017).

Donde por medio de contestar un número muy pequeño de preguntas, se puede tener una base muy clara del tipo de cliente. No obstante, este tipo de herramienta también puede ser usada en otros tipos de investigaciones, debido a que no es necesario un trabajo de campo para su elaboración. Cabe mencionar que, en caso de que el tema sea muy diferente al mencionado, la encuesta no pierde importancia, pero está debe contar con las recomendaciones básicas para su elaboración, las cuales consisten en que la encuesta debe contar con un número muy pequeño de interrogantes y que sean preguntas que ofrezcan gran aporte de importancia de la información en los resultados.

3.2.1.4. Investigación a implementar

Teniendo en cuenta la explicación de los tipos de investigaciones que se pueden implementar dentro de la presente investigación, se puede llegar a la conclusión que la investigación documental sería la más óptima para este caso, debido a que es necesario identificar las mejores métodos o buenas prácticas a implementar para determinar la viabilidad de la herramienta, este proceso se deberá realizar por medio de diversas comparaciones de diferentes fuentes, donde ni por medio de la investigación experimental y mucho menos por la exploración de campo se puede realizar este tipo de comparaciones. Mas específicamente se puede mencionar que se realizara una investigación documental exploratoria, ratificando de esta manera el tipo de investigación seleccionada, debido precisamente a que se debe realizar una comprobación de los resultados basada en la información adquirida.

3.2.2. Alcance

Finalmente, como alcance de la investigación es primordial, realizar un proceso de exploración de diferentes variables, que lleven a identificar la forma más optima de elaborar la herramienta; algunas de las variables a evaluar van desde los métodos de seguridad, como lo son:

- Autentificación de usuario,
- Protección de datos,
- Accesibilidad.

Así como, aspectos en la arquitectura que debe tener la herramienta. Además de lo anterior, es fundamental identificar el instrumento de almacenamiento de los datos, un punto a tener en cuenta es que se desea que la aplicación sea para dispositivos móviles, de este modo, varias herramientas muy conocidas como MySQL o SQL Server pueden no ser la mejor opción para el objetivo principal, por ende, una investigación argumentativa o también conocida como exploratoria, sería la mejor opción para el desarrollo de la investigación.

En aspectos generales se desea, explorar, analizar e identificar por medio de diferentes fuentes de información, la viabilidad de crear un aplicativo móvil, que permita almacenar los datos necesarios para la accesibilidad de correos electrónicos o cuentas de usuarios, permitiendo a los consumidores tener una accesibilidad alta de los datos almacenados, sin necesidad de una conexión a internet. Por último, pero no por esto menos importante, se desee identificar si es posible iniciar sesión en cualquiera de las cuentas de usuario, desde el mismo dispositivo móvil.

Cabe mencionar que el objetivo de la creación de la aplicación no es la de reemplazar los sistemas de seguridad que usan las grandes compañías para la protección de información, sino de convertirse en un facilitador de acceso que evite los procesos antes mencionados como, por ejemplo: (recuperación de contraseña).

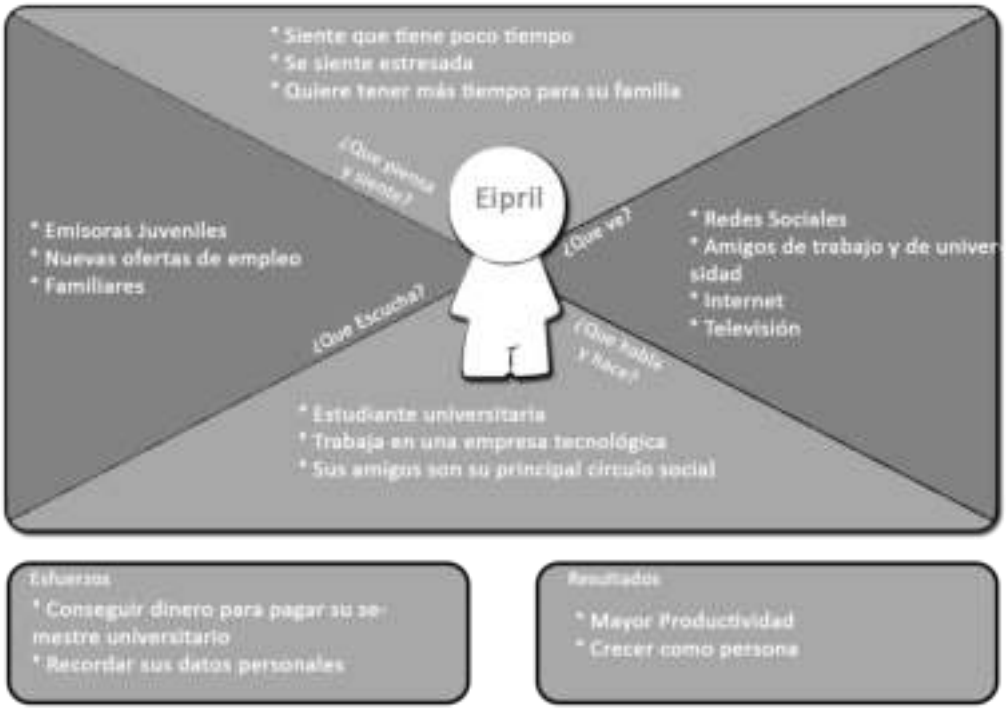
3.2.3. Población

Partiendo de la idea de que se desea crear una solución a una problemática de gran escala, la cual es la dificultad para recordar un gran número de contraseñas de las diferentes cuentas de usuarios, es difícil seleccionar una población puntual y mucho más una muestra de estudio. No

obstante, es posible identificar de manera general un posible modelo de tipo de población de este modo, seleccionar un posible arquetipo de cliente que puedan usar la aplicación; para realizar este proceso se usara la matriz de la empatía. Es importante tener en cuenta que la información plasmada será centrada principalmente para el producto o servicio que se ira a brindar, en esta ocasión la información deberá estar enfocada en la aplicación a desarrollar.

Figura 4

Matriz de la Empatía



Fuente: Elaboración propia

Luego de desarrollar la matriz de la empatía, podemos determinar de manera general que la población o cliente a la cual deberá estar enfocada la herramienta, son personas que tengan una edad aproximada entre 20 a 40 años de edad, que este cursando alguna carrera universitaria pero que a la vez se encuentren laborando, el motivo de que sean las principales personas destinadas a la creación de la herramienta, se puede basar en que son personas que por su estilo de vida,

necesiten manejar un número muy alto de información, ya sea dentro de las universidades o en la misma empresa, además, son personas que están en un proceso de crecimiento, no solamente económico sino también intelectual, la cual generalmente se encuentran rodeada de personas con el mismo perfil personal. Por su estilo de vida muy frecuentemente estas personas se encuentran en un nivel alto de estrés y de preocupación, lo que genera en mucho de los casos faltas de concentración y de memorización, no obstante, por encontrarse en una edad relativamente joven, son personas que usan frecuentemente la tecnología ya sea para informarse, comunicarse, realizar actividades para su universidad o trabajo e incluso para el ocio, finalmente, toman muy en cuenta las opiniones de sus familiares y de sus amigos más cercanos.

De esta manera se logra determinar un arquetipo general de cliente o de población para la investigación, sin embargo, es necesario mencionar que, por ser una problemática tan amplia, no se deben descartar rangos diferentes de edad u otras características que puede poseer el usuario, debido a que, el uso de la tecnología es cada vez más amplia lo que ha provocado que personas más jóvenes de la edad establecida, también manejen un gran número de información, incluso personas adulto mayores también cuentan con dispositivos móviles y por ende cuentas de usuario que tienen la necesidad de recordar estos datos, claro está, sin el mismo número de información.

3.3. Técnicas E Instrumentos De Recolección De Datos

Es indispensable para validar el diseño de la aplicación, determinar de qué forma o procedimiento será implementada dentro de esta investigación, en otras palabras, seleccionar la técnica de recolección de información más adecuada para cumplir con el objetivo; asimismo, los instrumentos deberán ser los más adecuados; se puede definir como instrumentos a los recursos que se usarán para recoger información. Es necesario para la selección de la técnica de los instrumentos tener en cuenta que, principalmente se desee realizar una validación de una

aplicación que efectúe ciertas condiciones, como lo son la verificación de usuarios, cifrado de información, generador de contraseñas, entre otros; para que finalmente cumpla con el objetivo final de almacenar la información de accesos de cuentas , por ende, es primordial realizar una comparación de información para determinar y seleccionar los métodos más acordes para la aplicación.

3.3.1. Técnica

En este apartado existen varias opciones para realizar el proceso o técnica de recolección de información, entre las más comunes se encuentran la técnica de observación, recopilación documental, entrevista, encuesta y demás, partiendo con la idea de que es necesario realizar una comparación de datos para identificar los mejores métodos de seguridad y buenas prácticas a implementar en la app, se puede definir que la más acorde seria la técnica de recopilación documental, considerando la definición dada por la escuela de suboficiales armara Argentina, donde menciona que, la recopilación documental consiste en un proceso de examinar a profundidad información sobre un tema en específico, obtenida por varios autores, y además que la documentación puede "definirse" como el testimonio sobre información investigada, durante un periodo de tiempo (Escuela de Soboficiales Armada Argentina, 2018); esta técnica es muy útil al momento en que se desee realizar un seguimiento o comparaciones sobre un tema puntual; el hecho de que se tomen varios resultados de diferentes autores o fuentes, puede anular una idea o de la misma manera ratificarla, por esta razón, es primordial realizar una revisión de la literatura o de la documentación precisa, ya que como objetivo principal dentro de esta técnica de recolección de información, se busca obtener nuevo conocimiento luego de analizar los datos; es totalmente innecesario realizar una investigación sobre un tema ya analizado previamente sin aportar algún tipo de conclusión diferente a los definidos.

Sin embargo, en ciertos puntos de la investigación, será necesario realizar un proceso diferente a la recolección documental, dirigido más a la técnica de observación y exploración, por ejemplo, es esencial identificar que funciones tienen herramientas ya creadas, que ofrezcan un servicio muy similar al que se desea diseñar, y posibles vulnerabilidades que puedan tener, para de esta manera crear un valor agregado.

3.3.2. Instrumentos

Es muy frecuente cuando hablamos de las bases de recopilación documental, imaginarse como principales y tal vez, únicas fuentes de información a los documentos escritos como tal, sin embargo, la selección de fuentes de información es mucho más amplia, así como lo expone nuevamente la escuela de suboficiales de Argentina, a través de su documento metodología de la investigación, donde menciona una lista muy completa sobre otras fuentes de información: (Escuela de Soboficiales Armada Argentina, 2018)

- Seminarios,
- Revistas,
- Boletines,
- Obras literarias,
- Fotografías,
- Documentales,
- Pinturas,
- Discos,
- Grabaciones, entre otros.

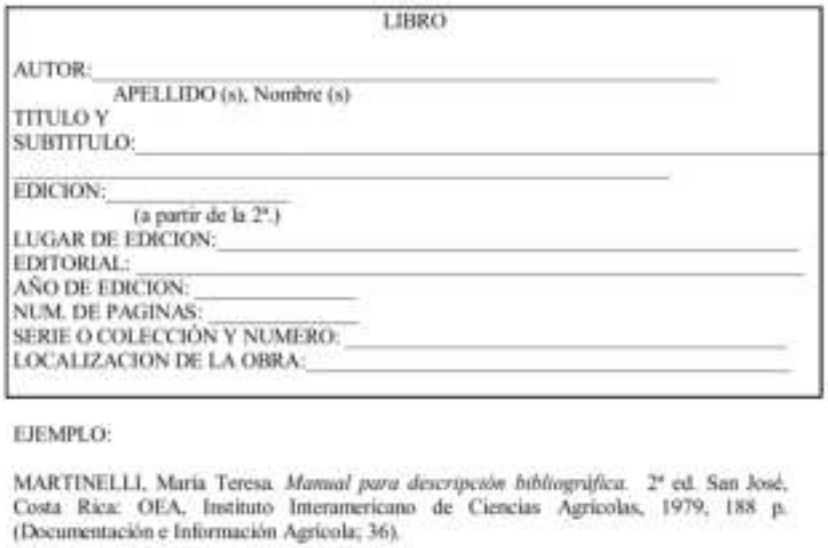
Además de las diferentes fuentes de información que pueden ser usadas para realizar la recolección de datos, existen igualmente un gran número de instrumentos; generalmente los

instrumentos usados dentro de la técnica de recopilación de información son por medio de fichas que pueden servir de apoyo para tener un seguimiento sobre la investigación respecto a ideas importantes que el autor considere. Dentro la investigación realizada por Patricia Bracamontes Perez, junto con sus 3 compañeros más de investigación, mencionan como mínimo la existencia de 12 fichas o instrumentos de recolección de información, dentro de las más notorias se encuentran: (Bracamontes Perez, Chapan Seba, Crispin Bapo, & Ronquillo Jimenez, 2016)

A pesar de que cada una de estas fichas tengan una función puntual dentro de la recolección de datos dependiendo del contexto y de la fuente de información, se puede definir que el objetivo general del uso de las fichas en una investigación consiste en realizar las respectivas citaciones de los autores en relación con la información obtenido de ellos. Por este motivo, las diferentes fichas contienen de manera general información muy similar entre ellas, como lo pueden ser el título de la obra, editorial, lugar de publicación, edición, número de páginas y por supuesto el nombre del autor; tal como se puede apreciar en la siguiente figura.

Figura 5

Ejemplo Ficha Bibliográfica.



LIBRO

AUTOR: _____
APELLIDO (s), Nombre (s)
TITULO Y
SUBTITULO: _____
_____
EDICION: _____
(a partir de la 2ª.)
LUGAR DE EDICION: _____
EDITORIAL: _____
AÑO DE EDICION: _____
NUM. DE PAGINAS: _____
SERIE O COLECCIÓN Y NUMERO: _____
LOCALIZACION DE LA OBRA: _____

EJEMPLO:

MARTINELLI, María Teresa. *Manual para descripción bibliográfica.* 2ª ed. San José, Costa Rica: OEA, Instituto Interamericano de Ciencias Agrícolas, 1979, 188 p. (Documentación e Información Agrícola; 36).

Fuente: (TIPOS DE FICHA BIBLIOGRAFICA)

No obstante, y como se ya se ha mencionado esto depende del contexto, ya que poniendo como ejemplo al momento de obtener algún tipo de información por medio electrónicos o digital, el formato de la ficha cambiará, donde esencialmente se deberá ingresar el enlace o URL de la página web.

Capítulo IV

Resultados De La Investigación

Luego de determinar la metodología junto con las técnicas e instrumentos de recolección de la información, el siguiente paso y en fundamento con las fases de la investigación aplicada, se inicia en este apartado la fase de ejecución, más específicamente las etapas de la validación de la hipótesis, mediante el desarrollo de la metodología selecciono con el fin de enfrentar de lleno con la ejecución de los objetivos, tal cual como se visualiza en la figura II.

4.1. Resultados Del Objetivo Específico N°1

Para el inicio de la investigación como tal y más puntualmente plasmar los resultados de la misma, debemos considerar en primera instancia y como guía los objetivos específicos establecidos al inicio de la presente investigación; haciendo una evocación de esto objetivos, podemos establecer que como primer objetivo específico se desea "validar por medio de la investigación, la creación de la aplicación, que permita la confidencialidad de datos", partiendo de que la idea "principal" de este objetivo es la validación de una aplicación, es esencial determinar que estructura o puntos debe contener la herramienta. De manera inicial se puede establecer que es básico que la aplicación tenga una opción de r**egistro, autentificación de usuario** y posteriormente el **inicio de sesión**, de esta manera crear un perfil donde se pueda almacenar la información necesaria para el inicio de sesiones en los correos electrónicos o cuentas de usuario en los diferentes sitios web donde se haya creado un perfil. En segunda instancia y como punto fundamental debido a la importancia de su implementación y que se logró establecer, es el **cifrado de datos**, de nada sirve tener una herramienta que permita almacenar información tan delicada y de suma importancia, si mínimamente no cuenta con este método de seguridad "básico" ya que, de lo contrario, más que una app que proporcione

seguridad y accesibilidad de datos a los usuarios será una herramienta que facilite el robo de los mismos. Como tercer punto a investigar y luego de determinar los riesgos que conlleva tener una contraseña con baja estructura de seguridad, se debe determinar la viabilidad de implementar un **generador de contraseñas**, que por supuesto cuente con las normas mínimas identificadas y plasmadas en el punto (contraseñas seguras); al hablar de gestión de contraseñas se puede hablar igualmente de **almacenamiento** de la información, por esta razón es necesario analizar la mejor forma de realizar este proceso que permita que los datos cumplan con los pilares que la seguridad informática menciona. Por último, pero no menos importante y como valor agregado se desea comprobar la capacidad de establecer la operación de inicio de sesión desde el mismo dispositivo móvil en otras palabras, un **acceso remoto**.

4.1.1. Registro y autentificación

Basándose en la idea de que el diseño se desea efectuar específicamente para dispositivos móviles que cuenten con Android como su sistema operativo, es conveniente usar como fuente de información la guía de desarrollador creada por la ampliamente conocida compañía Google.

Como experiencia personal y la de la mayoría de los usuarios de Android, al momento de crear una cuenta de usuario generalmente nos encontramos con un formulario de registro muy similar al siguiente:

Figura 6

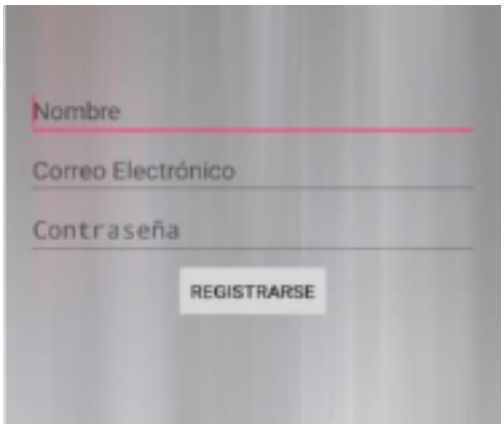
Ejemplo Registro General

Fuente: Elaboración propia

Esto igualmente lo podemos corroborar con lo que demuestra Carlos Flores Martín dentro de su trabajo de grado, cuyo objetivo principal fue el desarrollo de una aplicación móvil para la gestión y recomendación de información de actualidad, donde como registro de usuario para su aplicación implemento el siguiente formulario:

Figura 7

Registro de Usuario



Fuente: Tomado de (Flores Martín, 2017).

Como podemos visualizar, los formularios de registro son muy similares respecto a la recolección de datos solicitada para el proceso de registro, la única diferencia notoria es el campo de texto, o en palabras más tácticas el EdixText adicional que se encuentra en la figura 6, el cual es usado para confirmar que la contraseña se haya digitado correctamente.

No obstante, realizando una comparación del objetivo general entre la establecida dentro de este documento y la determinada por Carlos Martín en su proyecto la cual dice.

> La finalidad principal de este Trabajo Fin de Grado es el desarrollo de una aplicación móvil para poder recomendar ciertos aspectos de ocio, como es la cartelera de cine y las obras de teatro, además de poder mostrar las últimas noticias que han ocurrido en el mundo y los tweets de un determinado usuario o hashtag, entre otros (Flores Martín, 2017).

Podemos darnos cuenta que, la información que se planteó usar dentro la aplicación de Carlos es mucho más enfocada, como él lo dice, al ocio o al entretenimiento, datos que no se pueden considerar de alta importancia, sin embargo, la información que se ha planteado proteger y manejar dentro de este documento, es de origen muy personal y por ende con alto grado de importancia, donde por medio de esta idea podemos preguntarnos, ¿Es suficiente los datos mostrados dentro de las figuras usadas como ejemplo, para realizar un registro seguro y confiable que permita la confidencialidad de los datos personales de los usuarios?. Realizando un proceso de observación sobre aplicaciones que almacenan información muy delicada, como lo son las aplicaciones bancarias también conocidas como neobancos, entre las más conocidas en el territorio Colombiano se encuentran Daviplata, Movii y Nequi; se puede analizar que los métodos que utilizan estas herramientas para los registros son un poco más extensos pero a la vez extremadamente seguro; como ejemplo en este caso, se puede mencionar el proceso de la herramienta Nequi, en donde el primero paso, consiste en solicitar el número de celular, el uso

de esta dato dentro de la aplicación se debe a que este se convertirá en el número de cuenta y de paso, será utilizado como medio de verificación, a través del envió de un código vía mensaje de texto, tal como se puede visualizar dentro del video que se puede encontrar en la plataforma YouTube, específicamente dentro del mismo canal de la herramienta.

Figura 8

Código de Verificación Nequi

Fuente: Tomado de (Nequi, 2020).

Nota: El envió del código de verificación se hace por medio de un mensaje de texto, el cual en este caso es 2754.

Además del código de verificación, la herramienta solicita como dato la fecha de expedición de la cedula junto con una fotografía del propietario de la misma, confirmando de esta manera la identidad del usuario, por último, y de manera algo más general como la mayoría de los formularios de registro, se le es solicitado al usuario ingresar un correo electrónico y una clave de acceso.

Figura 9

Creación Clave Nequi

Fuente: Tomado de Nequi (Nequi, 2020).

Nota: La figura permite determinar que Nequi utiliza la autentificación de dos pasos por medio de un código de 4 dígitos.

Analizando el método de verificación usado por Bancolombia dentro de su aplicativo bancario (Nequi), se puede deducir que cuenta con uno de los métodos más utilizados en la actualidad que permite aumentar la seguridad en el proceso de autentificación de un usuario, conocida como activación por autentificación en dos pasos, también conocido como **2FA**, Indexa afirma que, este método consiste en el uso de una clave, generalmente entre 4 a 6 caracteres, que es enviado al teléfono celular por medio de mensajes de texto y en conjunto con la contraseña asignada por el usuario, se deberán digital en el dispositivo móvil, para inicialmente realizar el proceso de autentificación y posteriormente tener acceso a la cuenta de usuario o correo electrónico. Este método es muy usado actualmente por las entidades bancarias en sus aplicaciones móviles, debido a que es un sistema muy seguro, tanto así, que es casi necesario que el atacante deba tener

en sus manos el teléfono de la víctima, junto con la contraseña para el acceso a alguna cuenta. (Indexa Capital, s.f.)

Figura 10

Verificación 2FA por Celular

Fuente: Tomado de (Imperva).

Los códigos enviados al teléfono son de forma aleatoria, y solo tiene un ciclo de vida muy corto, en otras palabras, caduca luego de unos minutos desde su creación, de esta forma se garantiza que el usuario o propietarios del dispositivo sea el que esté realizando la operación. Además, de lo anterior, este método cuenta con más ventajas: (AMBIT TEAM, 2019)

- Obsolescencia del método de ciberataque phishing,
- Muro extra de protección de acceso,
- Permite la reducción de digitar la contraseña en varias ocasiones.

En términos generales, la verificación por el método 2FA, es un muy sencillo y el cual está compuesto por tres pasos principalmente, en el primero, el usuario como todo proceso de creación o acceso a una cuenta, deberá ingresar su nombre de usuario, junto con la contraseña y claro está, su número de celular, el objetivo de ingresar este último dato, es debido a que al dispositivo móvil se le enviara un código aleatorio, tal como se puede ver en la figura 10, por

ultimo este código deberá ser digitado en el formulario para finalizar el proceso de autentificación.

Este método extremadamente seguro es usado en la herramienta Nequi como su método de verificación, destacándose notoriamente en cuestión de seguridad, con los formularios de registro usados como ejemplo al inicio de este apartado.

De manera muy similar funciona el registro de la aplicación Daviplata, donde igualmente es solicitado al usuario una fotografía de su documento de identidad, para posteriormente recibir el código vía mensaje de texto, la diferencia en este caso es la longitud en el código, la cual está compuesta por 6 caracteres.

Figura 11

Autentificación Daviplata por Cedula

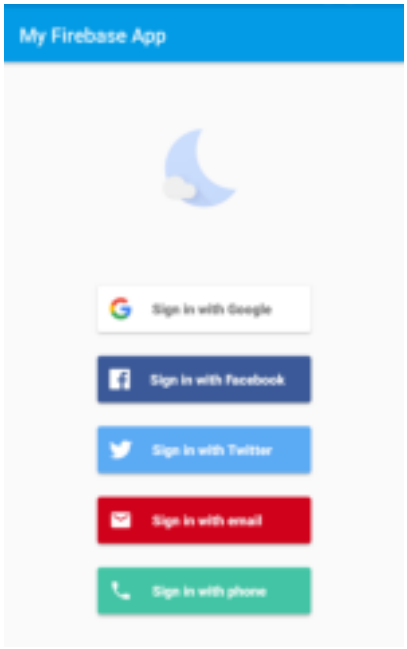
Fuente: (Banco Davivienda Colombia, 2020).

Los métodos de registro mencionados hasta el momento dentro del sistema operativo Android se han descrito de una manera muy general, por ende, adentrándonos algo más en el tema, por medio de un proceso de observación se puede identificar que igualmente existen registros “rápidos”, los cuales por medio de otras plataformas altamente conocidas se puede realizar el proceso de registro mediante la selección de alguna de ellas tal como se puede ver en

la figura 12 y en el cual los usuarios con un tiempo considerado usando los dispositivos Android pueden identificar con facilidad.

Figura 12

Ejemplo Registros Android



Fuente: Tomado de (Google LLC, 2020).

El método de registro o flujo de acceso varía dependiendo de la opción seleccionada, por ejemplo, está la opción de verificación por parte de un correo electrónico, cuyo medio de verificación consiste en el envío de un enlace al email digitado, el usuario posteriormente deberá ingresar a su correo y seleccionar el enlace que fue enviado inicialmente, por medio de este proceso se realizara la verificación de la cuenta, muy similar al proceso mencionado con anterioridad, donde es enviado al teléfono móvil un código, cabe aclarar que, a pesar de que lo medios son diferentes, el método es igual, implementado la autentificación 2FA. De igual manera, se puede realizar el registro directamente con una cuenta de correo electrónico de Gmail, donde generalmente la contraseña que se establecerá dentro de la nueva cuenta, será la misma

que el usuario seleccionó para su email. Google como actual poseedora de los derechos del sistema operativo Android desde el año 2005, menciona en su guía de desarrollador que esta función es denominada como **FirebaseUI**, proporcionando por medio de la implementación varias ventajas:

- Flujo de acceso por medio del correo electrónico, autentificación telefónica, Twitter, GitHub entre otros,
- Administración de cuentas, y restablecimientos de contraseñas,
- Vinculación de cuentas. (Google LLC, 2020)

Como se puede identificar el uso de esta función es muy importante y además provee utilidades bastante seguras y optimas respecto a registro de usuarios, el cual está siendo implementado en un gran número de aplicaciones; proporcionándoles un sistema seguro y confiable respecto a la verificación de usuarios.

Al Realizar una indagación más a profundidad sobre FirebaseUI es pertinente destacar que, es una de las tantas funciones con las que cuenta una de las plataformas de desarrollo más conocida dentro del mundo del desarrollo móvil, denominada como **Firebase** la cual es usada por organizaciones bastante conocidas e importantes, entre las que se encuentran The New York Times, Alibaba, Duolingo, Twitch e incluso YouTube; creada por Google con el objetivo de facilitar el desarrollo móvil (Android, IOS) e incluso desarrollo web, brindando a los desarrolladores varias herramientas, cada una con una utilidad diferente, pero en conjunto conforman un servicio altamente productivo ya sea a nivel de desarrollo e igualmente marketing, así lo afirma Google en la misma página oficial de la plataforma. Dentro de las herramientas que se mencionan en el sitio web y más usadas se encuentran:

- Cloud Firestore,

- Hosting,
- Realtime Database,
- Authentication,
- Remote config,
- Google Analytics.

Retomando el tema de autentificación y teniendo en cuenta las herramientas que ofrece Firebase, se puede identificar que ya existe una de ellas cuyo fin es la de proporcionar registro y autentificación de forma sencilla pero igualmente segura. (Google LCC, s.f.)

4.1.1.1. Firebase Authentication

Una de los instrumentos que proporciona la plataforma Firebase en el tema de verificaciones es la herramienta Authentication, disponible para (Android, IOS, Web, entre otros), la cual como su nombre lo indica, su función principal es realizar un proceso de autentificación de usuario dentro de las aplicaciones o páginas web; textualmente Google menciona que el instrumento.

