UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

Proyecto de Investigación previo a la obtención del título de Ingeniero en Sistemas y Computación

TRABAJO DE TITULACIÓN

MÓDULO DE SEGURIDAD INFORMÁTICA APLICANDO LA AUTENTIFICACIÓN DE DOBLE FACTOR PARA LA EMPRESA HOME OFFICE S. A. S.

Autor:

Byron Alfredo Barriga Rivera

Tutor:

Ing. Lady Espinoza. MsC

Riobamba - Ecuador

2021

PAGINA DE ACEPTACION

Los miembros del Tribunal de Graduación del proyecto de investigación de título: "MÓDULO DE SEGURIDAD INFORMÁTICA APLICANDO LA AUTENTIFICACIÓN DE DOBLE FACTOR PARA LA EMPRESA HOME OFFICE S. A. S.", presentado por el estudiante: Sr. Byron Alfredo Barriga Rivera y dirigida por la MsC. Lady Espinoza.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Por Constancia de lo expuesto firman:

MsC. Lady Espinoza
Tutora del Proyecto ……

MsC. Ana Congacha
Miembro del Tribunal ……

PhD. Lorena Molina
Miembro del Tribunal ……

DERECHOS DE AUTORIA

La responsabilidad del contenido de este Proyecto de Graduación corresponde exclusivamente al: Sr. Byron Alfredo Barriga Rivera autor del proyecto de investigación bajo la dirección de la MsC. Lady Espinoza y al patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.

Autor:

……..
Byron Alfredo Barriga Rivera
060404894-2

Directora del Proyecto:

……..
MsC. Lady Espinoza
070375234-5

DEDICATORIA

El presente proyecto de investigación está dedicado a todos mis maestros, quien siempre han sido guías y me han permitido mejorar gracias a sus enseñanzas tanto en el ámbito profesional como en el humano.

A mis padres y hermana que siempre me han apoyado de manera incondicional en todos estos años a pesar de las situaciones difíciles que hemos vivido, siempre dando un consejo que motivaba a seguir adelante y jamás han permitido que me dé por vencido. A mis amigos de la carrera con quienes compartí varios momentos inolvidables.

Finalmente dedico a todos mis amigos y familiares que me han apoyado incondicionalmente en este duro transcurso para la obtención de un título profesional.

Byron Alfredo Barriga Rivera

AGRADECIMIENTOS

Agradezco a mis padres, a mi hermana, mis amigos y compañeros por el apoyo que siempre recibí por parte de ellos. A la escuela de Sistemas y Computación de UNACH, que me abrieron sus puertas para continuar con mis estudios, en donde adquirí nuevas experiencias y me formé profesionalmente. A mis docentes de la carrera que compartieron varios de sus conocimientos y fueron un gran complemento en mi vida universitaria. A los docentes MsC. Ana Congacha, PhD. Lorena Molina y en especial a MsC. Lady Espinoza que fueron una gran guía en la culminación del presente proyecto de investigación, agradezco al Ing. Cristian Morales por su guía y participación en este, siendo un pilar fundamental en el presente proyecto de investigación, además agradezco al Ing. Joseph Mosquera y al Ing. Cristian Muñoz por ser un apoyo incondicional en el trascurso de este proyecto de investigación.

Finalmente agradezco a todas aquellas personas que siempre me apoyaron para lograr que este sueño se haga realidad.

Byron Alfredo Barriga Rivera

INDICE GENERAL

PAGINA DE ACEPTACION ..... **I**
DERECHOS DE AUTORIA ..... **II**
DEDICATORIA ..... **III**
AGRADECIMIENTOS ..... **IV**
INDICE DE TABLAS ..... **VII**
INDICE DE FIGURAS ..... **VIII**
RESUMEN ..... **X**
ABSTRACT ..... **XI**
INTRODUCCION **1**
CAPITULO I **3**
PLANTEAMIENTO DEL PROBLEMA **3**
1.1. Problema y Justificación 3
1.2. Objetivos 4
1.2.1. Objetivo General 4
1.2.2. Objetivos Específicos 4
CAPITULO II **5**
MARCO TEORICO **5**
2.1. Seguridad 5
2.1.1. Seguridad Informática 6
2.2. Identificación 8
2.3. Autorización 8
2.4. Autentificación 9
2.4.1. Autentificación Informática 9
2.4.2. Métodos de Autentificación 9
2.4.3. Estudio Comparativo de los Métodos de Autentificación 16
2.5. Criptografía 17
2.5.1. Tokens 17
2.5.2. Codigo QR 17
2.6. Algoritmo TOTP 18
2.6.1. Validación de un OTP 19
2.6.2. Sistemas que Integran TOTP 19
2.7. Estándar de Calidad ISO 25010 21

CAPITULO III **23**
METODOLOGIA **23**
3.1. Tipo y Diseño de la Investigación 23
3.1.1. Según la fuente 23
3.1.2. Según el nivel de medición y análisis de la información 23
3.1.3. Según el objeto de estudio 23
3.1.4. Según el tipo de Inferencia 24
3.2. Unidad de Análisis 24
3.3. Población y Muestra 24
3.4. Técnicas de Recolección de Datos 24
3.5. Técnicas de Análisis e Interpretación de la Información 25
3.6. Desarrollo de la Investigación 25
3.6.1. Análisis de métodos para implementar factores de posesión en el proceso de Autentificación por Doble Factor 25
3.6.2. Desarrollo del Módulo de Seguridad Contra Ataques Informáticos 26
3.6.3. Integración del Proceso de Autentificación de Doble Factor al Módulo de Seguridad 33
CAPITULO IV **34**
RESULTADOS Y DISCUSION **34**
4.1. Aplicación de la metodología de Evaluación 34
4.2. Aplicación del Método Delphi para la Evaluación del Módulo de Seguridad 37
4.3. Resultado Final del Módulo de Seguridad 45
CONCLUSIONES **46**
RECOMENDACIONES **47**
REFERENCIAS BIBLIOGRAFICAS **48**
ANEXOS **51**

INDICE DE TABLAS

Tabla 1: Estudio Comparativo de los Métodos de Autenticación 16
Tabla 2: Características de la Norma ISO 25010 21
Tabla 3: Factores y Métodos de Autenticidad Implementados 26
Tabla 4: Actividades para el Desarrollo del Módulo de Seguridad..... 28
Tabla 5: Descripción de Criterios de Evaluación..... 34
Tabla 6: Métricas de Evaluación para las Subcategorías 36
Tabla 7: Criterios de Evaluación del Primer Ciclo de Evaluación..... 37
Tabla 8: Cumplimiento de las Métricas de Seguridad Primera Evaluación..... 38
Tabla 9: Criterios de Evaluación del Segundo Ciclo de Evaluación..... 40
Tabla 10: Cumplimiento de las Métricas de Seguridad Segunda Evaluación..... 40
Tabla 11: Roles de Usuarios del Sistema 51
Tabla 12: Requerimientos Funcionales del Módulo de Seguridad..... 51
Tabla 13: Requerimientos No Funcionales 55
Tabla 14: Recursos Tecnológicos..... 56
Tabla 15: Tabla ho_genero..... 60
Tabla 16: Tabla ho_institucion_bancaria 60
Tabla 17: Tabla ho_paises..... 61
Tabla 18: Tabla ho_tipo_cuenta..... 61
Tabla 19: Tabla ho_intentos_ataque..... 62
Tabla 20: Tabla ho_usuarios 62
Tabla 21: Tabla ho_userlog..... 65
Tabla 22: Tabla ho_historial..... 66
Tabla 23: Primera Aplicación de Criterios de Evaluación Primer Evaluador..... 125
Tabla 24: Primera Evaluación de las Métricas de Seguridad Primer Evaluador..... 125
Tabla 25: Primera Aplicación de Criterios de Evaluación Segundo Evaluador..... 125
Tabla 26: Primera Evaluación de las Métricas de Seguridad Segundo Evaluador..... 126
Tabla 27: Primera Aplicación de Criterios de Evaluación Tercer Evaluador 126
Tabla 28: Primera Evaluación de las Métricas de Seguridad Tercer Evaluador 126
Tabla 29: Primera Aplicación de Criterios de Evaluación Cuarto Evaluador..... 127
Tabla 30: Primera Evaluación de las Métricas de Seguridad Cuarto Evaluador..... 127
Tabla 31: Primera Aplicación de Criterios de Evaluación Quinto Evaluador..... 127
Tabla 32: Primera Evaluación de las Métricas de Seguridad Quinto Evaluador 128
Tabla 33: Segunda Aplicación de Criterios de Evaluación Primer Evaluador..... 128
Tabla 34: Segunda Evaluación de las Métricas de Seguridad Primer Evaluador..... 129
Tabla 35: Segunda Aplicación de Criterios de Evaluación Segundo Evaluador..... 129
Tabla 36: Segunda Evaluación de las Métricas de Seguridad Segundo Evaluador 129
Tabla 37: Segunda Aplicación de Criterios de Evaluación Tercer Evaluador 129
Tabla 38: Segunda Evaluación de las Métricas de Seguridad Tercer Evaluador..... 130
Tabla 39: Segunda Aplicación de Criterios de Evaluación Cuarto Evaluador..... 130
Tabla 40: Evaluación de las Métricas de Seguridad Cuarto Evaluador 130
Tabla 41: Segunda Aplicación de Criterios de Evaluación Quinto Evaluador 131
Tabla 42: Segunda Evaluación de las Métricas de Seguridad Quinto Evaluador 131

INDICE DE FIGURAS

Figura 1: Mecanismo de Autentificación de un Único Factor 10
Figura 2: Mecanismo de Autentificación de Doble Factor 12
Figura 3: Mecanismo de Autentificación con contraseña SMS 14
Figura 4: Autentificación Biométrica..... 15
Figura 5: Autentificación por Click Pattern 16
Figura 6: Estructura General de un Codigo QR 18
Figura 7: Aplicación Móvil Google Authenticator 20
Figura 8: Autentificación de Doble Factor de la App Authy 21
Figura 9: Seguridad General del Módulo Informático 39
Figura 10: Seguridad General del Módulo Informático 41
Figura 11: Análisis de la Métrica de Confidencialidad..... 42
Figura 12: Análisis de la Métrica de Integridad..... 42
Figura 13: Análisis de la Métrica de No Repudio..... 43
Figura 14: Análisis de la Métrica de Responsabilidad..... 44
Figura 15: Análisis de la Métrica de Autenticidad..... 44
Figura 16: Análisis General del Módulo de Seguridad Informática 45
Figura 17: Modelo Vista Controlador (MVC) 57
Figura 18: Modelo Entidad-Relación..... 58
Figura 19: Modelo Relacional..... 58
Figura 20: Diagrama de Casos de Uso..... 59
Figura 21: Modelo de Base de Datos 59
Figura 22: Vista Principal del Sistema..... 75
Figura 23: Vista de Registro de Cliente (Vacía) 75
Figura 24: Vista de Registro Cliente (Llena) 76
Figura 25: Vista de Registro Exitoso de Cliente..... 76
Figura 26: Email enviado al Correo Electrónico..... 77
Figura 27: Activación de Cuenta de Cliente 77
Figura 28: Vista de Login..... 78
Figura 29: Vista Autentificación Doble Factor Cliente 78
Figura 30: Codigo de la App Google Authenticator del Cliente..... 79
Figura 31: Vista Autentificación Doble Factor Administrador..... 79
Figura 32: Codigo de la App Google Authenticator del Administrador..... 80
Figura 33: Vista Autentificación Doble Factor SuperAdministrador 80
Figura 34: Codigo de la App Google Authenticator del SuperAdministrador..... 81
Figura 35: Email enviado del inicio de sesión de usuario (Gmail) 81
Figura 36: Email enviado del inicio de sesión de usuario (Outlook)..... 82
Figura 37: Panel Principal del Cliente..... 82
Figura 38: Vista del cambio de contraseña del usuario..... 83
Figura 39: Vista del Perfil del Cliente..... 83
Figura 40: Vista de la Hoja de Vida del Cliente 84
Figura 41: Vista de los Datos Bancarios del Cliente..... 84
Figura 42: Vista de la Imagen de Perfil del Cliente 85
Figura 43: Vista Principal del Panel del Administrador 85
Figura 44: Vista de Datos Generales del Administrador..... 86

Figura 45: Vista de Hoja de Vida del Administrador 86
Figura 46: Vista de Datos Bancarios del Administrador 87
Figura 47: Vista de la Imagen Perfil del Administrador 87
Figura 48: Vista de Clientes 88
Figura 49: Datos Generales del Cliente Registrado 88
Figura 50: Hoja de Vida del Cliente Registrado 89
Figura 51: Datos Bancarios del Cliente Registrado 89
Figura 52: Imagen de Perfil del Cliente Registrado 90
Figura 53: Historial del Cliente Registrado 90
Figura 54: Historial por Sesión del Cliente Registrado 91
Figura 55: Historial detallado de la Sesión del Cliente Registrado 91
Figura 56: Vista de los Clientes Bloqueados 92
Figura 57: Vista de los Ataques Informáticos realizados al sistema 92
Figura 58: Vista del Panel Principal del SuperAdministrador 93
Figura 59: Vista de Datos Generales del SuperAdministrador 93
Figura 60: Vista de la Hoja de Vida del SuperAdministrador 94
Figura 61: Vista de Datos Bancarios del SuperAdministrador 94
Figura 62: Vista de la Imagen de Perfil del SuperAdministrador 95
Figura 63: Vista de Administradores 95
Figura 64: Vista de Registro de un Administrador 96
Figura 65: Vista de un Administrador Registrado de manera correcta 96
Figura 66: Email enviado al Administrador 97
Figura 67: Datos Generales del Administrador Registrado 97
Figura 68: Hoja de Vida del Administrador Registrado 98
Figura 69: Datos Bancarios del Administrador Registrado 98
Figura 70: Imagen de Perfil del Administrador Registrado 99
Figura 71: Historial del Administrador Registrado 99
Figura 72: Vista de Administradores Bloqueados 100
Figura 73: Vista de los Clientes Registrados 100
Figura 74: Vista de los Clientes Bloqueados 101
Figura 75: Vista de los Ataques Informáticos 101
Figura 76: Vista de Errores del Sistema 102
Figura 77: Certificado de Implementación del Módulo de Seguridad 132

RESUMEN

En la actual era, las tecnologías han evolucionado a tal punto de estar presente en nuestro diario vivir, por lo que mejorar la seguridad de todos los sistemas informáticos se ha convertido en prioridad para las empresas. La empresa Home Office S.A.S, dedicada a la compra y venta de productos digitales requiere una alta seguridad en todos sus procesos informáticos, siendo el acceso exclusivo al personal autorizado su máxima prioridad referente a la seguridad informática.

Por esta razón se implanto un módulo de seguridad informática aplicando la autentificación de doble factor para la empresa Home Office S.A.S., con el propósito de gestionar y validar la información de los usuarios, detectar y neutralizar ataques informáticos y garantizar el acceso exclusivo de sus usuarios autorizados.

En el desarrollo de la presente investigación se utilizaron varios métodos y metodologías dependiendo de cada una de sus fases, siendo para el desarrollo del módulo informático la metodología cascada, el análisis de los factores de posesión mediante fuentes bibliográficas.

La evaluación del módulo informático se realizó por medio del método Delphi bajo las métricas de seguridad de la norma ISO 25010, para realizar este procesos se utilizaron dos ciclos, la primera sin la implementación de la autentificación por doble factor y la segunda con la implementación, dando como resultado en la primera interacción un cumplimento del 83% en general y en la segunda cumpliendo con un 100% de todas las métricas, mejorando la seguridad informática de la empresa Home Office .S.A.S.

Palabras clave: Ataques Informáticos, Autentificación por Doble Factor, Desarrollo de Aplicaciones Web, Métodos de Autentificación Informática, Seguridad Informática.

ABSTRACT

In the current era, technologies have evolved to the point of being present in our daily lives, so improving all computer systems' security has become a priority for companies. The company Home Office S.A.S, dedicated to the purchase and sale of digital products, requires high security in all its computer processes, exclusive access to authorized personnel its highest priority regarding computer security.

For this reason, a computer security module was implemented applying two-factor authentication for the company Home Office S.A.S. to manage and validate user information, detect and neutralize computer attacks, and ensure exclusive access for its authorized users.

Several methods and methodologies were used depending on each of its phases, including developing the computer module, the cascading techniques, and analyzing the factors of possession through bibliographic sources.

The computer module evaluation was carried out through the Delphi method under the security metrics of the ISO 25010 standard.

Two cycles were used to complete this process, the first without implementing double-factor authentication and the second with the implementation. It resulted in the early interaction compliance of 83% in general and in the second compliance with 100% of all the metrics, improving the Home Office S.A.S company's computer security.

Keywords: Computer Attacks, Computer Authentication Methods, Computer Security, Double Factor Authentication, Web Application Development.

Reviewed by:
Ms.C. Ana Maldonado León
ENGLISH PROFESSOR
C.I.0601975980

INTRODUCCION

En la última década el desarrollo de sistemas informáticos y en especial los sistemas web se han convertido en una base del desarrollo tecnológico a tal punto de estar presentes en la vida cotidiana por lo que la información que está en internet debe estar siempre segura (Lagreca, 2017). Según estudios realizados en Perú se analizaron las políticas de seguridad que deben ser cumplidas tomando en cuenta los sistemas informáticos, el comportamiento humano, conociendo que la información es el mayor bien a proteger (Altamirano, 2017).

La seguridad en sistemas informáticos tiene la finalidad de proteger la información de sus usuarios, teniendo en cuenta que la autentificación al momento de ingresar a un sistema es muy vulnerable. Se han creado varias técnicas para mejorar los métodos de autentificación en sistemas informáticos (Singh, 2017). Es por eso, que uno de los métodos más usados para mejorar la autentificación de usuarios en un sistema es la Autentificación por Doble Factor (2FA) (Alzahrani, 2018).

En Arabia Saudita se realizaron investigaciones acerca de los mejores métodos de autentificación para accesos de sistemas informáticos demostrando que la autentificación por doble factor es uno de los métodos más usados en sistemas bancarios junto a la autentificación biométrica, la seguridad en la banca digital es considerada la más importante entre sistemas que requieren la autentificación de sus usuarios, siendo la base para cualquier sistema que requiera mejorar su seguridad al momento de la autenticación de sus usuarios (Alzahrani, 2018). Además, en China y Estados Unidos son países que más utilizan la autentificación de usuarios, a tal punto en que todos sus sistemas cuentan con diferentes formas de autentificación por doble factor siendo los biométricos los más usados en China y los basados en OTP por Arabia (Kuang & Xu, 2019).