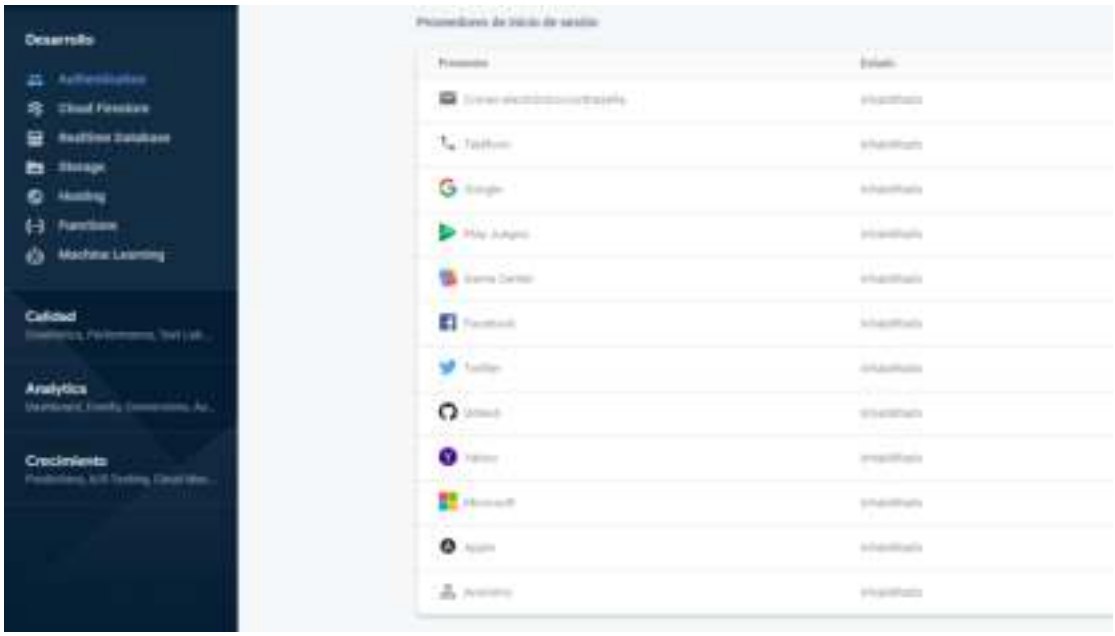
> Busca facilitar la creación de sistemas de autenticación seguros, a la vez que mejora la experiencia de integración y acceso para los usuarios finales. Proporciona una solución de identidad de extremo a extremo, compatible con cuentas de correo electrónico y contraseñas, autenticación telefónica, acceso mediante Google, Twitter, Facebook y GitHub, y mucho más (Google LCC., s.f.).

Analizando lo definido por Google, se puede identificar que el proceso de registro y autentificación por medio de algunas redes sociales y otros instrumentos, está basado bajo la implementación de esta herramienta, proporcionando alta confiabilidad durante el proceso.

Luego de ingresar a la plataforma, podemos encontrar un número amplio de proveedores de inicio de sesión aparte de los medios de autentificación mencionados hasta el momento, tal como se puede visualizar con la siguiente imagen:

Figura 13

Proveedores Firebase Authentication



Fuente: Tomado de (Google LCC).

Nota: Método de verificación proporcionados por Firebase Authentication.

Al realizar un análisis de estos proveedores se puede identificar que algunas de ellas funcionan de una manera distinta; algunos métodos como lo son la autentificación por teléfono (Phone Auth) y correo electrónico, implementan el proceso de autentificación de dos factores (2FA). La gran mayoría de los demás proveedores mostrados en la figura 13, realizan un proceso diferente, donde estos métodos de autentificación funcionan por medio de un token OAuth de identidad federara, cuyo proceso de registro se realiza por medio una red social o sitio web, tal como se había explicado anteriormente.

Figura 14

Autentificación OAuth

Fuente: Tomado de (Google LCC, 2020).

Es importante conocer los limites o restricciones de uso, puntualmente la frecuencia con lo que se puede ejecutar la herramienta o las operaciones dentro de la misma.

Como primer límite, se encuentra la creación y eliminación de cuentas, donde para crearlas solo se podrán ingresar 100 cuentas/dirección IP/hora; asimismo, para la eliminación existe una limitación de 10 cuentas/segundo. Identificadas estas variables se puede identificar que, afectarían en gran medida cuando la aplicación maneje información masiva o en palabras técnicas Big Data, ya que, en un número muy reducido de usuarios, sería poco probable que existan dificultades para alcanzar algunos de estos límites.

Del mismo modo, existe un límite de usuarios por proyecto; cómo se puede ver en la figura 13, uno de los métodos de autentificación que proporciona la plataforma es por medio de una cuenta anónima, la cual tiene como restricción por aplicativo, el almacenamiento de 100 millones de ellas, cabe mencionar que, esta aplicación en caso dado no implementara esta función, debido a que es necesario que los usuarios realicen un registro como tal, permitiendo el proceso de autentificación y de paso realizar una copia de seguridad de la Data, cosa que con las cuentas

anónimos no sucede; no obstante, para cuentas de usuarios registrados no existen ningún límite, permitiendo de este modo, una gran concurrencia de usuarios, teniendo en cuenta al masivo público que ostentan la problemática inicialmente mencionada.

Para los siguientes limites (correos electrónicos, generación de vínculos), se tienen dos planes los cuales son: Spark, Blaze. Donde de manera general y basado en las siguientes tablas (3, 4), se puede determinar que el plan Blaze otorga limites menos estrictos en comparación con Spark. (Google LCC, 2020)

Tabla 3

Limites Correo Electrónico

Operación	Límite del plan Spark	Límite del plan Blaze
Mensajes de verificación de dirección	1.000 correos electrónicos/día	100.000 correos electrónicos/día
Correos electrónicos de cambio de dirección	1.000 correos electrónicos/día	10.000 correos electrónicos/día
Correos electrónicos de restablecimientos de contraseña	150 correos electrónicos/día	10.000 correos electrónicos/día
Correos electrónicos de acceso al vinculo del correo electrónico	2.000 correos electrónicos/día	25.000 correos electrónicos/día

Fuente: Tomado de (Google LCC, 2020).

Tabla 4

Límites de Generación de Vínculos de Correo Electrónico

Operación	Límite del plan Spark	Límite del plan Blaze
Vinculo de verificación de dirección	10.000 correos electrónicos/día	1.000.000 correos electrónicos/día

Operación	Límite del plan Spark	Límite del plan Blaze
Vínculos de restablecimiento de contraseña	1.500 correos electrónicos/día	100.000 correos electrónicos/día
Vinculo de acceso	20.000 correos electrónicos	250.000 correos electrónicos/día

Fuente: Tomado de (Google LCC, 2020).

Los limites en mención para este caso, son de gran importancia, debido a que puede ser uno de los métodos más usados por su seguridad para realizar las autentificaciones; no obstante, hay un inconveniente dentro de esta forma de verificación que sucedería precisamente en el proceso de registro de usuarios, el cual consiste en una necesidad de conectarse a la red, sin embargo, el más apropiado y que no necesitaría de alguna conexión, es el método de autentificación a través de mensaje de texto (SMS), el cual, como los demás métodos previamente identificados tienen límites de uso tal como se definen a continuación.

Tabla 5

Límites de Accesos con Número de Teléfono

Operación	Limite
Acceso de usuario	1.600 por proyecto y por minuto, así como los precios y limites especificados en la página **Precios**
Mensajes SMS con código de verificación	50 mensajes/dirección IP/minuto, 500 mensajes/dirección IP/hora, 1500 mensajes/proyecto/minuto
Solicitud de verificación	150 solicitudes/dirección IP/hora

Fuente: Tomado de (Google LCC, 2020).

Complementando la información mostrada en la tabla 5 y más específicamente el apartado Acceso de usuario (precios), se debe mencionar que, existe una cuota gratuita de verificación por medio de este método, cuyo limite va hasta las 10.000 autentificaciones; sin embargo, luego de superado este límite, se generaran costos, cabe destacar que, los precios varían dependiendo de la

zona geográfica, dentro de (Canadá, EE.UU. e India) cada verificación tendrá un valor de USD 0.01, de la misma manera, para los demás países cada comprobación costaría USD 0.06 luego de superado el límite gratuito. (Google LCC)

En fundamento a los pilares de seguridad informática, puntualmente a la disponibilidad, se determina como la mejor manera de autentificación el método por mensajería por texto, facilitando de este modo el registro sin la necesidad de una conexión a la nube, sin embargo, por lo seguro del sistema de verificación por correo eléctrico, no se descartaría su implementación, dado a que esto no incurriría en procesos complejos de ejecución, debido a que estas dos técnicas vienen de la misma plataforma (Firebase Authentication).

4.1.1.2. Inicio De Sesión

Luego de realizar un proceso de registro en algún sitio web o aplicativo móvil, es una necesidad realizar un proceso de inicio de sesión para ingresar al perfil de usuario; de la misma manera en que es necesario realizar un proceso de registro seguro, es igualmente importante realizar el proceso de inicio de sesión por un método de confianza, pero a la vez como se planteó al inicio y basado en los pilares de la seguridad informática, cuente con alta disponibilidad.

De la misma manera que los formularios de registro, los de inicio de sesión contienen información reducida y básica muy conocidos por las personas, generalmente el formato contiene datos como el correo electrónico, contraseña y en algunos de los casos el nombre de usuario, un ejemplo de esto lo podemos visualizar en la siguiente imagen:

Figura 15

Ejemplo Formato De Inicio De Sesión

Fuente: Elaboración propia

Sin embargo, el uso de este formato provoca que las personas por necesidad tengan que usar una contraseña, donde como se mencionó en el planteamiento del problema es muy recurrente que estos datos se olviden con facilidad, y para evitar esto, se haga uso de una misma contraseña o se implemente a contraseñas poco seguras, cosa que entre las recomendaciones dadas respecto al uso de contraseña no es aconsejable realizar.

Haciendo un recuento de la plataforma Firebase y más puntualmente de las funciones que proporciona Authentication, se puede identificar que el proceso de verificación no solamente está enfocado al tema de registros, sino igualmente para el proceso de acceso o inicio de sesion; así lo corrobora Marina García en su proyecto de grado, cuyo objetivo fue desarrollar un aplicación móvil de apuesta, donde menciona que "Firebase proporciona un método de registro e inicio de sesión que no solo incluye autenticación a través de correo, sino que también permite la autenticación a través de proveedores externos como Facebook, Twitter, Github y Google."

Basándonos en lo anterior, pero principalmente en el objetivo del trabajo de grado de Marina, donde si tenemos en cuenta que los datos que se manejan en una aplicación de apuestas son

sumamente delicados, se puede concluir que Firebase Authentication igualmente sería un método seguro para el acceso, donde de la misma manera se realizará el uso de la autentificación de dos pasos, mejorando sustancialmente la seguridad del proceso. No obstante, debemos analizar que el proceso de inicio de sesión se debe realizar un gran número de veces, regularmente cada vez que el usuario desee ingresar al perfil de la cuenta, muy en contraste con el de registro, el cual se debe realizar una sola vez, por esta razón, debemos evaluar que el recibir un código de seguridad por medio de un mensaje de texto cada vez que se desee acceder a una cuenta, para luego ser digitado, se convertiría en una serie de pasos cansino, punto que se desee evitar ya que se convertiría en un proceso tortuoso muy similar al de la recuperación de contraseña; en base a esto, se puede preguntar ¿Qué método se puede implementar en la aplicación que permita un acceso seguro, pero a la vez, brinde gran disponibilidad al usuario?; realizando un análisis de varias aplicaciones que manejan información delicada, como los son Daviplata y Blockchain, donde la primera maneja las cuentas bancarias de muchos usuarios en Colombia y la otra es una aplicación muy conocida globalmente cuyo fin es la gestión de dinero virtual también conocidas como criptomonedas, se puede evidenciar que sus métodos de acceso son de la misma manera, por medio de la detección de la **huella dactilar,** conocido igualmente como autentificación biométrica.

Haciendo una revisión del proceso de registro de la aplicación Daviplata, se puede evidenciar que durante este proceso el aplicativo no solicita en ningún momento registrar las huellas, sin embargo, para prestar el servicio hace uso de las huellas almacenadas por el usuario dentro del dispositivo móvil; de este modo se permite un alto nivel de protección de los datos en caso de un robo de datos, debido a que, la “clave” de acceso no estaría almacenada en una base de datos en la nube, sino en el mismo dispositivo de manera local, esto obligaría a que necesariamente se

tenga disponibilidad del dispositivo para ingresar a los datos, favoreciendo así mismo, el acceso de los registros sin la necesidad de una conexión a la internet convirtiéndose en un sistema muy seguro, muy diferente al uso de un pin donde es necesario almacenar este dato dentro de la nube para realizar la comparación con la contraseña que el usuario ingrese al momento de querer iniciar sesión.

Figura 16

Acceso Huella Digital Daviplata

Fuente: Tomado de (Banco Davivienda S.A., 2020).

Nota: Captura de pantalla realizada a la APP móvil Daviplata donde se puede identificar que esta permite el acceso a la cuenta de usuario por medio de la huella dactilar.

4.1.1.3. Detección dactilar

El método de acceso a los dispositivos móviles por medio de la huella dactilar se ha convertido en una de las maneras más comunes, pero a la vez segura, para el acceso en los móviles, tanto así que, en el presente es muy inusual encontrar dispositivos móviles que no cuenten con este tipo de

tecnología; en la actualidad esta función se puede encontrar dentro de las mismas pantallas de los teléfonos, muy diferente a como se encontraba en los inicios de la implementación de esta tecnología, donde era muy común encontrar junto con los botones de desbloque el sensor, sin embargo, el funcionamiento y objetivo son el mismo, permitir el desbloque del celular por medio de la huella dactilar, permitiendo que el uso de un pin o patrón de seguridad pasara a un segundo plano.

Esta función fue implementada inicialmente para los dispositivos que contaban con el sistema operativo Android 6.0 (Marshmallow), de esta manera Google proporcionaba una manera segura de desbloquear los equipos y de paso solucionar de alguna manera que el usuario olvide su contraseña y por ende el acceso a su dispositivo. El método por patrones a pesar de ser un modo seguro de desbloqueo, heredo el problema que tienen las contraseñas seguras, donde existen patrones altamente seguros y complejos de cifrar, no obstante, mientras más complicado o seguro que sea el patrón, más difícil será memorizarlo; por esta razón los usuarios tienden a crear patrones fáciles de memorizar, pero poco seguros, por esta razón se optó por implementar el desbloque por huella digital. Además, tiene como ventajas que es una forma de desbloque muy veloz reduciendo procesos de digitación, de hecho, introducir de manera incorrecta una contraseña, conlleva al usuario digitar nuevamente el código demorando mucho más el proceso de desbloqueo, de la misma manera de que no hay la necesidad de digitar un código o patrón respectivamente, favorece en que no exista la posibilidad de que otras personas pueden de alguna manera observar lo digitado por el usuario en el dispositivo. (Ferreño, 2019) No obstante, a pesar de ser una técnica segura, también posee una desventaja muy notoria, el cual consiste en la suplantación de identidad, existen inventivas que permiten de alguna forma realizar una copia de una huella digital, igualmente sin la necesidad de estos técnicas, se puede realizar el acceso en

momentos en que el usuario puede no encontrarse lucido o en palabras más coloquiales no esté en sus cinco sentidos, permitiendo que otras personas puedan usar la misma huella de la mano para vulnerar el sistema.

Teniendo en cuenta esta desventaja, se llega a la conclusión de que a pesar de que el uso de la huella digital es muy seguro, permite de alguna manera el acceso a personas no autorizadas, por ende, por si solo puede no ser el sistema de seguridad más eficiente, sin embargo, para evitar esta desventaja y en base al funcionamiento de método de protección implementado en el sistema operativo de Android 6.0 para el desbloqueo de dispositivos, donde en trabajo en conjunto con un pin de seguridad y la detección por huella se realiza el acceso al dispositivo, cabe destacar que el pin es solicitado periódicamente, de este modo evitar que el proceso se convierta cansino y de paso permitir que el usuario llegue a olvidar el código de seguridad; cabe mencionar que, para dispositivos que no tengan este tipo de sensor o para personas que por alguna razón no puedan usar la tecnología de detección dactilar, la detección será netamente a través de una contraseña maestra.

4.1.1.4. Cifrado de datos

Además de las medidas de seguridad declararas en los puntos previos, es igualmente importante identificar el método o algoritmo de cifrado que permita la confidencialidad y la integridad de la información, previamente se ha podido identificar la necesidad de implementar un algoritmo que evite la legibilidad de los datos, de la misma manera, basándonos nuevamente en el robo o filtro de información que sufrió LastPass, donde una de los puntos a favor que evito el acceso en gran masa de los datos, fue debido a que la información se encontraban cifrada.

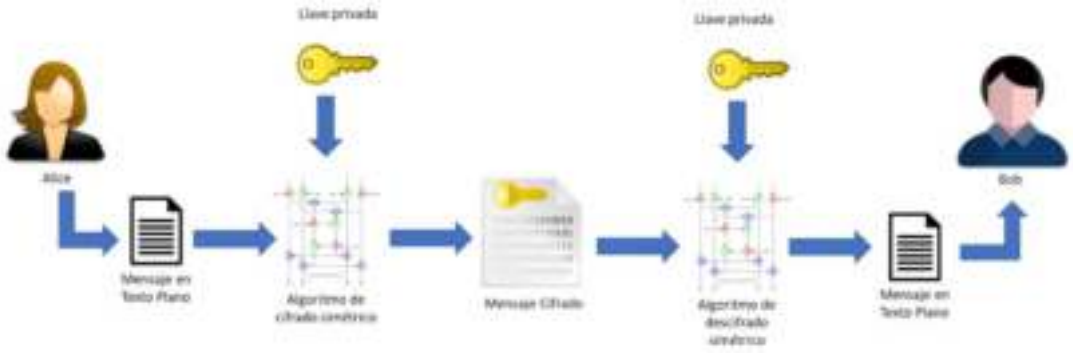
En complemento con lo explicado anteriormente respecto al tema de cifrado, existen 2 tipos de sistemas de métodos criptográficos, los cuales son:

4.1.1.4.1. Cifrado Simétrico

Este tipo de sistema de cifrado se basa en una contraseña secreta, el cual debe ser conocida únicamente por el emisor y receptor del mensaje original, donde a través de la misma se realiza el proceso de cifrado y descifrado, esta contraseña es denominada dentro del cifrado simétrico como secreto compartido, el uso es muy simple: el emisor realiza inicialmente el proceso de cifrado al mensaje inicial, donde por medio de la contraseña, creada igualmente por él, se protegerá la información y no podrá ser legible; posteriormente, el mensaje junto con la contraseña serán enviados directamente al receptor, en este punto por medio de la contraseña se podrá descifrar el mensaje y podrá ser legible; cabe mencionar que, se recomienda enviarlos a través de medios totalmente diferentes, de este modo en caso de que el mensaje o contraseña sean hurtado por un tercero no pueda acceder. El proceso en mención se puede explicar y entender mejor a través de la siguiente figura:

Figura 17

Esquema Cifrado Simétrico



Fuente: Tomado de (Vargas Salvador, 2019).

De igual modo existen dentro de este sistema dos tipos de cifrado el cual trabajan de una manera totalmente diferente; el primero de ellos es el **cifrado por bloque,** el cual consiste en que el mensaje será dividido en varios grupos de bits, para posteriormente cifrar cada uno de estos

bloques. De manera muy diferente funciona el **cifrado de flujo,** donde en este caso se realiza una división del mensaje o archivo en cada uno de los bits que lo componen, para de este modo realizar el cifrado y descifrado. (Sanjuan, Universidad del Norte)

Existen diversos algoritmos que funcionan por medio de este método y cada uno tiene diferentes características en su implementación, entre los más conocidos se encuentran:

- DES,
- 3DES,
- Blowfish,
- IDEA,
- RC5,
- AES.

Cada uno de estos algoritmos maneja una capacidad de clave de cifrado distinto manejado en bits, tal como se puede observar en la siguiente tabla:

Tabla 6

Claves de Cifrados Algoritmos Simétricos

Algoritmo	Clave de Cifrado (Bits)
DES	56
3DES	128
Blowfish	128
IDEA	128
RC5	32, 64, o 128
AES	128, 192 o 256

Fuente: Elaboración propia basada en (Sanjuan, Universidad del Norte).

De manera general sin importar el tipo de algoritmo seleccionado, el cifrado simétrico se destaca por ser un método rápido y altamente eficiente, además, es generalmente usado por su eficacia para archivos de grandes volúmenes; no obstante, dado a que para cifrar y descifrar los datos

solo se requiere de una sola contraseña, es muy riesgoso realizar el intercambio de la clave; además, debido a que por cada pareja de interlocutores (emisor - receptor) se necesita una contraseña distinta, puede incrementarse el número de claves dependiendo de la cantidad de usuarios a los que se desee enviar un mensaje.

4.1.1.4.2. Cifrado Asimétrico

En comparación con el cifrado simétrico, cuyo funcionamiento solo necesita de una llave, el cifrado asimétrico en este caso hace uso de dos claves, conocidas como clave pública y clave privada, donde igualmente el objetivo es cifrar un mensaje para que solo el remitente y destinatario sean los únicos que tengan acceso como tal al mensaje. Inicialmente es necesario que tanto el remitente como el destinatario creen cada uno de ellos una llave pública y privada; donde posteriormente tal como su nombre lo indica la clave publica será distribuida a diferentes equipos, de forma contraria funcionara la contraseña privada, la cual se mantendrá oculta. Es importante mencionar que, las contraseñas no deben ser iguales, sin embargo, tanto la clave privada como la publica permite realizar el proceso de cifrado y descifrado, para esto, los algoritmos de cifrado asimétricos deben contar con propiedades matemáticas muy altas, para permitir la legibilidad e ilegibilidad de los datos por medio de contraseñas distintas; una de las de las reglas con las que cuenta este tipo de cifrado, es que, la información que se cifra por medio de la clave pública, solo podrá ser descifrado por medio de la clave privada del receptor. (Sanjuan, Universidad del Norte)

Figura 18

Cifrado Asimétrico

Fuente: Tomado de (Vargas Salvador, 2019).

Entre los algoritmos más destacados que funcionan bajo esta arquitectura se encuentran:

- MD5,
- SHA,
- RSA,
- Diffie-Hellman,
- DSA.

Como **ventaja** se puede aludir que, el funcionamiento o arquitectura del cifrado asimétrico, permite que las contraseñas privadas no sean necesarias o conocidas por otro usuario para procesar los datos, permitiendo de este modo un grado más alto respecto a la confidencialidad, para enviar de manera segura un mensaje hacia un receptor puntual, tan solo será necesaria la clave pública del mismo, posteriormente el destinatario por medio de su clave privada descifrara el mensaje; del mismo modo, a pesar de que se puede considerar una desventaja el hecho de que en este método se requieran de dos claves por usuario, la realidad es otra, y esto se puede ver más claramente como ventaja al momento en que se desee compartir uno o varios archivos con un grupo grande de personas, ya que en este punto, y de manera muy diferente al cifrado

simétrico, no se requieren de nuevas claves por grupo interlocutores, reduciendo de esta manera el espacio de claves. Sin embargo, debido a que por medio de este método se facilita descifrar y cifrar un archivo por medio de diferentes contraseñas, esto conlleva un número más alto de procesamiento, así como también, un archivo de mayor tamaño que el original. Para garantizar una mayor seguridad, las claves de seguridad son de mayor tamaño; por último, es necesario una correcta gestión respecto al tema de autentificación de las contraseñas públicas, ya que estas se pueden definir como el ID de un usuario en la red, por lo que, en caso de que no se realice un proceso correcto, los mensajes podrán ser enviados a una persona totalmente diferente al destinatario correcto (Mac Millan Education).

Tabla 7

Claves de Cifrados Algoritmos Asimétricos

Algoritmo	Clave de Cifrado (Bits)
MD5	128
SHA	160
RSA	1024 – 2048
DSA	1024

Fuente: Elaboración propia basada en (Sanjuan, Universidad del Norte).

Es importante mencionar que, un número amplio de bits respecto al tamaño de la clave de cifrado, generara una seguridad mucho más amplia, debido a que se crearan cadenas de caracteres con mayor longitud. No obstante, por este mismo hecho, los tiempos de procesamiento de cifrado y descifrado de información se incrementarán, por este motivo, la selección del algoritmo no solo debe recaerá en la variable (Tamaño de clave de cifrado).

Lo anterior, se puede determinar teniendo en cuenta la siguiente tabla creada por Hernán Darío Serrato donde realiza una comparación de tres de los algoritmos más usados en la actualidad y más seguros.

Tabla 8

Comparación de Tiempos Algoritmos

Algoritmo	Clave de cifrado (Bits)	Tamaño de archivo (kb)	Tiempo de cifrado (Segundos)	Tiempo de descifrado (Segundos)
AES	128, 192 o 256		0,562	0,815
DES	56	2048	0,620	0,997
RSA	1024 – 2048		2,636	30,779
AES	128, 192 o 256		1,006	1,293
DES	56	4096	1,238	1,561
RSA	1024 – 2048		4,508	64,319
AES	128, 192 o 256		1,658	1,971
DES	56	6144	1,863	2,107
RSA	1024 – 2048		6,785	95,254
AES	128, 192 o 256		2,137	2,417
DES	56	8192	2,476	2,768
RSA	1024 – 2048		9,032	126,594
AES	128, 192 o 256		2,819	3.096
DES	56	10240	3,002	3.289
RSA	1024 – 2048		11,294	160,164

Fuente: Tomada de (Serrato Losada ,2019).

Donde se puede evidenciar que el algoritmo RSA, al funcionar bajo una clave de cifrado tan grande, generara tiempos de cifrado y descifrado mucho más amplios en comparación con los demás algoritmos, sin embargo, también se puede evidenciar que, a pesar de que el algoritmo DES funciona con una clave de cifrada tan pequeño, genera tiempos muy similares en comparación con AES, el cual maneja un mayor tamaño de almacenamiento en sus claves, en base a lo anterior, se puede determinar que el algoritmo AES tiene un nivel de seguridad considerado y además en tiempos muy cortos de procesamiento.

Igualmente, Yuri Tatiana Medina junto con Haider Andrés Miranda realizan una comparación de estos mismos algoritmos, respecto a las características generales de cada uno.

Tabla 9

Características generales Algoritmos (AES, RSA, DES)

	Algoritmos		
Factores	**AES**	**RSA**	**DES**
Longitud de clave	128, 192 o 256 bits	1024 – 2048	56 bits
Tipo de cifrado	Simétrico	Asimétrico	Simétrico
Tamaño bloque	128, 192 o 256 bits	1024 – 2048	64 bits
Año de desarrollo	2000	1978	1977
Seguridad	Considerado seguro	Ataque de Tiempo	Resultados insuficientes

Nota: El Algoritmo AES presenta en el factor seguridad un alto nivel en comparación a los demás.

Fuente: Tomada de (Medina Varga & Miranda Mnedez, 2015).

De manera general se puede determinar que el algoritmo AES, es actualmente uno de las herramientas más seguras y con gran rendimiento respecto al cifrado de datos, dado al hecho de ser un tipo de cifrado simétrico, donde ya se logró determinar que entre sus características son sus cortos tiempos de proceso y que, a pesar de manejar únicamente una clave, es altamente seguro. Sin embargo, no se puede descartar el uso del algoritmo RSA dentro del aplicativo a pesar de sus altos tiempos de cifrado y descifrado, debido al formato que se administrara (Texto) donde generalmente consume poco espacio de almacenamiento (Bytes), lo cual, lo podemos evidenciar usando como ejemplo la siguiente contraseña (KiohPD82xaN^Ew6EP@v4) cuyas características son de una contraseña segura, donde si se realiza la conversión a bytes, esta contraseña tendría un peso de almacenamiento de 20 bytes (0.02 Kilobytes), un byte por cada carácter que compone el texto, por lo tanto, si se tiene en cuenta los resultados mostrados en la tabla 9, cuyo estudio de análisis más pequeño fue de archivo de 2048 kilobytes, dando resultados de cifrado y descifrado de 2,636 y de 30,799 segundos respectivamente, los tiempos pueden

reducirse notoriamente debido al reducido tamaño del texto en comparación con el evaluado por Hernán Serrato; por ende, se puede conseguir un alto nivel de seguridad sin altos tiempos de procesos.

4.1.1.1. Acceso remoto

Además de querer ofrecer una herramienta de gestión de contraseña, igualmente se desea establecer un protocolo que permita de algún modo, iniciar sesión en las cuentas de usuario que posea el usuario desde el mismo dispositivo, permitiendo de este modo realizar este proceso de una manera mucha más rápida. Sin embargo, es importante mencionar que entre algunas de las herramientas descritas al inicio de este documento ya cuentan con una función muy similar; por ejemplo, Google Chrome cuenta con una función de almacenar los sitios web donde el usuario haya creado un perfil de usuario junto con la contraseña y si se requiere, el usuario.

Figura 19

Acceso Contraseñas Google Chrome

Fuente: Tomado de (Google LCC., 2020).

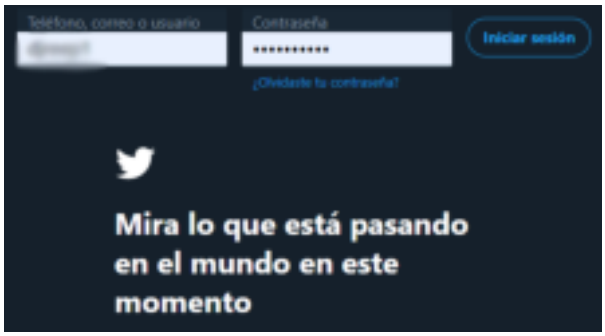
Nota: Captura de pantalla donde se puede evidenciar el almacenamiento de contraseñas con su respectivo nombre de usuario y páginas web.

Como se puede evidenciar en la figura XVII, toda la información necesaria para realizar los inicios de sesión, se encuentran totalmente organizada y de fácil accesibilidad; sin embargo, pueda que terceras personas tengan fácil disponibilidad de los datos, ya que el acceso requiere de un número reducido de pasos, tan solo estar ubicado en el navegador, para luego ingresar a "Personalizar y controla Google Chrome/Configuración/Autocompletar/ Contraseñas", de este modo obtendremos la lista de las contraseñas tal como se puede constatar. Además, a pesar de que las contraseñas se encuentren de forma oculta dado el formato establecido para este tipo de dato (●●●●●●), se pueden visualizar de manera muy sencilla a través del icono en forma de ojo, que se encuentra en la parte derecha de la figura 17. No obstante, omitiendo o corrigiendo esta vulnerabilidad del navegador, se puede implementar otra manera para poder conocer la contraseña de las cuentas, lo único necesario para realizar este proceso consiste en tener conocimientos básicos de programación; el proceso es el siguiente:

Google Chrome para facilitar al usuario el iniciar sesión, auto rellena el formulario de acceso de los sitios web, con los datos almacenados desde el momento de la creación de la cuenta, de esta manera el usuario solo tendrá que seleccionar el botón de ingresar para acceder al perfil de usuario, de la siguiente manera:

Figura 20

Auto Llenado Formulario



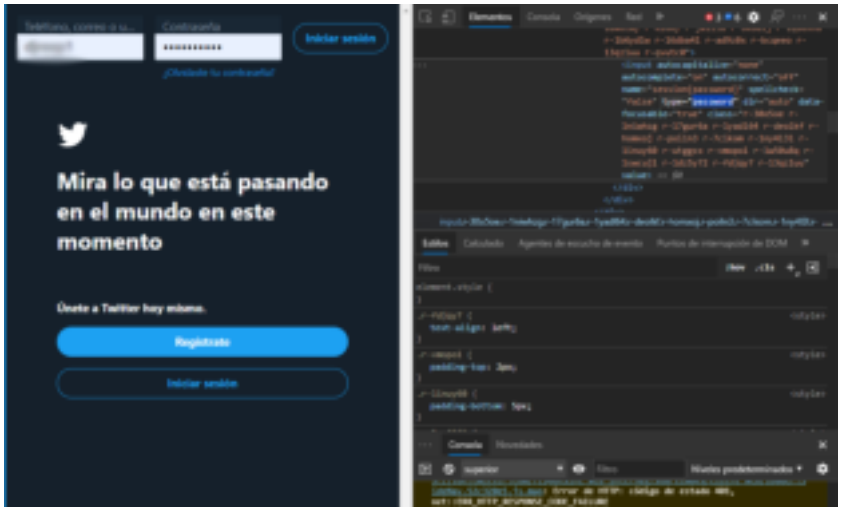
Fuente: Tomado de (Twitter, Inc, 2006).

Nota: Captura de pantalla de la interfaz de Twitter, el cual permite identificar el auto relleno que realiza el navegador Google Chrome, para facilitar el inicio de sesión.

Realizar estos procesos de auto llenado proporciona una debilidad o vulnerabilidad que da una posibilidad para el robo de información, muchas veces para evitar que el registro contraseña sea copiado y posteriormente pegado, para realizar el proceso de "descifrado", se programa la opción de que al momento de pegar este dato, sea modificado totalmente dando un registro totalmente diferente al original; sin embargo, continuando con el método, la manera de visualizar el registro por medio de programación es el siguiente: ingresar a "Personalizar y controla Google Chrome/ Más Herramientas/ Herramientas de desarrollador"; en este punto se abrirá una consola con el código de la página web.

Figura 21

Consola Google Chrome



Fuente: Tomado de (Google LCC., 2020).

Nota: Modificación que se realiza a la plataforma Twitter por medio de la consola de código del navegador Google Chrome.

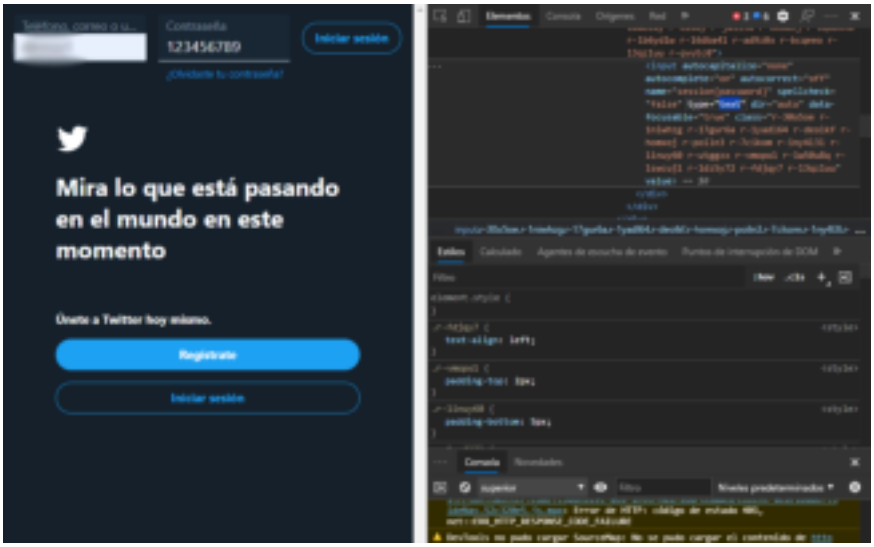
Nota: Se realiza un cambio de formato de dato, en la parte derecha de la imagen se evidencia, por medio de una selección que el formato es tipo "password".

Personal con básicos conocimientos de programación sabe que el type o tipo de formato que debe tener los datos de contraseñas debe ser establecida como "password" en varios lenguajes de

programación, tal como se ve en la figura XIX, cuyo registro se encuentra resaltado, No obstante, el visualizar la contraseña es tan fácil en este punto, que el único proceso a realizar es cambiar el type del dato, de "password" por "text", de esta forma el campo de texto que contiene cambiara su formato y por ende mostrara la contraseña.

Figura 22

Contraseña Expuesta Google Chrome



Fuente: Tomado de (Google LCC., 2020).

Nota: Modificación que se realiza a la plataforma Twitter por medio de la consola de código del navegador Google Chrome.

Nota: En la parte derecha de la figura (Consola de Código), se realiza un cambia de tipo de dato a un tipo "text", de este modo se realiza el cambio de formato en el campo de texto en la parte izquierda de la figura evidenciando la contraseña.

De esta manera, se evidencia que no es necesario tener conocimientos avanzados de programación para realizar este proceso, tan solo es necesario tener disponibilidad del equipo cuyo navegador tenga asociado una cuenta de Gmail.

Chrome evitando suplir esta dificultad, permite el inicio de sesión automática, tal como se muestra en la parte superior de la figura 17, saltando el proceso de auto llenado, sin embargo, el desactivar esta función no conlleva ningún proceso de autentificación de usuario, lo que permitiría que cualquier persona en cualquier momento lo desactivara y posteriormente realizar el proceso de "descifrado" por medio de la consola del navegador, explicado anteriormente.

Es importante recordar que los datos serán almacenados dentro del correo electrónico asociado al navegador, lo que provocaría una dificultad en seguridad y accesibilidad al momento de querer ingresar una cuenta, frecuentemente es común olvidar cerrar sesión directamente en el navegador.

En base a lo anterior, se justifica el objetivo de querer implementar la función de iniciar sesión sin necesidad de auto llenados y directamente desde el dispositivo, fortaleciendo la seguridad, **disponibilidad** y **confidencialidad** en el proceso.

4.1.1.1.1. Extensión

Una extensión se puede describir en pocas palabras como un software que es instalado en los navegadores los cuales permiten adicionar funciones a los mismos, cumpliendo una función puntual.

Complementando lo anterior, Mozilla Firefox mencionan que las extensiones

> Permiten añadir a dichas aplicaciones cualquier cosa, desde un botón para una barra de herramientas hasta características totalmente nuevas. Permiten personalizar completamente la aplicación para ajustarla a las necesidades de cada usuario, sin aumentar de forma significativa el tamaño de la misma (Corporación Mozilla, 2019).

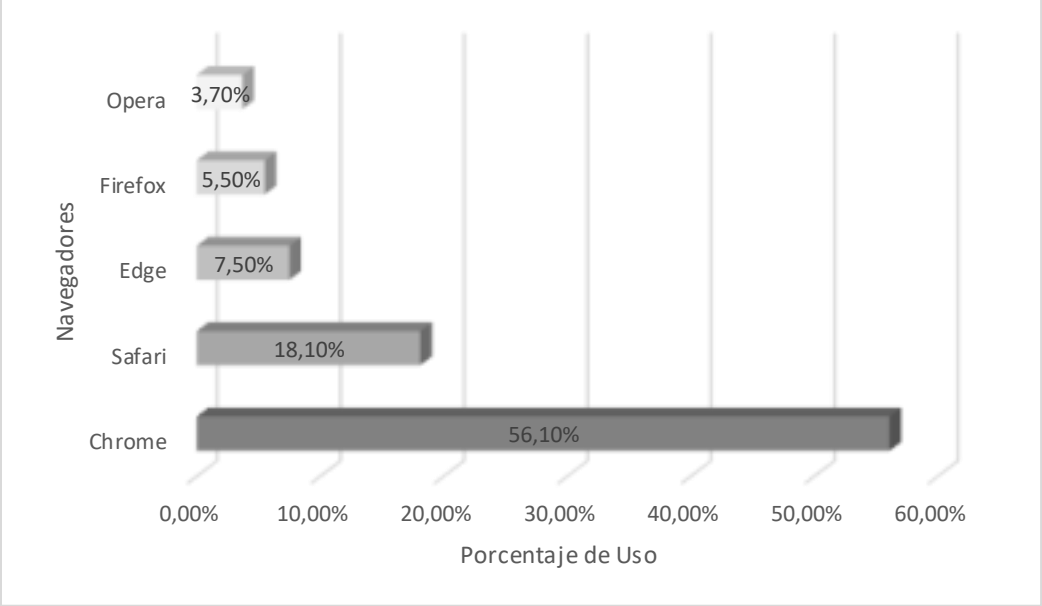
Entre las extensiones popularmente más conocidos, se encuentran los VPN, los cuales permiten modificar la dirección IP del dispositivo tecnológico, igualmente existen los bloqueadores de

anuncios y también lo traductores, como por ejemplo Google Translate, cuya función es realizar traducciones completas de un sitio web.

El objetivo principal para la creación de esta herramienta dentro del sistema de gestión de contraseñas, es para que funcione como un tipo de intermediario entre los sitios web, principalmente en los formularios de inicio de sesión y registro, con el aplicativo, para de este modo el usuario pueda desde el mismo dispositivo ingresar a cualquier cuenta de usuario de su propiedad, sin la necesidad de auto relleno de formularios, ya que, como se logró identificar este proceso puede dar oportunidad de robo de datos; además de lo anterior, tendría la función de recuperar la información almacenada de manera remota (Servidor), en caso de que el usuario extravié su dispositivo.

Figura 23

Navegadores Mas Usados



Nota: Elaboración propia tomado de (Mora, 2020).

En base a que en la actualidad el navegador más usado a nivel mundial es Google Chrome, con algo más del 56% de uso a nivel mundial, muy lejano a su competidor más cercano Safari donde

su uso es del 18.1%; la creación de la extensión estaría enfocada a Chrome, donde gracias a que Microsoft Edge esta desarrollaba bajo Chromium, el cual es el código fuente en el que está basado Chrome, igualmente la extensión tendría compatibilidad, por ende, se estaría abarcado un número de usuarios más amplio, aproximadamente al 73%.

Para iniciar la creación de la extensión dentro de Chrome, se deberá realizar por medio del lenguaje de etiquetas HTML y de programación JavaScript, junto con el formato JSON el cual según Deyimar A. afirma que es un formato que almacena información estructurada y se utiliza principalmente para transferir datos entre un servidor y un cliente (A., 2020). En base a lo anterior, se puede identificar claramente que por medio de este formato se podrá enviar la información necesaria para los inicios de sesión desde el dispositivo móvil hasta la extensión por medio de la red; de igual manera, cuando un usuario desee obtener su información alojada en la nube, más específicamente la copia de seguridad.

Del mismo modo que el proceso establecido para los registros de la aplicación, para realizar la conexión (Smartphone – Extensión), se requeriría de una autentificación en dos pasos, donde claramente debido a que la conexión que se realizara con el dispositivo móvil y en base a lo seguro que resulta ser la autentificación por mensaje de texto, se implementara este método. El proceso en base a la figura 10, se inicia cuando un usuario debe ingresar su número telefónico dentro de la extensión, para posteriormente realizar la solicitud de envió de código de verificación por medio de un MSN, para posteriormente, el código recibido sea digitado dentro de la extensión, ya en este punto se realiza la conexión entre los dispositivos, teniendo en cuenta, los tipos de cifrados identificados, y más puntualmente el cifrado asimétrico, la implementación de este algoritmo dentro de esta arquitectura permitiría que una fluidez de datos seguros, ya que, tanto el dispositivo móvil, como la extensión del navegador contaran cada una con dos claves de

seguridad, recordando que una de ellas es descrita como la identificación del dispositivo en la red, esto generaría una mayor seguridad. Es importante destacar, que el proceso se realizaría por medio del protocolo HTTP, al cual permite la conexión (cliente – servidor).

Así como se realizó la conexión con el dispositivo móvil desde la extensión, de manera muy similar se establecerá una comunicación entre (Extensión – Servidor), donde tal como se hizo mención, de esta manera se podrá obtener acceso a la copia de seguridad, sin embargo, dado a que esta opción estaría habilitada únicamente cuando el usuario no tenga a su disposición su dispositivo, no se podría realizar una autentificación en dos pasos, por ende, y recordando la clave maestra establecida inicialmente al momento del registro, esta será usada como método de verificación, de este modo el usuario podrá acceder a sus datos.

El proceso de envío de datos luego de un registro como tal, se llevará a cabo por medio del objeto que proporciona JavaScript, conocido como XMLHttpRequest; Rafael Cueto con David Gutiérrez afirman.

> XMLHttpRequest es un objeto Javascript que incorpora la misma funcionalidad que el objeto originalmente desarrollado por Microsoft. Nos da una forma sencilla de obtener datos de una url. Aunque el nombre pueda despistar, XMLHttpRequest puede ser usado para obtener cualquier tipo de dato, no sólo XML (Gutiérrez & Cueto Felgueroso, 2020).

Entre otro de los objetivos de implementar un intermediario dentro del sistema, consiste en que el usuario al realizar el registro en una cuenta de usuario, los datos pueden ser enviados y almacenados en la nube, por medio de la misma extensión, en base a lo mencionado por Rafael y David Gutiérrez, donde gracias a la implementación de Firebase Cloud Firestone, los datos podran ser visualizados posteriormente en el dispositivo del usuario. Cabe mencionar que, así como los datos de usuario, contraseña y correo electrónico, generalmente usados para el registro,

serán almacenados, la URL de la página web igualmente tendrá el mismo proceso, de este modo se podrá direccionar nuevamente a la misma más adelante.

Finalmente, para realizar la opción de acceso directo, se debe tener en cuenta elementos del lenguaje HTML; según Firefox en su página web afirma que la interface HTMLInputElement proporciona propiedades y métodos especiales para manipular las opciones, estructura y presentación de los elementos <input> (Corporación Mozilla, 2020). Cabe mencionar que, los elementos mencionados dentro del lenguaje de etiquetado HTML son la manera de estructurar la interfaz en una página web, un ejemplo de lo anterior se puede visualizar a continuación por medio de la siguiente tabla.

Tabla 10

Elementos Input HTML

Tipos de Input	Elemento
<input type="button">	Botón
<input type="checkbox">	Casilla de verificación
<input type="date">	Fecha
<input type="email">	Correo electrónico
<input type="password">	Contraseña
<input type="url">	Dirección electrónica

Fuente: Elaboración propia tomado de (w3schools, s.f.).

La información proveniente del dispositivo, luego de realizado el proceso de verificación, por medio del formato JSON será introducida en cada uno de los campos correspondientes, lo cual permitiría de este modo, que el usuario puede ingresar a la cuenta de usuario que él desee.

4.1.1.2. Generador De Contraseñas

Complementando la información y las cifras explicadas al inicio de esta investigación es importante mencionar que, según la organización Indexa capital, se estima que un 80% de los ataques informáticos realizados, son debido a la baja seguridad que conforma una contraseña, la baja combinación entre letras, números, símbolos, mayúsculas y minúsculas, provoca que estas contraseñas no conformen una estructura segura. El uso de contraseñas poco seguras es tan frecuente que la misma Indexa luego de una investigación identifico una lista de contraseñas de alta vulnerabilidad, tanto así, que pueden ser deducidas fácilmente, pero sin embargo de uso frecuente, las cuales son las siguientes:

- 123456,
- Password,
- 12345678,
- Qwerty,
- 12345

A pesar de que es de conocimiento general la necesidad de implementar contraseñas seguras y que cuenten con características especiales, el uso de estas claves es muy común debido a que los usuarios tienen más temor a olvidar sus contraseñas a que terceras personas tengan acceso a sus cuentas y hasta un posible robo.

Además de la recomendación tanto conocida que es la de utilizar diferentes tipos de caracteres para crear una contraseñas, también es recomendable cambiar periódicamente la contraseña, donde muy frecuentemente se recomienda que cada 6 meses se debe realizar este proceso, asimismo, no es aconsejable que una contraseña sea usada para diferentes cuentas de usuario o en correos electrónicos; por ultimo y una de las más recomendadas, es claramente evitar escribir

este tipo de información tan importante en algún papel o post-it, debido a que es muy frecuente extraviarlos. En complemento a estas recomendaciones, se sugiere que las contraseñas tengan como mínimo 8 caracteres, entre una combinación de mayúsculas, minúsculas, números, y símbolos; aunque lo ideal en una estructura de contraseña segura, es que la longitud de la contraseña se encuentre entre 10 a 20 caracteres. (Indexa Capital, s.f.)

En base a la anterior información, un ejemplo de una contraseña segura tendría un aspecto muy similar a la siguiente: **KiohPD82xaN^Ew6EP@v4**, tal como se mencionó anteriormente, la cual está compuesta con una longitud de 20 caracteres, además una combinación de minúsculas, mayúsculas y números, muy contrario a la estructura que tienen las contraseñas mostradas por Indexa, pero como se ha mencionado, es muy difícil recordar este tipo de contraseñas.

Además de las recomendaciones dadas por Indexa, la misma organización Panda Media Center, creadora de uno de los antivirus más conocidos a nivel global, cuyo nombre es Panda Security, menciona algunas otras recomendaciones a implementar para la creación de contraseñas seguras:

- Crear contraseñas por medio de una frase muy personal,
- Combinación de dos o más palabras,
- Modificar las vocales por números,
- Establecer una frase muy conocida para posteriormente retirar las vocales,
- Formar la contraseña por medio de una combinación de números y letras. (Panda Media Center, 2016)

4.1.1.3. Almacenamiento

Como la idea es que los datos tengan alta disponibilidad, es importante determinar la manera en que los datos sean de fácil acceso, para fortalecer este punto se puede optar por el uso de una base de datos local, de esta manera no existe la necesidad de un conexión a la internet, además

justificando esta opción, se puede mencionar que en Colombia, específicamente en el año 2019, 4 de cada 10 personas no cuentan con una conexión a internet móvil según Portafolio (Portafolio, 2020), lo que equivale a que el 40% de los ciudadanos no cuentan con este servicio, porcentaje muy alto teniendo en cuenta que la población estimada en el 2018 son de unos 48 millones de personas según el DANE (DANE , 2018), lo que equivaldría a unos 19 millones de personas.

4.1.1.3.1. SQL

Para el almacenamiento de información interno o local Android no cuenta con muchas opciones, la usada para estos casos y mencionada en la guía de desarrollador de Android Studio, es el motor de base de datos SQLite, donde en la página oficial de la herramienta se menciona que.

> SQLite es una biblioteca de lenguaje C que implementa un motor de base de datos SQL pequeño, rápido, autónomo, de alta fiabilidad, con todas las funciones. SQLite es el motor de base de datos más utilizado en el mundo. SQLite está integrado en todos los teléfonos móviles y la mayoría de las computadoras y viene incluido dentro de innumerables otras aplicaciones que la gente utiliza todos los días (SQLite, s.f.).

Existen diversas funciones o aplicaciones para las cuelas está hecha SQLite, aparte de las mencionadas previamente se pueden evidenciar muchas otras:

- Dispositivos integrados a internet de las cosas,
- Sitios web,
- Caché para datos empresariales,
- Formato de transferencia de datos,
- Bases de datos internas o temporales,
- Extensiones experimentales de lenguaje SQL.

En general es una herramienta muy completa que puede brindar muchas posibilidades, por esta razón se ha establecido como la base de datos más usada en los dispositivos móviles.

La integración de esta base de datos en el sistema operativo Android, es por medio de una API, la cual funciona por medio de una implementación de un paquete en la herramienta de desarrollo, la más conocida y que fue creada por Google, es Android Studio, el paquete es conocido de la siguiente manera: **android.database.sqlite;** el cual debe ser implementada como una librería más en el proyecto. Existen diferentes versiones de SQLite dependiendo de la versión en la que va a ser utilizada o instalada.

Tabla 11

Versiones SQLite

Android API	SQLite Versión
API 27	3.19
API 26	3.18
API 24	3.9
API 21	3.8
API 11	3.7
API 8	3.6
API 3	3.5
API 1	3.4

Fuente: Tomado de (Google LCC, 2020)

De esta manera se garantiza la disponibilidad de los datos por parte de los usuarios, sin verse afectado la seguridad de acceso, usando la función de la autentificación por huella digital.

No obstante, el implementar una base de datos local provocaría que la información se extraviara con gran facilidad por ejemplo en el caso del robo del dispositivo en el que la información se perdería igualmente, por esta razón y recordando las recomendaciones que se deben implementar en la seguridad informática, donde se menciona que es necesario realizar una copia de seguridad

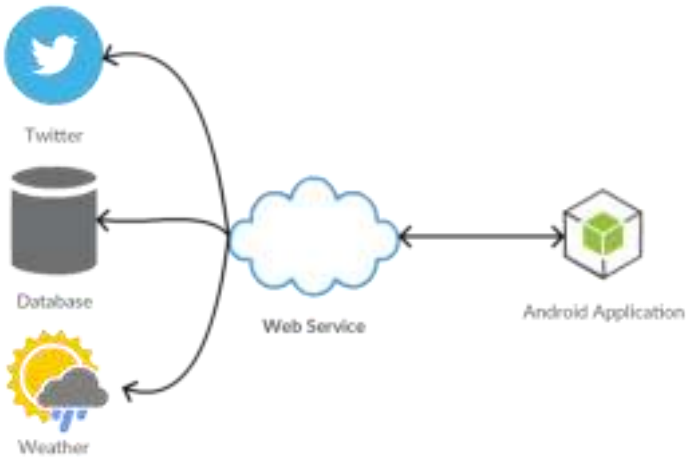
de la información también conocido como Back-up para tener una copia de respaldo, por obvias razones esta copia de seguridad no deberá estar dentro el mismo dispositivo sino de manera remota (Cliente - servidor), en este punto es necesario una conexión a la red ya que por medio de esta vía se enviaran los datos a una base de datos remota. Existen diferentes motores de bases de datos que permiten almacenar esta información, sin embargo, una de las más usadas para esta función es MySQL, el cual está muy enfocado para el desarrollo web, sin embargo, puede ser usada para dispositivos móviles, cabe destacar que la implementación no es directa con el servidor debido a que las aplicaciones no cuentan con esta arquitectura de manera directa, por esta razón para realizar una conexión entre la aplicación móvil y una base de datos remota se debe implementar un web service.

4.1.1.3.2. Web Services

Andrés Pastorini describe a un Web Service o en su traducción al español servicios web como "un conjunto de servicios para ser consumidos a través de la red. En otras palabras, un servicio web especifica un conjunto de operaciones (funciones que retornan determinado valor, reciben un conjunto finito de parámetros, y retorna un resultado), a través de una URL, donde una aplicación cliente remota los puede consumir (podría haber cuestiones de seguridad en el medio)." (Pastorini) La arquitectura que maneja esta función se muestra en la siguiente figura, ratificando lo mencionado por Andrés Pastorini:

Figura 24

Arquitectura Web Service



Fuente: Tomado de (Loganathan, 2018).

Nota: Una aplicación móvil (Android) el cual para tomar recursos o mostrar los mismos realiza una conexión con un Web Service, el cual dentro de la arquitectura se realiza por medio de la nube.

Gobinath Loganathan en su experiencia como ingeniero de sistemas, pero puntualmente como desarrollador Android recomienda implementar dentro una aplicación de nivel industrial un Web Service, que funcionara como intermediario entre la base de datos y el app, ya que como ventaja se puede obtener una menor complejidad en el funcionamiento, primordialmente evitando la dependencia de operaciones en las bases de datos, debido a que no existe una comunicación directa con la base de datos por medio del lenguaje SQL.

Además de lo anterior, la Inter operatividad es una más de las ventajas que sobresale en el Web Services, permitiendo una completa comunicación entre los mismo servidores web y clientes, incluso permitiendo una comunicación completa entre los sistemas, esto es debido a que el código de comunicación usado es en Extensible Markup Language más conocido dentro de los entendidos como XML. El medio utilizado para enviar y recibir peticiones es a través del

protocolo HTTP muy usado y visto en las páginas web, su objetivo es convertirse en un intermediario entre el cliente y servidor.

Igualmente es importante mencionar que es de fácil implementación, ya que existen herramientas que permiten implementar estos servicios sin la necesidad de tediosos procesos de programación; una de las compañías más conocidas que ofrecen este servicio es la muy conocida Amazon, denominada por la misma compañía como Amazon Web Services (AWS).

Debido a que la comunicación cliente servidor se realiza por medio de la internet, esto permite que los Web Services sean de alta accesibilidad, ya que un número amplio de dispositivos tienen la posibilidad de acceder a este servicio; debido a que sin importar el lenguaje de programación que utilice estos dispositivos, la comunicación se hará sin ninguna contrariedad. (Fuquen Barrera & García Hurtado, 2015)

Luego de lo explicado se puede identificar que el Web Services son conjuntos de operaciones que brinda grandes ventajas al momento de su implementación, permitiendo y facilitando la comunicación con los gestores de bases de datos y el cliente. No obstante, los servicios mencionados deberán en un punto conectarse entre sí, para que cualquier cambio realizado en alguno de estos servicios se vea reflejado igualmente en la otra herramienta o base de datos, permitiendo de este modo la **integridad** de los datos. Ahora bien, esto puede crear complicaciones de comunicaciones, por ejemplo, en el momento en que el servidor donde se esté almacenando la información tenga alguna falla, y durante este periodo se realice alguna modificación en la información en el dispositivo; por esta razón una herramienta que puede realizar los dos servicios (Almacenamiento local y almacenamiento en la nube), y que es muy cercana al sistema operativo Android es Firebase Cloud Firestore.

4.1.1.4. Firebase Cloud Firestore

Tal como lo indica su nombre es una herramienta más de la plataforma Firebase, la cual permite almacenar información en la nube, pero así mismo, permite a la vez un almacenamiento local, donde la aplicación que implemente este servicio permitirá realizar modificaciones, consultas sin ningún tipo de conexión a la red, la aplicación realizara la sincronización con la base de datos alojada en la nube luego de realizar la conexión con la red, para que en este punto de forma automática realizar los cambios hechos respecto a la información, ya sea desde el dispositivo hacia el almacenamiento en la nube o viceversa.

La manera en que se podrá realizar cambios "provisionales" en el dispositivo será por medio del cache del mismo equipo.

Al igual que Firebase Authentication esta función o SDK puede ser usada en diferentes plataformas, entre ellas se encuentras Android, IOS, C++, Web y Unity plataforma muy conocida para el desarrollo de video juegos, de esta manera se podrá implementar una conexión directa entre estas plataformas.