En el Ecuador existen estudios referentes a la problemática de ciberdefensa y ciberseguridad según los estudios de (Vargas, 2016) argumentan que unos de los motivos que causa el problema en ciberseguridad es el aumento de servicios y productos por internet (transacciones, banca online, pago del agua, luz etc.).

La empresa Home Office S.A.S, se dedica a la compra y venta de productos digitales por lo que al trabajar con entidades bancarias requiere una mayor seguridad en todos sus

procesos informáticos incluyendo un método de seguridad al ingreso del sistema, con el fin de validar el acceso exclusivo al personal autorizado dentro del sistema.

Por lo tanto, surgió la presente investigación que implanto un Módulo de Seguridad Informática para la empresa Home Office S.A.S aplicando la autentificación por doble factor con el fin de mejorar la seguridad del sistema de la empresa, la evaluación de la seguridad del sistema informático se lo realizo mediante las métricas de seguridad de la norma ISO 25010.

El Módulo de Seguridad se desarrolló bajo los lenguajes de programación PHP y JavaScript, bajo el patrón de diseño Modelo Vista Controlador (MVC), la autentificación por doble factor se lo realizo al ingreso del sistema mediante el uso del algoritmo Time-based One-time Password (TOTP) implementado en la aplicación Google Authenticator. Se utilizo la arquitectura Cliente – Servidor, para desarrollar la aplicación web permitiendo realizar validaciones por lado del cliente y del servidor, para el desarrollo de software se utilizó el modelo Cascada con cada una de sus respectivas fases.

El presente documento está estructurado de la siguiente manera: En el capítulo I se describe el planteamiento del problema, capítulo II se encuentra el marco teórico que permite conocer los conceptos relacionados de la temática abordada, en el capítulo III se plasma la metodología a utilizada para el desarrollo del módulo de seguridad junto a los factores de posesión para la autentificación por doble factor, finalmente en el capítulo IV se encuentran los resultados de medir la calidad de la seguridad del módulo informático mediante el cumplimiento de las métricas de seguridad dadas en la norma ISO 25010, para posteriormente realizar las conclusiones hechas durante esta investigación

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Problema y Justificación

A lo largo del tiempo la tecnología ha cambiado y es parte fundamental de nuestra vida cotidiana, a tal punto que se confían los datos a varios sistemas informáticos. Debido a esto las empresas e instituciones han optado por un enfoque prioritario en la seguridad de software. Las brechas de seguridad (el crimen digital y el fraude en internet), han dado origen a varios métodos de seguridad en torno al ingreso a los sistemas informáticos, siendo el más utilizado la Autenticación por Doble Factor (2FA). Este proceso de seguridad sirve para que el usuario confirme su identidad mediante dos factores de autenticación diferentes (clave estática y clave dinámica) (Waheed, 2016).

Con la finalidad de contribuir a la seguridad informática en general y al desarrollo tecnológico de la empresa Home Office S.A.S, existe la necesidad de mejorar la seguridad de su sistema informático. Por lo tanto, la decisión de desarrollar un módulo de seguridad contra ataques informáticos, incluyendo un método de seguridad para el ingreso y transacciones (2FA), permitirá mejorar la validación del acceso exclusivo al personal autorizado dentro del sistema según un rol determinado.

1.2. Objetivos

1.2.1. Objetivo General

Implantar un módulo de seguridad informática aplicando la autentificación de doble factor para la empresa Home Office S.A.S.

1.2.2. Objetivos Específicos

- Analizar métodos para implementar factores de posesión en el proceso de Autentificación por Doble Factor.
- Diseñar e implementar un módulo de seguridad contra ataques Informáticos aplicando la autentificación de doble factor.
- Evaluar la seguridad del Módulo mediante el estándar de calidad ISO 25010.

CAPITULO II

MARCO TEORICO

En la actual era digital casi todos nuestros equipos y dispositivos se encuentran interconectados, guardando una gran cantidad de información confidencial en cada uno de ellos, por lo que es siempre necesario contar con contraseñas robustas que no permitan que usuarios no permitidos obtengan la información personal.

Fernando Corbato, reconocido como el padre de la contraseña moderna, en los años 60 ideo el actual modelo de organización de seguridad en la que para cada usuario solo pueda acceder a los archivos que le corresponda, pero la existencia de dicho método se rumora que viene desde la época del imperio romano.

En este capítulo se ha realizado una descripción de varios conceptos que guardan relación con la autentificación, además de diferentes factores que pueden añadir una capa extra de seguridad tanto para sistemas como para usuarios bajo el concepto de autorización.

2.1. Seguridad

La seguridad como concepto no tiene un solo punto de vista sobre su significado, depende mucho del contexto en el que se aplique y del factor humano que lo involucra, en la antigüedad se relacionaba con la confianza, por el contrario, en nuestra época actual guarda mayor relación con la responsabilidad de proteger (Instituto de Estudios Estrategicos, 2011). Las primeras manifestaciones de seguridad que llevaron a cabo los seres humanos fueron llaves para pertenencias, criptografía básica para mensajes escritos y armas de todo tipo para proteger sus propias vidas.

El uso de Criptografías viene desde la época de Heródoto hasta la actualidad, pasando por el cifrado de Julio Cesar en el que consistía en sustituir cada letra de un texto original con la letra tres lugares más adelante, considerando que a las tres últimas letras del alfabeto le correspondía las primeras letras del alfabeto (Tábara, 2011). Todos estos métodos de encriptación han ido evolucionado junto a la tecnología. Se puede destacar el mayor cambio de estos tipos de criptografías en la maquina Enigma, que consistía en una máquina de rotores que permitía descifrar y cifrar mensajes al frente alemán, dando una ventaja estratégica en las comunicaciones del bando alemán (Morales, 2013).

Según (INCIBE, 2015) la seguridad ha evoluciona a tal punto que se evidencio en el ámbito empresarial teniendo en cuenta las décadas descritas a continuación:

- En los 70, la seguridad tenía un enfoque centrado en la garantía del buen uso de la información, siendo una época con varios inconvenientes como la falta backups, revisiones periódicas y medidas físicas.
- En la década de los 80, se dan a conocer los primeros virus informáticos y con estos la comercialización de antivirus para sistemas y ordenadores.
- En los 90, dan comienzo a los ataques por internet y las vulnerabilidades de las redes informáticas.
- En los 2000, comienzan los ataques organizados enfocados a corporaciones y el concepto de seguridad a todos los datos.
- Ya para los 2010, se evidencia varios métodos de seguridad para todo tipo de dispositivos y cifrado para la información personal y empresarial.

2.1.1. Seguridad Informática

Es un conjunto de reglas y procesos que ayudan a proteger la integridad, confidencialidad y disponibilidad de la información. Por otra parte, permite asegurar que los recursos de un sistema de información de una organización sean utilizados de manera correcta y por el personal autorizado (Tirado & Carreño, 2017).

Trata de reducir los riesgos de acceso y utilización de ciertos sistemas de manera no autorizada y malintencionada. Su objetivo principal es precautelar por la integridad de los recursos informáticos de gran valor para una organización. Con las buenas prácticas de seguridad informática ayuda a la organización a proteger sus recursos tangibles e intangibles. (Vera & Vera, 2017)

El objetivo primario de la seguridad informática es optimizar los riesgos sobre los recursos informáticos y con esto aportar con el funcionamiento normal de las operaciones de la empresa dejando en segundo plano la administración de riesgos informáticos El objetivo secundario de la seguridad informática consiste en asegurar que los documentos tengan confiabilidad total donde deben cumplir con unas características importantes las cuales son: permanecía, accesibilidad, disponibilidad, confidencialidad, autenticidad y aceptabilidad (Zambrano & Valencia, 2017). Hay que tener en cuenta que la Seguridad Informática es un proceso en constante cambio, actualizando métodos, herramientas,

procedimientos y técnicas que ayuden a contrarrestar los ataques informáticos que van apareciendo día con día (Suárez & Ávila, 2017).

2.1.1.1.Clasificación de la Seguridad Informática

Según (Alegre & Garcia, 2011) la seguridad Informática tiene la siguiente clasificación:

- **Seguridad Activa:** Son todas las medidas a tomar en cuenta al detectar una o varias amenazas, y en caso de que existan se generan los mecanismos necesarios para que se evite el problema. Algunos ejemplos de la seguridad activa son las claves de acceso, antivirus, cortafuegos o firewall.
- **Seguridad Pasiva:** Son todas las medidas ocupadas para que una vez que se produzca uno o varios ataques o falle el sistema de seguridad se activen los mecanismos para recuperación del mismo y lograr que el impacto sea el menor posible.

2.1.1.2. Ataques Informáticos

Entiéndase por ataque informático a la acción de aprovechar alguna debilidad o vulnerabilidad en el software, en el hardware e incluso en el personal involucrado en el ambiente informático, con el fin de obtener un beneficio en su mayoría de índole económico (Mieres, 2009). Estos ataques causan daños directo a la seguridad de los sistemas informáticos, que luego repercute directamente a la información de la organización, además de producir daño monetario (Cañón, 2015) .

Hoy en día existen una gran cantidad de ataques informáticos enfocados en el software. Entre los ataques más frecuentes destacan un grupo que se describen a continuación:

- **Brute Force (Ataques de Fuerza Bruta)**

  Este ataque consiste en intentar romper todas las combinaciones posibles de usuario y contraseña, enfocado para descifrar contraseñas débiles, las maneras de protegerse son limitando el número de intentos fallidos, utilizando contraseñas fuertes y eligiendo usuarios no comunes como “admin, administrador, etc” (Cañón, 2015).

- **SQL Injection (Ataques de Inyección de SQL)**

  Este ataque consiste en explotar la flexibilidad del lenguaje SQL enviando ataques de texto simple, buscando leer todos los registros privados almacenados en la base de datos, esto se evidencia en los aplicativos que, por falta de experiencia en las búsquedas avanzadas, los métodos para solucionar son dos enviar una búsqueda

parametrizada y una configuración inteligente del motor de administración de la base de datos (García, Montenegro, & Velandia, 2016).

- **Code Injection (Ataque de Inyección de Codigo)**

El ataque principal consiste en introducir a un programa o software una serie de instrucciones que no formaban parte de la composición original del software provocando modificaciones en el funcionamiento y su rendimiento (Xiao, Yan, & Jiang, 2015).

- **Cross-Site-Scripting (Ataque XSS)**

Es una vulnerabilidad presente en las apps web, caracterizada por una inyección de codigo VBScript o JavaScript en la experiencia del usuario final al ingresar a alguna página, siendo usada para phishing por medio de una URL, el riesgo de que la víctima envié sus credenciales de usuario es muy alta (Serrato, 2016).

- **Cross-Site Request Forgeries (Ataque CSRF)**

Consiste en él envió de peticiones HTTP específicas, a un sitio web por medio de un navegador web de un usuario sin el conocimiento del mismo (Manaswini & Sahoo, 2016). Se aprovecha la confianza que tiene la app web en el usuario que está realizando las peticiones HTTP (Shernan & Traynor, 2015).

2.2. Identificación

La identificación corresponde al proceso de distinción de un usuario de otro, muchas veces es confundido con la autentificación, diferenciándose en que la autentificación valida que el usuario es realmente el identificado (Areitio & Areitio, 2007).

2.3. Autorización

La autorización es de igual manera confundido con la autenticación, pero corresponde a un paso posterior a la de la autentificación en el cual se encarga de proteger los recursos permitiendo que solo los usuarios autorizados puedan acceder a los mismos. El mecanismo más usado para la autorización es el Acceso Basado en Roles (RBAC Role-Bassed Access Control), el cual funciona como un mecanismo de control de acceso definido por el sistema basado en políticas de roles y privilegios realizados al momento de la creacion de cada uno de los sistemas informáticos (Ferraiolo & Kuhn, 1995).

2.4. Autentificación

Capacidad que permite identificar que un usuario es realmente quien dice ser, es un proceso principal utilizado para el control de acceso de un sistema. Tradicionalmente se utilizan los campos de usuario y contraseña, pero con el tiempo se han ido implementado nuevas formas interesantes de autenticación como la autenticación por dos factores. Es uno de los pasos del proceso para ser identificado consiste en determinar si un usuari**o** u organización tiene acceso al sistema o recurso. Con respecto a la autenticación basado con tokens el usuario porta un objeto que le permite identificarse con un sistema informático. (Rodriguez & Socorro, 2018).

2.4.1. Autentificación Informática

El sistema de autentificación basado en usuario y contraseña sigue siendo el más usado para acceder a distintos servicios online. Pero no significa que sea actualmente el más seguro debido a que la mayoría de usuarios optan por contraseñas débiles, ya sea por la facilidad de recordar o por el desconocimiento acerca de lo fácil que resulta obtenerlas para un ciberdelincuente.

2.4.2. Métodos de Autentificación

La autenticación es muy importante para la seguridad. De hecho, es muy difícil seleccionar un método de autenticación adecuado. Algunos métodos de autenticación se describen.

2.4.2.1.Autentificación Convencional

Este método es el más fácil de implementar para un acceso seguro de sesión de usuario los requerimientos para llevar a cabo es el más barato debido a que no se requiere implementar Hardware o Software adicional, este método es muy sencillo y consiste en aplicar contraseña junto a un nombre de usuario, pero la mayor desventaja son las vulnerabilidades en especial los ataques informáticos (Cheng, 2019). Este es el método más antiguo para la autentificación por lo que se lo considera como un método principal para el inicio seguro de sesión, pero presenta eventuales problemas debido a la memoria de los usuarios al momento de recordar sus contraseñas, las cuales a pesar de ser largas no son lo más efectivo por los múltiples ataques que se puede realizar (Waheed, 2016).

- **La Autentificación de un Único Factor**

Consiste la utilización de contraseñas para validar la autentificación de un usuario frente un proceso de verificación de identidad ante cualquier servicio que lo necesite, siendo así que el usuario es realmente quien dice ser y no un impostor

La Autentificación de un Único Factor (SFA Single-Factor Authentication) consiste en el uso de credenciales basadas en una identificación de usuario y contraseña de acceso para el sistema o servicio. En la Figura 1 se muestra el proceso de autentificación de un único factor, en el cual solo con un usuario y una contraseña ya tiene un usuario el acceso al sistema.

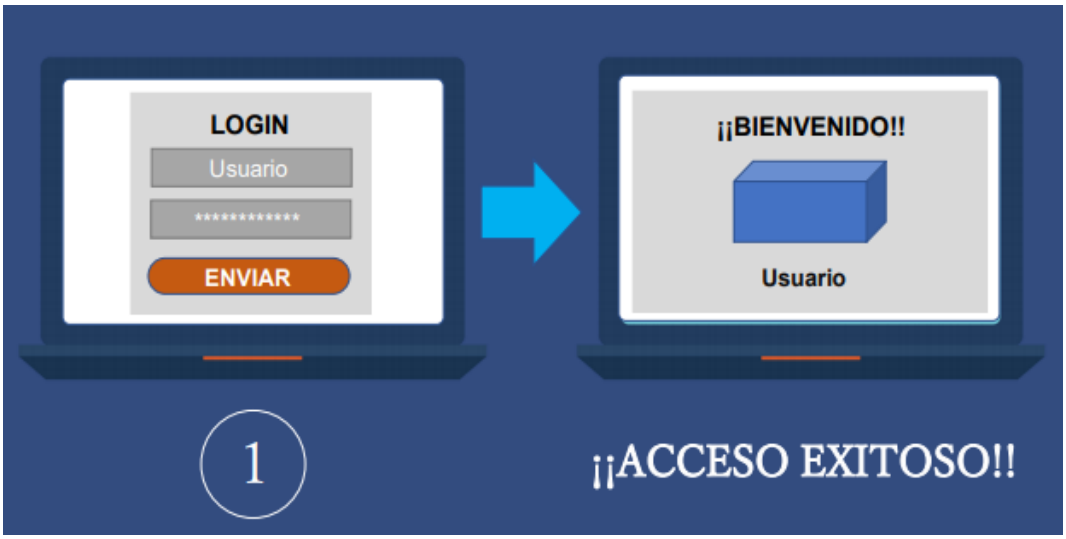

Figura 1: Mecanismo de Autentificación de un Único Factor

- **Contraseña Robusta**

Siendo las contraseñas simples uno de los mayores errores de los usuarios al momento de ingresar a un sistema tanto de escritorio como online, se recomienda el uso de contraseñas robustas para mitigar los problemas de autentificación. Según (Panda Security, 2016) define algunas sugerencias para poder crear una contraseña robusta las cuales se muestran a continuación:

  - Obtener la contraseña partiendo de una frase significativa para el usuario.
  - Combinar dos palabras mesclando sus letras para crear una nueva.
  - Remplazar las vocales por números de una palabra.
  - Eliminar todas las vocales de una frase o palabra.
  - Usar un servicio de contraseñas para múltiples cuentas.

Cabe destacar que no importa lo complicado o robusta sea una contraseña sigue siendo la única barrera entre un usuario y los ciberdelincuentes, por esta razón se recomienda siempre aumentar una capa de seguridad, siendo este cualquier otro factor para la protección de la información sensible tanto del usuario como del propio sistema.

2.4.2.2.Autentificación de Doble Factor

Dada la problemática que surge del uso de un único factor de autentificación y la fácil sustracción por los ciberdelincuentes, los expertos de ciberseguridad empezaron una campaña de recomendación en la utilización de una capa extra de seguridad en la fase de autentificación requiriendo un factor extra en el momento de verificación de la identidad de un usuario.

El concepto de la autenticación de dos factores es usado como un protocolo para prevenir muchos ataques. Esta autentificación se basa en la suposición que tienes algunos de estos factores de identidad, la identificación. Se puede dar una serie de contraseñas temporales llamada OTP que solo se puede utilizar una vez. Cuando se aplica ese código o contraseña temporal, el banco inicia el proceso y verificación del token. Para realizar el inicio de cualquier operación el token debe ya estar registrado (Waheed, 2016). Según Alzahrani puede haber dos factores de autenticación que son muy seguros. Un dispositivo móvil de verificación se puede utilizar junto con la contraseña en lugar de usar tarjetas, fichas, etc. El costo de la implementación de la autenticación de doble factor se reduce mediante el uso de dispositivos móviles (Alzahrani, 2018).