Puntualmente las características que proporciona Firebase Cloud Firestore y que están especificadas en la misma página oficial de la plataforma son:

- Sincronización en tiempo real,
- Permite el acceso a datos por medio de una base de datos local,
- Permite desarrollo sin servidor,
- Se integra con las demás herramientas de Firebase (Dufetel, 2017).

Existe igualmente una herramienta que cumple con un servicio muy similar a Cloud Firestone el cual se conoce como Realtime Database, no obstante Cloud ofrece servicios más potentes en general, tanto así que, Cloud toma lo mejor que ofrece Realtime y provee muchos más valores

agregados, incluso en la misma página oficial de Firebase se realiza una comparación de estás dos herramientas donde sobresale notoriamente en varios apartados como los son:

- Modelo de datos: facilitando la organización a escala de datos complejos y jerárquicos,
- Compatibilidad sin conexión: donde la principal diferencia consiste en el soporte para plataforma web, además de Andriod y IOS, mientras que Realtime solo proporciona el servicio en los sistemas operativos móviles más conocidos (Andriod, IOS),
- Consultas: Búsquedas o consultas indexadas permitiendo una gestión más compuesta,
- Confiabilidad y rendimiento: uno de los puntos de más diferencia dado que Cloud funciona geográficamente a un nivel más amplio totalmente diferente a Realtime donde solo trabaja dentro de una solo región,
- Escalabilidad: Permitiendo un número de concurrencia más alto, hasta de 1'000.000 de conexiones simultaneas y además de una cifra muy alta de operaciones por segundo, puntualmente en unos 10.000 procesos, asimismo, realiza un escalamiento automático, muy divergente a Cloud cuyo escalamiento es muy inferior, ya que solo permite unas 200.000 conexiones simultaneas y tan solo 1.000 procesos por segundo; para aumentar estas cifras, se deberá implementar diversas bases de datos para el almacenamiento. (Google LLC, 2019)

Existen diferencias muy notorias entre las dos plataformas, donde claramente se puede identificar mejor rendimiento en la herramienta Cloud; sim embargo, el uso de Realtime no está obsoleta ni mucho menos descartada, incluso se puede implementar las dos en un mismo proyecto, todo depende en gran medida al objetivo y tipo de aplicación que se desea desarrollar.

Dado a las diversas herramientas que ofrece Cloud, se puede considerar que es una herramienta muy recomendada solo en aplicaciones de niveles industriales, no obstante, esto es totalmente incorrecto, incluso en la plataforma afirma lo siguiente respecto a este punto.

> Recomendamos Cloud Firestore para la mayoría de los desarrolladores que buscan comenzar proyectos nuevos. Cloud Firestore ofrece más funciones, rendimiento y escalabilidad en una infraestructura diseñada para admitir funciones más potentes en las próximas actualizaciones. Entre las funciones avanzadas planificadas para Cloud Firestore habrá nuevos tipos de consultas, reglas de seguridad más sólidas y mejoras en el rendimiento (Google LLC, 2019).

En base a las características mencionadas, la implementación de esta plataforma permitiría que los datos de contraseña y usuarios necesarios para el acceso a un perfil de usuario, estén accesibles en todo momento incluso cuando el aplicativo no esté conectado a la internet, además por el hecho de que permite la integración con otras herramientas de la misma plataforma se puede fortalecer la idea de implementar la herramienta Authentication dentro del aplicativo, permitiendo de esta manera la disponibilidad, confidencialidad e integridad de los datos.

Cabe mencionar que, la herramienta en contextos muy pequeños de gestión de datos, no incurrirá en ningún tipo de costos, sin embargo, en almacenamientos de alto nivel de información se generar algunos cobros para su funcionamiento; los puntos que serán evaluados o que incurrirían a costos son los siguientes:

- Cantidad de banda de ancha,
- Cantidad de almacenamiento en la base de datos en la nube,
- Modificaciones, lecturas y eliminaciones ejecutadas.

Las características o restricciones básicas establecidas por Firebase en su cuota gratuita, están establecidas de la siguiente manera:

Tabla 12

Limites Cloud Firestone Versión Gratuita

Nivel Gratuito	Cuota
Datos almacenados	1 GiB
Lecturas de documentos	50.000 por día
Escrituras de documentos	20.000 por día
Eliminación de documentos	20.000 por día
Salida de red	10 GiB por mes

Fuente: Tomado de (Google LCC, 2019).

Conociendo que la problemática de gestión de contraseña es tan amplia, es claro determinar que se manejaran grandes volúmenes de datos dentro de la aplicación, por esta razón, es indispensable identificar los costos que se podrán generar; existen diferentes costos de Cloud, todo depende de la región desde donde se haya implementado la herramienta, a continuación, se mostraran los precios de las regiones con las que cuenta Cloud:

Tabla 13

Precios Cloud Firestone

Regiones	Lecturas de documentos (Por 100.000 documentos)	Escrituras de documentos (Por 100.000 documentos)	Eliminación de documentos (Por 100.000 documentos)	Datos almacenados (Por GiB al mes)
EE.UU. (Multirregión)	USD 0.06	USD 0.18	USD 0.02	USD 0.18
Los Ángeles	USD 0.036	USD 0.108	USD 0.012	USD 0.108

Regiones	Lecturas de documentos (Por 100.000 documentos)	Escrituras de documentos (Por 100.000 documentos)	Eliminación de documentos (Por 100.000 documentos)	Datos almacenados (Por GiB al mes)
Virginia del Norte	USD 0.033	USD 0.099	USD 0.011	USD 0.099
Carolina del Sur	USD 0.06	USD 0.018	USD 0.02	USD 0.018
Montreal	USD 0.033	USD 0.099	USD 0.011	USD 0.099
São Paulo	USD 0.045	USD 0.135	USD 0.015	USD 0.135
Europa (Multirregión)	USD 0.06	USD 0.18	USD 0.02	USD 0.18
Zúrich	USD 0.042	USD 0.126	USD 0.014	USD 0.210
Fráncfort	USD 0.039	USD 0.117	USD 0.013	USD 0.117
Londres	USD 0.039	USD 0.117	USD 0.013	USD 0.117
Bombay	USD 0.035	USD 0.104	USD 0.012	USD 0.104
Sídney	USD 0.038	USD 0.115	USD 0.013	USD 0.115
Hong Kong	USD 0.06	USD 0.18	USD 0.02	USD 0.18
Tokio	USD 0.038	USD 0.115	USD 0.013	USD 0.115
Osaka	USD 0.038	USD 0.115	USD 0.013	USD 0.195

Fuente: Tomado de (Google LCC, 2019).

Es importante aclarar, específicamente en el punto de datos de almacenamiento, que los costos están basados bajo la unidad de almacenamiento gigabytes, lo que equivaldría a unos 1 073 741 824 bytes de espacio.

4.2. Resultados Del Objetivo Específico N°2

Teniendo en cuenta el objetivo específico No. 2 (Definir los requerimientos del sistema dependiendo de los resultados de la investigación, y la necesidad a suplir teniendo en cuenta, la definición del problema), puntualmente en base a los resultados obtenidos en el apartado anterior, a continuación, se estipularan los requerimientos que debe tener el aplicativo móvil, cabe destacar que, la estructura que se manejará estará fundamentada bajo la norma IEEE 830, conocida como "especificaciones de los requerimientos del software" (ERS) (Institute of Electrical and Electronics Engineers, 1998).

4.2.1. Introducción

Como primer paso dentro de la estructura del documento IEEE 830, se debe identificar el nombre del proyecto, por esta razón, se asignará de manera provisional un nombre al actual proyecto, cuyas características deberán ser: fácil de memorizar y corto, por ende, se nombrará de aquí en adelante al proyecto como GinToo.

4.2.1.1. Propósito

Determinar cada componente presente dentro del aplicativo GinToo, para dar una guía al lector respecto a los mismos, en donde aquí se analizarán si estos pueden ser implementados o no, teniendo en cuenta aspecto como la dificultad, condiciones, y especialmente tiempos, asimismo, serán distribuidas dentro de la metodología escogida y explicada más adelante.

La información presente en el documento está dirigida a los tutores encargados del proyecto de grado:

- Jurado,
- William Mendoza Rodríguez (Tutor),
- Ricardo Ceballos (Coordinador investigación de ingenierías).

Los cuáles serán los encargados de evaluar los componentes del proyecto respectivamente y darle su aprobación.

Asimismo, el presente apartado da a conocer con mesura los aspectos del aplicativo principalmente, (Para quien va enfocado, restricciones, para que sirve, sus funciones etc.)

4.2.1.2. Alcance

La idea de la creación de GinToo resulto luego de ver una necesidad por parte diferentes personas que tenían la misma problemática; específicamente la necesidad es la dificultad de memorizar las contraseñas, por ende, generar contraseñas de baja seguridad o repetidas en varias plataformas. Por este motivo le idea es crear un aplicativo enfocada a los sistemas operativos Android, en donde los beneficiados o usuarios principales estaban enfocados especialmente en personas adultas que se encuentran laborando y estudiando al mismo tiempo, esto genera que deban administrar una gran cantidad de información; en donde podrán por medio de GinToo gestionar y establecer contraseñas seguras, de paso acceder desde el mismo móvil en cualquier cuenta de usuario, mientras que tenga una conexión a la red, de lo contrario, los datos estarán disponibles para que el mismo usuario pueda tener a la palma de la mano la información necesario para acceder a cualquier perfil creado por el mismo.

A futuro, principalmente se buscaría que GinToo inicialmente sea lanzada en pequeña escala, teniendo en cuenta los limites gratuitos que ofrecería la plataforma Firebase y sus herramientas; además, esto permitiría realizar modificaciones, antes ingresar a un público más amplio.

Tabla 14

Descripción General

Fuente: Elaboración propia.

4.2.1.3. Apreciación Global

Luego de identificar la idea básica de GinToo, especificada en los puntos anteriores, el turno ahora es dar a conocer más a profundidad cada aspecto de los componentes que conforman el aplicativo, iniciando por una descripción de la idea y del porque nació la misma.

Durante la lectura del presente apartado, podrá encontrar información relevante a los usuarios o más específicamente a los roles presentes para el uso de GinToo, y sus funciones de cada uno dentro de esta.

Al igual, se especificarán las características a tener en cuenta durante el desarrollo del aplicativo; aspecto como el tamaño de resolución y los elementos que serán usados durante cada Activity para cumplir con el objetivo final, serán aclarados y justificados, al igual, mencionar que características debe tener el dispositivo móvil, para que el aplicativo funcione con normalidad durante su ejecución; en este aspecto entra la versión de Android base en la que funcionara el

aplicativo, al igual que código o funciones externas o prediseñadas serán usadas dentro de GinToo.

Aunque para este documento el punto principal para su elaboración son los requerimientos los cuales serán especificados y categorizados según su función dentro del aplicativo, se bebe tener en cuenta aspectos como las funciones presentes dentro del sistema, y los tiempos estimados para el desarrollo de este. Dentro de los requerimientos que podemos que podrá encontrar son:

- Restricción de Diseño.
- Restricción de Desempeño

Estos puntos tendrán como objetivo, analizar las funciones que debe realizar el aplicativo en su versión final, en donde por medio de un Check-List, se corroboran cada uno de estos requerimientos y determinar si cumplen o no con cada uno de los mismos. Los requerimientos serán también usados como método de guía principalmente durante el desarrollo.

Otro punto a tratar son las restricciones que presenta el aplicativo, ya sea a nivel de software o de hardware, dentro de este punto se tomaron en cuenta:

- La versión Android (Base),
- Las características mínimas que debe contar un dispositivo para la ejecución del aplicativo,
- Que necesita el usuario para el uso de GinToo.

Finalmente, aspectos generales de todo aplicativo,

- Seguridad,
- Interfaz,
- Disponibilidad.

serán aclarados y justificados, para mejor entendimiento de la información por parte del lector.

4.2.2. Descripción Global

4.2.2.1. Perspectiva del producto

Un gran número de personas cuentan hoy en día una gran cantidad de cuentas de usuarios y correos electrónicos (Redes sociales, correos electrónicos, entre otros); dado al gran número de datos a manejar, las personas cuentas con grandes dificultades, respecto a la gestión de esta información, por ende, adquirir una herramienta que permita gestionar esta información, es necesario, además, evitar que las malas prácticas optadas por los mismos usuarios serán suplidas, tales como contraseñas con bajo nivel de seguridad, repetición de las mismas en varias cuentas de usuarios.

Dado a lo anterior, el aplicativo deberá generar contraseñas con los parámetros mínimos de seguridad, del mismo modo, brindar de forma organizada todas las cuentas de usuario que el usuario tenga en propiedad junto con los correos electrónicos. Teniendo claramente un alto nivel de seguridad, pero igualmente una alta accesibilidad.

4.2.2.2. Interfaces Del Sistema

GinToo aparte de su aplicación móvil, enfocada inicialmente para sistemas operativos Android, contará con una extensión en los navegadores, el cual será el software que permitirá realizar la conexión entre el mismo y el smartphone, además, se implementará herramientas de la plataforma Firebase desarrollados y puestos al público por Googlo LCC, donde se deberá tener en cuenta los costos del servicio, luego de cumplir con los requerimientos básicos en el servicio gratuito.

4.2.2.3. Interfaces Con El Usuario

La interfaz con el usuario consistirá en el conjunto de ventanas y botones, imágenes y campos de texto. Estos serán construidos específicamente para la aplicación utilizando la API 4.4.

Tabla 15

Interfaz con el Usuario

Interfaz Con El Usuario	
Elementos	**Características**
Interface Gráfica:	• Botones: Interfaz que permitirá al usuario desplazarse entre ventanas y almacenar información en la aplicación. ejemplo: el registró. • Imágenes: Interfaz usada para facilitar al usuario reconocer las cuentas de usuarios.
Extensión	• Interfaz usada como intermediario para verificación del dispositivo y disponibilidad de la información en caso de pérdida del dispositivo.
Campos de Texto:	• Usados para generar y almacenar los registros digitados por el usuario.
API KitKat:	• Las especificaciones de la API KitKat son realmente básicas, todo dispositivo smartphone con conexión wifi o datos podrá acceder a la aplicación sin ningún inconveniente.

Fuente: Elaboración Propia.

4.2.2.4. Interfaces Con El Usuario

Lo necesario para poder utilizar la aplicación GinToo en cuestión de hardware es: poseer un smartphone y una conexión a la red esporádica, debido a que algunas de las funciones que proporcionara la herramienta requieren de una conexión, cabe destacar que, la calidad de internet no afecta demasiado la operación de la herramienta, dado al tipo de datos que se manejara (Texto); además, para usar por completo las funciones, se requiriera de una extensión en los navegadores web, por ende, será necesario en algunos de los casos el uso de un ordenador de cómputo.

4.2.2.5. Interfaces con el software

Para el correcto funcionamiento de la herramienta, la aplicación debe de interactuar con este software:

Tabla 16

Interfaz de Software

Producto de Software	Android 4.4	Base de Datos	Extensión
Descripción	La aplicación será desarrollada a partir de esta versión del sistema operativo Android en adelante, dado que es la versión que la gran mayoría de dispositivos móviles tienen en la actualidad.	El aplicativo se construirá bajo la herramienta Cloud Firestore dado a la función que proporciona esta plataforma	Software que servirá como intermediario con el objetivo de asegurar una autentificación con el dispositivo.
Propósito de Uso	Asegurar que la mayoría de los usuarios finales puedan utilizar el producto sin inconvenientes, pues este sistema operativo es el más difundido y usado en la actualidad. Los requerimientos a nivel de hardware que requiere este SO, son suficientes para que el aplicativo funcione.	La plataforma admite realizar almacenamiento local, permitiendo de este modo al usuario la disponibilidad de la información sin necesidad de una conexión a la internet.	Permitir el acceso directo desde el móvil y la recuperación de datos (copia de seguridad).
Versión	SDK tools 29.0.1 Android 4.4 en adelante	Cloud Firestone 22.0.0	JSON HTML 5 JavaScript ECMAScript 2016.
Comentarios Adicionales	Adicionales la aplicación no soportará versiones anteriores a la estipulada aquí.	No aplica.	Inicialmente será desarrollado para Chrome y otros navegadores basados en su código fuente.

Fuente: Elaboración Propia.

4.2.2.6. Restricción De Memoria

GinToo dentro de los dispositivos móviles, respecto al almacenamiento local, no manejara información de gran tamaño, teniendo en cuenta que, los datos a almacenar serán netamente texto, por ende, no se requerirá de grandes tamaños de memoria dentro de los dispositivos; los requerimientos mínimos en memoria que tienen los Smartphone cuyo SO es Android KitKat 4.4, soportara de manera notoria los datos almacenados; específicamente las características mínimas son: 512 MB de memoria RAM, 850 MB de memoria y resolución de pantalla 480 x 800. (Intel)

Para el almacenamiento en la nube, la capacidad de almacenamiento será la misma, por cada usuario; no obstante, para un número masivo de beneficiarios de la aplicación, estará basado inicialmente en el límite gratuito el cual fue descrita en la tabla 12.

4.2.2.7. Operaciones

Inicialmente el aplicativo deberá admitir el acceso a nuevos usuarios, realizando el respectivo proceso de autentificación por medio de la verificación en dos pasos, el cual se realizará por medio de la plataforma Firebase.

Igualmente se realizará el desarrollo de inicio de sesión, el cual se determinó por motivos de seguridad que será por medio de la huella digital, sin embargo, también será requerida una contraseña maestra la cual esporádicamente el usuario deberá ingresar, permitiendo de esta forma una mayor seguridad y de paso evitar que el consumidor olvide este dato; en los casos en que el dispositivo no cuente con un sensor de huella, el proceso se ejecutará netamente por medio de la contraseña. Además del uso de esta clave maestra para los para acceder a una copia de seguridad por medio de la extensión de los navegadores web, en caso de pérdida del dispositivo.

La herramienta tendrá la función de conexión con un software externo el cual, y como se ha mencionado, consiste en una extensión de los navegadores, inicialmente será desarrollado para los programas Google Chrome y Microsoft Edge, debido a que este último está basado en Chromium, el cual también está desarrollado por la compañía Google LLC.

Por motivos de seguridad, y en base a las buenas prácticas establecidas para los sistemas de seguridad, es indispensable que la herramienta realice una copia de seguridad de la información, la cual dado a la investigación realizada se determina que la mejor herramienta para realizar este proceso es la plataforma Cloud Firestone.

De igual modo la herramienta generara contraseñas seguras, permitiendo de este modo que los usuarios pueden seleccionar de manera aleatoria, la mejor contraseña que él considere segura para establecer como su clave de inicio de sesión, el objetivo de que el dato sea aleatorio, está basado a la recomendaciones identificadas y explicadas previamente, respecto a la no utilización de una misma contraseña en diferentes cuentas.

Por último, pero no por esto menos importante, entre las funciones más destacas se permitirá al usuario realizar un acceso directo, por medio de una conexión (Smartphone – Extensión web), sin necesidad de generar auto relleno de campos de texto.

De manera general se puede describir las funcionalidades con las que contara GinToo de la siguiente manera.

- Generador de contraseñas,
- Realizar un filtro de información,
- Autentificación en 2 pasos (2FA),
- Acceso directo (Sin auto llenado de campos de texto),
- Cifrado de información,

- Back-up de datos,
- Autentificación por huella dactilar,
- Contraseña maestra.

4.2.2.8. Requerimientos De Adaptación Del Sitio

En este caso GinToo de manera general manejara un solo tipo de usuario, no obstante, este rol será dividido en dos grupos, dependiendo de la versión que adquiera; los cuales a través de la siguiente tabla se puede identificar claramente las operaciones que puede realizar dentro de la herramienta, del mismo modo los periodos de actividad e inactividad, en otras palabras, la disponibilidad como tal de la herramienta, para con los usuarios.

Tabla 17

Operación De Usuario

Modos de operación de usuarios	
Usuario	**Función**
Basic	• Gestor de contraseñas, para tener disponibilidad de la información, • Se le permite acceso al generador de contraseñas, • Inicio de sesión por medio de huella dactilar (Dependiendo de la disponibilidad del sensor en el dispositivo) • Recuperar contraseña asignada en la aplicación al momento del registro.
Pro	• Gestor de contraseñas, para tener disponibilidad de la información, • Se le permite acceso al generador de contraseñas, • Inicio de sesión por medio de huella dactilar (Dependiendo de la disponibilidad del sensor en el dispositivo) • Recuperar contraseña asignada en la aplicación al momento del registro. • De manera adicional, podrá acceder a la opción de acceso directo.

Fuente: Elaboración Propia.

Tabla 18

Periodos de Actividad e Inactividad

Periodos de Actividad e Inactividad	
Estado	**Función**
Activo	El aplicativo como buena práctica deberá como mínimo estar en un 96% disponible al usuario, por ende, se justifica el hecho de querer implementar Firebase Cloud Firestone, dado a que permite el acceso local y en la nube, realizando actualizaciones automáticamente, cada vez que el dispositivo realice una conexión a la red. Sin embargo, el porcentaje de disponibilidad no puede determinarse con exactitud, debido a que algunos proceso o funciones dependen terceros.
Inactivo	En base al dato anterior, se estima que como máximo, la herramienta debe esta inactiva un 4%, donde los factores que conlleven a esto, estará enfocado a los tiempos de mantenimiento que puedan generarse directamente dentro de la aplicación, del mismo modo, es importante mencionar que, uno de los factores externos que puede afectar la disponibilidad consiste en los servicios que ofrece Firebase y que serán implementados (Authentication, Cloud Firestone), los cuales también podrán entrar en etapa de proceso de mantenimiento.

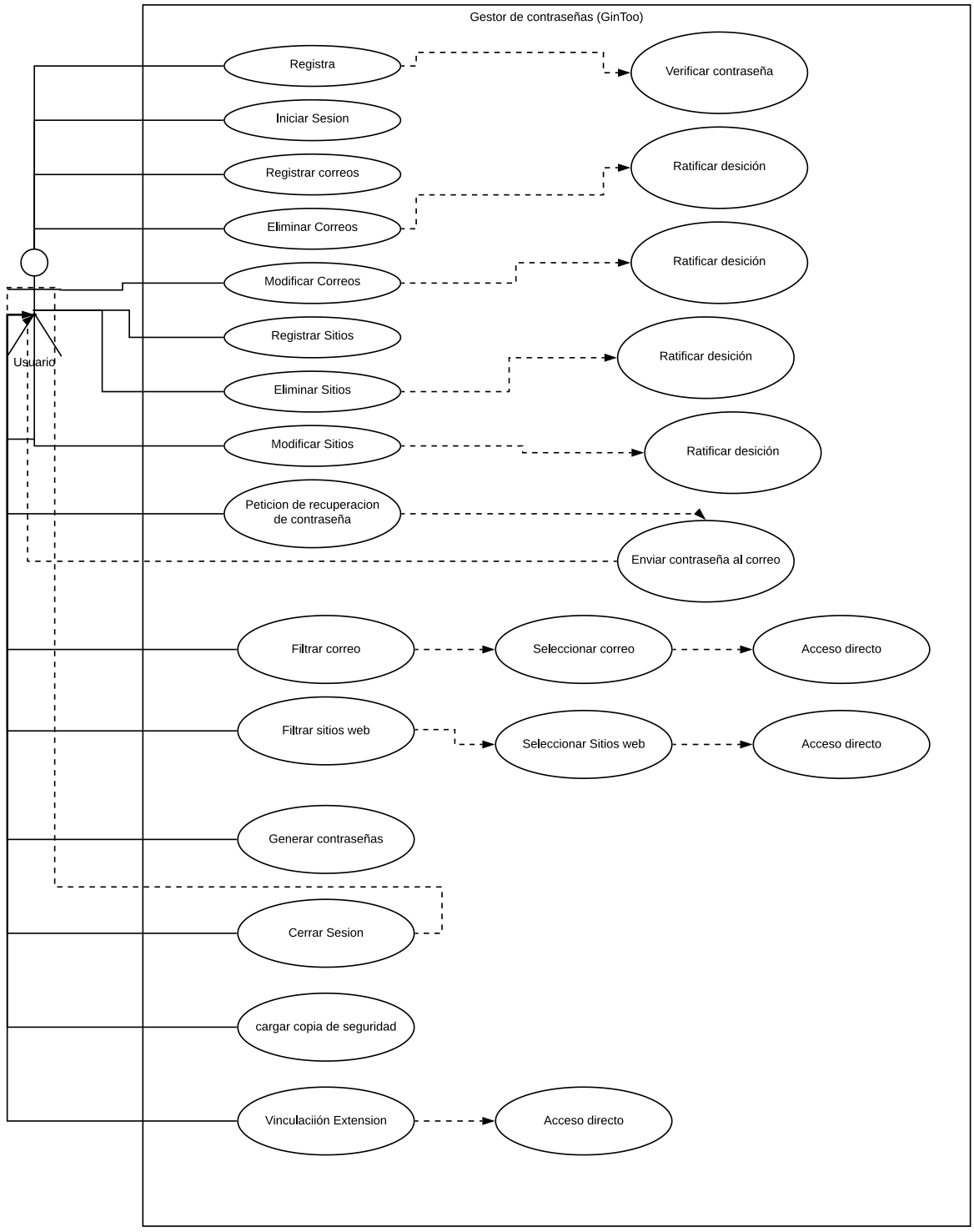
Fuente: Elaboración Propia.

4.2.2.9. Funciones Del Producto

A continuación, se puede observar la funcionalidad básica que presenta GinToo a los usuarios involucrados, a través de un Diagrama de casos de uso, el cual por medio grafico se dará a entender las funciones y pasos que deberá realizar el usuario para poder manipular la herramienta.

Figura 25

Diagrama UML



Fuente: Elaboración propia.

4.2.2.10. Características del usuario

El aplicativo únicamente contará con un solo rol dentro del mismo, ya que no será necesario el uso de administradores como otras aplicaciones, el cual puede ser denominado de manera general como usuario, donde será el único que tendrá acceso a sus datos, sin embargo, cabe destacar que, como método de mercadeo, se podrá dividir en dos grupos como tal a los usuarios, (Basic y Premium).

Donde el usuario "Premium" contara con una versión completa de la herramienta, dado que, este deberá realizar un pago único, puntualmente y como se mostrará más adelante, contaran con la función de acceso remoto, no obstante, los usuarios "Basic" obtendrán con una versión bastante completa, donde se puede indicar en un 90% del aplicativo.

Tabla 19

Características de Usuarios

Roles	Descripción	Experiencia técnica	Frecuencia de uso
Basic	Usuario que tendrá acceso limitado a las funciones de la herramienta.	Conocimiento básico del uso de Smartphone.	El usuario "Basic", utilizara la aplicación cada vez que necesite conocer las contraseñas de usuario al momento de querer ingresar al mismo.
Premium	Usuario que tendrá acceso total a la aplicación, permitiendo una experiencia completa.	Conocimiento básico del uso de Smartphones y sobre extensiones de navegadores web.	El uso para usuarios Premium está enfocada de manera muy similar que el usuario Basic, sin embargo, la función de acceso directo le permitirá un tiempo de proceso más cortos, pero con una frecuencia más alta.

Fuente: Elaboración Propia.

Adicionalmente se mostrará a continuación la tabla en la cual se relacionan las funcionalidades y privilegios disponibles para cada uno de los "roles" mencionados anteriormente.

Tabla 20

Funcionalidades de los Usuarios

Usuarios		
Funcionalidades / privilegios	**Basic**	**Premium**
Interface de Usuario	X	X
Autorización dactilar	X	X
Agregar información	X	X
Llave maestra	X	X
Generador de contraseñas	X	X
Back-up	X	X
Acceso extensión web	X	X
Acceso Remoto		X

Fuente: Elaboración Propia.

4.2.2.11. Restricciones

Las restricciones del aplicativo serían las siguientes:

Tabla 21

Restricciones del Sistema

Restricción	Descripción
Software	La aplicación está diseñada bajo el sistema operativo Android, para ser desarrollado bajo el lenguaje de programación Java, Kotlin o Flutter y archivos con extensión .xml.
Legales	La ejecución de la aplicación no requerirá de licenciamientos pagos, sin embargo, teniendo en cuenta las bases legales determinadas con anterioridad, es necesario al momento de llegar a grandes escalas o a la manipulación de información de forma masiva, la implementación de las normas, principalmente la ISO 27001.
Hardware	Dispositivos Android con los recursos mínimos para la ejecución del sistema operativo Android KitKat4.4 (512 MB de memoria RAM, 850 MB de memoria y resolución de pantalla 480 x 800), por el momento no se puede determinar un tamaño puntual del aplicativo, sin embargo, cabe mencionar que el uso de memoria dentro de la dispositiva variará en valores muy bajos, dependiendo de la información que será almacenada dentro del mismo.

Restricción	Descripción
Cliente	Como tal no existe un cliente puntual dentro del aplicativo.
Arquitectura	La arquitectura a seleccionar será elegida más adelante, por medio de una comparación de varias de ellas, de este modo implementar las más acorde. Entre las arquitecturas a evaluar se encuentran (MVVM, MVC, Cliente - Servidor).
Generales	Los fallos más significativos se pueden presentar al momento de realizar una mala implementación de las normas de seguridad, permitiendo de este modo posibles robos de información, afectado como tal los pilares de la seguridad informática.

Fuente: Elaboración Propia.

4.2.2.12. Modelo de Dominio

Tabla 22

Modelo De Dominio (Registro)

ID:	01	Elemento del dominio:	Registro
Objetivo	Proporcionar un perfil de usuario al cliente, además, poder asignar un ID dentro de la base de datos.		
Descripción	Es importante que se realice un proceso de verificación del usuario, el cual se determinó que el mejor método consiste en la implementación de la autentificación en dos pasos (2FA) por medio de la herramienta Firebase Authentication. Dentro de los métodos a usar son la verificación por correo electrónico y mensajes de texto. El usuario deberá ingresar una contraseña maestra, la cual debe cumplir con la estructura de una clave segura, esto se verificará por medio de codificación.		

Fuente: Elaboración Propia.

Tabla 23

Modelo de Dominio (Inicio de Sesión)

ID:	02	Elemento del dominio:	Iniciar sesión
Objetivo	Otorgarle al usuario ingresar como tal a la cuenta creada luego de realizado el registro.		

ID:	02	Elemento del dominio:	Iniciar sesión
Descripción	Para realizar la verificación del usuario se usará el método de huella digital como el método más seguro, dado que no será necesario almacenar el registro dactilar en la nube, dado que este se realiza de manera local, de esta manera generar un nivel más alto de seguridad. Cabe mencionar que la contraseña maestra será solicitada de manera esporádica, en caso de que el dispositivo cuente con un sensor de huella, de lo contrario, esta clave será el principal método de seguridad.		

Fuente: Elaboración Propia.

Tabla 24

Modelo de Dominio (Administrar Datos)

ID:	03	Elemento del dominio:	Administrar datos
Objetivo	Es necesario mencionar que los datos que tendrá acceso a operar el usuario son: Correo electrónico, contraseñas, usuarios, sitios web. En un número muy reducido de casos el cliente podrá gestionar estos datos, debido a posibles errores de digitación en caso de registros manuales.		
Descripción	En algunos casos el usuario no podrá realizar el almacenamiento de los datos de forma automática, principalmente cuando el dispositivo no cuente con una conexión a internet, por ende, el usuario podrá realizar ciertos cambios, los cuales no pongan en riegos la integridad de los datos, enfatizada mente se podrán realizar registros con bajos controles, sin embargo, para eliminar y modificar se deberá realizar un ratificación de la acción, dado a que es muy riesgoso realizar cambios dentro de la información involucrada. Los cambios se podrán realizar dada a la implementación que se realizara para el almacenamiento, el cual, la plataforma seria Firebase Cloud Firestone, el cual permite un almacenamiento local.		

Fuente: Elaboración Propia.

Tabla 25

Modelo de Dominio (Recuperar Contraseña)

ID:	04	Elemento del dominio:	Petición de recuperación contraseña
Objetivo	Permitir al usuario que este pueda recuperar la contraseña maestra en caso de que sea olvidada		

ID:	04	Elemento del dominio:	Petición de recuperación contraseña
Descripción	A pesar de que el aplicativo pedirá de forma recurrente la contraseña maestra, es primordial brindar al usuario un método que le permita recordar este dato, por ende, se usará la verificación en 2 pasos para determinar la identificación, para posteriormente enviar el link de autentificación al correo, dado a lo anterior como requerimiento obligatorio se le solicitará al usuario algún correo electrónico al momento de realizar el registro.		

Fuente: Elaboración Propia.

Tabla 26

Modelo de Dominio (Filtro de Información)

ID:	05	Elemento del dominio:	Filtro de información
Objetivo	Otorgar al usuario un mecanismo que le permita encontrar de manera más rápida un dato puntual, sin la necesidad de realizar una búsqueda por sí mismo, entre registro y registro.		
Descripción	Cuando un perfil de usuario maneje una cantidad reducida de datos, el encontrar un registro preciso, puede ser una tarea nada tediosa, no obstante, en caso de que el número de registro sea mayor, esto puede convertirse en una problemática, por ende, el usuario deberá tener acceso a una herramienta de filtro de datos, además, para más facilidad se crearan dos grupo de datos, los cuales se clasificarían entre (Correos electrónicos y Sitios web), donde los correos electrónicos será el grupo principal de datos, y los sitios web serán organizadas por el correo que fue usado para la creación de la cuenta.		

Fuente: Elaboración Propia.

Tabla 27

Modelo de Dominio (Generador de Contraseñas)

ID:	06	Elemento del dominio:	Generador de contraseña
Objetivo	El brindar un generador de contraseñas al usuario, permitirá que este, pueda evitar el engorroso proceso de creación de claves.		
Descripción	A pesar de que es bien sabido que se debe crear contraseñas con alto nivel de seguridad, los usuarios no realizan este proceso, primero por el hecho de que en ciertas ocasiones el		

ID:	06	Elemento del dominio:	Generador de contraseña
	proceso resultado complicado y tedioso, por ende, lo recurrente es implementar contraseñas débiles y poco segura pero fáciles de memorizar. Los datos a usar será una combinación de mayúsculas, minúsculas junto con números, con una longitud mínima de 10 caracteres, máximo 20, el cual se le deberá permitir al usuario otorgar la longitud de clave como él más lo crea conveniente. Cabe destacar que, como recomendación también se sugiere el uso de caracteres especiales, sin embargo, en este caso no serán usados, dado que el proceso es aleatorio, y esto puede incurrir a contraseñas difíciles de digitar en caso de que el usuario desee acceder de manera manual, por medio de un ordenador que no tenga dentro de los navegadores web, la extensión.		

Fuente: Elaboración Propia.

Tabla 28

Modelo de Dominio (Cerrar sesión)

ID:	07	Elemento del dominio:	Cerrar Sesión
Objetivo	Los datos no se encontrarán disponibles, solo hasta que el mismo usuario, propietario de los mismos, inicie nuevamente sesión.		
Descripción	Es generalmente conocido que en muchos casos los datos pueden ser visualizados por terceras personas, dado que los usuarios olvidan cerrar la sesión dentro de una cuenta de usuario, en base a esto, y teniendo que la forma de sustraer datos es por medio de una captura de pantalla, también conocidos como screenshot, se tendrá en cuenta el método de protección que utiliza el aplicativo Blockchain, el cual no permite capturas de pantalla, para evitar crear archivos externos los cuales serán usados para almacenar información de forma fraudulenta. Del mismo, el aplicativo cerrara sesión automáticamente luego de pasado un tiempo sin detectar operación por parte del usuario; para esto se debe tomar en consideración los ciclos de vida de un aplicativo móvil, más específicamente, el ciclo de vida de un Activity. Las cuales se puede identificar en la figura 26.		

Fuente: Elaboración Propia.

Tabla 29

Copia de Seguridad

ID:	08	Elemento del dominio:	Copia de seguridad
Objetivo	En base a las buenas prácticas de la seguridad de la información, es importante que todo dato almacenado en una SGSI cuente con una copia de seguridad.		
Descripción	Gracias a la implementación de Firebase Cloud Firestone, las copias de seguridad en la nube se realizará de manera automática cada vez que se realice algún cambio dentro del aplicativo instalado dentro del móvil o la extensión agregada en los navegadores, además, es importante que la data se encuentre protegida, en otras palabras, cifrados.		

Fuente: Elaboración Propia.

Tabla 30

Modelo de Dominio (Acceso directo)

ID:	09	Elemento del dominio:	Acceso directo
Objetivo	Como valor agregado, y por motivos de seguridad en base a las vulnerabilidades detectadas en los navegadores, se implementará un acceso directo a las cuentas de usuario desde le móvil.		
Descripción	Es fundamental realizar la implementación de un XMLHttpRequest que permita enviar los datos al servidor luego del registro realizado por el usuario, del mismo modo la implementación de HTMLInputElement para el inicio de sesión directo.		

Fuente: Elaboración Propia.

Tabla 31

Modelo de Dominio (Almacenamiento Local)

ID:	10	Elemento del dominio:	Almacenamiento local
Objetivo	Permitir un alto disponibilidad de la información al usuario, donde podrá acceder de manera continua a la información sin necesidad de alguna conexión a la internet.		
Descripción	En base al alto número de usuario que no poseen una conexión a internet móvil, e igualmente teniendo en cuenta los pilares de la seguridad informática, es esencial que los datos puedan ser accedidos por el usuario, cada vez que este lo desee, por ende se implementara un almacenamiento local, donde no se requerirá de una conexión a la red, claro está que, la función de acceso directo no estará disponible bajo este estado, sin		

ID:	10	Elemento del dominio:	Almacenamiento local
	embargo, el usuario podrá acceder a la información en caso de que este desee iniciar sesión en alguna de sus cuentas de usuario, digitando de manera manual los datos.		

Fuente: Elaboración Propia.

Figura 26

Ciclo de Vida Activity

Fuente: Tomado de (Google LCC, 2020).

4.2.2.13. Suposiciones Y dependencias

Las suposiciones se entienden como elementos que se dan por entendido que se cumplen, de otra manera no se puede efectuar con los objetivos exitosamente con respecto a la utilización de GinToo por parte de los usuarios. Las dependencias se entienden como elementos de los cuales depende el aplicativo para su ejecución completa y exitosa.

Tabla 32

Suposiciones del Sistema

Suposiciones
• Tener una conexión a internet, ya sea por: wifi o datos móviles; disposición para una computadora con navegador web (Google Chrome, Microsoft Edge). • Cumplimiento de las especificaciones y requerimientos básicos como lo son: tener un Smartphone, capacidad mínima de 512 MB de memoria RAM, resolución de pantalla 480 x 800 y 50 MB de memoria (Disposición estimada). • Es necesario que el usuario opere plenamente con las funciones, especialmente la asignación de contraseñas seguras, de lo contrario el nivel de vulnerabilidad aumentara. • Manipulación en general de las herramientas, dado que este como la mayoría de aplicaciones no estará excepta de posibles malware, como lo son el phishing.

Fuente: Elaboración Propia.

Tabla 33

Dependencias del Sistema

Dependencias
• A pesar de que gran parte de la información va a estar disponible en un alto porcentaje, el uso de ciertas funciones dependerá de una conexión a internet. • Las copias de seguridad necesitaran de una conexión recurrente a la internet, para ser almacenadas a la nube • El estado del teléfono puede afectar algunas funciones de la aplicación, como puede ser un sensor dañado. • La función de acceso directo podrá ser usada únicamente por medio de la extensión, por ende, será necesario su instalación en los ordenadores, puntualmente en los navegadores.

Fuente: Elaboración Propia.

4.2.2.14. Distribución de requerimientos

Es necesario realizar de manera general una distribución de los requerimientos establecidos luego de realizada la investigación.

Tabla 34

Distribución de Requerimientos

Distribución de requerimientos					
Funcionalidad o Modulo	**Servidor**	**Usuario (Basic)**	**Usuario (Premium)**	**Casos de Uso**	
				Nombre	**ID**
Registro y Autenticación	X	X	X	Registro	1
		X	X	Inicio Sesión	2
	X	X	X	Validación Datos	3
	X	X	X	Recuperación Cuenta	4
Administración		X	X	Registrar correos	5
				Modificar correos	6
		X	X	Eliminar correos	7
		X	X	Registrar correos	8
		X	X	Modificar correos	9
		X	X	Eliminar correos	10
Consultas		X	X	Filtro correos	11
				Filtro sitios web	12
Protección		X	X	Generar de contraseñas	13
	X	X	X	Copia de seguridad	14
		X	X	Cerrar sesión automáticamente	15
	X	X	X	Ratificación de elecciones	16
Extensión, navegador web	X		X	Acceso directo	17
	X	X	X	Copia de seguridad	18

Nota: los requerimientos mostrados están clasificados por grupos en base a las características principales del aplicativo, no reemplaza la identificación ni la clasificación de la totalidad de los requemamientos (Funcionales / No Funcionales). Fuente: Elaboración Propia.

4.2.3. Requerimientos Específicos

4.2.3.1. Requerimientos De Interfaces Del Usuario

Tabla 35

Requerimientos de Interfaces con el Usuario

Interfaz	Funcionalidad	Información lógica	Observaciones
Splashscreen	Presentación inicial del aplicativo, generalmente funciona como pantalla de carga.	• Resolución Adaptable • Imagen nombre del aplicativo.	Es recomendable implementar dentro del aplicativo imágenes con formato .SVG
Registro	Formulario donde el usuario creara la cuenta, ingresando datos fundamentales para el proceso, donde igualmente seleccionara el medio de autentificación. Cabe mencionar que solo se permitirá el registro de un solo usuario por dispositivo, debido a temas de privacidad.	• Resolución Adaptable • Icono registro, • 4 Campos de texto, uso de teclado, • Selección método de verificación (Correo o mensaje de texto), • Botón registrar, • Uso del teclado.	Es importante añadir como campo obligatorio el correo electrónico del usuario, ya que por este medio podrá recuperar la contraseña en caso de olvido.
Inicio de sesión	Finalizando el proceso de registro el usuario será enviado a otro Activity el cual tendrá los campos necesarios para acceder a la cuenta, por medio de los datos almacenados en el paso anterior.	• Resolución Adaptable • Icono de la aplicación, • Nombre de la herramienta, • 2 Campos de texto, uso de teclado, • Botón inicio de sesión, • Uso del teclado, • Detección huella dactilar.	El dato contraseña será solicitada de manera esporádica por ende el campo solo podrá visualizarse cuando la herramienta lo indique, luego de ingresar el nombre del usuario y la huella digital se podrá acceder.
Tutorial	Es importante brindar al usuario un breve recorrido por las opciones que brindaría la herramienta, por	• Resolución Adaptable • Descripción automática luego	El proceso de tutorial solo se realizará una sola vez, además, se ejecutará por medio de la librería (material tap target).

Interfaz	Funcionalidad	Información lógica	Observaciones
	ende, se implementará un breve tutorial.	de acceder al perfil.	
Listado de datos	Luego de mostrar el tutorial, se visualizará el Activity con el perfil como tal del usuario. Igualmente, aquí se ingresarán los datos necesarios para el acceso de las cuentas de usuario.	• Resolución Adaptable • Opción de filtrado, • Fotografía del usuario, • Floating button, • Uso de teclado, • Listado de correos, sitios web, • Almacenado de contraseñas, usuarios, correos electrónicos, • Campo de filtrado.	Es importante reducir consumo de recursos en el dispositivo, por medio de la implementación de Fragments, donde cada grupo de listas se encontrará en un fragment diferente, los cuales estarán en el mismo Activity; las listas deberán ser creadas por medio de la librería (Recycler View).
Ingresar datos	Se creará una interfaz que le permita al usuario administrar los datos, ya sean para registrar, eliminar o modificar.	• Resolución Adaptable • 2 a 3 campos de texto, • Uso de teclado, • Botón de ingresar, • Icono registrar nuevo correo,	Pensando igualmente con mejorar el rendimiento, evitando añadir nuevos Activitys, se implementar la librería (Bottom sheet), la cual se ejecutará dentro del mismo Activity donde se encuentran las listas de datos. Es indispensable que no existan varios registros con los mismos datos, por ende, se realizara un proceso de verificación previo al registro como tal.
Eliminar datos	Otorgar al usuario la posibilidad de eliminar algún registro puntual	• Notificación de alerta de ratificación de decisión. • 2 botones (Cancelar, aceptar).	Dado a que la visualización de los datos se realizara por medio de la librería (Recycler view), se implementara (ItemTouchHelper), para realizar el proceso.

Interfaz	Funcionalidad	Información lógica	Observaciones
Modificar datos	El usuario podrá realizar alguna modificación respecto a algún registro puntual, tal como él lo considere necesario,	• Resolución Adaptable • 2 a 3 campos de texto, • Uso de teclado, • Botón de modificar, • Icono modificar nuevo correo.	Reutilizando interfaz, se usará igualmente en este caso la herramienta (Bottom sheet), donde de la misma manera, se ejecutará en el mismo Activity.

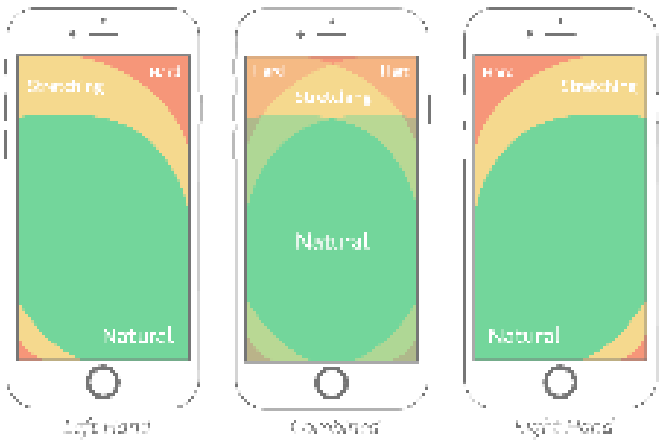
Nota: las características pueden modificarse al momento de realizar como tal el proceso de Mockups del aplicativo.

Fuente: Elaboración Propia.

Cabe especificar que, la disposición en la pantalla de los atributos mencionados, estará basados bajo la disposición del pulgar, conocido en el idioma inglés como: the thumb zone, dado que esto es sumamente importante al momento de diseñar la interfaz, dado a que, por este medio, se puede proporcionar una mejor experiencia al usuario, así lo afirma Pamela Hazelton, donde igualmente menciona que, "aproximadamente la mitad de los 169 millones de usuarios de teléfonos inteligentes en los Estados Unidos, favorecen la operación con una sola mano". (Hazelton, 2018)

Figura 27

The Thumb Zone



Fuente: Tomado de (Hazelton, 2018).

Por medio de la figura 27 se puede evidenciar los accesos que tiene el dedo pulgar en las pantallas de celular, donde se puede identificar que el uso de una combinación de las dos manos, es el modo más óptimo para tener un alto acceso de los atributos dentro de las aplicaciones, sin embargo, teniendo en cuenta el dato dado por Pamela Hazelton, se debe realizar el diseño de la interfaz enfocado a una sola mano, es necesario mencionar que, dentro la imagen muestra rangos de calor dentro de una pantalla nada específica respecto a resoluciones, por ende, se puede estimar que en pantallas muy amplias los accesos difíciles pueden ser más amplios, sin embargo el límite natural del dedo no tendrá grandes variaciones.

4.2.3.2. Requerimientos De Interfaces Del Hardware

Por el momento el aplicativo GinToo no tendrá alguna interacción con otro dispositivo por medio del hardware, la única interacción que se tendrá dentro del dispositivo será la conexión con la extensión del navegador, no obstante, cabe mencionar que este tipo de unión es más enfocada a la parte de software. Esto debido a que, sería poco seguro que los datos puedan ser enviados por medio de otros dispositivos, por ejemplo, vía bluetooth. Sin embargo, la única herramienta necesaria para su completo funcionamiento consiste en el uso del sensor de huella, el cual será usado para el inicio de sesión, no obstante, no será una necesidad para realizar el proceso.

Tabla 36

Características recomendadas generales hardware

Elementos	Características
Sistema Operativo	• Android 4.4.4 o superiores.
Procesador	• Doble núcleo 1.6 GHz.
Almacenamiento	• Entre 850 MB y 1,2 GB, dependiendo de la cantidad de información a almacenar.
RAM	• Mínimo de 512 MB, se recomiendan 2 GB.

Elementos	Características
Disco duro	• 2 GB de espacio en disco duro disponible para su instalación y posteriormente para el almacenamiento de datos. • No puede instalar utilizando un dispositivo de almacenamiento flash extraíble.

Nota: Las características mostradas son las mínimas para que un equipo puede ejecutar el sistema operático KitKat.

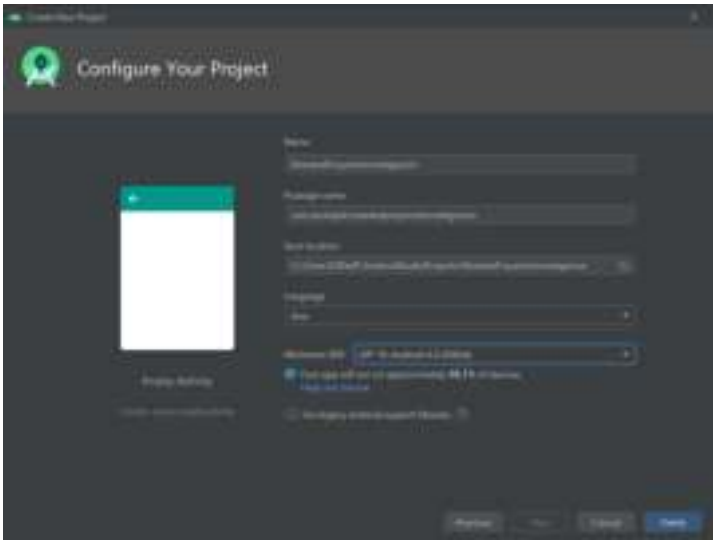
Fuente: Elaboración Propia.

4.2.3.3. Requerimientos De Interfaces Con El Software

Para la realización del aplicativo, específicamente enfocada a smartphone con el sistema operativo (SO) Android, se tomó la decisión de que GinToo se desarrollara para smartphone con la versión de KitKat (Api 19-20) en adelante, esta decisión se tomó teniendo en cuenta que, un gran número de personas posee este tipo de versión en sus celulares, además de lo planteado anteriormente, se tuvo en cuenta que dentro del aplicativo se usara varias de las herramientas de Firebase, tal como se explicó en el apartado (Modelo de dominio).

Figura 28

Porcentaje Estimado De Dispositivos Kitkat



Fuente: Tomado de (Google LCC, 2020).

Nota: Captura de pantalla tomada de la herramienta de desarrollo Android Studio.

Además, en base a la Figura XXVI se puede identificar que con el SDK seleccionado (API 19: KitKat 4.4) que provee la plataforma Android Studio, para la creación de aplicativos, un alto número de dispositivos podrán ejecutar la herramienta, específicamente un 98.1%.
Es necesario tener mínimo celulares categoría gama baja - media debido al Api que se estará usando, esto evitará que se generen bloqueos durante el uso de este aplicativo, este es otro motivo de la decisión de usar Kit Kat como la versión base.

4.2.3.4. Requerimientos de interfaces de comunicación

Por motivos de seguridad la única conexión o comunicación será por medio de una red LAN la cual se realizará entre el aplicativo y el software dentro del navegador (extensión). La comunicación que se hará dentro de GinToo, será por medio de la Internet ya sea por medio de:

- ADSL
- Telefonía móvil GSM, GPRS, 4G, 3G etc.
- Wireless

El objetivo es mandar y recibir información entre los dos softwares, en caso de que el usuario desee realizar el proceso de acceso directo, la comunicación será por medio del canal (Internet), el objetivo de realizar una comunicación LAN, es para que el usuario tenga más control sobre su información, ya que la conexión se realizara por medio de la misma señal de WI-Fi.

4.2.3.5. Requerimientos de desempeño

Debido a los límites de costos identificados dentro de las plataformas de Firebase el aplicativo estará inicialmente enfocado a un público muy pequeño (menos de 10.000), donde gracias a esto, es muy poco probable que en algún momento la aplicación sufra bajos rendimientos; del mismo modo, teniendo en cuenta que el almacenamiento en la nube se realizara por medio de los servidores que provee Google para la ejecución de las plataformas (Firebase). Además, dado que

el almacenamiento será igualmente por medio local, esto evitará que los servidores realicen altos procesos en periodos de tiempos muy cortos.

La forma en que se va a diseñar o desarrollar el aplicativo, proporcionara un bajo consumo de recursos dentro de los diferentes equipos en los que se va a instalar, ya que se van a utilizar dentro del desarrollo el uso de fragments, esto evitara el uso de un gran número de Activitys; los cuales entre los entendidos en el desarrollo de aplicativos móviles dentro de Android Studio, conlleva una mala práctica y un consumo mayor de recursos.

Una gran ventaja de GinToo, es el número reducido de pasos que se deben realizar para cumplir con el objetivo principal de esta.

Registro: en este paso se manejarán pocos datos (los necesarios para realizar un registro), de esta forma se busca que los tiempos sean cortos, específicamente entre 1 a 2 minutos, teniendo en cuenta aspectos como:

- Habilidad de Digitación.
- Posibles errores de digitación durante la escritura
- Confirmación de contraseña errónea.
- Tiempo de almacenamiento.
- Desplazamiento de Activity.
- Autentificación por MSM.

4.2.3.5.1. Inicio de Sesión:

En este caso el número de datos se reduce en comparación a los de la etapa de registro (Usuario, contraseña, huella), por ende, los tiempos se reducirán significantemente, favoreciendo el desempeño de la aplicación, se estima que este proceso se encuentre dentro del rango de 5 a 15

segundos, los tiempos varían dependiendo si el usuario realiza el proceso por medio del sensor de huellas.

4.2.3.5.2. Filtro de información

Por motivos que los datos que se manejen en este proceso son mínimos debido al tipo de dato (Texto) y a un almacenamiento local principal, la información se filtraría en pocos segundos, se estima que sea aproximadamente de 20 segundo, desde el mismo momento en que se selección la opción, para dar este valor se tiene en cuenta que todos los usuarios inicialmente, serán principiantes y no entenderán desde el primer momento el modo de filtración, con el pasar del tiempo se espera que los tiempos se reduzcan en unos 5 a 10 segundos aproximadamente.

4.2.3.5.3. Generador de contraseñas

Gracias a que el proceso está fundamentado principalmente en cadenas de caracteres aleatorios donde automáticamente el aplicativo los generara, el proceso no requerirá de altos tiempos para realizar el proceso, no obstante, debido a que el usuario tendrá la posibilidad de gestionar la longitud de la cadena, los tiempos pueden verse aumentados, aproximadamente en un 1 a 2 minutos.

4.2.3.5.4. Acceso Remoto

Dado a que el proceso se realizara de forma directa (Sin necesidad de auto relleno de formularios), se estima que los tiempos no sean muy altos, sin embargo, para este proceso se requiere de una conexión a la red, fundamentalmente con la misma red LAN; teniendo en cuanta que como método de seguridad se realizara un proceso de autentificación, el tiempo estimado desde el momento en que el usuario inicia sesión hasta el acceso como tal a una cuenta de usuario, se encontraría entre unos 4 a 5 minutos.

4.2.3.6. Restricción de diseño

GinToo está enfocada a desarrollarse dentro del sistema operativo Android; por este motivo el lenguaje de programación que será usado para el desarrollo del aplicativo será Java, Kotlin o Flutter además de tener muy en cuenta los archivos .XML presentes en el proyecto (String.xml, Colors.xml, Style.xml etc.),

En caso de restricciones de software, y teniendo en cuenta lo explicado anteriormente, no podrá ser instalado en IOS; dentro de los diferentes sistemas operativos presentes en Android, solo podrá ser usado, en el API (19-20) y superiores, debido a que la mayoría de dispositivos que poseen esta versión disponen de los requerimientos mínimos para el funcionamiento.

Una de las restricciones identificadas dentro de Firebase Authentication y Cloud Firestone son los límites de servicio gratuito, explicados dentro de las tablas (5 y 12), los cuales, restringen la herramienta en niveles altos de usuarios registrados dentro la herramienta.

Por ende, es recomendable realizar estudios de expansión enfocado al lucro, permitiendo de este modo un número mayor de usuarios.

4.2.4. Atributos Del Sistema De Software

4.2.4.1. Fiabilidad

De manera general la información que se manejara dentro de la aplicación está dentro de un ámbito muy personal y de alta importancia (contraseña, usuarios, correos electrónicos), por ende, es importante que la herramienta cumpla de manera sobresaliente con la protección, disponibilidad y en este caso confiabilidad, el cual dado que Google será en este caso la proveedora del almacenamiento y de verificación, por medio de Firebase, incurriría a una alta confiabilidad respecto a la información alojada en los servidores.

El hecho de que el almacenamiento se implementaría principalmente de manera local, no indicaría que los datos, pueden ser extraviados al momento de la pérdida del dispositivo, debido a que, de manera automática al momento de realizar una conexión a la internet, se realizara una copia de seguridad dentro de la nube, en los servidores de Google; donde esta información será accedida de manera provisional por medio de la extensión, claro está, luego de realizar el proceso de verificación por medio de un mensaje al correo electrónico.