En la Figura 2 se muestra el proceso de la Autentificación de Doble Factor (2FA), que consiste en que luego del inicio de sesión con sus credenciales, recibe un codigo (PIN/TOKEN) a su teléfono móvil para que lo devuelva al sistema de autentificación y sea verificado correctamente y acceda al sistema.

Figura 2: Mecanismo de Autentificación de Doble Factor

- **Reglas Generales**

Según el NIST (NIST, 2017), define tres reglas generales sobre la autentificación electrónica también conocidas como categorías de factores de autentificación:

  - **"Algo que el usuario sabe":** Este factor incluye cualquier cosa que sea de conocimiento del usuario.
  - **"Algo que el usuario tiene":** Este factor incluye algo que físicamente posea el usuario.
  - **"Algo que el usuario es":** Este factor es uno de los niveles más altos de seguridad, debido al uso de biometría.

- **OTP (One-Time Password)**

Un "One-Time Password" (OTP) o también conocido como "One-Time Pin", es una contraseña válida para un solo uso, es decir es una única transacción, en un sistema o dispositivo digital. Los OTP mejoran la seguridad asociado a sistemas con autentificación de un solo factor evitando las vulnerabilidades a ataques de inyección de codigo, o una denegación de servicio (Buccafurri & Nardone, 2020).

Según (Microcosm Ltd, 2018) los OTPs más importantes se pueden clasificar de la siguiente manera:

  - **HOTP (HMAC-based One-Time Password),** mejor conocida como contraseña de un solo uso basada en eventos: se basa en el algoritmo HMAC y depende de 2 factores de información. La primera es la clave secreta denominada "inicialización", la cual solo conoce el token y el servidor que

realiza la validación de los códigos OTP envidos. El segundo factor cambiante, que consiste en un contador almacenado en el token y el servidor, el valor del contador se incrementa cuando se valida correctamente una OTP.

- **TOTP (Time-based One-Time Password),** mejor conocida como contraseña de un solo uso basada en el tiempo**:** está basada en el algoritmo HOTP, pero su segundo factor es diferente, tomando el tiempo en lugar de un contador, se suele usar incrementos denominados "timestep", que suele variar de 30 a 60 segundos, siendo así que el OTP será válida mientras dura el periodo de tiempo.

2.4.2.3.Contraseña SMS basado en tiempo (SMS One Time Password)

Los dispositivos móviles son usados como una parte de la autentificación, resultando muy conveniente, debido a la facilidad del usuario de tenerlo siempre con él, además de la facilidad de usar y conectarse a internet o la red de telefonía. Este método se utiliza en la banca para transacciones seguras (Alzahrani, 2018). Es un sistema basado en teléfono móvil en el que el usuario solicita la autenticación aplicando algún ID y recibe una contraseña a través de SMS (Short Message Service).

Por otro lado, los SMS suelen ser el factor más débil en una autentificación (The Hacker News, 2014) ,debido a la facilidad de un ciberdelincuente en interceptarlos debido a los problemas de la tarjeta SIM que poseen la mayoría de las operadoras de telecomunicaciones "Signaling System Number 7" (SS7).

En la Figura 3 se muestra el proceso de autentificación por medio de un SMS basado en tiempo, el cual consiste en que luego del inicio de sesión con sus credenciales, recibe un codigo (TOKEN) al teléfono móvil en formato SMS, el mismo que será enviado por un servidor para realizar la autentificación y devolverá al sistema si el usuario es correctamente identificado.

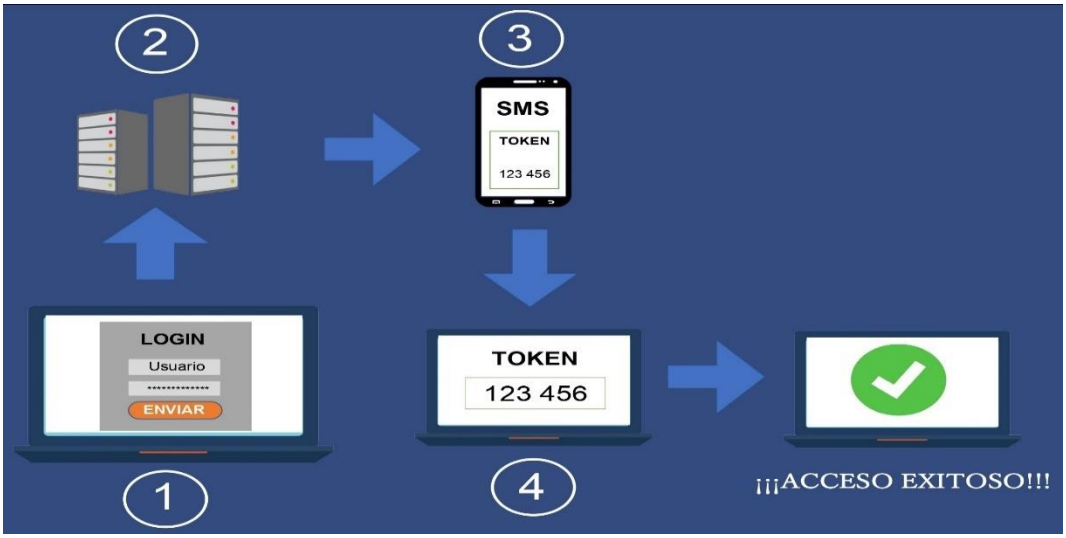

Figura 3: Mecanismo de Autentificación con contraseña SMS

Un OTP mediante un SMS debe ser encriptado mediante el estándar A5/x, el cual varios grupos de hackers han informado que puede ser desencriptado en minutos. Además, muchos expertos consideran que un mensaje de texto no es algo que un usuario sabe, ni algo que tiene, ni algo que es, sino algo que recibe, según el Instituto Nacional de Estándares de los Estados Unidos (NIST) (Verizon Media., 2016), declaro que los SMS son métodos inseguros en la autentificación.

2.4.2.4. Autentificación Biométrica

Como medida frente al fraude de documentación y suplementación de identidad se desarrollan nuevas soluciones tecnológicas, una de estas es las basadas en la Biometría, usado como método de identificación y autentificación más rápida y confiable.

Biométrica significa el propio usuario. Entendiendo que las características físicas que un usuario tenía no pueden ser hackeadas. Puede ser huellas dactilares, reconocimiento de iris, y puede ser la voz del usuario (Singh, 2017)**.** Debido a las características biométricas únicas, los seres humanos pueden ser verificados de manera única para la identidad. Una contraseña puede ser robada, pero no las características naturales. La biometría ofrece una forma infalible de verificar la identidad de alguien (Waheed, 2016)**.** La Biometría establece dos categorías de tecnologías biométricas:

- **Mediciones Fisiológicas**: Contemplan los análisis morfológicos del individuo, como son las huellas dactilares, retina, iris, fisionomía del rostro, el ADN, entre otros.

- **Mediciones del Comportamiento:** Analizan el reconocimiento de la voz, firmas, pulsaciones, sonidos, gestos, entre otros.

En la Figura 4 se muestra el proceso de la Autentificación Biométrica, que consiste en que luego del inicio de sesión con sus credenciales, se envía un factor biométrico a comparar hacia un servidor o base de datos para que lo devuelva al sistema de autentificación y sea verificado correctamente.

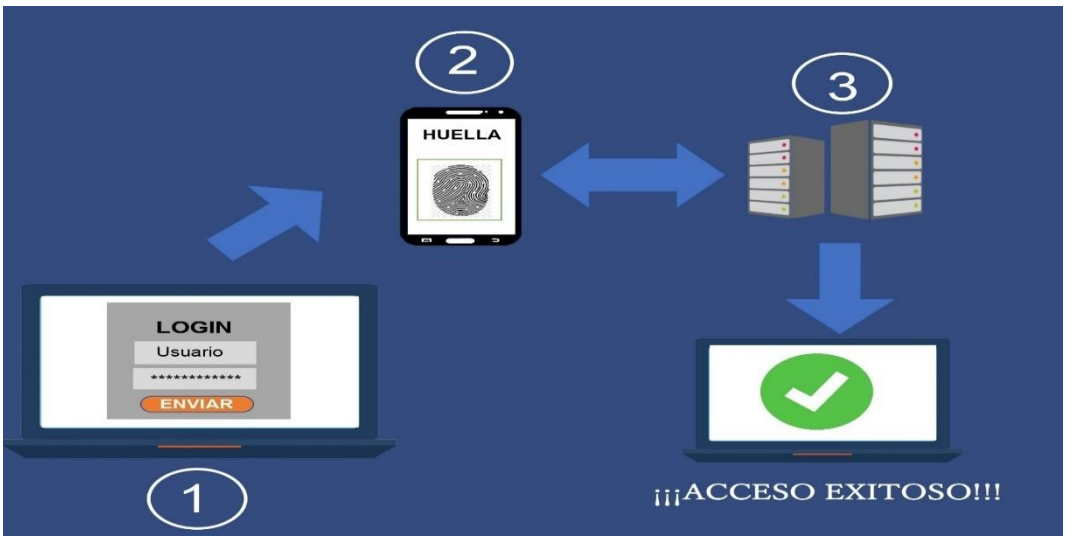

Figura 4: Autentificación Biométrica

La Autentificación Biométrica es un proceso de comparación de datos entre las características de una persona con una plantilla biométrica obtenida con anterioridad de la misma persona con el fin de encontrar semejanzas.

2.4.2.5. Autentificación Click Pattern

El avance de la tecnología se muestra siempre presente en los sistemas, y en el apartado de seguridad no es la excepción, la inteligencia artificial, ha tomado un rol fundamental en la implementación de autentificación de usuarios, el término "CAPTCHAs" son más común hoy en día, de lo que parece, los usuarios validan su información por medio de captchas. (Sinha & Kumar, 2019)

El proceso de autentificación por click pattern, consiste en que la contraseña es el patrón que realiza el usuario con el clic del ratón, este esquema de autentificación se basa en que el ratón tiene que realizar clics en la pantalla de símbolos en los que se pueden encontrar cuadrículas de color (Waheed, 2016). En este método de seguridad el atacante puede ser engañado por el patrón de clic como por la contraseña. No es necesario de hardware adicional (Alzahrani, 2018).

En la Figura 5 se muestra de forma gráfica la Autentificación Click Pattern que consiste en que luego del inicio de sesión con sus credenciales, se envía un captcha para comparar hacia el servidor o base de datos para que lo devuelva al sistema de autentificación y sea verificado correctamente.

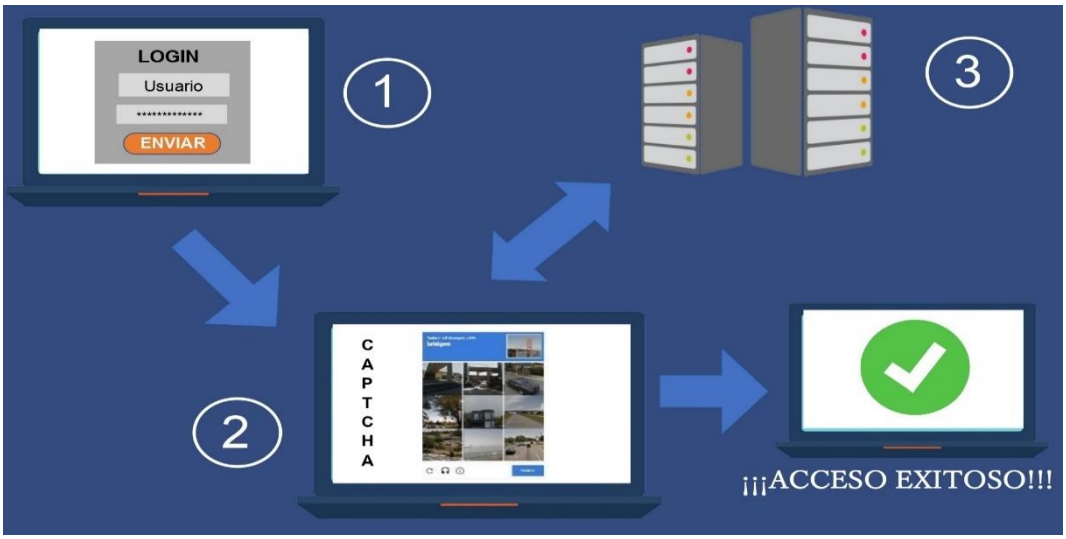

Figura 5: Autentificación por Click Pattern

2.4.3. Estudio Comparativo de los Métodos de Autentificación

Tabla 1: Estudio Comparativo de los Métodos de Autenticación

Métodos de Autentificación	***Seguridad frente Ataques Informáticos***	***Ventajas***	***Desventajas***	***Costo***
Convencional	Fuerza Bruta	Implementación	Única seguridad	No
Biométricos	Adivinaciones de contraseñas KeyLogger Fuerza Bruta	Alta Seguridad	Velocidad de Respuesta	Si
Click Pattern	Adivinaciones de contraseñas KeyLogger Fuerza Bruta	Implementación	Depende del hardware	No
Doble Factor	Fuerza Bruta Inyección SQL y Code KeyLogger	Alta Seguridad	Seguridad en el segundo factor	Si
Contraseña SMS	Phishing KeyLogger	Seguridad Transaccional	Retraso de la transacción móvil por la operadora	Si

2.5. Criptografía

La Criptografía guarda gran relación con la autentificación, según (Universidad Complutense de Madrid, 2016),para que un sistema se considere seguro, se debe tomar en cuenta los siguientes requerimientos que se muestran a continuación:

- La autentificación debe ser de cada parte.
- La confidencialidad de los datos.
- La integridad de datos.
- El no repudio

Para todo esto se utiliza la criptografía, se puede definir a la criptografía como aquel que se encarga de cifrar, siendo el cifrado el proceso de transformar un texto claro en texto codificado

2.5.1. Tokens

Los Tokens se refiere generalmente algo que el usuario posee y controla que puede hacer uso el usuario para verificar su identidad, siendo un factor importante que debe ser protegido ya sea esta un codigo alfabético, numero o alfanumérico, donde su autentificación en un sistema se realiza a través de la red, un ciberdelincuente podría robar la clave encriptada y encontrar la contraseña para usar el token.

En el campo criptográfico las tres principales funciones son MD4, MD5 y SHA, las cuales deben ser manejables pero incapaz de ser reversibles. Estos algoritmos tienen la capacidad de aceptar una entrada de longitud amplia y producir una salida fija de 64 bits.

2.5.2. Codigo QR

Un codigo QR (Quick Response) consiste en un sistema utilizado para almacenar en una matriz de puntos bidimensionales, este compuesto de 3 cuadrados que se encuentra en las esquinas que permiten detectar el codigo al lector. (García R. , 2020)

En la Figura 6 se muestra la estructura general de un codigo QR

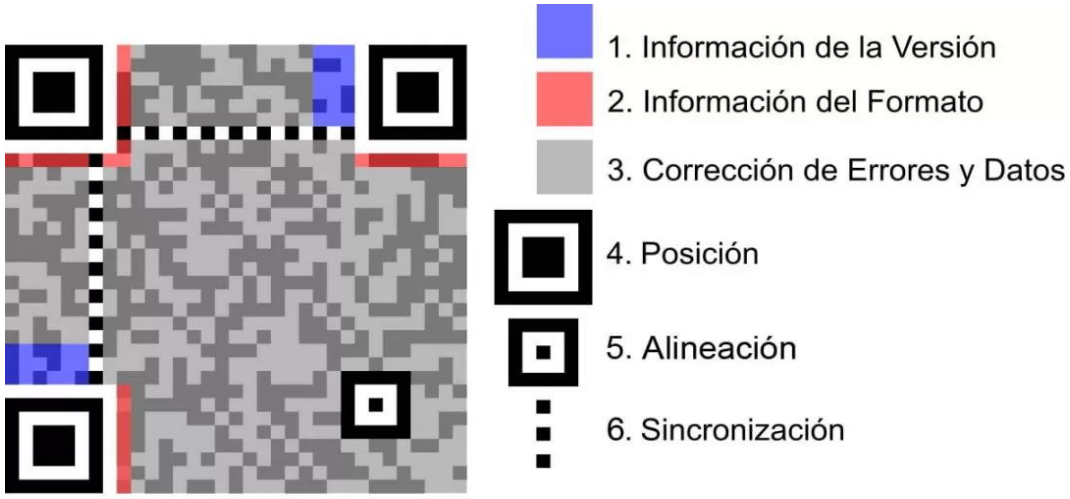

Figura 6: Estructura General de un Codigo QR
Fuente: Como funciona un codigo QR y Porque cada codigo es único (García R. , 2020)

2.6. Algoritmo TOTP

Como se dio a conocer en el apartado de Autentificación por Doble Factor la existencia del algoritmo TOTP, en el presente apartado se procede a detallar su funcionamiento, además de conceptos necesarios para su comprensión e implementación. El Algoritmo TOTP se considera una variante del algoritmo HOTP que se centra en el cálculo de un valor OTP en una representación de un contador incremental como un factor de tiempo (IETF- RFC, 2011).

Según los conceptos revisados con anterioridad se puede definir básicamente la fórmula del algoritmo TOTP de la siguiente manera:

$$T = \frac{Current\ Unix\ Time - T0}{X}$$

Donde:

X, representa el paso de tiempo en segundos y es un parámetro del sistema.

Siendo X= 30 por defecto;

T0, es el tiempo Unix para empezar a contar los pasos de tiempo.

Siendo T0 = 0 por defecto;

T, se define como un numero entero y representa el número de pasos entre T0 y el tiempo actual.

Se utiliza un redondeo hacia abajo por defecto. Por ejemplo, si T0=0, X=30, T=1, si el tiempo de UNIX es 59 segundos, y T=2 si el tiempo actual UNIX es de 60 segundo. El

algoritmo debe soportar un valor T mayor que un número entero de 32 bits, los valores de T0 y X son prestablecidos durante el proceso de aprovisionamiento y comunicación entre el usuario y el servidor.

2.6.1. Validación de un OTP

El OTP debe ser el mismo cuando sea generado y recibido por el servidor de validación por lo que el servidor ocupa un sello de tiempo para realizar la comparación, sin embrago se debe tener en cuenta las posibles latencias en la red, y otros margenes de errores de tiempo entre la generación y comparación de un OTP.

El tiempo de espera tiene un impacto muy profundo en la seguridad y usabilidad de un sistema de verificación, mientras más grande sea el tiempo de validación se arriesga a posibles ataques. Por lo que se recomienda un tiempo de 30 segundos por defecto y máximo uno de 60 segundos, debido a que el usuario debería esperar un tiempo prolongado para la obtención de un próximo OTP lo cual dificulta mucho la usabilidad del sistema al que requiere acceder.

Debido al desface de tiempo entre el reloj del usuario y el servidor de validación se puede recomendar que se ajuste un límite especifico al número de pasos que el usuario puede estar desincronizado antes de invalidar el OTP, este límite puede ser ajustado tanto hacia adelante como hacia atrás del tiempo OTP calculado.

2.6.2. Sistemas que Integran TOTP

Hoy en día existen varios sistemas que utilizan el algoritmo TOTP para su autentificación de usuarios, es decir que ocupan la autentificación por doble factor ocupando una contraseña estática y una dinámica y esta última basada en un tiempo determinado, con lo que la implementación del algoritmo TOTP en servicios empresariales es una realidad a continuación se mostrara algunas de estos sistemas:

- **Google Authenticator**

  Desarrollada por la gigante GOOGLE (Ramirez, 2019) es un software basada en la autenticación de un solo uso, ofreciendo un codigo numérico de 6 dígitos que el usuario debe proporcionar su información y credenciales, estos códigos se basan en los estándares “The Initiative for Open Authenticator” (OATH). Google Authenticator puede también generar códigos para terceros, generando una clave secreta de 80 bits para cada usuario, la cual se suministra como una cadena de 16 caracteres codificados en base32 o como un codigo QR.

En la Figura 7 se muestra la aplicación de Google Authenticator en la que se crea un mensaje codificado que sirve como clave secreta con una duración máxima de 30 y una disponibilidad máxima de 60 segundos.

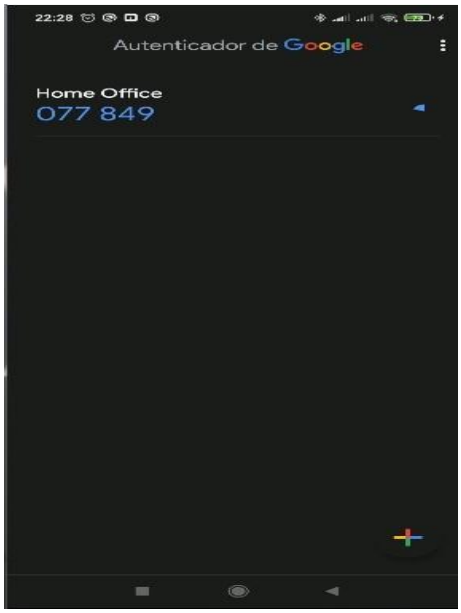

Figura 7: Aplicación Móvil Google Authenticator

- **Authy**

Según la página Oficial de Authy Permite que un cliente pueda gestionar cuentas de servicios online utilizando la autentificación por doble factor de una manera sencilla y con la capacidad de sincronización entre algunos dispositivos, tanto de manera online y offline, al ser una app compatible con varias plataformas como son Android, iOS, para acceder a los tokens de doble factor se debe activar la autentificación por medio de un codigo QR y activando la autentificación en la cuenta además de un condigo PIN o una contraseña.

En la Figura 8 se muestra como genera un codigo de 6 dígitos para un usuario, por medio de la aplicación Authy, el mismo que solo tiene una duración de 30 segundos.

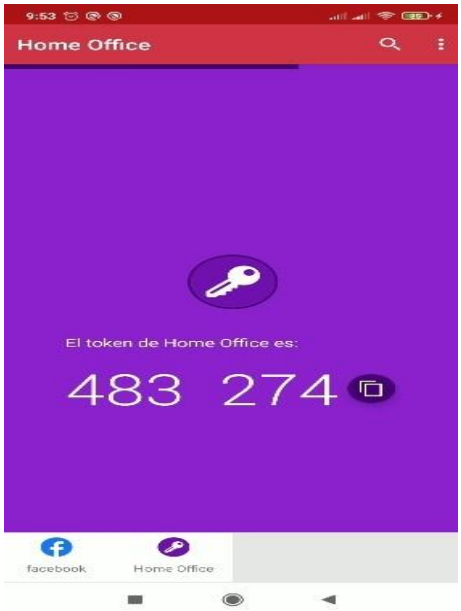

Figura 8: Autentificación de Doble Factor de la App Authy

2.7. Estándar de Calidad ISO 25010

Según el estándar de calidad ISO/IEC 25010 (ISO25000, 2015), tiene el objetivo de evaluar y determinar la excelencia de un software, para lo que en este modelo de evaluación determina por 8 características principales, cada una con sus respectivas métricas las cuales se listan a continuación. En la Tabla 2 se resume cada una de las características de la norma ISO 25010, tomando una breve descripción de cuál es su fin y enlistando cada una de sus subcaracterísticas de manera particular.

Tabla 2: Características de la Norma ISO 25010

Característica	*Descripción*	*Subcaracterística*
Adecuación Funcional	Representa la capacidad de un software para satisfacer las necesidades especificadas por el cliente	Completitud Funcional Corrección Funcional Pertinencia Funcional
Eficiencia de Desempeño	Representa el nivel efectivo de los recursos bajo determinadas condiciones	Comportamiento temporal Utilización de recursos Capacidad
Compatibilidad	Representa la habilidad que posee los sistemas o componentes de los mismos para intercambiar información o llevar a cabo una función determinada en el mismo ambiente	Coexistencia Interoperabilidad

Característica	*Descripción*	*Subcaracterística*
Usabilidad	Representa la habilidad que tiene el software para ser usado, entendido y usado por el usuario bajo determinadas condiciones	Capacidad para reconocer su adecuación Capacidad de aprendizaje Capacidad para ser usado Protección contra errores de usuario Estética de la Interfaz de usuario Accesibilidad
Fiabilidad	Representa la habilidad que posee el software en cumplir con funciones determinadas en un entorno controlado	Madurez Disponibilidad Tolerancia a Fallos Capacidad de recuperación
Seguridad	Representa la habilidad que posee el software en proteger la información hacia usuarios no autorizados	Confidencialidad Integridad No Repudio Responsabilidad Autenticidad
Mantenibilidad	Representa la habilidad que posee el software en adaptarse a los cambios en el transcurso del tiempo de manera eficiente	Modularidad Reusabilidad Analizabilidad Capacidad para ser modificado Capacidad para ser aprobado
Portabilidad	Representa la habilidad que posee el software para ser transferido a diferentes entornos de manera eficiente.	Adaptabilidad Capacidad para ser instalado Capacidad para ser reemplazado

CAPITULO III

METODOLOGIA

El desarrollo de la presente investigación contiene métodos y metodologías usadas dependiendo de cada una de las fases de la investigación, es así como se empleó un enfoque exploratorio revisando fuentes bibliográficas para la construcción del Marco Teórico, fue aplicada, pues, se requiero evaluar la seguridad del sistema informático. Es prospectivo porque se tomaron mediciones propias, las mismas que fueron medidas de manera transversal, puesto que, la investigación se lo realizo en un mismo lapso de tiempo, el estudio fue analítico, planteando una hipótesis que fue comprobada, además se ocupó el método Delphi, como técnica de investigación social con el objetivo de obtener una opinión grupal fidedigna a partir de un grupo de expertos, en este caso sirvió como herramienta para obtener información y determinar la calidad de la seguridad del sistema informático bajo el estándar ISO/IEC 25010.

3.1. Tipo y Diseño de la Investigación

3.1.1. Según la fuente

Investigación Bibliográfica: La información recolectada se basó en la consulta de artículos científicos, tesis, páginas web, guías oficiales, entre otros esto permitió conocer conceptos referentes al tema principal de investigación, factores para la implementación del concepto de doble factor y ataques informáticos, logrando tener una visión panorámica del tema.

3.1.2. Según el nivel de medición y análisis de la información

Investigación Mixta: Cuantitativa porque cuenta con las métricas de Seguridad de la norma ISO 25010 y Cualitativa porque se proporcionó una descripción correspondiente al cumplimiento de las métricas de seguridad de la norma ISO 25010.

3.1.3. Según el objeto de estudio

Investigación Aplicada: Con el conocimiento de las métricas de seguridad obtenidos de la norma ISO 25010, se demostró si se cumple con la calidad del módulo informático con respecto a la seguridad.

3.1.4. Según el tipo de Inferencia

Investigación Inductiva: A través de cada una de las métricas correspondiente a la categoría de seguridad perteneciente a la norma ISO 25010 se obtuvieron resultados específicos, los mismos que servirán dar formar una conclusión de manera general sobre la calidad del módulo informático.

3.2. Unidad de Análisis

Mediante el método Delphi se realizó un proceso de selección de 5 evaluadores también conocidos como expertos, quienes fueron los encargados de evaluar la calidad de la seguridad del software mediante las métricas ya establecidas en el estándar de calidad ISO 25010.

3.3. Población y Muestra

Para garantizar que la selección de los expertos sea la más eficiente se generaron criterios de formación académica tanto internos de la empresa Home Office S.A.S., como externos a la empresa. Los 3 expertos de la empresa Home Office S.A.S., del departamento de desarrollo y 2 expertos de distintos establecimientos educativos de educación superior en el área de informática, dando un total de 5 expertos.

3.4. Técnicas de Recolección de Datos

3.4.1. Encuestas

Se utilizaron encuestas para la evaluación de la seguridad del módulo informático, empleando un cuestionario basada en los criterios de evaluación dados por las subcaracterísticas de seguridad de la norma ISO 25010 hacia los expertos establecidos.

3.4.2. Entrevista

Se utilizo la entrevista con el objetivo de determinar los requerimientos para el desarrollo del módulo de informático, además de las tecnologías necesarias para el desarrollo del mismo, y finalmente se utilizó para la evaluación del funcionamiento del módulo de seguridad.

3.5. Técnicas de Análisis e Interpretación de la Información

Tras obtener la información de la entrevista se realizó un análisis para definir las directrices del desarrollo del proyecto, considerando las necesidades reales de seguridad informática de la empresa, además de la elección de los componentes necesarios para el correcto funcionamiento del aplicativo.

3.5.1. Norma Utilizada

- **ISO 25010:** Se aplica esta norma para medir la calidad en base a la seguridad del módulo por medio de un cuestionario

3.6. Desarrollo de la Investigación

3.6.1. Análisis de métodos para implementar factores de posesión en el proceso de Autentificación por Doble Factor

Mediante el análisis de la teoría se obtuvo que existen varios métodos y factores para la implementación en el proceso de la Autentificación por Doble factor (2FA), los cuales pueden variar según las necesidades de cada sistema de seguridad.

Para el caso de este módulo de seguridad informática se debe cumplir no solo un método de autentificación, sino por lo menos tener 2 métodos, debido a la calidad de información que se requiere para dicha entidad, además se debe considerar los recursos tanto informáticos como económicos que posee antes de la implementación de dichos métodos de autentificación.

3.6.1.1. Factores de Implementación para la Autentificación de Doble Factor para el Módulo de Seguridad Informática

Al analizar los recursos económicos, informáticos de la empresa Home Office S.A.S. se implementó la Autentificación por Doble Factor (2FA), en partes específicas del módulo de seguridad, teniendo en cuenta que se aplique no solo un factor en el proceso de Autentificación de Usuarios, además de la implementación de algunos otros métodos de autentificación en el sistema, En la Tabla 3 se muestra cada uno de los métodos de autentificación y en qué acción especifica fue implementada, además del recurso necesario para la implementación en cada acción.

Tabla 3: Factores y Métodos de Autenticidad Implementados

Factor	*Método de Autentificación*	*Acción*	*Recurso*
Captcha	Click Pattern	Registro de un nuevo Cliente	Google Captcha
Mail	Doble Factor	Activación de Cuenta de Cliente	Gmail
Captcha	Click Pattern / Doble factor	Inicio de Sesión	Google Captcha
QR	Doble Factor	Inicio de Sesión	Autenticador de Google (App Móvil)
Contraseña	Convencional	Inicio de Sesión	Base de datos

3.6.2. Desarrollo del Módulo de Seguridad Contra Ataques Informáticos

Para el desarrollo del módulo de seguridad se implementó la metodología cascada que consiste en 5 fases las cuales son: Análisis, Diseño, Desarrollo, Evaluación y Mantenimiento en este caso se desarrolló hasta la fase de Evaluación.

3.6.2.1. Fase de Análisis

Para este ciclo de la Ingeniería de Software se implementaron las siguientes etapas correspondientes a la fase de Análisis, los cuales se mencionan a continuación:

- **Roles de Usuarios**

  Para esta etapa se definieron un total de 3 roles para el sistema en general y el módulo de seguridad, los cuales son: Cliente, Administrador y Superadministrador.

- **Requerimientos Funcionales**

  Los requerimientos de funcionalidad fueron detallados en base a las necesidades de cada uno de los roles de los usuarios, se establece en general que el cliente tiene acceso solamente a su información personal, mientras que el Administrador tiene acceso al historial e información del Cliente y el Superadministrador tiene el acceso al historial tanto de Administradores y Clientes, además de la revisión de su información de los 2 últimos mencionados y finalmente acceso a los ataques detectados y neutralizados del sistema.

- **Requerimientos No Funcionales**

  Para los requerimientos no funcionales se tomaron en cuenta las siguientes métricas: Eficiencia, Usabilidad, Funcionalidad, Compatibilidad, Fiabilidad y

Seguridad, este último siendo de vital importancia para el desarrollo de la presente investigación.

- **Recursos Tecnológicos**

  Dentro de los recursos tecnológicos se estableció a Visual Studio Code como plataforma de desarrollo, a PHP y JavaScript como lenguajes de programación, y a MySQL como gestor de base de datos.

En el desarrollo de cada una de estas etapas se obtuvo una gran cantidad de información y datos, para ver toda la información ver Anexo I.

3.6.2.2. Fase de Diseño

Para este ciclo de la Ingeniería de Software se implementaron las siguientes etapas correspondientes a la fase de Diseño, los cuales son necesarios para la construcción del módulo de seguridad, los mismos que se enlistan a continuación:

- **Arquitectura de Software**

  Se ocupo el patrón MVC para el desarrollo arquitectónico del módulo de seguridad, debido a la facilidad de implementación en el sistema general, además de la experiencia ya desarrollando bajo este patrón.

- **Modelo Entidad Relación**

  Se utilizó el modelo Entidad Relación para evidenciar las atributos y relaciones de cada una de las entidades del Módulo de Seguridad, además sirvió como base para la construcción de los siguientes modelos y la base de datos final.

- **Modelo Relacional**

  Se utilizó el modelo relacional para la definición de datos y estructura ya formalizada del modelo Entidad Relación.

- **Diagrama de Casos de Uso**

  El modelo de caso de uso se ocupó para ver las acciones de cada uno de los usuarios en base a sus roles y requisitos funcionales ya definidos, el cual sirvió para el modelado de la Base de datos.

- **Modelo de Base de Datos.**

  Se realizo un modelo Final de Base de Datos tomando en cuenta todos los modelos y diagramas antes realizados para el desarrollo del módulo de seguridad.

- **Diccionario de Datos**

  En esta etapa se detalló cada uno de los datos utilizados para la creacion tablas, los mismos que sirvieron la correcta construcción de la base de datos, dado por cerrado la fase de Diseño del Módulo de Seguridad.

Para la visualización de cada una de estas etapas correspondientes a la fase de Diseño, ver Anexo II.

3.6.2.3. Fase de Desarrollo

De acuerdo a la información recolectada en cada fase desarrollada, se establece a Visual Studio Code como plataforma de desarrollo para el Módulo de Seguridad, a MySQL como gestor de base de datos y Apache como servidor web los dos por medio del programa XAMPP, y el patrón utilizado para construir el Módulo de Seguridad es el patrón MVC. Para la fase de Desarrollo se elaboró la Tabla 4, en la que se detalla cada una de las actividades realizadas durante esta fase, tomando en cuenta el tiempo y las tareas desarrolladas para la construcción del Módulo de Seguridad.

Tabla 4: Actividades para el Desarrollo del Módulo de Seguridad

ACTIVIDAD	*TAREA*
Elaboración de la estructura de las carpetas del Módulo de Seguridad	Creacion de las carpetas del Modelo: • "assets" (librerías) • "controller" (controladores) • "files" (archivos) • "model" (modelos) • "plugins" • "view" (vistas) Carga de librerías a la carpeta "assets" entre las cuales se carga los archivos CSS, Fuentes para el Bootstrap, la carpeta de imágenes para los logotipos, y las librerías para el uso de Javascript. Quedando estructurada de la siguiente manera: • "css" • "fonts" • "images" • "img" • "js" Carga de archivos a la carpeta "plugins", se cargaron las librerías de JavaScript para tablas, las fuentes e iconos para el módulo de seguridad, además de la librería de php Mailer para el envío de mensajes para el correo electrónico, y la librería de Captcha de Google.