4.2.4.2. Disponibilidad

Como se ha hecho mención, el aplicativo deberá como mínimo tener una disponibilidad del 96%, ya sea para el usuario "Basic y Premium", para esto, se debe tener en cuenta que varias de las funciones que prestaría la herramienta, funcionarían por medio de terceros, puntualmente Google con la plataforma Firebase, donde es difícil determinar de forma exacta la disponibilidad de los servicios; por ende, gracias al almacenamiento local, por medio de Cloud Firestone, se incrementaría notoriamente la disponibilidad, dado que no se requiere de una conexión para acceder a la información. Cabe mencionar que, cuando el aplicativo entre al ciclo de vida onPause, onStop u onDestroy (figura 26) la sesión se mantendrá activa solo por un periodo corto de tiempo luego de iniciada la sesión de usuario, el motivo de esto está basado en los riesgos que puede tener la información en caso de que el usuario olvide cerrar su cuenta, y su dispositivo sea operado por terceras personas. A pesar de que puede resultar un poco cansino realiza el proceso de inicio de sesión, es importante destacar que, gracias a la autentificación por huella dactilar, el ingreso solo requerirá de pocos segundos.

La única manera en que dicha aplicación no estará disponible con respecto a la sesión será cuando el usuario decida cerrar la misma o sea cerrada de manera automática; sin embargo, la sesión se mantendrá activa mientras que el aplicativo se encuentre en la fase de Activity running.

Si nos enfocamos en la aplicación en general, debemos tener en cuenta que el uso de internet dentro de esta aplicación no es altamente necesario, debido al almacenamiento local, no obstante, es fundamental al momento de querer mantener un Back-up de la información en la nube, y poder acceder a funciones avanzadas (Acceso Remoto).

Otro punto es que la aplicación estará disponible solo para celulares con versión KitKat y superiores de esta forma nos aseguramos de que funcione de la manera más fluida posible, en base a que la versión antes mencionada debe tener ciertas características de hardware para su funcionamiento, las cuales son las recomendadas para que GinToo funcione, debido a que los datos son netamente texto.

4.2.4.3. Portabilidad

A pesar de que el aplicativo esta inicialmente enfocado al sistema operativo Android, la implementación de las herramientas de Firebase, permite una fácil portabilidad teniendo en cuenta que estas pueden ser implementadas en diferentes plataformas, tal como se determinó en los respectivos puntos dentro de este documento (Firebase Authentication, Cloud Firestone), inicialmente se estimaría ampliar la herramienta dentro de los dispositivos de IPhone, cuyo sistema operativo es IOS.

4.2.4.1. Seguridad

La seguridad para GinToo comenzara desde el primero momento en que un usuario ingrese y realice el proceso de registro, comenzando por la confirmación de contraseña, de esta manera nos aseguraremos que la contraseña sea la deseada por el usuario. Además, que se realizar el proceso de autentificación por medio de Firebase Authentication, el cual maneja uno de los sistemas más seguros respecto a las verificaciones, puntualmente se implementara la verificación Phone auth.

Entre los datos de registro se encuentra el correo electrónico, este permitirá en caso de que la contraseña sea olvidada por parte del usuario, tener la posibilidad de recuperarla; la manera de realizar este proceso será por medio de un mensaje que se enviara automáticamente al correo que el usuario indico al momento del registro, de este modo la única forma en que este pueda recuperar su clave será ingresando a su correo personal; de la misma forma que en la etapa de registro, el proceso se realizara por medio de la autentificación en dos pasos.

Como se ha podido determinar los datos son de alta importancia y sensibles, por ende, es necesario el uso de un algoritmo de cifrado, que permita convierta los datos, en un formato no legible, mientras que no se tenga disponible las claves necesarias para descifrar el texto, tal como se pudo determinar en el esquema de cifrado (Fig. I).

Por medio de la siguiente tabla se puede identificar de manera más clara, las medidas de seguridad identificadas y a establecer dentro de GinToo.

Tabla 37

Características Básicas de Seguridad

Características Básicas de seguridad	
Métodos	**Justificación**
Contraseña	Confirmación de Contraseña, mediante un campo de texto adicional.
Correo Electrónico	Recuperación de contraseña por medio de un correo electrónico, que será enviado al correo registrado por el usuario.
Autentificación	Proceso de verificación por medio de la autentificación en dos pasos 2FA, por medio de un código enviado al dispositivo por mensaje de texto.
Algoritmo De Cifrado	Código que será usado solo por los administradores para ingresar a la sección de administrador que se encuentra oculto para los usuarios del común.
Cerras Sesión	Cerrar sesión de forma automática, luego de un tiempo sin detectar algún tipo de operación.

Captura De Pantalla	Evitar la captura de pantalla, permite evitar posibles robos de información por medio de esta función.

Fuente: Elaboración Propia.

4.2.4.2. Mantenibilidad

La forma de poder mantener el funcionamiento como tal del aplicativo, es fundamental tener en cuenta los procesos de detección de riesgos tal como lo sugiere la norma ISO 27001; dado a la importancia de la información que se manejaría dentro de la aplicación, los esfuerzos estarían principalmente en la prevención, dado que, en caso de que se deba en algún momento realizar alguna corrección de algún error, daría a entender que el sistema fue vulnerado y por ende posibles robos de información, sin embargo dado a que gran parte de las herramientas a implementar serán de terceros, los esfuerzos irían principalmente al dispositivo móvil como tal y de su almacenamiento local.

4.3. Resultados Del Objetivo Especifico N°3

Finalmente, luego de identificar de manera general los requerimientos con los que va a contar la herramienta, teniendo en cuenta accesibilidad, integridad, pero ante todo seguridad, y continuando con el proceso de diseño del aplicativo, dentro de este apartado tal como se estableció al inicio del presente documento como uno de los objetivos específicos se: (seleccionara una arquitectura, y metodología de software que más se ajuste al diseño del aplicativo móvil). Cabe mencionar, que dentro de la ingeniería de software es importante establecer de manera correcta una estimación respecto al proceso o pasos al momento de ejecutar el proyecto, con el objetivo de crear un software de calidad, así lo afirma Roger S. Pressman, autor del libro Ingeniería de software un enfoque practico, donde textualmente menciona que "la ingeniería de software está formada por un proceso, un conjunto de métodos (prácticas) y un arreglo de herramientas que permite a los profesionales elaborar software de cómputo de alta calidad." (S. Pressman, 2010) Para lo anterior, se debe tener en cuenta tres factores sumamente

importantes para que un proyecto cumpla de manera óptima con el objetivo estipulado inicialmente, los cuales son:

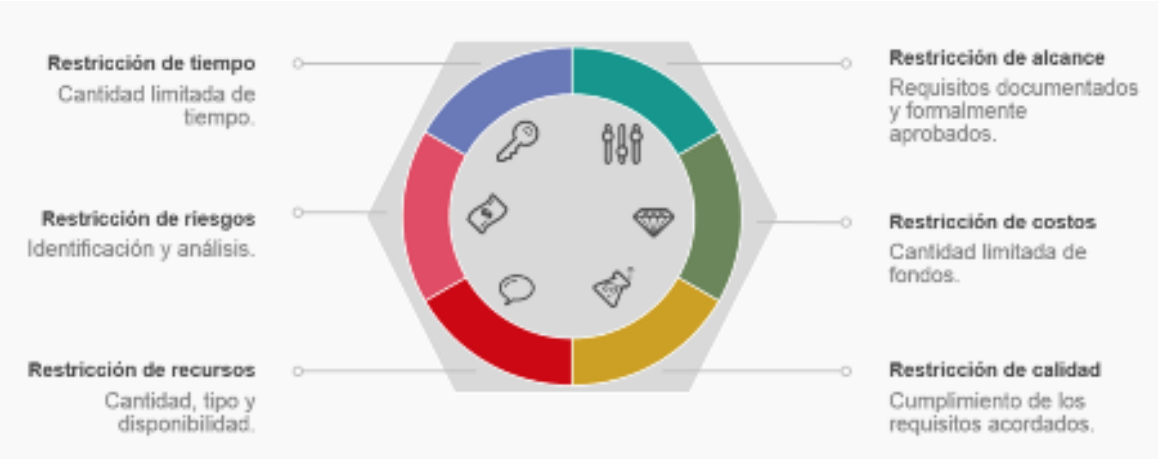
- Alcance,
- Tiempo,
- Costos.

Dentro de un proyecto a esto se le denomina la triple restricción el cual, debe establecerse de manera clara al momento de la planeación del proyecto, el objetivo de implementación de la triple restricción consiste en un equilibrio entre estos tres elementos, de lo contrario cuando alguno de esto factores se vea altamente alterado con respecto a lo establecido inicialmente, con el fin de que el proyecto, en algún momento de la ejecución, no pueda encontrarse en riesgo; cabe destacar que en algunos proyectos no solamente se tienen en cuanta los puntos antes mencionados, sino además, implementan un número mayor de factores, conocida como una triple restricción ampliada, donde además de los elementos anteriores se tienen en cuenta:

- Riesgos,
- Recursos,
- Calidad.

Figura 29

Triple Restricción Ampliada



Fuente: Tomado de (Gascón Busio)

Por ende y en base a lo anterior, es necesario identificar una arquitectura y la metodología que se usarían para el desarrollo del aplicativo, por ende, es fundamental realizar una comparación de varios de estos elementos, para posteriormente seleccionar de manera eficiente la mejor para la implementación.

Para la selección de una arquitectura, y en base a lo determinado hasta el momento, se pueden identificar como los más acordes tres tipos, las cuales son: (MVVM, MVC y Cliente – Servidor). De la misma manera, para el proceso de ejecución se evaluarán tres metodologías, también conocidas como ciclos de vida, entre ellas se encuentran: (XP, Espiral, Scrum).

4.3.1. Arquitectura

4.3.1.1. MVC

De manera general y básica la arquitectura MVC, se encuentra dividida en tres componentes, en ingles están denominamos como Model, View y Controller, en su traducción al español

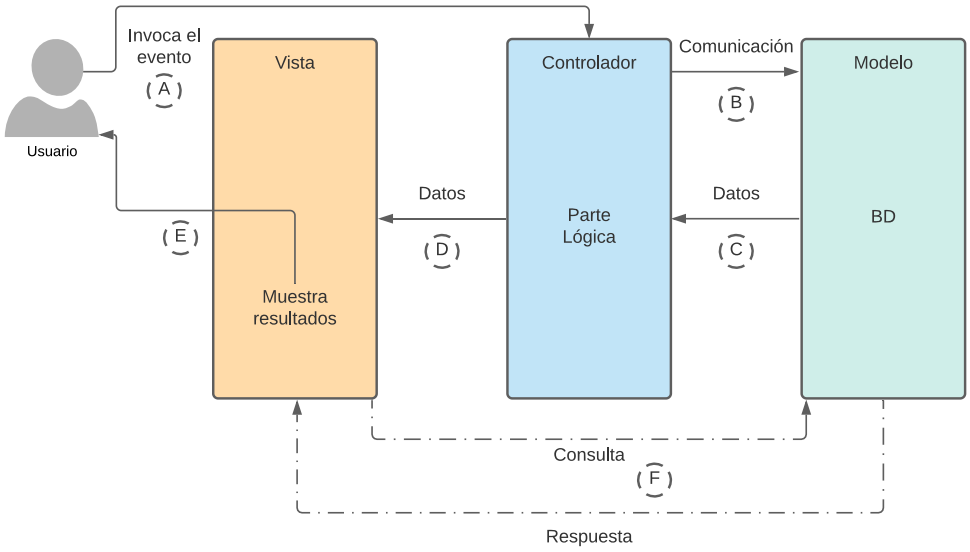
corresponde a Modelo, Vista, Controlador, los cueles se encuentran conectados entre sí. Nilsen Espitia, Oscar Armao junto con Jhonnathan Carbajo mencionan que, una arquitectura MVC.

> Es un patrón de diseño de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de control en tres componentes distintos de forma que las modificaciones al componente de la vista, o a cualquier parte del sistema puedan ser hechas con un mínimo impacto en el componente del modelo de datos o en los otros componentes del sistema" (Espitia , Armao, & Carbajo, 2016).

Lo anterior se puede ver más detalladamente por medio de la siguiente figura.

Figura 30

Arquitectura (MVC)



Fuente: Elaboración propia basado de (C. Martínez, 2020).

Para describir el proceso que realiza esta arquitectura, se tomará como ejemplo el inicio de sesión de una cuenta de usuario, donde existe la aplicación como tal y un SGBD, el proceso inicia con un usuario que realiza una solicitud de acceso (paso A), conocida dentro de la misma arquitectura como un evento; por medio de la capa **Controlador (C)** y teniendo en cuenta los

elementos mencionados, en este caso el controlador es el SGBD, que toma el evento ejecutado por el usuario, para posteriormente realizar una comunicación con la capa **Modelo (M)** (Paso B) con el fin de tomar la información necesaria para verificar la identidad del usuario (paso C, D), finalmente luego de determinada la identidad del usuario, los datos almacenados dentro de la cuenta serán mostrados en la capa **Vista (V)** (Paso F); cabe destacar que dependiendo de la información a manejar, no se requerirá del intermediario (Controlador), esto último se puede identificar en el paso G. Tal como se explicó, se debe realizar una comunicación entre estas dos capas (Controlador - Modelo), generalmente y dependiendo del gestor de base de datos, el lenguaje utilizado es el SQL.

A continuación, se podrá identificar de manera más clara como está conformado cada componente que conforman la arquitectura.

- **Modelo:** Representa a la estructura de almacenamiento con la que está conformada el aplicativo, generalmente es una base de datos, junto con sus tablas y relaciones entre ellas.
- **Vista:** En pocas palabras la vista, es la interfaz gráfica de la aplicación o sitio, el cual permite al usuario interactuar como tal con el software, más específicamente, seria todo elemento que pueda ver el consumidor por medio de la pantalla.
- **Controlador:** Es la parte lógica del sistema, intermediario entre la vista y el modelo, el cual tiene la capacidad de analizar y procesar los eventos realizados por el usuario, igualmente encargado de tomar la información de la capa modelo, para posteriormente cargados a la capa vista.

El objetivo de estructurar una aplicación por medio de esta arquitectura es debido a que, gracias a que está dividida por medio de tres capas definidas claramente, permite una escalabilidad de

manera muy sencilla sin la necesidad de realizar grandes cambios en los demás componentes, teniendo en cuanta los atributos de software, mejoraría notoriamente la modificabilidad del software.

Tabla 38

Ventajas / Desventajas (MVC)

Ventajas	Desventajas
• Facilita los cambios dentro de las capas y realizar pruebas de manera separa. • Se puede añadir diversas vistas para un solo modelo sin la necesidad de realizar cambios en este último. • La capa vista de manera automática realiza cambios, dado que el encargado de realizar dichas modificaciones es la capa (controlador). • Gestiona en un alto rendimiento los recursos del servidor, evitando errores de rendimiento. • La comunicación entre las vistas y el modelo se realiza cada vez que se detecte un evento por parte del controlador.	• Debido a que sus capas están de manera separa, la implementación resulta compleja. • Difícil de programar en lenguajes, cuya estructura no está basada en POO. • Se necesita de altos conocimientos técnicos para su implementación. • Es necesario un número elevado de archivos para desarrollar. • Genera grandes costos.

Fuente: Elaboración Propia basada en (Jiménez & Mayorga).

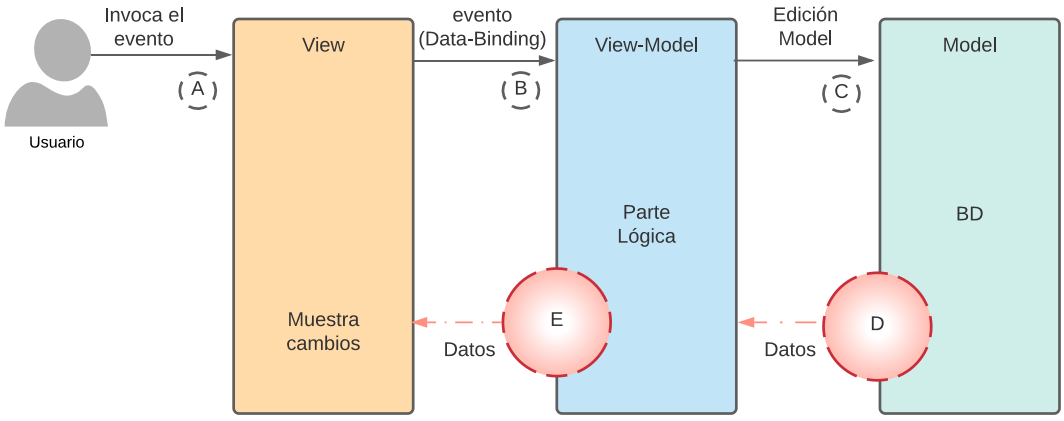
4.3.1.2. MVVM

Es patrón de diseño de arquitectura, el cual está conformado por tres elementos: Model, View y ViewModel, al español Modelo, Vista y Vista – Modelo, donde de manera similar que el patrón MVC, se busca dividir la estructura de un proyecto en diferentes capas con el objetivo de poder realizar cambios en alguna de ellas, sin verse afectadas los demás elementos; Rodrigo Solís Morales confirma lo mencionado afirmando que el MVVM es un patrón de diseño basado en MVC y en MVP que busca separar el desarrollo de interfaces gráficas del desarrollo de la lógica

de negocio. Existen distintas implementaciones, pero la base de todas estas es el data-binding. (Solís Morales).

Figura 31

Metodología (MVVM)



Fuente: Elaboración propia basado de (C. Martínez, 2020).

- **View:** Debido a que es una variación del patrón Modelo Vista Controlador, la vista es igualmente la parte grafica de la aplicación o software como tal, es la capa donde el usuario puede operar o realizar acciones (Paso A), del mismo modo, es aquí donde se mostrara la información obtenida de la capa Model. En complemento a lo mencionado, Borja Guzmán López afirma que la capa vista contiene las responsabilidades de manejar los controles de interfaz y la sincronización de la presentación. Es el encargado de realizar todas las peticiones al presentador para solicitar las acciones que indique el usuario y la información que se tenga que representar en la interfaz. (Guzman Lopez, 2018).

  Dentro de la figura previa, se puede identificar que, se realiza un proceso de comunicación entre la capa View y View–Model medio del data-binding (Paso B),

mencionado previamente, el cual y en pocas palabras, es un mecanismo que permite un canal de comunicación entre esta vista (View) y el View–Model.

- **View – Model:** La capa View–Model, se podría comparar con la capa controlador en la arquitectura MVC, ya que de manera muy similar es un intermediario entre las dos capas, previamente explicadas, de aquí su nombre (View-Model), el cual es el encargado de tomar las peticiones del usuario, procesarlas y realizar una comunicación entre la capa Model (Paso C); cabe mencionar que la información generalmente puede encontrarse bajo un formato de protección por ejemplo un cifrado, donde claramente esta información tal cual esta almacenada en la base de datos no puede ser enviado en este formato a la capa vista, para posteriormente ser mostrada al usuario, por ende, esta capa (View – Model) será la encargada de transformar los datos a un formato legible y ser mostrados al usuario. (Solís Morales), teniendo en cuenta el proceso data-binding, es por medio de este mecanismo donde la View-Model, puede comunicar cualquier cambio que se haya realizado en la capa Model a la capa View. Del mismo modo, es el encargado de realizar la comunicación con fuentes o aplicaciones externas, generalmente con web services.
- **Model:** De manera muy similar que la arquitectura MVC y como se puede detallar en la figura 30, el modelo es la capa donde se encuentra la estructura donde la información se encuentra almacenada, comúnmente dentro de una base de datos o bodega de datos, principalmente está enfocada a la estructura de esta base de datos (Tablas, clases y demás), conocida igualmente como la capa de lógica de negocio.

Tabla 39

Ventajas / Desventajas (MVVM)

Ventajas	Desventajas
• Permite separar el proyecto en diferentes capas fáciles de modificar. • Otorga facilidad al momento de querer realizar pruebas de cada componente. • Dado a desvinculación entre capas del proyecto, se puede realizar procesos de mantenimiento con alta facilidad. • Gracias a la implementación Data–pinding la separación entre la capa (View y View-Model) es mayar, permitiendo mejores procesos de mantenimiento, modificabilidad en comparación a otros patrones. • Sus capaz permiten ser reutilizadas en diferentes proyectos.	• Se requiere de un número alto de ficheros en caso de una repartición alta de los componentes. • En desarrollo móvil, puede resultar complejo cuando se quiera obtener información por medio de la nube. • No existe una estandarización establecida, lo que puede complicar su implementación. • Debido a que no existe una estandarización, en las clases en que se implemente, se deberá realizar procesos distintos.

Fuente: Elaboración propia basada en (Loor Vargas, 2015).

En base a lo examinado hasta el momento respecto al patrón de arquitectura MVVM, podemos identificar que el mecanismo de operabilidad es muy similar a la arquitectura MVC, además que, cada una de ellas está enfocada al desarrollo dentro de aplicativos Android. No obstante, existen diferencias entre ellas.

- La capa View en el caso de la arquitectura MVVM no tiene la capacidad de recibir información de manera directa con la capa modelo, por esta razón se requiere del intermediario (View-Model) para realizar este proceso. Mientras que, en MVC según el caso la vista si podrá obtener información directamente.
- Además, la comunicación entre las capas (View y ViewModel) es unidireccional, esto se puede apreciar en la figura 31, mientras que la comunicación (Vista–Controlador) en MVC es bidireccional, permitiendo enviar y obtener información entre ellas.

- Debido a que la comunicación es unidireccional en entre la (View y View-Model) la forma de "enviar" datos a la View se realiza medio de un proceso de notificaciones al momento de identificar algún cambio en el sistema (Paso E), este proceso es conocido como **Live Data** junto con el método Data- binding, cuyo mecanismo no es tan directo como en MVC.
- Del mismo modo en que funciona la comunicación (View y View-Model), él envió entre (Model y View-Model) se realiza por medio de notificaciones entre estas dos capas (Paso D), los cuales se generan cada vez que en la capa Model se realice algún tipo de modificación; mientras que en MVC existe una comunicación directa y continua. (C. Martínez, 2020)

4.3.1.3. Cliente / Servidor

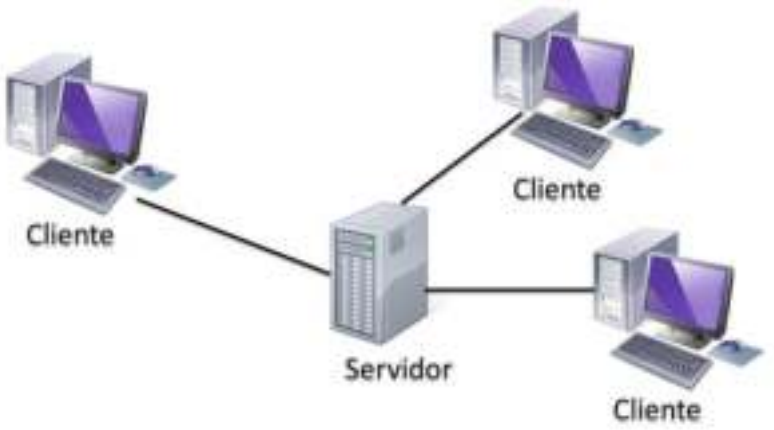
Tal como su nombre lo indica dentro de esta arquitectura distribuida se encuentran dos elementos esenciales para su estructura, el **cliente** y **servidor**, el funcionamiento de este diseño consiste en que el servidor, ya sea de manera local o remota, está a la espera de recibir instrucciones por parte del cliente, solicitando un servicio en específico, para luego el servidor procesar dicha solicitud, para enviar una respuesta al cliente, en donde de este modo, se genera una comunicación entre ellos realizando diversas operaciones.

Lo anterior, se puede corroborar teniendo en cuenta lo explicada por el departamento de informática de la Universidad de Valladolid, donde menciona que, en la arquitectura cliente / servidor, los clientes están representados dentro de la computación como programas que ofrecen una prestación de una entidad, los cuales necesitan de un servicio a nivel de informática; y un servidor seria, en pocas palabras el encargado de proporcionar estos servicios, de hecho, y de manera textual menciona que, "un cliente hace una petición de un servicio y recibe la respuesta a

dicha petición; un servidor recibe y procesa la petición, y devuelve la respuesta solicitada un cliente". (Universidad de Valladolid)

Figura 32

Arquitectura cliente servidor



Fuente: Tomado de (Huertas, 2019).

Es importante mencionar que, a pesar de que se pueda creer que la comunicación solo se realizaría entre un ordenador y un servidor, en realidad este tipo de arquitectura permite un gran número de dispositivos o programas (clientes) conectados a un solo servidor, tal como se puede visualizar en la figura 32, dado a que el servidor contiene características de rendimientos muy altos, con el objetivo de procesar un gran número de solicitudes al mismo tiempo y de diferentes clientes. Igualmente es importante mencionar que, en algunos casos, dependiendo de la cantidad de datos que se maneje dentro de un sistema de información, para otorgar una concurrencia alta y de paso favorecer la tolerancia a fallos, se implementarían varios servidores conectados entre sí para que de este modo se puedan realizar procesos más complejos en un número menor de tiempo, a este tipo de estructura se le es denomino como un clúster.

Existen diferentes tipos de servidores, donde cada uno realizar diferentes operaciones:

- **Servidores de archivos:** El cual tal como su nombre lo indica, está enfocado al almacenamiento de archivos, tales como: (hojas de cálculo, documentos, etc.); es conocido igualmente como un repositorio, un ejemplo de esto, pueden ser los almacenamientos de ciertas universidades donde se almacenan documentos, libros, tesis, proyectos de grado, entre otros.
- **Servidores de bases de datos:** Generalmente enfocado al almacenamiento de información tipo texto, comúnmente por medio tablas, a través de gestores de bases de datos, ya sean relacionales o no relaciones; entre las relaciones se encuentran: (Oracle, MariaDB, MySQL, y demás); por parte de las no relacionales se pueden mencionar (mongoDB y Cassandra).
- **Servidor de transacciones:** En pocas palabras este tipo de servidor es el que recibe y procesa solicitudes, por medio de un proceso inicial de validación para posteriormente enviar un pedido de información a otro tipo de servidos.
- **Servidores Groupware:** Tal como lo dice en su traducción al español (Trabajo en grupo), este tipo de servidor consiste en un grupo de varias herramientas alojadas en un mismo servidor con el objetivo de cumplir un objetivo puntual y en común.
- **Servidores de objetos:** En este caso, el servidor de objetos realiza un proceso de almacenamiento más amplio respecto al formato de archivos que permite alojar, el cual, permite el depósito de archivos multimedia (Videos, música, imágenes).
- **Servidores web:** Enfocado principalmente a la gestión de información en la red, principalmente a páginas web y web services, por medio del protocolo HTTP (Muñoz Cerón, 2000).

Dentro de las **ventajas** que se obtiene al momento de la implementación de la arquitectura Cliente/Servidor, es que permite un **aumento de productividad**, así lo afirma, Pablo Fernando Muñoz, en su trabajo de titulación en la Universidad de las Américas, donde menciona que, debido al tipo de datos que se pueden almacenar (Texto y archivos multimedia), los usuarios podrán realizar soluciones particularizadas, y en diferentes partes y por diferentes medios. Del mismo modo menciona que, los **costos de operaciones** son menores, dado a que la información tendrá un acceso mucho más amplio, por diferentes clientes al mismo tiempo, algo muy similar al método de funcionamiento de la herramienta GitHub, donde varios usuarios al mismo tiempo pueden manipular un mismo archivo, además que, los procesos pueden ser distribuidos desde un servidor hacia diferentes dispositivos (Clientes); igualmente mejora el rendimiento en la red, ya que la arquitectura permite un escalamiento, el cual puede ser (Horizontal o vertical), donde el escalamiento vertical consiste en la implementación de nuevo hardware dentro de los equipos que se encuentran en el esquema puesto en marcha hasta el momento, mientras que un escalamiento horizontal está basado en la adición de nuevos equipos, generalmente consiste en este caso en la adición de nuevos servidores, los cuelas como se mencionó previamente se pueden conectar por medio de un sistemas tipo clúster. Por último, existe un grado más elevado de **seguridad** por medio de esta arquitectura, comparado con un sistema basado únicamente por medio de un ordenador centralizado.