ACTIVIDAD	*TAREA*
Elaboración del Archivo Index.php	Creacion del archivo Index.php Estructuración del patrón MVC para el funcionamiento del módulo de seguridad Pruebas del Archivo Index.php
Creacion del Archivo de Conexión	Creacion del archivo conexion.php Configuración del archivo conexión.php Pruebas de conectividad entre la aplicación y la base de datos
Creacion de las Clases Modelos del Módulo de Seguridad	Creacion del Archivo usuario.php Carga de atributos al archivo usuario.php Pruebas de funcionalidad del archivo usuario.php Creacion del Archivo genero.php Carga de atributos al archivo genero.php Pruebas de funcionalidad del genero.php Creacion del Archivo institucionbancaria.php Configuración del archivo institucionbancaria.php Carga de atributos al archivo institucionbancaria.php Pruebas de funcionalidad del institucionbancaria.php Creacion del Archivo país.php Carga de atributos al archivo país.php Pruebas de funcionalidad del país.php Creacion del Archivo tipocuenta.php Carga de atributos al archivo tipocuenta.php Pruebas de funcionalidad del tipocuenta.php
Creacion de las Vistas de las vistas principales del Módulo de Seguridad	Creacion de la vista de contacto.php Creacion de la vista footer.php Creacion de la vista header.php Creacion de la vista inicio.php Creacion de la vista suscribir.php
Creacion de las vistas de Usuarios Anónimos	Creacion de la vista y Validación de Campos con Javascript de la vista de registro.php Creacion de la vista y Validación de Campos con Javascript de la vista de login.php Creacion de la vista y Validación de Campos con Javascript de la vista de login-blocked.php Creacion de la vista y Validación de Campos con Javascript de la vista de recuperarpass1.php Creacion de la vista y Validación de Campos con Javascript de la vista de recuperarpass2.php Creacion de la vista y Validación de Campos con Javascript de la vista de recuperarpass3.php Creacion de la vista y Validación de Campos con Javascript de la vista de recuperarpass4.php Creacion de la vista y Validación de Campos con Javascript de la vista de recuperarpass5.php

ACTIVIDAD	*TAREA*
Creacion del Controlador de Usuario Anónimo	Creacion del archivo usuario.controller.php Creacion de Funciones del controlador Validación entre la Funciones la Base de Datos y las vistas del Usuario Anónimo Implementación del Captcha de Google en las vistas requeridas
Creacion de las vistas del Usuario Cliente	Creacion de la vista y Validación de Campos con Javascript de la vista de activación-usuario.php Creacion de la vista y Validación de Campos con Javascript de la vista de escoger-panel.php Creacion de la vista y Validación de Campos con Javascript de la vista de cliente-editar.php Creacion de la vista datos-bancarios.php Validación de Campos con Javascript de la vista de datos-bancarios.php Creacion de la vista y Validación de Campos con Javascript de la vista de hojavida.php Creacion de la vista y Validación de Campos con Javascript de la vista de chg_pass.php Creacion de la vista y Validación de Campos con Javascript de la vista de imagenperfil.php Creacion de la vista inicio.php Creacion de la vista registro-exitoso.php Creacion de la vista registro-incorrecto.php Creacion de la vista suscribir.php
Creacion del Controlador del Cliente	Creacion del archivo cliente.controller.php Creacion de Funciones del controlador Creacion de las Funciones de Cierre de Sesión por tiempo e historial Validación entre la Funciones la Base de Datos y las vistas del Usuario Cliente
Creacion de las vistas del Usuario Administrador	Creacion de la vista y Validación de Campos con Javascript de la vista de escoger-panel.php Creacion de la vista y Validación de Campos con Javascript de la vista de admin-editar.php Creacion de la vista y Validación de Campos con Javascript de la vista de datos-bancarios.php Creacion de la vista y Validación de Campos con Javascript de la vista de imagenperfil.php Creacion de la vista y Validación de Campos con Javascript de la vista de hojavida.php Creacion de la vista y Validación de Campos con Javascript de la vista de chg_pass.php Creacion de la vista y Validación de Campos con Javascript de la vista de clientes.php

ACTIVIDAD	*TAREA*
	Creacion de la vista y Validación de Campos con Javascript de la vista de clientesproblema.php Creacion de la vista y Validación de Campos con Javascript de la vista de verdatosbancarios.php Creacion de la vista y Validación de Campos con Javascript de la vista de verimagenperfil.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhojavida.php Creacion de la vista y Validación de Campos con Javascript de la vista de vercliente.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorial.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialdetallado.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialsesion.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialsesionp.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialproblema.php Creacion de la vista y Validación de Campos con Javascript de la vista de ataques.php Creacion de la vista y Validación de Campos con Javascript de la vista de ataquesin.php Creacion de la vista y Validación de Campos con Javascript de la vista de ataquesfb.php Creacion de la vista inicio.php
Creacion del Controlador del Administrador	Creacion del archivo admin.controller.php Creacion de Funciones del controlador Creacion de las Funciones de Cierre de Sesión por tiempo e historial Validación entre la Funciones la Base de Datos y las vistas del Usuario Administrador
Creacion de las vistas del Usuario SuperAdministrador	Creacion de la vista y Validación de Campos con Javascript de la vista de escoger-panel.php Creacion de la vista y Validación de Campos con Javascript de la vista de admin-editar.php Creacion de la vista y Validación de Campos con Javascript de la vista de datos-bancarios.php Creacion de la vista y Validación de Campos con Javascript de la vista de imagenperfil.php Creacion de la vista y Validación de Campos con Javascript de la vista de hojavida.php Creacion de la vista y Validación de Campos con Javascript de la vista de chg_pass.php Creacion de la vista y Validación de Campos con Javascript de la vista de clientes.php

ACTIVIDAD	*TAREA*
	Creacion de la vista y Validación de Campos con Javascript de la vista de clientesproblema.php Creacion de la vista y Validación de Campos con Javascript de la vista de verdatosbancarios.php Creacion de la vista y Validación de Campos con Javascript de la vista de verimagenperfil.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhojavida.php Creacion de la vista y Validación de Campos con Javascript de la vista de vercliente.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorial.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialdetallado.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialsesion.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialsesionp.php Creacion de la vista y Validación de Campos con Javascript de la vista de verhistorialproblema.php Creacion de la vista y Validación de Campos con Javascript de la vista de ataques.php Creacion de la vista y Validación de Campos con Javascript de la vista de ataquesin.php Creacion de la vista y Validación de Campos con Javascript de la vista de ataquesfb.php Creacion de la vista inicio.php Creacion de la vista y Validación de Campos con Javascript de la vista de registraradmin.php Creacion de la vista admins.php Creacion de la vista y Validación de Campos con Javascript de la vista de admins.php Creacion de la visa y Validación de Campos con Javascript de la vista de adminsb.php Creacion de la vista y Validación de Campos con Javascript de la vista de veradmindatosbancarios.php Creacion de la vista y Validación de Campos con Javascript de la vista de veradminimagenperfil.php Creacion de la vista y Validación de Campos con Javascript de la vista de veradminhojavida.php Creacion de la vista y Validación de Campos con Javascript de la vista de veradmin.php Creacion de la vista y Validación de Campos con Javascript de la vista de veradminhistorial.php Creacion de la vista y Validación de Campos con Javascript de la vista de veradminhistorialdetallado.php Creacion de la vista y Validación de Campos con Javascript de la vista de veradminhistorialsesion.php

ACTIVIDAD	*TAREA*
Creacion del Controlador del Administrador	Creacion del archivo superadmin.controller.php Creacion de Funciones del controlador Creacion de las Funciones de Cierre de Sesión por tiempo e historial Validación entre la Funciones la Base de Datos y las vistas del Usuario SuperAdministrador
Creacion del Archivo httaccess	Creacion del archivo .httaccess Creacion de las vistas de Errores

3.6.2.4. Fase de Evaluación

Para la evaluación del módulo de seguridad se realizaron encuestas y entrevistas acerca de la funcionalidad con las que cuenta el módulo de seguridad hacia el personal de desarrollo de la empresa Home Office S.A.S, además de la evaluación de los requerimientos No Funcionales sin tomar en cuenta la Seguridad. Ver Anexo III y IV.

3.6.3. Integración del Proceso de Autentificación de Doble Factor al Módulo de Seguridad

Para el proceso de integración de la autentificación al módulo de seguridad se utilizó el codigo QR y la aplicación Google Authenticator, generando un codigo de 6 dígitos con la duración de 30 segundos y un máximo de disponibilidad de 60 segundos, integrado entre el proceso de autentificación de usuario y el ingreso a su respectivo panel, generando por cada usuario un codigo y mostrando su nombre registrado en la aplicación.

3.6.3.1. Evaluación de la Seguridad del Módulo Informático

Finalmente, mediante el método Delphi se procedió a la evaluación del módulo de seguridad para la cual se realizaron dos encuestas para la toma de información. Las cuales mediante técnicas de análisis e interpretación de datos permitió evaluar la calidad de la seguridad del módulo de informático bajo las métricas recomendadas por la norma ISO 25010. Ver Anexos VI, VII y VIII.

CAPITULO IV

RESULTADOS Y DISCUSION

4.1. Aplicación de la metodología de Evaluación

Para la aplicación de la metodología de evaluación se utilizó una encuesta basada en las subcategorías de Seguridad, correspondiente a la norma ISO 25010. Se definieron un grupo de preguntas basadas en el enfoque GQM (Goal, Question, Metric), siendo este método orientado a determinar una métrica que evalué un objetivo determinado, los mismos que consecuentemente mediante conectores lógicos mostrara la satisfacción de los objetivos planteados (Calabrese & Pesado, 2017). Ver Anexo VI. Para la evaluación del módulo de seguridad se tomó como base el artículo "Asistente para la evaluación de características de calidad de producto de software propuestas por ISO/IEC 25010 basado en métricas definidas usando el enfoque GQM".

4.1.1. Descripción de los Criterios de Evaluación

Para el análisis de los resultados se establecieron una serie de criterios de evaluación basados en las subcategorías de la métrica de seguridad correspondiente a la norma ISO 25010 y el articulo "Asistente para la evaluación de características de calidad de producto de software propuestas por ISO/IEC 25010 basado en métricas definidas usando el enfoque GQM", elaborado por (Calabrese & Pesado, 2017). En la Tabla 5, se establece cada criterio en base a las preguntas establecidas en el cuestionario de evaluación, obteniendo la formula y la equivalencia de cada uno de los valores representados en puntos.

Tabla 5: Descripción de Criterios de Evaluación

ID	*Nombre*	*Descripción*	*Formula*	*Ptos.*
C-1	Conexiones Seguras	Se considera una conexión segura si cuenta con certificado HTTPS y si no redirige hacia sitios inseguros	P5 & ~P12 = V	**1**
C-2	Control de Acceso	El sistema debe ser capaz de contralar el acceso a funcionalidades, base de datos, codigo de la aplicados, servidores solo a personal autorizado	P7 | P8 | P9 | P10 | P11 | P22 = F	**1**
C-3	Encriptación de datos	Por lo menos debe existir algún dato importe encriptado dentro de la base de datos	P6 = V	**1**

ID	*Nombre*	*Descripción*	*Formula*	*Ptos.*
C-4	Contraseña de bajo nivel	La contraseña se considera de bajo nivel si posee menos de 7 caracteres, no posee letras mayúsculas y minúsculas, no posee letras y números	P1 | P2 | P3 | P4 = F	**0**
	Contraseña de nivel medio	La contraseña se considera de nivel medio si posee al menos 7 caracteres o letras y mayúsculas y minúsculas o letras y números	P1 | P2 | P3 | P4 = V	**0.5**
	Contraseña de alto nivel	La contraseña se considera de alto nivel si posee al menos 7 y menos de 15 caracteres, con letras minúsculas y mayúsculas y números	P1 & P2 & P3 & P4 = V	**1**
I-5	Prevención de Accesos	El sistema debe ser capaz de prevenir el acceso a base de datos, acceso de codigo, funcionalidades especificas a personal no autorizado, además que no se permitan inyecciones de Javascript y/o de SQL	P7 | P8 | P9 | P16| P21 = F	**1**
I-6	Prevención de Modificaciones	Se debe establecer que no se altere el codigo del sistema sin una autorización establecida	P14 | P15 = F	**1**
I-7	Confirmación de datos	Se debe efectuar una revalidación de los datos del registro por medio de un mail	P13 = V	**1**
NR-8	Operaciones Realizadas	Se debe contar con un historial de antecedentes de acciones realizadas e informar del inicio de sesión por mail, además de poseer un cierre forzado en el caso de un determinado tiempo de no uso del sistema o luego de finalizar la sesión	P17 & P25 | P26 = V	**1**
NR-9	Mecanismo de Cifrado	Se debe implementar métodos de encriptación ya sea por algoritmos o mecanismos criptográficos	P18 | P19 = V	**1**
NR-10	Verificación de Acciones	Se debe requerir una validación de los datos antes de realizar una determinada acción	P20 = V	**1**
R-11	Registro de Acciones y Datos	Se debe tener un expediente de las acciones realizadas, un registro por hora y fecha o capturar el direccionamiento IP desde que se ingresa al sistema	P17 | P27 | P28 = V	**1**
R-12	Detección de Posibles Ataques	Se debe llevar un registro de los posibles ataques realizados, detectándolos y neutralizándolos y guardando los datos causantes de los mismos	P23 & P24 = V	**1**
A-13	Comprobación de Identidad	El sistema debe ejecutar una verificación de identidad mediante cualquiera de los siguientes métodos: datos biométricos, Captchas, QR	P29 | P32 | P33 | P35 = V	**1**
A- 14	Comprobaciones adicionales	Se debe contar con un sistema de autentificación en dos pasos,	P13 | P30 | P31 | P34 = V	**1**

ID	*Nombre*	*Descripción*	*Formula*	*Ptos.*
		aplicaciones externas de autentificación o se debe recurrir a una clave de segundo nivel para el ingreso al sistema o confirmación del registro mediante un mail		

4.1.2. Métricas de Evaluación para las Subcategoría

Se combinaron los criterios de evaluación establecidos con anterioridad para definir las métricas con el fin de satisfacer los objetivos de cada una de las subcategorías. En la Tabla 6 se definió un nombre, un propósito y el método de aplicación de cada una de las métricas, en el cual se establece las fórmulas y los criterios de evaluación.

Tabla 6: Métricas de Evaluación para las Subcategorías

Métrica	*Propósito*	*Método de Aplicación*	*Formula*
Confidencialidad	Medir que tan eficiente es el sistema al momento de proteger el acceso a los datos contra personal no autorizado ya sea en condiciones de experimentación o reales	Se debe contestar los Criterios de Evaluación correspondientes a la característica de "Confidencialidad", y luego obtener su media aritmética	X = (C-1+C-2+ C-3+C-4) / 4
Integridad	Medir la capacidad que posee el sistema para prevenir los accesos o modificaciones no autorizadas hacia los datos y/o componentes del mismo	Se debe contestar los Criterios de Evaluación correspondientes a la característica de "Integridad", y luego obtener su media aritmética	X = (I-5+I-6+I-7) / 3
No Repudio	Medir la capacidad que tiene el sistema en demostrar que acciones o eventos han sido realizado, de manera que tales hechos no puedan ser repudiados anteriormente	Se debe contestar los Criterios de Evaluación correspondientes a la característica de "No Repudio", y luego obtener su media aritmética	X = (NR-8+NR-9+NR-10) / 3
Responsabilidad	Medir la capacidad que tiene el sistema en rastrear de manera correcta y sin equivocaciones las acciones realizadas por una determinada entidad	Se debe contestar los Criterios de Evaluación correspondientes a la característica de "Responsabilidad", y luego obtener su media aritmética	X = (R-11+R-12) / 2

Métrica	*Propósito*	*Método de Aplicación*	*Formula*
Autenticidad	Medir la capacidad que tiene el sistema en identificar y validar a un usuario del sistema o algún recurso definido	Se debe contestar los Criterios de Evaluación correspondientes a la característica de "Autenticidad", y luego obtener su media aritmética	X = (A-13+A-14) / 2

4.2. Aplicación del Método Delphi para la Evaluación del Módulo de Seguridad

Para la aplicación del Método Delphi se utilizaron 2 ciclos del proceso de evaluación en los que se realizaron una encuesta a cada una de los expertos, con el fin de cumplir en su totalidad cada una de las métricas de seguridad dadas por la norma ISO 25010, Ver Anexos VII y VIII.

4.2.1. Análisis e Interpretación de Datos

Para el análisis e interpretación de datos se utilizó la metodología descrita con anterioridad a cada una de las encuestas realizadas a los evaluadores, los resultados se encuentran detallados en el Anexo IX.

4.2.1.1. Primer Ciclo de Evaluación

En este primer ciclo de evaluación se tomó el módulo de seguridad sin la implementación de la Autentificación por Doble Factor, en el cual no se implementó ningún factor de autentificación externa al propio modulo ya implementado.

Tabla 7: Criterios de Evaluación del Primer Ciclo de Evaluación

ID	*Nombre*	*Valor Obtenido del Primer Evaluador*	*Valor Obtenido del Segundo Evaluador*	*Valor Obtenido del Tercer Evaluador*	*Valor Obtenido del Cuarto Evaluador*	*Valor Obtenido del Quinto Evaluador*
C-1	Conexiones Seguras	**0**	**0**	**1**	**0**	**0**
C-2	Control de Acceso	**1**	**1**	**1**	**1**	**1**
C-3	Encriptación de datos	**1**	**1**	**1**	**1**	**1**
C-4	Contraseña de alto nivel	**1**	**1**	**1**	**1**	**1**

ID	*Nombre*	*Valor Obtenido del Primer Evaluador*	*Valor Obtenido del Segundo Evaluador*	*Valor Obtenido del Tercer Evaluador*	*Valor Obtenido del Cuarto Evaluador*	*Valor Obtenido del Quinto Evaluador*
I-5	Prevención de Accesos	**1**	**1**	**1**	**1**	**1**
I-6	Prevención de Modificaciones	**1**	**1**	**1**	**1**	**1**
I-7	Confirmación de datos	**1**	**1**	**1**	**1**	**1**
NR-8	Operaciones Realizadas	**1**	**1**	**1**	**1**	**1**
NR-9	Mecanismo de Cifrado	**1**	**1**	**1**	**1**	**1**
NR-10	Verificación de Acciones	**1**	**0**	**1**	**1**	**0**
R-11	Registro de Acciones y Datos	**1**	**1**	**1**	**1**	**1**
R-12	Detección de Posibles Ataques	**1**	**1**	**1**	**1**	**1**
A-13	Comprobación de Identidad	**0**	**0**	**0**	**0**	**0**
A- 14	Comprobaciones adicionales	**1**	**1**	**1**	**1**	**1**

Tabla 8: Cumplimiento de las Métricas de Seguridad Primera Evaluación

Métrica	*Porcentaje de Cumplimiento de cada Métrica*				
	Primer Evaluador	*Segundo Evaluador*	*Tercer Evaluador*	*Cuarto Evaluador*	*Quinto Evaluador*
Confidencialidad	75%	75%	100%	75%	75%
Integridad	100%	100%	100%	100%	100%
No Repudio	100%	67%	100%	100%	67%
Responsabilidad	100%	100%	100%	100%	100%
Autenticidad	50%	50%	50%	50%	50%

Análisis: En la tabla 8 se evidencia el cumplimento de cada una de las métricas de seguridad en el primer ciclo de evaluación, en el que se muestra que apenas dos métricas son cumplidas a cabalidad. En la métrica de Confidencialidad existe un cumplimento en general del 75%, siendo el 25% restante debido a la falta de seguridad en el

redireccionamiento de sitos seguros, en la métrica de No Repudio existe una discrepancia entre los evaluadores siendo en el peor de los casos una falta del 33% de cumplimento en esta métrica, dado a la falta de verificación de los datos al realizar una acción. Finalmente, en la métrica de Autenticidad existe apenas un 50% de cumplimento de la métrica debido a que no existe ningún tipo de autentificación externa por parte del módulo informático.

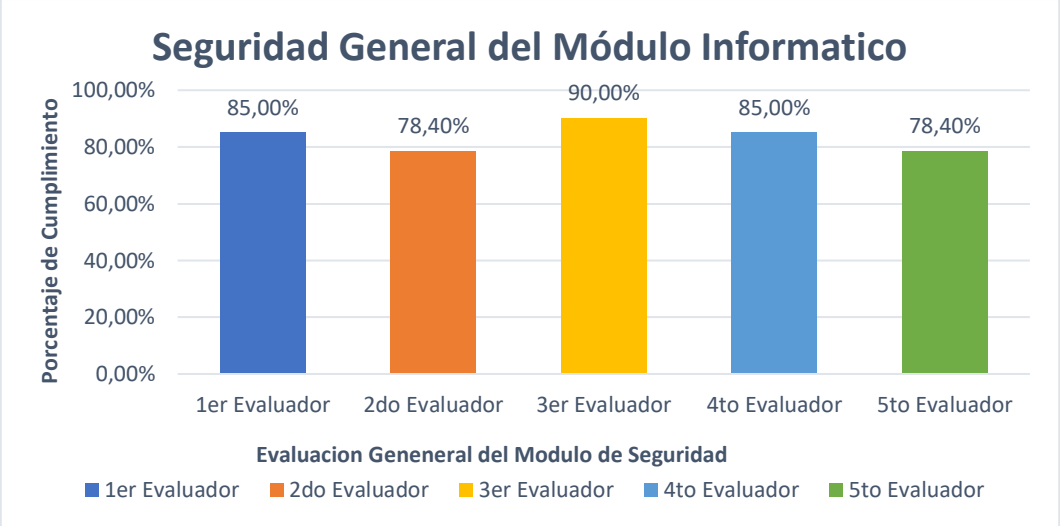

Figura 9: Seguridad General del Módulo Informático

Análisis: En la figura 9 se muestra el cumplimiento promedio de cada una de las métricas según el criterio de evaluación de cada experto, en el cual se evidencia que la seguridad general del módulo informático se encuentra en un mínimo del 78.40% y en un máximo del 90.00%, siendo el módulo informático altamente aceptable según la norma ISO 25010, debido a que un cumplimento inferior al 60% ya se considera un módulo inseguro.

4.2.1.2. Segundo Ciclo de Evaluación

En este segundo ciclo de evaluación se tomó el módulo de seguridad con la implementación de la Autentificación por Doble Factor, además de mejorar el cumplimiento de varias métricas vistas en el anterior ciclo de evaluación.

Tabla 9: Criterios de Evaluación del Segundo Ciclo de Evaluación

ID	*Nombre*	*Valor Obtenido del Primer Evaluador*	*Valor Obtenido del Segundo Evaluador*	*Valor Obtenido del Tercer Evaluador*	*Valor Obtenido del Cuarto Evaluador*	*Valor Obtenido del Quinto Evaluador*
C-1	Conexiones Seguras	**1**	**1**	**1**	**1**	1
C-2	Control de Acceso	**1**	**1**	**1**	**1**	**1**
C-3	Encriptación de datos	**1**	**1**	**1**	**1**	**1**
C-4	Contraseña de alto nivel	**1**	**1**	**1**	**1**	**1**
I-5	Prevención de Accesos	**1**	**1**	**1**	**1**	**1**
I-6	Prevención de Modificaciones	**1**	**1**	**1**	**1**	**1**
I-7	Confirmación de datos	**1**	**1**	**1**	**1**	**1**
NR-8	Operaciones Realizadas	**1**	**1**	**1**	**1**	**1**
NR-9	Mecanismo de Cifrado	**1**	**1**	**1**	**1**	**1**
NR-10	Verificación de Acciones	**1**	**1**	**1**	**1**	**1**
R-11	Registro de Acciones y Datos	**1**	**1**	**1**	**1**	**1**
R-12	Detección de Posibles Ataques	**1**	**1**	**1**	**1**	**1**
A-13	Comprobación de Identidad	**1**	**1**	**1**	**1**	**1**
A- 14	Comprobaciones adicionales	**1**	**1**	**1**	**1**	**1**

Tabla 10: Cumplimiento de las Métricas de Seguridad Segunda Evaluación

Métrica	*Porcentaje de Cumplimiento de cada Métrica*				
	Primer Evaluador	*Segundo Evaluador*	*Tercer Evaluador*	*Cuarto Evaluador*	*Quinto Evaluador*
Confidencialidad	100%	100%	100%	100%	100%
Integridad	100%	100%	100%	100%	100%
No Repudio	100%	100%	100%	100%	100%

Métrica	*Porcentaje de Cumplimiento de cada Métrica*				
	Primer Evaluador	***Segundo Evaluador***	***Tercer Evaluador***	***Cuarto Evaluador***	***Quinto Evaluador***
Responsabilidad	100%	100%	100%	100%	100%
Autenticidad	100%	100%	100%	100%	100%

Análisis: En la tabla 10 se evidencia el cumplimento total de cada una de las métricas recomendadas por la norma ISO 25010, según los resultados obtenidos, la implementación de factores de autentificación externas mejora en el cumplimento de todas las métricas, la métrica de Autenticidad es la más afectada pasando de un 50% a 100%, esto debido a la implementación de la autenticidad por Doble Factor.

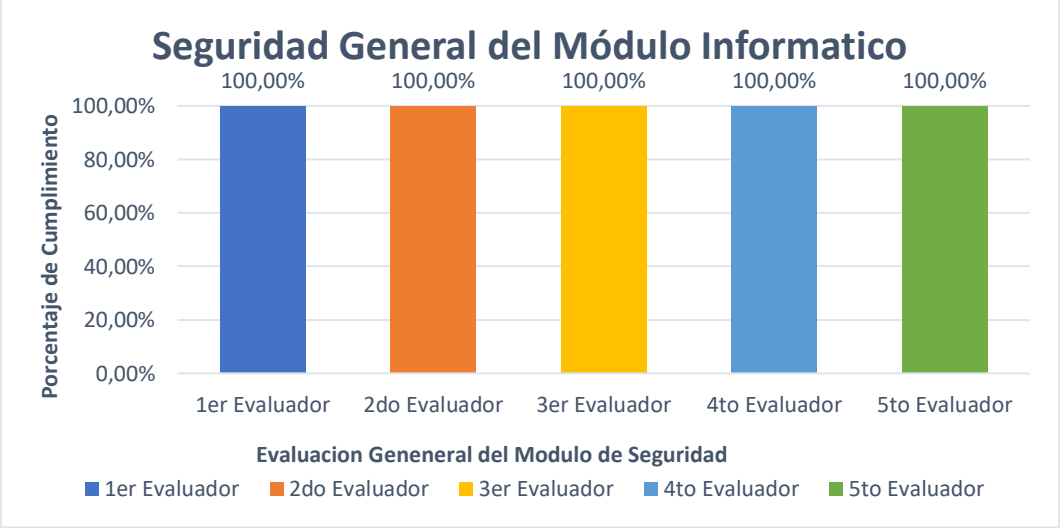

Figura 10: Seguridad General del Módulo Informático

Análisis: En la figura 10, se muestra el promedio de cumplimiento de cada uno de las métricas de seguridad según los evaluadores, en el que se evidencia que la implementación de métodos de autentificación y en especial la autentificación por doble factor mejora la seguridad general del módulo informático, dando un nivel de satisfacción total del cumplimiento de las normas ISO 25010.

4.2.2. Resultados Finales según cada métrica

Para los resultados finales se analizó cada una de las métricas de seguridad, tomando en cuenta los dos ciclos de evaluación realizado por los expertos para definir una opinión general de cada una de las métricas de seguridad.

4.2.2.1. Análisis de la Métrica de Confidencialidad

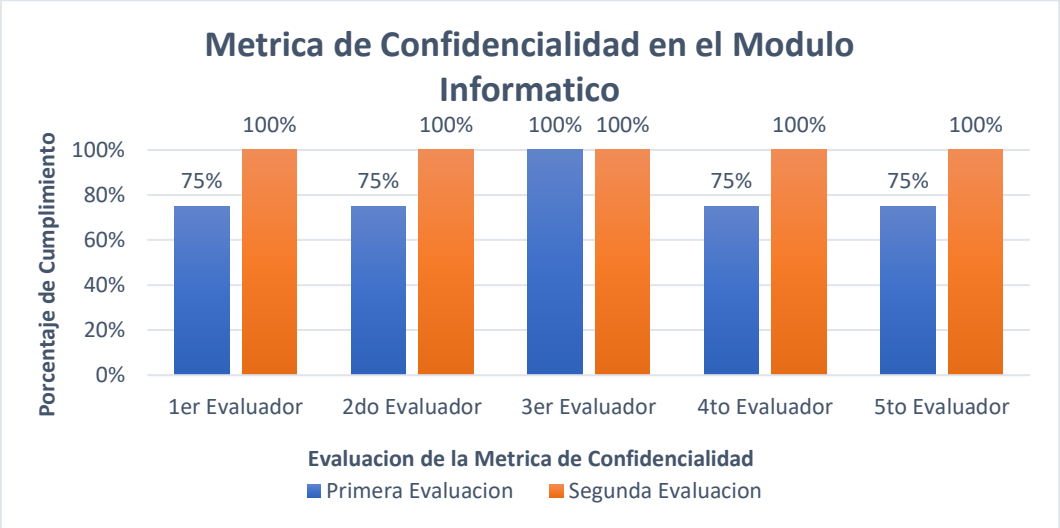

Figura 11: Análisis de la Métrica de Confidencialidad

Análisis: En la figura 11, se evidencia la diferencia existente entre los dos ciclos de evaluación, dando como resultado una diferencia del 25% del cumplimiento de esta métrica, dicha diferencia es debido a la falta de factores de autenticación externa para el redireccionamiento a otras páginas web.

4.2.2.2. Análisis de la Métrica de Integridad

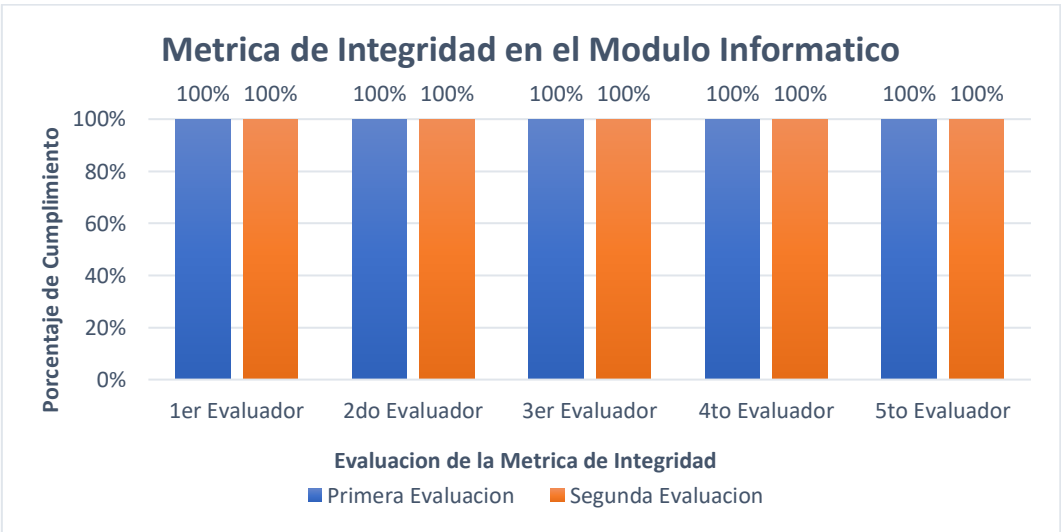

Figura 12: Análisis de la Métrica de Integridad

Análisis: En la figura 12, se evidencia el cumplimiento total de la métrica en sus dos ciclos de evaluación, esto se debido al cumplimiento total de los requerimientos establecidos en el módulo de seguridad tanto funcionales como no funcionales, por lo que

se mantiene que el acceso exclusivo a funcionalidades según el rol, la seguridad del codigo fuente y finalmente la confirmación de identidad por medio de un mensaje de correo electrónico al momento de registrase en el sistema.

4.2.2.3. Análisis de la Métrica de No Repudio

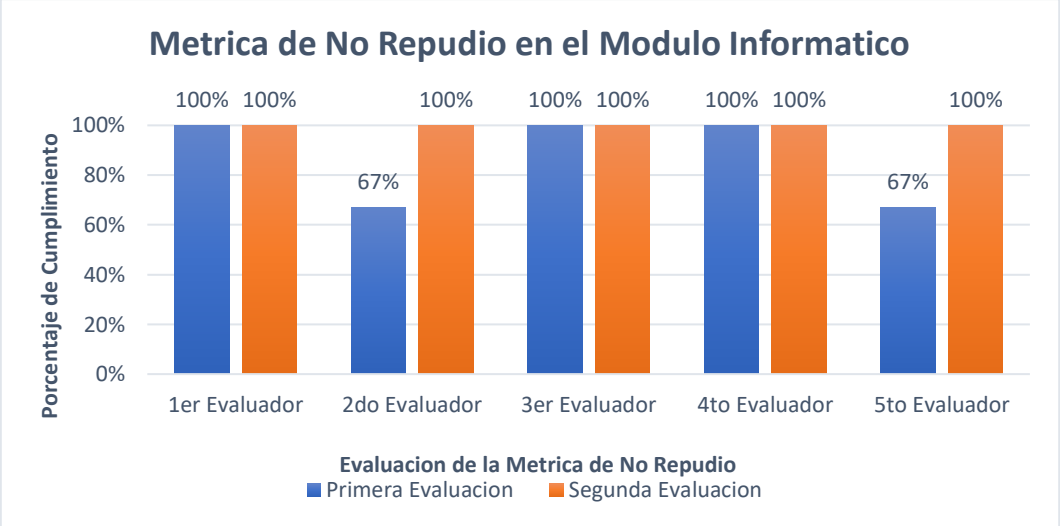

Figura 13: Análisis de la Métrica de No Repudio

Análisis: En la figura 13, se evidencia la diferencia existente entre los dos ciclos de evaluación, dando como resultado una diferencia del 33% del cumplimiento de esta métrica, dicha diferencia es debido a falta de verificación de los datos al realizar una acción, la misma que se resuelve al implementar factores de validación externos al sistema.

4.2.2.4. Análisis de la Métrica de Responsabilidad

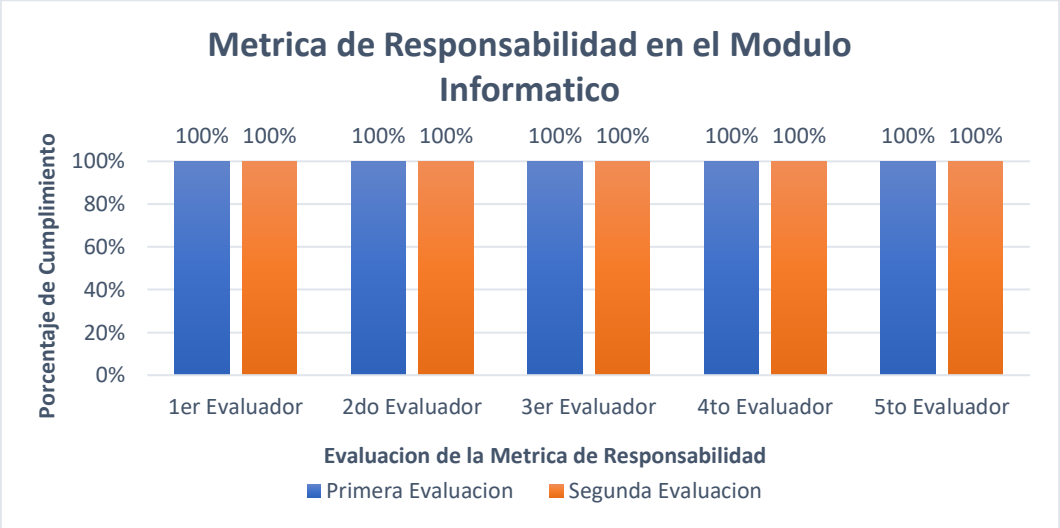

Figura 14: Análisis de la Métrica de Responsabilidad

Análisis: En la figura 14, no se evidencia la diferencia entre la primera y segunda evaluación, debido que desde la primera evaluación existió un acatamiento del 100%, esto es debido a dos componentes indispensables en el modulo informático los cuáles son la capacidad de detectar y neutralizar posibles ataques informáticos y el de llevar un historial de laca acción realizada por los usuarios del sistema, en el que se fomenta el control de lado del sistema y del cliente por igual.