Sin embargo, como **desventajas** Pablo Muñoz menciona que a pesar de que el **escalamiento** puede ser una ventaja, del mismo modo puede convertirse en un inconveniente, debido a que puede resultar un proceso tecnológico complejo, al tener que añadir una gran variedad de productos, principalmente cuando el proceso es realizado de manera remota, además, porque es necesario rediseñar como tal el sistema en diferentes apartados, como son: (Interfaces,

comunicación, almacenamiento, y demás.). El hecho de que se permita un gran número de usuarios al mismo tiempo, donde a este fenómeno se le denomina concurrencia, puede resultar en **degradaciones** en procesos y rendimiento visualizados por los clientes, por ende, es necesario determinar de manera aproximada el número de usuarios que permite el sistema, para evitar posibles fallos. Del mismo modo en que el escalamiento puede resultar ser una ventaja y una desventaja, los **costos** indistintamente funcionan del mismo modo, dado que, pueden existir costos que no fueron previstos, pero con el pasar del tiempo y durante su ejecución pueden generar gastos de dinero, entre los factores que poder recurrir a esto, se encuentran: (Licencias, cambios organizativos, implementación de nuevo hardware o software, etc.). (Muñoz Cerón, 2000)

4.3.2. Metodología

4.3.2.1. Metodología XP

Conocida igualmente en el lenguaje inglés como eXtreme Programming, en su traducción al español la podemos identificar como metodología de programa extrema, es una de las metodologías agiles, utilizada para el desarrollo de proyectos de software con baja complejidad, y con tiempos estimados de ejecución muy cortos, dado que está enfocada principalmente al desarrollo como tal, muy diferente a otros tipos de metodologías donde la documentación es un factor fundamental, sin embargo, esto no quiere decir que la documentación en la programación extrema pasara a ser nula, dado que igualmente se debe realizar dicho proceso, no obstante en un escala mucho menor y con puntos netamente importante; además de lo anterior, Sintya Meléndez, María Gaitan y Neldin Pérez afirman que la programación extrema “es una Metodología ligera de desarrollo de aplicaciones que se basa en la simplicidad, la comunicación

y la realimentación del código desarrollado. (Meléndez Valladarez, Gaitan, & Pérez Reyes, 2016)

Asimismo, es importante destacar que, el grupo de trabajo dentro de la esta metodología, está restringida a un número muy pequeño de integrantes, donde en este caso el máximo sugerido son 12 miembros por proyecto, y además distribuidos por parejas, esto permitirá que la comunicación entre ellos sea más directa, a diferencia de metodologías que manejan un grupo más amplio donde la comunicación se realiza por medio de correos electrónicos, u otros medios similares, lo que genera retrasos de respuestas, y ver perjudicada principalmente el factor tiempo, en los variables de un triple restricción o restricción ampliada; cabe mencionar que, dentro de la programación extrema se tienen en cuenta cuatro factores, para lograr el éxito del proyecto, las cuales son: (tiempo, costo, alcance, calidad). Del mismo modo una de las características principales, es que permite realizar modificaciones dentro del proyecto con facilidad.

Figura 33

Ciclo de Vida (Metodología XP)

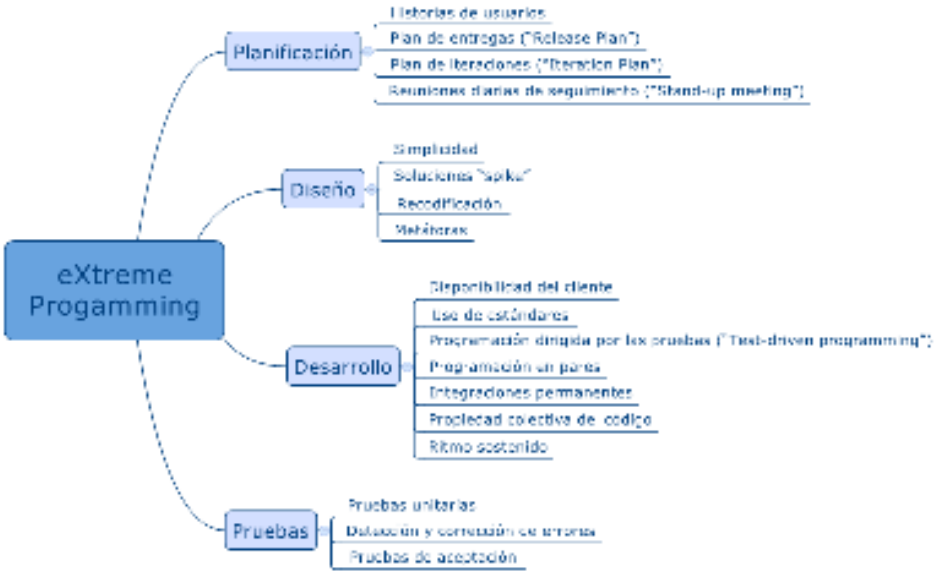
Fuente: Elaboración propia.

Igualmente es importante destacar que esta metodología ágil, funciona por medio de iteraciones, donde cada una de ellas consta de cuatro fases:

- **Planificación:** Un proyecto con metodología XP, inicia con una fase de planificación, donde en este punto se realiza una primera comunicación directa con el cliente como tal, cuyo propósito es realizar una primera toma de historias de usuarios, conocidos igualmente como requerimientos del software, donde posteriormente serán evaluados y clasificados.
- **Diseño:** Etapa donde se realiza un esquema simple con el fin de determinar los métodos de ejecución de las historias de usuarios, establecidas en el paso anterior. Puntos fundamentales a tener en cuenta, son la **recodificación**, **simplicidad**, además de identificar de manera clara y puntual el propósito del proyecto, donde a este proceso es conocido como **metáfora**.
- **Codificación:** Como su nombre lo da a entender es la fase donde se realiza como tal el proceso de desarrollo, donde se ejecutará lo planeado en la fase anterior, el proceso debe está basado bajo estándares de programación, permitiendo de este modo reducir los tiempos en el proceso; como factor esencial, se recomienda que el cliente esté disponible en todo momento.
- **Pruebas:** Por último, luego de finalizado cada fase de desarrollo es importante entrar en una fase de testeo, donde se ejecutará una verificación del avance realizado en la etapa de codificación, determinando y corrigiendo errores, para finalmente realizar un test de aprobación de cada historia de usuario. (Meléndez Valladarez, Gaitan, & Pérez Reyes, 2016)

Figura 34

Elementos Fases Metodología XP



Fuente: Tomado de (Vila Grau , 2016).

Como características generales se pueden mencionar que la metodología está basada en pruebas y error, con el fin de conseguir un software de calidad, asimismo, tal como se hizo mención, el rol del cliente es fundamental y debe estar disponible cada vez que el equipo de desarrollo lo requiera, de manera puntual se puede destacar que el rango exacto de miembros recomendado, se encuentra entre 2 a 12 integrantes, donde cada uno de ellos deberá contar con elevados conocimientos técnicos y de programación, por ultimo los cambios están bien vistos durante el proceso de desarrollo (Meléndez Valladarez, Gaitan, & Pérez Reyes, 2016).

Figura 35

Ventajas y Desventajas (Metodología XP)

Ventajas	Desventajas
• No se requiere de una gran inversión monetaria, dado a que admite un número reducido de integrantes y	• Debido a que se permite los cambios, no se puede determinar con exactitud los tiempos ni costos requeridos.

Ventajas	Desventajas
además teniendo en cuenta que se trabaja por parejas en cada ordenar. • Debido a la implementación de estándares establecidos la programación resulta ser un proceso muy organizado. • El trabajo en parejas permite una retroalimentación de conocimiento. • No se requiere de tiempos elevados de desarrollo. • Se permite realizar cambios más fácilmente.	• No es posible implementarlo en proyecto sumamente complejos ni extensos. • No se puede estimar claramente desde un inicio los requerimientos. • Debido a que está basado en la prueba y error, en caso de fallas puede alterar en gran medida el equilibrio de las variables del proyecto.

Nota: Dado a las ventajas y desventajas, se puede identificar que este tipo de metodología funcionaria muy bien en trabajos de baja complicidad y con una disponibilidad muy baja en recursos.

Fuente: Elaboración propia basada en (Vera Salavarría, 2018).

4.3.2.2. Espiral

El modelo en espiral en el desarrollo de un proyecto se caracteriza por ser un modelo de desarrollo iterativo e incremental, el objetivo al final de cada iteración es obtener una evolución del proyecto.

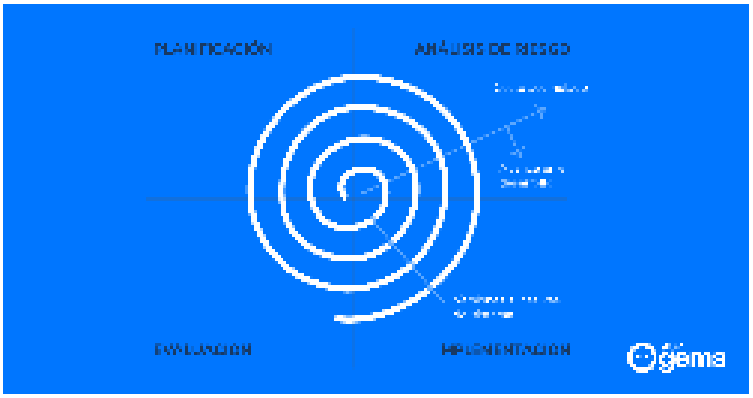
El modelo en espiral comienza determinando los objetivos del proyecto, luego de determinar los objetivos se rebe evaluar los riesgos, a continuación, se realiza la ejecución de lo planteado al inicio de la iteración y finalmente se realiza una evaluación general de la iteración, estos pasos se pueden ver más claramente a continuación:

- **Planeación:** Se toman decisiones luego de identificar los objetivos del proyecto o luego de finalizada una iteración; se realiza un estudio de viabilidad, teniendo en cuenta que los requisitos son alcanzables, y finalmente se realiza una planificación detallada de las actividades a desarrollar durante la iteración.

- **Análisis de riesgo:** Se realiza un análisis detallado de los posibles riesgos que se puedan presentar durante la fase de ejecución, luego se determina de qué manera prevenir estos errores.
- **Implementación:** En cortas palabras en esta fase se realiza la ejecución de lo acordado en la fase de planificación, con el objetivo de alcanzar la meta y el valor agregado que se espera obtener en esta fase.
- **Evaluación:** En la última fase de la iteración, el objetivo de esta fase es identificar los errores para posteriormente prevenirlos, además se evalúa si los objetos fueron alcanzados y se obtiene la satisfacción del cliente (Fariño R., 2011).

Figura 36

Ciclo de vida (Espiral)



Fuente: Tomado de (ASP Gems, 2019).

Figura 37

Ventajas / Desventajas (Metodología Espiral)

Ventajas	Desventajas
• No requiere una definición o identificación de todos los	• Puede ser difícil identificar los riesgos.

Ventajas	Desventajas
requerimientos del proyecto para iniciar. • Permite realizar cambios del proyecto con facilidad. • Es muy probable que luego de cada iteración se apruebe satisfactoriamente por el cliente.	• Se requiere la participación constante del cliente, lo que puede generar un incremento en los cambios de requerimientos. • Altas exigencias de cambios, lo que puede afectar la triple restricción o triple restricción ampliada.

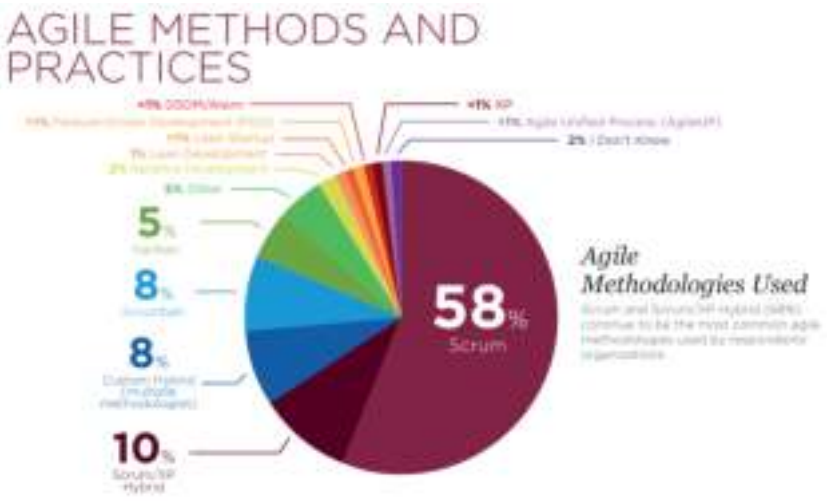
Fuente: Elaboración propia (Fariño R., 2011).

4.3.2.3. SCRUM

Generalmente es confundida como otra metodología respecto al desarrollo de proyectos de software, debido a que está clasificada como una más de las metodologías agiles, sin embargo, es considero más como un marco de trabajo, el cual, debido a su simplicidad al momento de su implementación, se ha establecido como uno de las "metodologías" más usada dentro de las empresas; lo anterior se puede verificar teniendo en cuenta un estudio realizado por Collabnet en el año 2016, donde demuestra que, en ese año, el 58% de las empresas que fueron objeto de su investigación, declararon implementar el método de trabajo dentro de sus proyectos.

Figura 38

Porcentaje de Uso Metodologías Agiles



Fuente: Tomado de (VersionOne inc., 2017).

El cual de manera similar a la metodología XP, tiene la capacidad de realizar cambios durante el proyecto, y su implementación está basado en iteraciones, los cuales, dentro del marco, son conocidos como Sprints.

Dentro de la Guía Sbok, (Una guía para el cuerpo de conocimiento de SCRUM) tercera edición menciona que el marco de trabajo.

> Es un framework adaptable, iterativo, rápido, flexible y eficaz, diseñado para ofrecer un valor considerable en forma rápida a lo largo del proyecto. Scrum garantiza transparencia en la comunicación y crea un ambiente de responsabilidad colectiva y de progreso continuo (Scrumstudy targeting success, 2016).

Lo explicado por la guía, justifica por qué Scrum se ha convertido en la metodología más usada por las organizaciones.

Scrum está compuesta por tres roles:

- **Scrum Master:** Dentro del equipo scrum será el encargado de dar transparencia y claridad a los demás integrantes del equipo scrum, respecto al marco scrum como tal, por medio de sus artefactos, eventos, time box, etc. Además, motiva los cambios con el objetivo de que el equipo de desarrollo cree productos de alto valor, para esto se asegura de guiar al equipo a ser autoorganizado y funcional, teniendo en cuenta los impedimentos que el Development Team pueda tener y eliminarlos, esa es una de las características principales de scrum master estar en frente del equipo liderando el proyecto y que el marco scrum sea usado de forma correcta. Debe asegurarse de que el equipo trabaje ajustándose a la Teoría, Practica y Reglas, todo dentro de un entrono empírico. Del mismo modo también estará encargado de que los eventos que se encuentren dentro del sprint se realicen y con los tiempos indicados dentro del marco.

- **Producto Owner:** Es el que realice el primer contacto con el cliente, y tomara nota de los requerimientos del proyecto, para crear las historias de usuarios, para luego almacenarlos dentro del Product Backlog, ya en el Sprint Planning, él es el que decide como ordenar el Product Owner como él lo considere mejor, y a la vez aclararlo ante todo el scrum master para dar claridad y trasparencia.

  Entre los diferentes roles, el Product Owner es el que debe saber más sobre el objetivo de negocio y sobre la lista de producto y asegurarse de que haya sido entendida por el Development Team.

  Durante los diferentes Sprint que tenga el proyecto, será el único rol autorizado para cancelar o no el sprint, esto lo podrá determinar con la colaboración del equipo de desarrollo.

- **Development Team:** Tal como su nombre lo indica este rol está compuesto por el equipo de desarrolladores presentes en el proyecto, este deberá ser auto organizado, y tendrá el poder de proporcionar las estimaciones del Backlog, de esta manera predecir la lista de pendientes e identificar que funcionalidad ira en el siguiente sprint; igualmente son los encargados de dirigir el Daily Scrum o Daily Stand Up, y nadie más puede intervenir durante este tiempo, y durante este evento, se debe analizar principalmente los impedimentos que estos pudieron tener durante su trabajo de desarrollo con el objetivo de cumplir el Sprint Goal. Estos deberán estar conformado por mínimo 3 y máximo 9 desarrolladores, para poder realizar sprint un poco más largos y que el equipo no resulte difícil de manejar.

Durante el uso de la metodología scrum, se debe llevar un control de proceso que permita conocer el trabajo que se está realizando y que se está cumpliendo con lo estipulado al inicio del

proceso, para esto la transparencia es fundamental, y los eventos que conforman el marco Scrum nos permiten lograr esta transparencia:

- Daily Scrum o Daily Stand Up,
- Sprint Planning Meeting,
- Sprint Review,
- Sprint Retrospective.

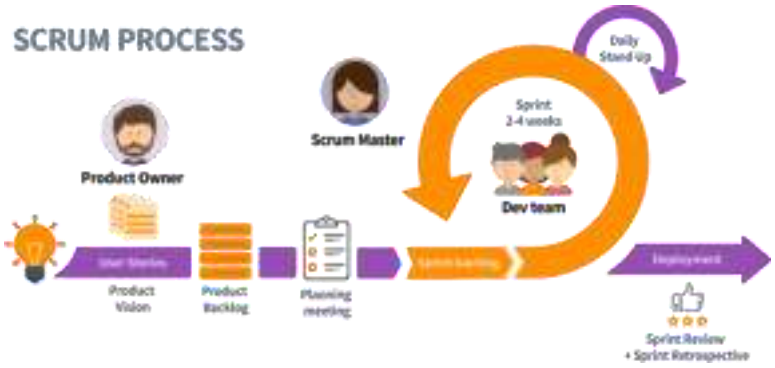
Además, el tener presente los artefactos (son explicados con detalle más adelante) y el objetivo de estos, contribuye a que el concepto de terminado sea igual para todo el equipo scrum. Algunos elementos que facilitan optimizar la transparencia dentro del marco son:

- Burndown Chart,
- Product Backlog,
- Spring Backlog,
- Product Increment,
- Scrumboard.

El proceso de scrum su puede describir en 7 pasos los cuales son:

Figura 39

Proceso SCRUM



Fuente: Tomado de (ENALEAN S.A.S.).

1. El Primer contacto con el cliente lo debe realizar el Product Owner, con la idea de crear la lista de requerimientos o historias de usuario, aquí es donde nace el Product Backlog, que al desarrollar cada una de estas tareas obtendremos el producto final de alto valor. El orden de prioridad del Product Backlog debe realizarlo el Product Owner.
2. El siguiente paso será el primer evento del modelo, llamado Sprint Planning Meeting, para la creación de la supercomputadora será de 4 horas cada reunión, debido a los sprint de 2 semanas, aquí el Product Owner ya con el Product Backlog de forma clara y priorizada, el equipo scrum (Scrum Master, Product Owner, Development Team), debe seleccionar o elegir cuales de estas historias de usuario podrán ser desarrolladas y entregadas al final del sprint, la lista que fue seleccionada se llamara Spirnt Backlog.
3. Con el sprint backlog definido se realiza el proceso de Tasking, aquí se identificará las tareas que se van a realizar, el tiempo estimado y generalmente se plasman en un Taskboard (tablero de tareas).
4. Diariamente durante el time box del sprint, se debe realizara los Daily Scrum, con el objetivo de que el equipo scrum puede tener una retrospectiva y control del trabajo realizado y por hacer, estos serán de 15 minutos y serán dirigidos por el equipo de desarrollo.
5. Ya al final del sprint, se realiza el Sprint Review que será de 2 horas, para el sprint de 2 semanas, el objetivo es evaluar el producto "terminado" o incremento del proyecto que fue estimado durante el Sprint Planning al inicio del sprint, eso si el Product Owner decide no cancelar el sprint anteriormente. Los invitados o asistentes a esta

reunión son el Scrum master y los invitados autorizados por el Product Owner generalmente es el cliente como tal, junto con los demás integrantes del equipo scrum.

6. Antes de finalizar el Sprint se realiza el Sprint Retrospective, y todo el equipo scrum debe estar presente, el objetivo de la reunión es analizar lo ocurrido durante el sprint terminado, teniendo en cuenta procesos, herramientas y el incremento realizado, de esta manera determinar posibles mejoras a tener en cuenta en el próximo Sprint, consiguiendo un mejor rendimiento.

Una forma que podemos usar para tener una guía al momento de determinar los procesos realizados durante el sprint, es responder las siguientes preguntas:

- ¿Que estuvo bien durante el Sprint?
- ¿Qué se pudo mejorar durante este Sprint?

7. Finalmente, para cerrar el sprint se realiza el ultimo evento que es el refinamiento, que es una Reevaluación del Product Backlog, dependiendo de lo ocurrido durante el Sprint que finaliza.

Principalmente scrum es utilizado para proyectos complejos, donde debido al protocolo establecido dentro del marco, pueden contribuir a obtener el proyecto de forma exitosa, sin afectar la gran medida la triple restricción (Tiempo, costo y calidad), debido a la facilidad que tiene para adaptarse al cambio. Sus tiempos en los eventos ya concretos o Timebox facilitan el control de los procesos e identificación de posibles impedimentos que tenga el equipo, durante cada Sprint.

Se debe tener en cuenta que el "líder" es el scrum master, quien debe elaborar la metodología que se usara y al finalizar explicarlo al equipo, con el objetivo de crear transparencia (punto

fundamental dentro del marco scrum), el trabajo empírico debe ser promovido por el scrum master.

El objetivo del uso de los sprint, es que el controlar las tareas a desarrollar y examinar que mejoras se pueden realizar y que no se puede volver a hacer. De esta manera se retroalimenta el equipo, creando una mejor adaptación a las futuras tareas a crear en los siguientes sprint. Al igual se debe tener en cuenta que las historias de usuarios dadas desde la primera reunión o contacto (dueño del producto y cliente) generalmente cambian con el paso del tiempo y de las entregas del incremento, por esta razón el uso de las iteraciones proporciona la manera de modificar estas historias de usuario al final de cada sprint junto después de un incremento "terminado" y aprobado.

Al igual que el scrum master el Product Owner, debe exponer la información que maneja de manera clara y asegurarse que fue entendida, principalmente información que se maneje del Product Backlog.

Algunos de los beneficios que podemos encontrar con el uso de scrum son:

- Flexibilidad al cambio,
- Mayor productividad,
- Predicciones de tiempo,
- Reducción de riesgo en la triple restricción,
- Mayor claridad de software.

Tabla 40

Ventajas / Desventajas (SCRUM)

Ventajas	Desventajas
• Adaptabilidad dado al uso de iteraciones, donde al inicio de cada una, se evaluará los avances y posibles cambios que se deseen realizar. • Transparencia debido a las herramientas que se implementaran. • Retroalimentación y mejora continua, debido al análisis que se realiza al final de cada Sprint. • Valor agregado al final de cada sprint. • Ritmo continuo de trabajo de los diferentes roles. • Permite resolver los problemas que aparezcan de manera rápida. • Fácil escalabilidad.	• En compañías con un numero alto de personal, se deberá generar varios grupos que cumplan con los límites establecidos por cada rol. • Puede resultar tedioso implementar todas las herramientas y eventos. • Preferiblemente se requiere de personal con avanzada experiencia en proyectos.

Nota: Se permite identificar que gracias a sus diversas herramientas se generan grandes ventajas para proyectos complejos.

Fuente: Elaboración propia basada en (Scrumstudy targeting success, 2016).

Capítulo V

Conclusiones y Recomendaciones

El memorizar las contraseñas, siempre ha sido una dificultad muy grande entre los ciber usuarios; tanto así, que se implementan frecuentemente contraseñas de baja seguridad, a pesar, de que es conocido entre los mismos sobre la importancia de crear claves con una estructura segura; por esta razón se deseó determinar la viabilidad de un aplicativo móvil.

Se evaluaron diferentes aspectos con respecto a la seguridad, enfocadas a la protección de la información, desde la autentificación de usuarios hasta de un acceso remoto a cuentas de usuario a través de un dispositivo móvil; cabe mencionar, que el almacenar toda esta información dentro del mismo "lugar" tiene sus ventajas y desventajas, dado que recopilar estos datos puede facilitar de gran manera la disponibilidad y además fortalecer la estructura de seguridad de las contraseñas; no obstante, en caso de robo, se posibilita que dicha data se encuentre a la mano de los crackers, tal como se identificó con el hurto sufrido por la herramienta LastPass, donde varias de las contraseñas fueron sustraídas de sus servidores, cuyo método de seguridad que impidió la legibilidad de los datos está en base a que se encontraban cifrados; de esta manera, cuando la falla fue detectada, se les recomendó a los usuarios de este aplicativo modificar su contraseña maestra; cabe recordar que, las cuentas de usuarios más expuestas fueron las que poseían claves maestras poco seguras. De esta manera se estableció la importancia que los datos no estén legibles, del mismo modo es fundamental reducir en lo más posible el acceso a través de una contraseña maestra, a menos que esta sea segura; por esta razón y teniendo en cuenta las apps que administran fuentes delicadas, se determinó que muchas de estas herramientas utilizan como "clave" de acceso la huella digital del usuario, es importante destacar que este registro se encuentra almacenado localmente favoreciendo así en caso de un ciberataque, que el

ciberdelincuente deba tener el dispositivo del usuario en su mano junto con la información sustraída; sin embargo para quienes no cuentes con dispositivos que tenga sensores de huellas, es necesario el uso de un password único, tal como se evidencia en los neobancos (Daviplata, BlockChain y Nequi). Por ende, para la protección de datos respecto al cifrado de datos, se logró determinar que el algoritmo más seguro en la actualidad es el AES, el cual presenta un elevado nivel de protección y además, periodos muy cortos de procesamiento; no obstante, al determinar los bajos volúmenes de almacenamiento que usara el aplicativo, ya sea en la nube o nivel local, podría igualmente implementar el algoritmo RSA, quien dado a su número elevado respecto a su clave de cifrado puede establecerse como un método seguro para proteger la información; sin embargo, este mismo hecho puede provocar un mayor ocupación dentro de los servidores, donde teniendo en cuenta los limites gratuitos dados por Google respecto al almacenamiento, se podría alcanzar de una manera mucho más rápida, en comparación al AES, el cual tiene bajos y diferentes tamaños en sus claves de cifrado; no obstante, se puede evaluar la implementación de los dos algoritmos dentro de la misma aplicación, dependiendo de los servicios o datos que más se desee proteger y a los que más rápido se desee acceder.

Favoreciendo la integridad, disponibilidad y confidencialidad, para el inicio de sesión y registro se implementaría la autentificación en dos pasos (2FA), a través de correo electrónico o mensaje de texto; inicialmente, la viabilidad dependerá del límite gratuito que ofrece la plataforma.

Respecto al acceso, se determinó que no es necesario adecuar, de manera separada dos métodos de almacenamiento, los cuales inicialmente fueron SQLite para el depósito local y un web-service para la copia de seguridad en la nube en donde sería usada como copia de seguridad en caso de pérdida o robo del dispositivo. De hecho, dentro de la misma plataforma Firebase

existe igualmente una única herramienta que permite realizar los procesos mencionados, reduciendo de esta manera procesos de interconectividad entre varias herramientas; del mismo modo, la ventaja que proporciona la mencionada respecto a las actualizaciones automáticas al momento de detectar un cambio de información desde el Smartphone o la nube; el cual, se realizará cuando se efectúe una conexión a internet; así, se conseguirá la disponibilidad de los datos y al mismo tiempo un Back-up, tal como lo establece la seguridad informática y las diversas normas creadas para la protección de los SGSI.

Luego de identificar la vulnerabilidad que conlleva el auto relleno de los formularios de inicio de sesión vistos en el navegador Google Chrome, como ventaja competitiva se creó una hipótesis en cuanto a la estrategia de acceso directo a través del Smartphone favoreciendo la confidencialidad eh integridad.

El proceso se realizará a través de una extensión de los navegadores, el cuál será usado como intermediario para realizar el proceso de verificación con el dispositivo; es importante mencionar que este proceso igualmente contaría con el método de autentificación en dos pasos.

Igualmente es importante destacar que es poco productivo el desarrollar una aplicación que gestione contraseñas y que permita a los usuarios dejar en segundo plano el memorizarlas y realizar accesos directos mientras que estos datos sigan encontrándose bajo una estructura poco segura (111111, 123456, fechas de cumpleaños, etc.).

Por esta razón y facilitando a los usuarios el proceso de crear las contraseñas con todas las características que debe contener una contraseña, se desea crear un generados de contraseñas, el cual será usado cuando el usuario desee crear una cuenta de usuario, o igualmente cuando este desee cambiar su contraseña.

En muchos casos no se podrá realizar una conexión (Celular - Extensión), que permita realizar los inicios de sesión desde el dispositivo debido a la necesidad de implementar la extensión en un navegador web, sin embargo, los usuarios en algún momento deberán realizar el acceso a una cuenta en algunos de estos navegadores, dado a lo anterior y para evitar el proceso de instalación de la extensión y la posterior autentificación con el mismo, el usuario podrá visualizar la contraseña en el aplicativo, para que él mismo pueda digitarla en el navegar; el hecho de que el usuario deba ingresar la contraseña puede también convertirse en proceso bastante complicado teniendo en cuenta la estructura que pueda tener una contraseña segura, mostrada anteriormente, por esta razón y sin reducir dramáticamente la seguridad, el aplicativo deberá generar contraseñas con las siguientes características:

- Uso de Mayúsculas,
- Minúsculas,
- Números,
- Aleatoria,
- Extensión ajustable según lo desee el usuario, pero no menor a 10 caracteres.