4.2.2.5. Análisis de la Métrica de Autenticidad

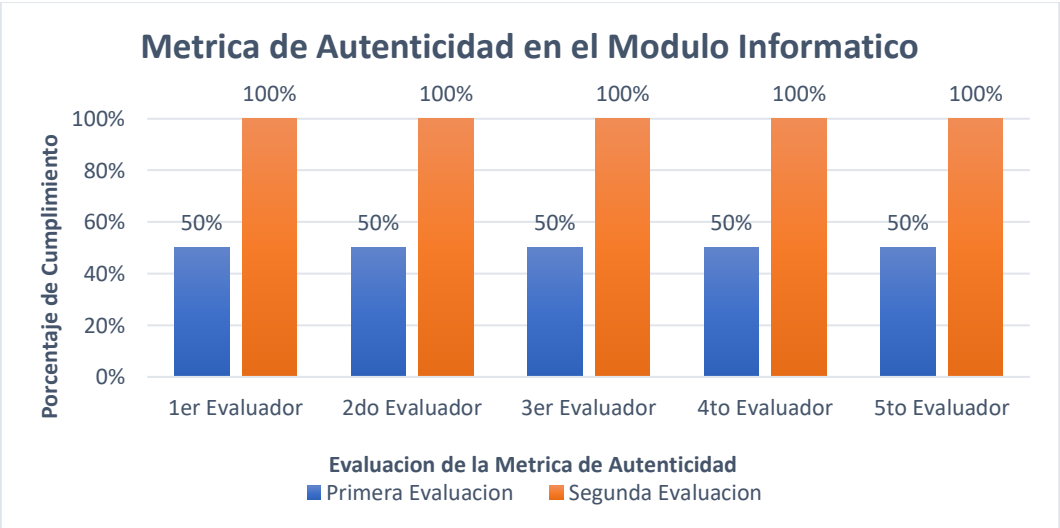

Figura 15: Análisis de la Métrica de Autenticidad

Análisis: En la figura 15, se evidencia la diferencia entre la primera y segunda evaluación, en la que se muestra una notable diferencia entre ambos ciclos pasando del 50% al 100% en el cumplimiento de esta métrica, el gran cambio se da debido a la implementación de la Autentificación por Doble Factor y métodos de autenticidad externas a la propia aplicación.

4.3. Resultado Final del Módulo de Seguridad

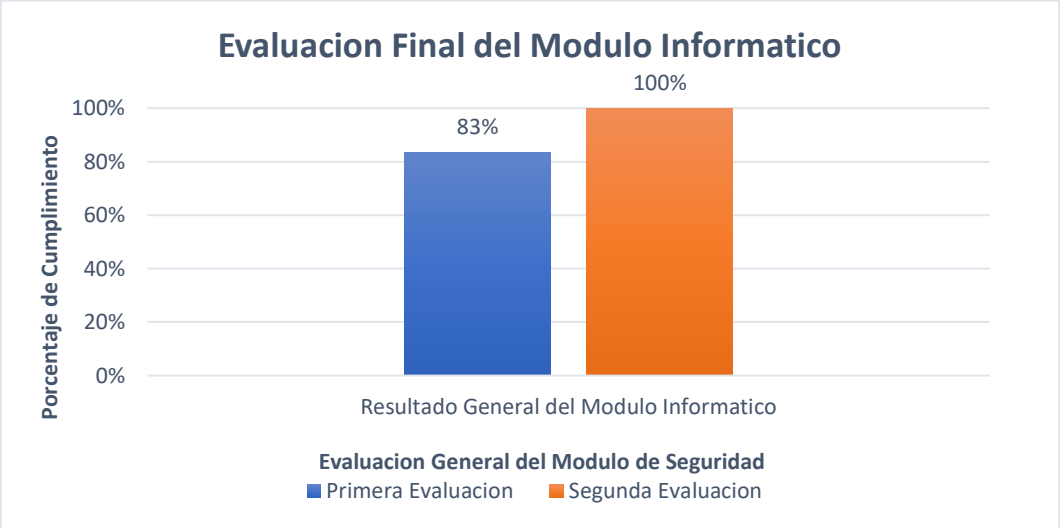

Figura 16: Análisis General del Módulo de Seguridad Informática

Análisis: En la figura 16, se muestra la diferencia que existe entre los dos ciclos de evaluación, demostrando que en la primera evaluación existe un cumplimento del 83% y luego de la implementación del doble factor aumento a un cumplimiento del 100%. Entre estos dos ciclos existe una diferencia del 17%, dicha diferencia en términos generales no es muy notoria, pero al revisar cada una de las métricas, se muestra que la implementación de métodos de autentificación externas mejora la seguridad de todas las métricas y en especial la métrica de Autenticidad.

CONCLUSIONES

Los sistemas informáticos, con sus respectivos usuarios se encuentran en un gran peligro debido al incremento de ciberdelincuentes y a los métodos de robo de contraseñas y de suplantación de identidad, además de las múltiples formas de realizar un ataque informático directo al sistema. Todo sistema informático debe ser capaz de neutralizar y detectar ataques, deben incluir varios métodos de autentificación tanto externas como internas, además de un historial de cada acción realizadas por sus múltiples usuarios y finalmente debe tener algoritmos de encriptación y cifrado de datos.

Para la Autentificación por Doble Factor existen varios métodos para llevarla a cabo donde, cada uno de ellos posee una serie de factores, los mismos que todos pueden ser utilizados dependiendo de las necesidades del sistema informático y de los recursos disponibles para el mismo, siendo el presupuesto uno de los factores fundamentales para la implementación de cada uno, la implementación de Captchas, contraseña convencional, y codigo QR desde una aplicación externa son los más utilizados, debido a su facilidad de implementación, costo muy bajo y facilidad de uso tanto para el usuario como para el sistema.

El módulo de seguridad permite llevar un registro de usuarios con sus respectivos datos y roles, por lo que dependiendo del rol puede acceder a distintas funcionalidades del mismo, cada usuario posee un historial de cada una de las acciones realizadas además de un bloqueo en el caso de no cumplir las condiciones correctas al momento de ingresar y actualizar su información. El ingreso del sistema cuenta con una autentificación de doble factor, la primera cuenta con una contraseña y un Captcha, mientras que el segundo cuenta con un codigo QR y la aplicación Google Authenticator. Finalmente se da una comprobación de inicio de sesión por medio de un mensaje de correo electrónico al usuario. El módulo de seguridad posee un historial con los datos más relevantes de los ataques informáticos que detecto y neutralizo.

Para la evaluación del módulo de seguridad informática se utilizó las métricas de la categoría de seguridad recomendada por la norma ISO 25010, de acuerdo al criterio para

el análisis de la seguridad se establece que solamente cuando este cumplidas todas las métricas al 100 % se definirá al módulo de seguridad como seguro. A través del análisis de seguridad por medio del Método Delphi permitió evaluar el módulo de seguridad en dos ciclos, el primero sin contar con la autentificación por doble factor obteniendo un porcentaje de aceptación del 83% en general, mientras que en el segundo ciclo se implementó la autentificación de doble factor dando como resultado el acatamiento del 100% de cada una de las métricas dando un porcentaje de aceptación del 100%, evidenciado que la implementación de la Autenticación por doble Factor mejora la seguridad informática del sistema y por lo tanto mejora la seguridad informática de la empresa Home Office .S.A.S.

RECOMENDACIONES

Para el uso del módulo de seguridad es necesario una fuerte infraestructura de servidores y de red, debido a las múltiples peticiones realizadas al momento del proceso de Autentificación del Sistema, se recomienda incorporar protocolos de seguridad a nivel de red para fortalecer al sistema no solo a nivel de software.

Analizar los beneficios de la implementación de la autentificación de doble factor con datos biométricos para el desarrollo de una app móvil manteniendo la misma estructura desarrollada con sus respectivas validaciones por parte del servidor y cliente.

En el desarrollo de aplicaciones web y móviles es recomendable utilizar un controlador de versiones en este caso GitHub, debido a que permite a los desarrolladores aportaciones de codigo fuente y registrar un historial en los cambios de cada version, además de ser compatible con distintos sistemas operativos y soportar varios lenguajes de programación.

REFERENCIAS BIBLIOGRAFICAS

Alegre, M., & Garcia, A. (2011). *Seguridad Informatica.* Madrid, España: Paraninfo.

Altamirano, J. (2017). Politicas de Segurdad de la Informacion: Revision Sistematica de las Teorias que explican su Cumplimiento. *REVISTA IBERICA DE SISTEMAS E TECNOLOGIAS DE INFORMACAO*, 112-134.

Alzahrani, A. (2018). Useable Authentication Mechanisms for Secure Online Banking. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*.

Areitio, J., & Areitio, M. (2007). Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación. *Revista española de electrónica (Dialnet)*, 52-67. Obtenido de https://www.redeweb.com/_txt/630/52.pdf

Buccafurri, F., & Nardone, R. (03 de Abril de 2020). Securing MQTT by Blockchain-Based OTP Authentication. *MDPI, 20*(7). doi:https://doi.org/10.3390/s20072002

Calabrese, J., & Pesado, P. (2017). *Asistente para la evaluación de características de calidad de producto de software propuestas por ISO/IEC 25010 basado en métricas definidas usando el enfoque GQM.* Universidad Nacional de La Plata, Facultad de Investigacion en Informatica. La Plata: Centro Asociado Comisión de Investigaciones Científicas de la Pcia. de Bs. As. (CIC). Recuperado el 11 de Enero de 2021

Cañón, L. (2015). *ATAQUES INFORMÁTICOS, ETHICAL HACKING Y CONCIENCIA DE SEGURIDAD INFORMÁTICA EN NIÑOS.* Bogota: Universidad Piloto De Colombia.

Cheng, X. P. (2019). Implementing Fingerprint Recognition on One-Time Password Device to Enhance User Authentication. *Springer, Cham.*, 448-461.

Ferraiolo, D., & Kuhn, R. (1995). Role-based access control (RBAC): Features and motivations. *Proceedings of 11th annual computer security application conference*, 241-48. Obtenido de https://www.researchgate.net/profile/D_Kuhn2/publication/238743515_Role-based_access_control_features_and_motivations/links/562e7d3808ae04c2aeb5d98b.pdf

Garcia, M. (05 de Octubre de 2017). *MVC (Modelo-Vista-Controlador): ¿qué es y para qué sirve?* Recuperado el 16 de Diciembre de 2020, de Coding or Not: https://codingornot.com/mvc-modelo-vista-controlador-que-es-y-para-que-sirve

García, P., Montenegro, C., & Velandia, J. (2016). Modelo ontológico para la predicción de ataques informáticos a partir de Honeynets virtualizadas. *Revista Logos, Ciencia & Tecnología, 8*(1), 101-114.

García, R. (1 de Agosto de 2020). *Como funciona un codigo QR y Porque cada codigo es unico*. Recuperado el 28 de Diciembre de 2020, de tuexperto.com: https://www.tuexperto.com/2020/08/01/como-funciona-un-codigo-qr-y-por-que-cada-codigo-es-unico/

Gil, V., & Gil, J. (30 de Junio de 2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica, 22*(2), 193-197. doi:https://doi.org/10.22517/23447214.11371

IETF- RFC. (Mayo de 2011). *IETF Tools.* Recuperado el 15 de Diciembre de 2020, de RFC6238: https://tools.ietf.org/html/rfc6238

INCIBE. (11 de Marzo de 2015). *incibe.es*. Obtenido de La seguridad vista desde sus inicios: https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio

Instituto de Estudios Estrategicos. (01 de Junio de 2011). La Evolucion del Concepto de Seguridad. *DOCUMENTO MARCO 05/2011*. Madrid, España. Obtenido de http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf

ISO25000. (2015). *ISO/IEC 25010*. Recuperado el 16 de Diciembre de 2020, de ISO 25000: https://iso25000.com/index.php/normas-iso-25000/iso-25010?limit=3&limitstart=0

Kuang, G., & Xu, H. (2019). Realization of Identity Card and Face Recognition Two-Factor Authentication System Based on Wechat. *International Conference on Applications and Techniques in Cyber Security and Intelligence*, 929-936.

Lagreca, N. (2017). MODELO DE AUDITORIA PARA SERVICIOS TELEMATICOS DE LA UNIVERSIDAD SIMON BOLIVAR. *Telematique*, 79-95.

Manaswini, N., & Sahoo, P. (2016). CSRF Attacks On Web Applications. *IJACTA, 4*(1), 194-197.

Microcosm Ltd. (03 de Julio de 2018). *Microcosm*. Recuperado el 15 de Diciembre de 2020, de HOTP frente a TOTP: ¿En qué se diferencian?: https://es.microcosm.com/blog/hotp-totp-what-is-the-difference

Mieres, J. (2009). *https://www.evilfingers.net.* Obtenido de Ataques informáticos. Debilidades de seguridad comúnmente explotadas). : http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

Morales, G. (07 de Mayo de 2013). *cinvestav.mx.* Recuperado el 14 de Diciembre de 2020, de El heroe Alan Turing: Aportaciones de la Criptologıa a la victoria: http://cs.cinvestav.mx/~gmorales/12Enigma/enigma.pdf

NIST. (22 de Junio de 2017). *nist.gov.* doi:http://dx.doi.org/10.6028/NIST.SP.800-63-2

Panda Security. (23 de Febrero de 2016). *pandasecurity.com*. Recuperado el 15 de Diciembre de 2020, de 10 trucos nemotécnicos para crear contraseñas seguras y fáciles de recordar: https://www.pandasecurity.com/es/mediacenter/seguridad/10-trucos-para-crear-contrasenas-seguras/

Quiroz, S., & Macias, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3*(3), 676-688. doi:http://dx.doi.org/10.23857/dc.v3i3%20mon.663

Ramirez, I. (19 de Diciembre de 2019). *Xataka*. Recuperado el 15 de Diciembre de 2020, de Google Authenticator: qué es, cómo funciona y cómo configurarlo: https://www.xataka.com/basics/google-authenticator-que-como-funciona-como-configurarlo

Rodriguez, O., & Socorro, R. (2018). Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. *Revista Cubana de Ciencias Informáticas*, 13-27.

Serrato, G. (2016). Metodología para el análisis de vulnerabilidades. *Tecnologia, Investigacion y Academia (TIA), 4*(2), 20-27.

Shernan, E., & Traynor, P. (2015). More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. *Springer*.

Singh, S. (2017). Multi-factor authentication and their approaches. *International research journal of management, IT and social sciences*, 68-81.

Sinha, A., & Kumar, P. (09 de Marzo de 2019). A Pattern-Based Multi-Factor Authentication System. *SCPE, 20*(01). doi:https://doi.org/10.12694/scpe.v20i1.1460

Suárez, D., & Ávila, A. (04 de Julio de 2017). Una forma de interpretar la seguridad informática. *Journal of Engineering, 4*(2), 17-23.

Tábara, J. (2011). *openBoxer.* Obtenido de Breve Historia de la Criptografia Clásica: http://www.openboxer.260mb.com/asignaturas/criptografia/metodosCriptograficos.pdf?i=1

The Hacker News. (14 de Diciembre de 2014). *The Hacker News*. Recuperado el 15 de Diciembre de 2020, de Hackers Can Read Your Private SMS and Listen to Phone Calls: https://thehackernews.com/2014/12/hackers-can-read-your-private-sms-and.html

Tirado, N., & Carreño, S. (20 de Junio de 2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista Publicando, 4*(10), 462-473. Obtenido de https://revistapublicando.org/revista/index.php/crv/article/view/367

Universidad Complutense de Madrid. (10 de Noviembre de 2016). *Umc.es* . Obtenido de INTRODUCCIÓN A LA CRIPTOGRAFÍA: https://www.ucm.es/data/cont/docs/72-2016-11-10-2%20Comunicaciones%20seguras.pdf

Vargas, R. (2016). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, 31-45.

Vera, V. D., & Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia et technica, 22(2)*, 193-197.

Verizon Media. (2016 de Julio de 2016). *Techcrunch.com*. Recuperado el 15 de Diciembre de 2020, de NIST declares the age of SMS-based 2-factor authentication over: https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/

Waheed, A. A. (2016). Secure login protocols: An analysis on modern attacks and solutions. *2016 22nd International Conference on Automation and Computing (ICAC).* Islamabad, Pakistan : COMSATS Institute of Information Technology .

Xiao, X., Yan, R., & Jiang, Y. (2015). Detection and Prevention of Code Injection Attacks. *2015 Third International Conference on Advanced Cloud and Big Data*, 24-261.

Zambrano, S., & Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*, 676-688.