Una contraseña que puede generarse en base a las características mencionada tendría un aspecto muy similar al siguiente **tyju3j74THNE**, la cual está compuesta por una longitud de 12 caracteres, o en este caso **Zb4Zz4eeSHSmKw5Qm2mm** con una longitud de 20; cómo se puede identificar son contraseñas igualmente seguras pero que pueden ser digitadas con facilidad por usuario, cabe recordar que el proceso de digitación, solo sería usado en momentos en que la extensión del aplicativo no esté instalado en el navegador que se esté usando.

La selección del lenguaje de programación es un punto fundamental dentro de la selección de las historias de usuarios, principalmente al momento de la clasificación de los

requerimientos no funcionales, teniendo como base el hecho de que se ha seleccionado a Android Studio como la herramienta de desarrollo, el cual, da la posibilidad a los desarrolladores en crear aplicaciones por medio de dos lenguajes (Java, Kotlin), se debe evaluar cual se puede considerar como el mejor lenguaje para el desarrollo; cabe destacar que, a pasar de que no sea un lenguaje como tal, sino mas bien un Framework, Flutter se a convertido en una herramienta muy usada en la actualidad para la creación de aplicación en Android, dado a que permite realizar interfaces graficas complejas y llamativas de una manera más rápida, a comparación de los que se puede realizar en Android Studio por medio de los archivos .XML; no obstante, este Framework utiliza el lenguaje de programación Dart, muy poco conocido pero con una curva de aprendizaje muy bajo.

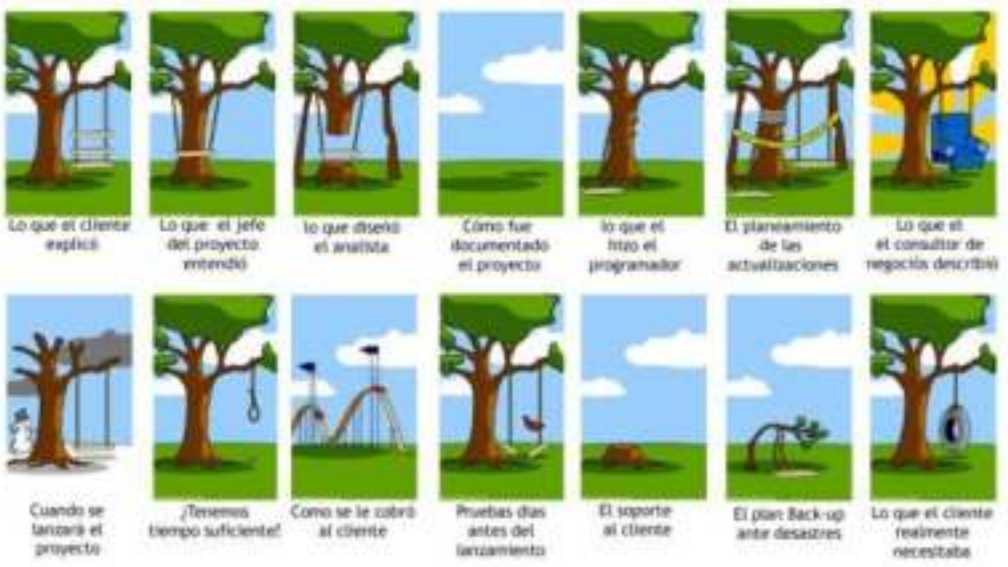
Dentro de la investigación se estableció como posibles usuarios del aplicativo a dos tipos de ellos (Basic, Premium), donde a los usuarios premium contarían con los servicios completos ofrecidos por el aplicativo en comparación con los Basic, los cuales solo tendrán un número limitado de funciones, el objetivo de lo anterior es debido a los costos que se generar respecto a los servicios de Google luego de superados los limites gratuitos, por ende, para ofrecer un servicio masivo a usuarios, se deberá analizar un método de mercadeo el cual permita identificar un posible costo que podría tener el aplicativo para los usuarios premium, de esta manera costear los costos que se podrán generar. Sin embargo y como se menciono es fundamental lanzar el aplicativo en un publico reducido, para evitar inicialmente superar los límites gratuitos.

A pesar de que se realizó una clasificación general de los requerimientos por grupos, es importante realizar un proceso mas profundo respecto a los mismos en base a los resultados obtenidos, específicamente la clasificación de requerimientos funcionales y no funcionales, en otras palabras los requerimientos específicos en base igualmente a las normas IEEE 830 (ERS),

los cuales para la recolección de estos tal como se recomienda, deberá realizarse por medio de lenguaje poco técnico y muy específico, de este modo evitar conceptos diferentes de cada uno de los requerimientos. La importancia de los anterior lo podemos visualizar por medio de la siguiente figura muy conocida dentro de la ingeniería de software.

Figura 40

Recolección de Requerimientos



Fuente: tomado de (CEMEBlog, 2012).

Nota: Ilustración muy utilizada para identificar la importancia de una toma de requerimientos clara, y donde se puede identificar el porque se debe realizar por medio de un lenguaje poco técnico, dado a que cada persona puede determinar de manera diferente una idea explicada de manera muy poco descriptiva.

Finalmente, así como es importante determinar que lenguaje de programación sería el más adecuado, la selección de una metodología lo es igualmente, por ende, identificar la más acorde, donde la selección de alguna de ellas, dependerá en gran medida del proceso que se llevara a cabo, estimación del tiempo, personal, controles, recursos, entre otros.

Bibliografía

A., D. (28 de Octubre de 2020). *Hostinger Tutoriales*. Obtenido de Hostinger: https://www.hostinger.co/tutoriales/que-es-json/

Alonso Serrano, A., García Sanz, L., Irene, L., García Gordo, E., Gil Álvaro, B., & Ríos Brea, L. (s.f.). *Universidad Nacional de Educación Enrique Guzmán y Valle.* Recuperado el 11 de Octubre de 2020, de http://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/10.pdf

AMBIT TEAM. (1 de Julio de 2019). *Ambit building solutions together.* Recuperado el 28 de Octubre de 2020, de https://www.ambit-bst.com/blog/sabes-que-es-la-autenticacion-de-dos-factores-o-2fa-y-cuales-son-sus-ventajas

ASP Gems. (5 de Abril de 2019). *ASP Gems.* Recuperado el 19 de Noviembre de 2020, de https://aspgems.com/metodologia-de-desarrollo-de-software-iii-modelo-en-espiral/

Baca Urbina, G. (2016). Vulnerabilidades y amenazas: causas y tipos. En *Introducción a la seguridad informática* (pág. 30). Mexico: Grupo Editorial Patria.

Baca Urbina, G. (2016). Definición y tipos de seguridad informática. En *Introducción a la seguridad informática* (pág. 12). México: Grupo editorial Patria.

BACSIRT Vamos Buenos Aires, Centro de Seguridad. (2018). En *Ataques Cibernéticos* (págs. 1-2). Buenos Aires.

Banco Davivienda Colombia. (30 de Julio de 2020). *YouTube.* Recuperado el 26 de Octubre de 2020, de https://www.youtube.com/watch?v=g-JRRzGF8ow&ab_channel=BancoDaviviendaColombia

Banco Davivienda S.A. (2 de Septiembre de 2020). Daviplata.

Bauzá Martorell, F. J. (2019). Notificación de una violación de la seguridad de los datos personales a la autoridad de control. En *El modelo europeo de protección de datos. Experiencias para la regulación chilena* (pág. 132). Islas Baleares.

Bauzá Martorell, F. J. (2019). Seguridad de los datos personales y autoridad de control. En *El modelo europeo de protección de datos. Experiencias para la regulación chilena* (pág. 131). Islas Baleares: http://arsboni.ubo.cl/index.php/arsbonietaequi/article/viewFile/353/326.

BBC Mundo, Tecnología. (27 de Abril de 2011). *BBC News.* Recuperado el 02 de Septiembre de 2020, de https://www.bbc.com/mundo/noticias/2011/04/110426_sony_playstaton_robo_datos_tarjetas_credito_jrg

Bex Technology. (s.f.). *BSR Bext-SelfReset.* Recuperado el 23 de 09 de 2020, de https://www.bextsa.com/autogestion-de-contrasena-con-bextselfreset

Bracamontes Perez, P., Chapan Seba, R., Crispin Bapo, L. I., & Ronquillo Jimenez, B. (29 de Septiembre de 2016). *Slideshare.* Recuperado el 21 de Octubre de 2020, de https://es.slideshare.net/LIvanCBapo/instrumentos-de-investigacin-documental

C. Martínez, D. (24 de Junio de 2020). *YouTube*. (Curso de Aplicaciones Web) Recuperado el 23 de Noviembre de 2020, de https://www.youtube.com/watch?v=LiudFkofPfw&ab_channel=CursodeAplicacionesWeb

Cajal, A. (2020). *lifeder.* Recuperado el 13 de Octubre de 2020, de https://www.lifeder.com/investigacion-de-campo/

Camargo Cardona, L. (2019). Seguridad informática y su definición. En *Regulación en Colombia de los Delitos Informaticos* (pág. 3). Colombia.

Camargo Cardona, L. (2019). SEGURIDAD INFORMÁTICA Y SU DEFINICIÓN. En *REGULACIÓN EN COLOMBIA DE LOS DELITOS INFORMATICOS* (pág. 03). Bogotá.

Camargo Cardona, L. (2019). Seguridad informática y su definición. En *Regulación en Colombia de los detilos informaticos.* (págs. 2-3). Colombia.

CEMEBlog. (1 de Mayo de 2012). *CEMEBlog*. Obtenido de CEMEBlog Apuntes sobre las TIC y las TAC: https://blog.cemebe.info/project-cartoon/

CNNMoney. (16 de Junio de 2015). *CNN*. Recuperado el 8 de Octubre de 2020, de https://cnnespanol.cnn.com/2015/06/16/hackean-empresa-de-contrasenas-de-seguridad/#:~:text=Este%20lunes%2C%20LastPass%20anunci%C3%B3%20que,contrase%C3%B1as%20maestras%20de%20la%20gente.&text=LastPass%20dijo%20que%20descubri%C3%B3%20el%20robo%20digital%20e

Coneo Rincón, M. (20 de Junio de 2020). *La República.* Recuperado el 02 de 09 de 2020, de https://www.larepublica.co/internet-economy/un-latinoamericano-tiene-en-promedio-nueve-cuentas-en-diferentes-redes-sociales-3020869

Constitución Política de Colombia. (2016). Articulo 15. En *Constitución Política de Colombia.* Bogotá.

Corporación Mozilla. (23 de Marzo de 2019). *MDN web docs*. Obtenido de Developer Mozilla : https://developer.mozilla.org/es/docs/Extensions

Corporación Mozilla. (25 de Agosto de 2020). *Developer Mozilla*. Obtenido de MDN web docs: https://developer.mozilla.org/es/docs/Web/API/HTMLInputElement

CRAI. (s.f.). *Centro de recursos para el aprendizaje y la investigación*. (Creative Commons) Recuperado el 10 de Octubre de 2020, de http://www.duoc.cl/biblioteca/crai/fases-de-la-investigacion-aplicada

Custódio, M. (07 de Diciembre de 2017). *RD Station.* Recuperado el 13 de 10 de 2020, de https://www.rdstation.com/es/blog/mapa-de-empatia/

DANE . (2018). *DANE Información para todos.* Recuperado el 28 de Octubre de 2020, de https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivenda-2018/cuantos-somos

Dufetel, A. (3 de Octubre de 2017). *Firebase.* Recuperado el 1 de Noviembre de 2020, de https://firebase.googleblog.com/2017/10/introducing-cloud-firestore.html

El congreso de la República. (31 de Diciembre de 2008). *Alcaldia de Bogotá.* Recuperado el 15 de Octubre de 2020, de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

ENALEAN S.A.S. (s.f.). *Tuleap.* Recuperado el 25 de Noviembre de 2020, de https://www.tuleap.org/agile-scrum-in-10-minutes/

Escuela de Soboficiales Armada Argentina. (2018). *Escuela de Soboficiales Armada Argentina.* Recuperado el 20 de Octubre de 2020, de http://www.essa.ara.mil.ar/cens/MATERIAS%20SEGUNDO%20A%C3%91O/2%C2%B0%20A%C3%91O/08-METODOLOGIA%20DE%20LA%20INVESTIGACION/SEGUNDO%20CUATRIMESTRE/Segundo%20cuatrimestre.pdf

Espitia , N., Armao, O., & Carbajo, J. (Febrero de 2016). *UAH Engineer´s today.* Recuperado el 21 de Noviembre de 2020, de https://espejodeantagno.files.wordpress.com/2016/04/modelo-vista-controlador-mvc.pdf

Farfán, O. y Pérez, K. (2020). Metodologías innovadoras para el diseño de nuevos proyectos de Emprendimiento de Base Tecnológica (EBT). *Mare Ingenii, 2*(1), 27-46. https://doi.org/10.52948/mare.v2i1.196

Fariño R., G. (2011). *Modelo Espiral de un proyecto de software.* Recuperado el 19 de 11 de 2020, de http://www.ojovisual.net/galofarino/modeloespiral.pdf

Ferreño, E. (28 de Julio de 2019). *El androide libre.* Recuperado el 27 de Octubre de 2020, de https://elandroidelibre.elespanol.com/2019/07/pin-o-sensor-de-huellas-ventajas-e-inconvenientes-de-estos-sistemas-de-bloqueo.html

Flores Martín, C. (Junio de 2017). *Core.* Recuperado el 22 de Octubre de 2020, de https://core.ac.uk/download/pdf/288500151.pdf

Framingham, Mass;. (14 de Febrero de 2019). *International Data Corporation* . Recuperado el 02 de Septiembre de 2020, de https://www.idc.com/getdoc.jsp?containerId=prUS44864619

Fuquen Barrera, L. M., & García Hurtado, H. A. (2015). *Universidad Libre.* Recuperado el 31 de Octubre de 2020, de https://repository.unilibre.edu.co/bitstream/handle/10901/8920/Proyecto%20de%20Grado.pdf?sequence=1&isAllowed=y

Gabriel, B. (2016). *Introducción a la seguridad.* Mexico: Grupo Editorial Patria.

Galeano, S. (31 de Enero de 2020). *marketing4ecommerce.* Recuperado el 02 de Septiembre de 2020, de https://marketing4ecommerce.net/usuarios-internet-mundo/

Gascón Busio, O. J. (s.f.). *TodoPMP*. Recuperado el 19 de 11 de 2020, de https://todopmp.com/la-famosa-triple-restriccion/

Google LCC. (3 de Diciembre de 2019). *Firebase*. Recuperado el 1 de Noviembre de 2020, de https://firebase.google.com/docs/firestore/quotas

Google LCC. (28 de Mayo de 2020). Android Studio.

Google LCC. (30 de Septiembre de 2020). *Developers Android*. Recuperado el 30 de Octubre de 2020, de https://developer.android.com/reference/android/database/sqlite/package-summary?hl=es-419

Google LCC. (23 de Junio de 2020). *Developers Android*. Recuperado el 15 de 11 de 2020, de https://developer.android.com/guide/components/activities/activity-lifecycle?hl=es

Google LCC. (08 de Agosto de 2020). *Firabase*. Recuperado el 25 de Octubre de 2020, de https://firebase.google.com/docs/auth/images/auth-providers.png?hl=es

Google LCC. (29 de Octubre de 2020). *Firebase*. Recuperado el 5 de Noviembre de 2020, de https://firebase.google.com/docs/auth/limits?hl=es-419

Google LCC. (s.f.). *Firebase*. Recuperado el 25 de Octubre de 2020, de https://firebase.google.com/

Google LCC. (s.f.). *Firebase*. Recuperado el 25 de Octubre de 2020, de https://console.firebase.google.com/u/2/project/fir-demo-project/authentication/providers

Google LCC. (s.f.). *Firebase*. Recuperado el 5 de Noviembre de 2020, de https://firebase.google.com/pricing?hl=es-419

Google LCC. (17 de Noviembre de 2020). Google Chrome.

Google LCC. (s.f.). *Firebase*. Obtenido de Firebase : https://firebase.google.com/products/auth?hl=es-419

Google LLC. (3 de Diciembre de 2019). *Firebase.* Recuperado el 1 de Noviembre de 2020, de https://firebase.google.com/docs/firestore/rtdb-vs-firestore

Google LLC. (14 de Octubre de 2020). *Firebase*. Recuperado el 23 de Octubre de 2020, de https://firebase.google.com/docs/auth/android/firebaseui?hl=es

Gutiérrez Pinzón, J. C. (2016). *Universidad de La Sabana.* Recuperado el 18 de 10 de 2020, de https://intellectum.unisabana.edu.co/bitstream/handle/10818/26176/Juan%20Camilo%20Guti%c3%a9rrez%20Pinz%c3%b3n%20%28Tesis%29.pdf?sequence=1&isAllowed=y

Gutiérrez, D., & Cueto Felgueroso, R. (Septiembre de 2020). *Velneo*. Obtenido de Documentación de Velneo: https://doc.velneo.com/velneo-vdevelop/scripts/lenguajes/javascript/clases/xmlhttprequest

Guzman Lopez, B. (2 de Julio de 2018). *Archivo Digital Universidad Politécnica de Madrid.* Recuperado el 23 de Noviembre de 2020, de http://oa.upm.es/54237/1/TESIS_MASTER_BORJA_GUZMAN_LOPEZ.pdf

Hazelton, P. (1 de Marzo de 2018). *Practical Ecommerce.* Recuperado el 16 de 11 de 2020, de https://www.practicalecommerce.com/mobile-site-pass-thumb-zone-test

Huertas, A. (7 de Febrero de 2019). Recuperado el 20 de 11 de 2020, de http://angelhuertasdam.blogspot.com/2019/02/sistemas-operativos-en-red.html

Imperva. (s.f.). *Imperva.* Recuperado el 19 de 10 de 2020, de https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/

Indexa Capital. (s.f.). *Clave Segura*. Recuperado el 19 de 10 de 2020, de https://www.clavesegura.org/es/

Institute of Electrical and Electronics Engineers. (1998). Especificaciónes De Los Requisítos Del Software.

Intel. (s.f.). *Intel Latinoamerica.* Recuperado el 12 de 11 de 2020, de https://www.intel.la/content/www/xl/es/support/articles/000006179/education/intel-education-software.html

International Organization for Standardization. (2013). *ISO Tools EXCELLENCE*. Recuperado el 25 de Septiembre de 2020, de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

ISO. (23 de Marzo de 2017). *ISOTools Excellence*. Recuperado el 8 de Octubre de 2020, de https://www.isotools.org/2017/03/23/iso-27018-la-primera-normativa-la-privacidad-la-nube/

ISO International Organization for Standardization. (16 de Marzo de 2017). *ISO 27017: Controles de seguridad para servicios en la nube.* Recuperado el 18 de Septiembre de 2020, de https://www.isotools.org/2017/03/16/iso-27017-controles-seguridad-servicios-la-nube/

ISOTools Ex. (11 de Junio de 2019). *ISO Tools Excellence.* Recuperado el 26 de Septiembre de 2020, de https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

Jiménez, R., & Mayorga, F. (s.f.). *bitstream*. Recuperado el 21 de Noviembre de 2020, de http://192.188.46.193/bitstream/123456789/37301/1/JIMENEZ%20RUIZ%20EDWIN%20RUBEN%20-2017.pdf

Loganathan, G. (2018). *Java Helps.* Recuperado el 30 de Octubre de 2020, de https://www.javahelps.com/2018/12/access-mysql-from-android-through.html

LogMein. (2020). *lastpass*. (LogMeIn, Inc) Recuperado el 23 de 09 de 2020, de https://blog.lastpass.com/

LogMein. (s.f.). *LastPass La mejor forma de gestionar contraseñas.* (LogMein, Inc) Recuperado el 23 de 09 de 2020, de https://www.lastpass.com/es/how-lastpass-works

LogMein. (s.f.). *LastPass Otras formas de conseguir LastPass.* (LogMeIn, Inc) Recuperado el 23 de 09 de 2020, de https://lastpass.com/misc_download2.php

Loor Vargas, C. A. (Marzo de 2015). *Universidad Politécnica Salesiana Ecuador.* Recuperado el 23 de Noviembre de 2020, de https://dspace.ups.edu.ec/bitstream/123456789/10327/1/UPS-GT001236.pdf

Mac Millan Education. (s.f.). *macmillaneducation.* Recuperado el 7 de 11 de 2020, de https://www.macmillaneducation.es/wp-content/uploads/2018/10/seguridad_informatica_libroalumno_unidad4muestra.pdf

Medina Varga, Y. T., & Miranda Mnedez, H. A. (Junio de 2015). *Mundo Fesc.* Obtenido de Mundo Fesc Web site: https://www.fesc.edu.co/Revistas/OJS/index.php/mundofesc/article/view/55/97

Meléndez Valladarez, S. M., Gaitan, M. E., & Pérez Reyes, N. N. (28 de Enero de 2016). *Universidad Nacional Autónoma de Nicaragua Managua.* Recuperado el 22 de Noviembre de 2020, de https://repositorio.unan.edu.ni/1365/1/62161.pdf

MINEDUCACIÓN . (2018). *MANUAL – SEGURIDAD INFORMÁTICA (Código: ST-MA-02).*

MINEDUCACIÓN. (2018). Vulnerabilidades. En *MANUAL – SEGURIDAD INFORMÁTICA* (págs. 29-30). Colombia.

Mora, A. (28 de Enero de 2020). *PCWorld.* Obtenido de PCWorld: https://www.pcworld.es/mejores-productos/internet/mejores-navegadores-web-3672988/

Munoz, J. M. (21 de Septiembre de 2016). *headsem*. Recuperado el 24 de 09 de 2020, de https://www.headsem.com/bsr-una-solucion-para-recuperar-contrasenas-y-reducir-costos-operativos/

Muñoz Cerón, P. F. (2000). *Sistema de facturación e inventarios.* Quito.

Murillo, J. (s.f.). *Universidad Nacional de Educación Enrique Guzmán y Valle.* Recuperado el 11 de Octubre de 2020, de http://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/10.pdf

Nequi. (13 de Abril de 2020). *YouTube*. Recuperado el 23 de Octubre de 2020, de https://www.youtube.com/watch?v=wZ7mPwDkGhc&ab_channel=Nequi

NQA. (s.f.). *NQA GLOBAL CERTIFICATION BODY.* Recuperado el 28 de Septiembre de 2020, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20PDFs/NQA-ISO-27701-Mini-Implementation-Guide-ES.pdf

Núñez, A. (03 de Septiembre de 2019). *Internet live stats.* Recuperado el 03 de Septiembre de 2020, de https://www.internetlivestats.com/total-number-of-websites/

Panda Media Center. (23 de Febrero de 2016). *Panda Security.* Recuperado el 19 de Octubre de 2020, de https://www.pandasecurity.com/spain/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/

Pastorini, A. (s.f.). *Universidad de la República* . Recuperado el 30 de Octubre de 2020, de https://www.fing.edu.uy/tecnoinf/mvd/cursos/ria/material/teorico/ria-06-ServiciosWeb.pdf

Portafolio. (28 de Enero de 2020). *Portafolio.* Recuperado el 28 de Octubre de 2020, de https://www.portafolio.co/economia/seis-de-cada-10-colombianos-tienen-acceso-a-internet-movil-537543

PORTAFOLIO. (07 de Octubre de 2020). *PORTAFOLIO*. Recuperado el 2020 de Octubre de 2020, de https://www.portafolio.co/economia/este-miercoles-se-aplica-la-primera-vacuna-experimental-de-covid-en-colombia-545411

QuestionPro. (s.f.). *QuestionPro*. Recuperado el 11 de 10 de 2020, de https://www.questionpro.com/blog/es/investigacion-documental/

REPÚBLICA DE COLOMBIA - GOBIERNO NACIONAL. (2009). LEY N° 1273. Bogotá D.C.

Restrepo García, L. M. (s.f.). *Universidad de Antioquia*. Recuperado el 11 de 10 de 2020, de http://aprendeenlinea.udea.edu.co/lms/moodle/file.php/658/Glosario_Invest_Documental_final_-_Lina_Rpo.pdf

Rodríguez, P., Rodríguez, D. y Bernal, M. (2020). *Re-ingeniería social para la promoción de la equidad y la prosperidad en las comunidades menos favorecidas*. Editorial Universitaria San Mateo.

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). Los tres pilares de la seguridad. En *INTRODUCCIÓN A LA SEGURIDAD* (pág. 27). ALICANTE: Editorial Área de Innovación y Desarrollo,S.L.

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Alicante: Editorial Área de Innovación y Desarrollo,S.L.

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). Introducción a la seguridad informática. En *Introducción a la seguridad informática y*

analisis de vulnerabilidades. (págs. 18-21). España: Editorial Área de Innovación y Desarrollo,S.L.

Romero Castro, M. I., Figueroa Moràn, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). Introducción al análisis de vulnerabilidades. En *Introducción a la seguridad informática y el análisis de vulnerabilidades* (págs. 41-42). Alicante: Editorial Área de Innovación y Desarrollo,S.L.

S. Pressman, R. (2010). *Ingeniería del software un enfoque práctico.* Mexico: McGrawHillEducation. Obtenido de http://cotana.informatica.edu.bo/downloads/ld-Ingenieria.de.software.enfoque.practico.7ed.Pressman.PDF

SAGE . (17 de Enero de 2018). *YouTube*. (SAGE España) Recuperado el 26 de 09 de 2020, de https://www.youtube.com/watch?v=oe7VWXXNwJQ&ab_channel=SageEspa%C3%B1a

Sanjuan, L. (s.f.). *Universidad del Norte.* Recuperado el 29 de 09 de 2020, de http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Criptograf%C3%ADa%20I.pdf?sequence=1&isAllowed=y

Sanjuan, L. (s.f.). *Universidad del Norte.* Recuperado el 29 de 09 de 2020, de http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Criptograf%C3%ADa%20I.pdf?sequence=1&isAllowed=y

Scrumstudy targeting success. (2016). *Una guía para el Cuerpo de Conocimiento de Scrum (Guía SBOK™) – 3ra Edición.* Avondale: VMEdu, Inc.

Serrato Losada , H. D. (2019). *Repositorio Universidad Abierta y a Distancia UNAD.* Recuperado el 26 de Noviembre de 2020, de

https://repository.unad.edu.co/bitstream/handle/10596/30318/hdserratol.pdf?sequence=1&isAllowed=y

Solís Morales, R. (s.f.). Recuperado el 23 de Noviembre de 2020, de http://oa.upm.es/55363/1/TFG_RODRIGO_SOLIS_MORALES.pdf

SQLite. (s.f.). *SQLite*. Recuperado el 28 de Octubre de 2020, de https://www.sqlite.org/index.html

(s.f.).*TIPOS DE FICHA BIBLIOGRAFICA*. Universitat Politècnica de València.

Trendic. (21 de Febrero de 2019). *Tendencias tecnológias y negocios (TrendTIC)* . Recuperado el 03 de Septiembre de 2020, de https://www.trendtic.cl/2019/02/%EF%BB%BFlas-redes-moviles-globales-registraran-mas-de-12-mil-millones-de-dispositivos-moviles-y-conexiones-de-iot-para-el-2022/

Twitter, Inc. (21 de Marzo de 2006). *Twitter*. Obtenido de Twitter.com: https://twitter.com/?lang=es

Universidad de Valladolid. (s.f.). *Departamento de informática Universidad de Valladolid.* Recuperado el 20 de Noviembre de 2020, de https://www.infor.uva.es/~fdiaz/sd/2005_06/doc/SD_TE02_20060305.pdf

Useche Samudio, C. (2016). Seguridad de la Información. En *Metodología para la Medición de la Efectividad de los Indicadores de Gestión del Modelo de* (pág. 29). Bogotá.

Vargas Salvador, J. P. (Agosto de 2019). *CIATEQDigital.* Recuperado el 16 de Septiembre de 2020, de https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/346/1/VargasSalvadorJuanP%20MSIM%202019.pdf

Vera Salavarría, I. M. (2018). *Repositorio Institucional de la Universidad de Guayaquil.* Recuperado el 22 de Noviembre de 2020, de http://repositorio.ug.edu.ec/bitstream/redug/30863/1/TESIS-IVANNA_VERA.pdf

VersionOne inc. (2017). *Agile247.* Recuperado el 25 de Noviembre de 2020, de https://www.agile247.pl/wp-content/uploads/2017/04/versionone-11th-annual-state-of-agile-report.pdf

Vila Grau , J. L. (8 de Julio de 2016). *Proagilist the Professional Agilist.* Recuperado el 22 de Noviembre de 2020, de https://proagilist.es/blog/agilidad-y-gestion-agil/agile-scrum/la-metodologia-xp/

w3schools. (s.f.). *w3schools*. Obtenido de w3schools: https://www.w3schools.com/html/html_form_input_types.asp