ANEXOS

ANEXO I. FASE DE ANALISIS DE SOFTWARE

- **Descripción de Roles**

Tabla 11: Roles de Usuarios del Sistema

Descripción	*Rol*
Superadministrador	Acceso al panel de Administrador, Acceso al Panel Personal, Acceso al panel de Cliente y Ataques Informáticos
Administrador	Acceso al Panel Personal, Acceso al Panel del Cliente; Vendedor y Ataques Informáticos
Cliente	Acceso al Panel Personal

- **Requerimientos Funcionales**

Tabla 12: Requerimientos Funcionales del Módulo de Seguridad

ID	*Rol*	*Funcionalidad*	*Resultados*	*Criterios de Aceptación*	*Observaciones*
C001	Como Cliente	Necesito poder regístrame para acceder al sistema	Con la finalidad de registrar a un cliente nuevo al sistema	El Cliente podrá registrarse en el sistema	Solo se podrá registrar una vez
C002	Como Cliente	Necesito poder activar mi cuenta para poder acceder al sistema	Con la finalidad de activar un nuevo cliente y pueda acceder al sistema	El Cliente podrá activar su cuenta desde un link enviado a su correo electrónico utilizado en el registro	La activación se lo realiza una única vez, y de ser satisfactoria puede ingresar directamente al sistema con su usuario y contraseña una única vez
C003	Como Cliente	Necesito poder ingresar al sistema	Con la finalidad de acceder al sistema	El cliente podrá acceder al sistema con su correo electrónico registrado y su contraseña registrada	Valido la autentificación, pero no autorizado para acceder al sistema
C004	Como Cliente	Necesito poder garantizar mi identidad para acceder al panel de Cliente	Con la finalidad de la seguridad del acceso al sistema y panel correspondiente	El cliente deber ser dirigido a una página de verificación de identidad aplicando algún tipo de autentificación extra además de la contraseña ya ingresada	Este proceso se lo realizara mediante codigo QR con la aplicación del Autenticador de Google, al finalizar todos los requerimientos

ID	*Rol*	*Funcionalidad*	*Resultados*	*Criterios de Aceptación*	*Observaciones*
C005	Como Cliente	Necesito poder acceder al Panel Personal	Con finalidad de Revisar la información personal registrada	El cliente deber ser capaz de ingresar al Panel personal con su información personal registrado en el sistema	
C006	Como Cliente	Necesito poder modificar la información personal registrada	Con finalidad de Registrar y Modificar la información personal registrada en el sistema	El cliente deber ser capaz de ingresar, modificar, su información personal	Aplicada para todas las vistas del panel personal del Cliente
C007	Como Cliente	Necesito poder actualizar la contraseña registrada en la base de datos	Con finalidad de modificar la información personal registrada en el sistema	El cliente debe ser capaz de modificar su contraseña actual	
C008	Como Cliente	Necesito poder actualizar su contraseña en el caso de olvidarla	Con finalidad de modificar y recuperar la información personal registrada en el sistema	El cliente debe poder modificar su contraseña actual mediante un Wizard de recuperación	Aplicada solamente para clientes registrados en el sistema con anterioridad
A001	Como Administrador	Necesito poder ingresar al sistema	Con la finalidad de acceder al sistema	El Administrador podrá acceder al sistema con su correo electrónico registrado y su contraseña registrada	Valido la autentificación, pero no autorizado para acceder al sistema
A002	Como Administrador	Necesito poder garantizar mi identidad para acceder al panel de Administrador	Con la finalidad de la seguridad del acceso al sistema y panel correspondiente	El Administrador deber ser dirigido a una página de verificación de identidad aplicando algún tipo de autentificación extra además de la contraseña ya ingresada	Este proceso se lo realizara mediante codigo QR con la aplicación del Autenticador de Google, al finalizar todos los requerimientos
A003	Como Administrador	Necesito poder acceder al Panel Personal	Con finalidad de Revisar la información personal registrada	El Administrador deber ser capaz de ingresar al Panel personal con su información personal registrado en el sistema	
A004	Como Administrador	Necesito poder modificar la información personal registrada	Con finalidad de Registrar y Modificar la información personal registrada en el sistema	El Administrador debe ser capaz de ingresar, modificar, su información personal	Aplicada para todas las vistas del panel personal del Administrador
A005	Como Administrador	Necesito poder actualizar la contraseña registrada en la base de datos	Con finalidad de modificar la información personal registrada en el sistema	El Administrador debe ser capaz de modificar su contraseña actual	

ID	*Rol*	*Funcionalidad*	*Resultados*	*Criterios de Aceptación*	*Observaciones*
A006	Como Administrador	Necesito poder actualizar su contraseña en el caso de olvidarla	Con finalidad de modificar y recuperar la información personal registrada en el sistema	El Administrador debe poder modificar su contraseña actual mediante un Wizard de recuperación	Aplicada solamente para administradores registrados en el sistema con anterioridad
A007	Como Administrador	Necesito poder Ingresar al panel de Clientes	Con finalidad de revisar la información de los clientes registrados en el sistema	El Administrador debe poder acceder al panel de clientes registrados del sistema	El panel de clientes debe estar todos los usuarios con el rol cliente registrado
A008	Como Administrador	Necesito poder Revisar la información del Cliente registrado	Con la finalidad de revisar la información del cliente registrado en el sistema	El Administrador debe poder acceder a la información de cada uno de los clientes registrados en el sistema	
A009	Como Administrador	Necesito poder revisar el historial de cada uno de los clientes registrados en el sistema	Con la finalidad de revisar la información realizada por el cliente registrado en el sistema	El Administrador debe poder acceder al historial de cada uno de los clientes registrados en el sistema	
A010	Como Administrador	Necesito poder desbloquear a un usuario que ha superado el número de intentos permitidos para acceder al sistema	Con la finalidad de permitir el acceso a un cliente si ha superado el número de intentos permitidos	El Administrador debe poder desbloquear a un cliente que ha superado el número de intentos permitidos	
A011	Como Administrador	Necesito poder revisar los ataques informáticos, detectados y evitados por el sistema	Con la finalidad de ver la seguridad del sistema y dar cuenta de las formas de ataques realizados	El Administrador debe poder revisar todos los ataques informáticos detectados y neutralizados por el sistema	
SA001	Como SuperAdministrador	Necesito poder ingresar al sistema	Con la finalidad de acceder al sistema	El SuperAdministrador podrá acceder al sistema con su correo electrónico registrado y su contraseña registrada	Valido la autentificación, pero no autorizado para acceder al sistema
SA002	Como SuperAdministrador	Necesito poder garantizar mi identidad para acceder al panel de Administrador	Con la finalidad de la seguridad del acceso al sistema y panel correspondiente	El SuperAdministrador deber ser dirigido a una página de verificación de	Este proceso se lo realizara mediante codigo QR con la aplicación del Autenticador de Google, al finalizar

ID	*Rol*	*Funcionalidad*	*Resultados*	*Criterios de Aceptación*	*Observaciones*
				identidad aplicando algún tipo de autentificación extra además de la contraseña ya ingresada	todos los requerimientos
SA 003	Como SuperAdministrador	Necesito poder acceder al Panel Personal	Con finalidad de Revisar la información personal registrada	El SuperAdministrador deber ser capaz de ingresar al Panel personal con su información personal registrado en el sistema	
SA 004	Como SuperAdministrador	Necesito poder modificar la información personal registrada	Con finalidad de Registrar y Modificar la información personal registrada en el sistema	El SuperAdministrador debe ser capaz de ingresar, modificar, su información personal	Aplicada para todas las vistas del panel personal del Administrador
SA 005	Como SuperAdministrador	Necesito poder actualizar la contraseña registrada en la base de datos	Con finalidad de modificar la información personal registrada en el sistema	El SuperAdministrador debe ser capaz de modificar su contraseña actual	
SA 006	Como SuperAdministrador	Necesito poder Ingresar al panel de Clientes	Con finalidad de revisar la información de los clientes registrados en el sistema	El SuperAdministrador debe poder acceder al panel de clientes registrados del sistema	El panel de clientes debe estar todos los usuarios con el rol cliente registrado
SA 007	Como SuperAdministrador	Necesito poder Revisar la información del Cliente registrado	Con la finalidad de revisar la información del cliente registrado en el sistema	El SuperAdministrador debe poder acceder a la información de cada uno de los clientes registrados en el sistema	
SA 008	Como SuperAdministrador	Necesito poder revisar el historial de cada uno de los clientes registrados en el sistema	Con la finalidad de revisar la información realizada por el cliente registrado en el sistema	El SuperAdministrador debe poder acceder al historial de cada uno de los clientes registrados en el sistema	
SA 009	Como SuperAdministrador	Necesito poder desbloquear a un usuario que ha superado el número de intentos permitidos para acceder al sistema	Con la finalidad de permitir el acceso a un cliente si ha superado el número de intentos permitidos	El SuperAdministrador debe poder desbloquear a un cliente que ha superado el número de intentos permitidos	
SA 010	Como SuperAdministrador	Necesito poder revisar los ataques informáticos,	Con la finalidad de ver la seguridad del sistema y dar cuenta	El SuperAdministrador debe poder revisar todos los ataques informáticos detectados y neutralizados por el sistema	

ID	*Rol*	*Funcionalidad*	*Resultados*	*Criterios de Aceptación*	*Observaciones*
		detectados y evitados por el sistema	de las formas de ataques realizados		
SA 011	Como SuperAdministrador	Necesito poder Ingresar al panel de Administradores	Con finalidad de revisar la información de los clientes registrados en el sistema	El SuperAdministrador debe poder acceder al panel de Administradores registrados del sistema	
SA 012	Como SuperAdministrador	Necesito poder Revisar la información del Administradores registrado	Con la finalidad de revisar la información del Administradores registrado en el sistema	El SuperAdministrador debe poder acceder a la información de cada uno de los clientes registrados en el sistema	
SA 013	Como SuperAdministrador	Necesito poder revisar el historial de cada uno de los Administradores registrados en el sistema	Con la finalidad de revisar la información realizada por el Administradores registrado en el sistema	El SuperAdministrador debe poder acceder al historial de cada uno de los Administradores registrados en el sistema	
SA 014	Como SuperAdministrador	Necesito poder desbloquear a un usuario que ha superado el número de intentos permitidos para acceder al sistema	Con la finalidad de permitir el acceso a un Administradores si ha superado el número de intentos permitidos	El SuperAdministrador debe poder desbloquear a un Administradores que ha superado el número de intentos permitidos	

- **Requerimientos No Funcionales**

Tabla 13: Requerimientos No Funcionales

Requerimientos No Funcionales	*Descripción*
Adecuación Funcional	El módulo de seguridad debe permitir las acciones únicamente bajo un rol definido
Eficiencia de Desempeño	El módulo de seguridad deberá responder a las peticiones solicitadas según sea el caso pertinente para mostrar los datos al momento de realizar una acción
Compatibilidad	El módulo de seguridad debe ser capaz de ser usado en diferentes ambientes y con componentes tanto internos y externos
Usabilidad	El módulo de seguridad debe ser fácil de aprender, utilizar, entender y ser atractivo para el usuario
Fiabilidad	El módulo de seguridad debe ser capaz de satisfacer cada una de las necesidades de los usuarios
Disponibilidad	El módulo de seguridad debe estar disponible todos los días del año para los usuarios
Seguridad	El módulo de seguridad debe llevar un historial de cada uno de los usuarios El módulo de seguridad debe tener algoritmos de encriptación para contraseñas El módulo de seguridad debe tener validaciones por lado del cliente y del servidor hacia los datos que se debe ingresar

Requerimientos No Funcionales	*Descripción*
	El módulo de seguridad debe tener una contraseña fuerte El módulo de seguridad debe detectar y neutralizar ataques informáticos El módulo de seguridad debe poseer por lo menos un método de autentificación extra al convencional El módulo de seguridad debe poseer un cierre forzado luego de un tiempo determinado, o al cerrar sesión en alguna ventana El módulo de seguridad debe informar a cada usuario del inicio de sesión por medio de un mensaje a su correo electrónico

- **Recursos Tecnológicos**

Tabla 14: Recursos Tecnológicos

Categoría	Nombre	Descripción
Software	Sistema Operativo W10	Sistema Operativo donde se desarrolla el módulo de seguridad.
Software	XAMMP	Sistema de gestión de bases de datos MySQL, el servidor web Apache.
Software	MySQL	Servidor de Base de Datos.
Software	Visual Studio Code	Editor de texto libre desarrollado por Microsoft para Windows, Linux y macOS.
Lenguaje de Programación	PHP	Lenguaje de programación de uso general que se adapta especialmente al desarrollo web.
Lenguaje de Programación	JavaScript	Lenguaje de programación estándar ECMAScript. Se define como orientado a objetos, utilizado por lado del Cliente.
Librería	Font Awesome	Conjunto de herramientas de fuentes e iconos basado en CSS y Less.
Software (App Móvil)	Google Authenticator	Software basado en autenticación con contraseña de un solo uso desarrollado por Google.
Hardware	Laptop	Laptop Lenovo ideapad 320, utilizada para el desarrollo del módulo de seguridad.

ANEXO II. FASE DE DISEÑO DE SOFTWARE

- **Arquitectura de Software**
    - **Modelo Vista Controlador**

El Modelo Vista Controlador (MVC) se define como un patrón de diseño arquitectónico de software, que sirve para clasificar la información, la lógica del sistema y la interfaz que se le presenta al usuario. En este tipo de arquitectura existe un sistema central o controlador que gestiona las entradas y la salida del sistema, uno o varios modelos que se encargan de buscar los datos e información necesaria y una interfaz que muestra los resultados al usuario final (Garcia, 2017). Este patrón permite modificar cada uno de sus componentes si necesidad de afectar a los demás.

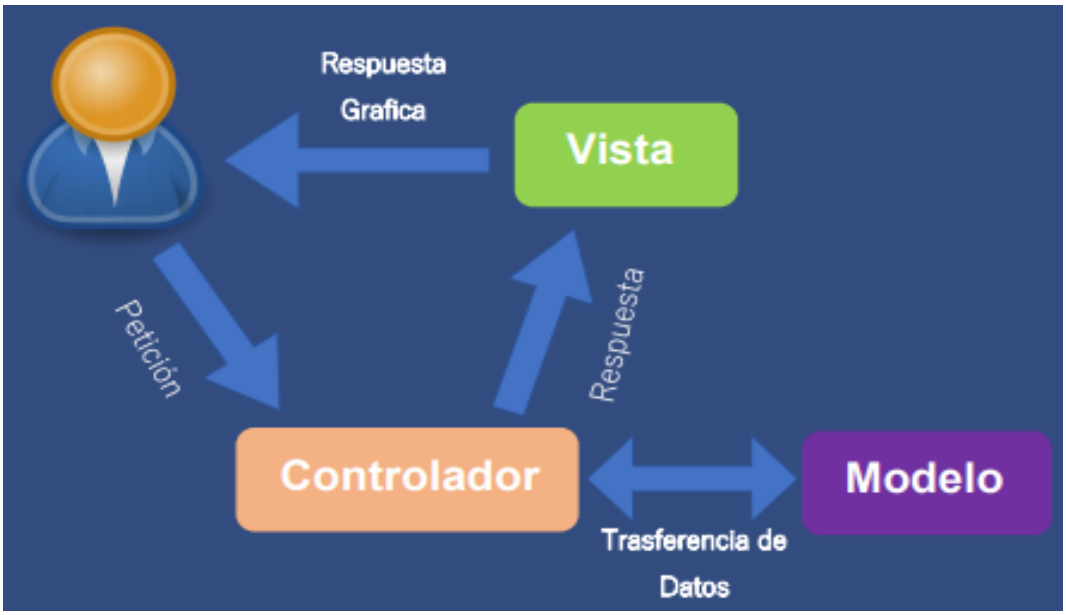

Figura 17: Modelo Vista Controlador (MVC)

- **Modelo Entidad Relación**

Para el desarrollo del módulo de la seguridad se esquematizo los requerimientos y se diseñó el modelo Entidad – Relación.

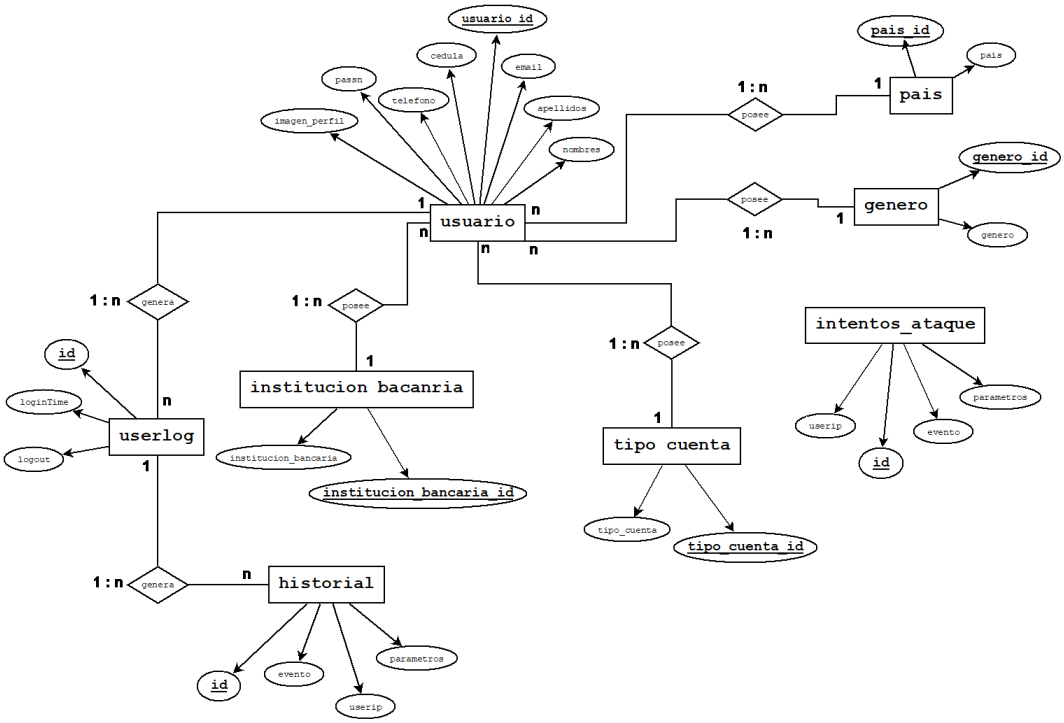

Figura 18: Modelo Entidad-Relación

- **Modelo Relacional**

En el proceso de diseño luego de realizar el modelo Entidad Relacional se continuo con la elaboración del modelo Relacional en el que se incluye ya las relaciones y tipos de datos que se definieron para el módulo de seguridad.

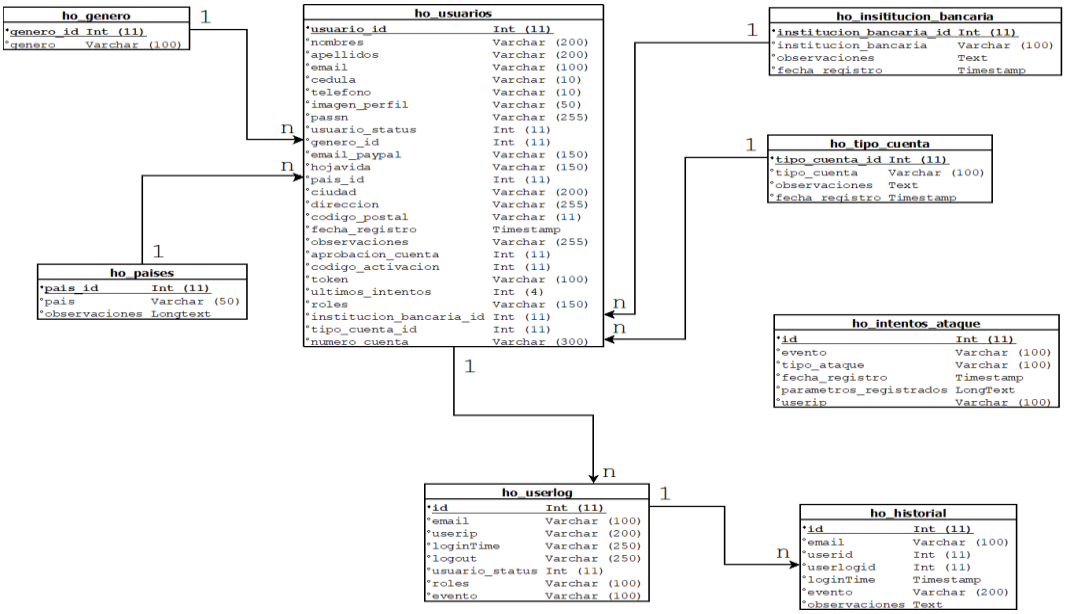

Figura 19: Modelo Relacional

- **Diagrama de Casos de Uso**

Se especifica según el modelado UML cada una de las acciones realizadas por cada uno de los roles establecidos en el módulo de seguridad.

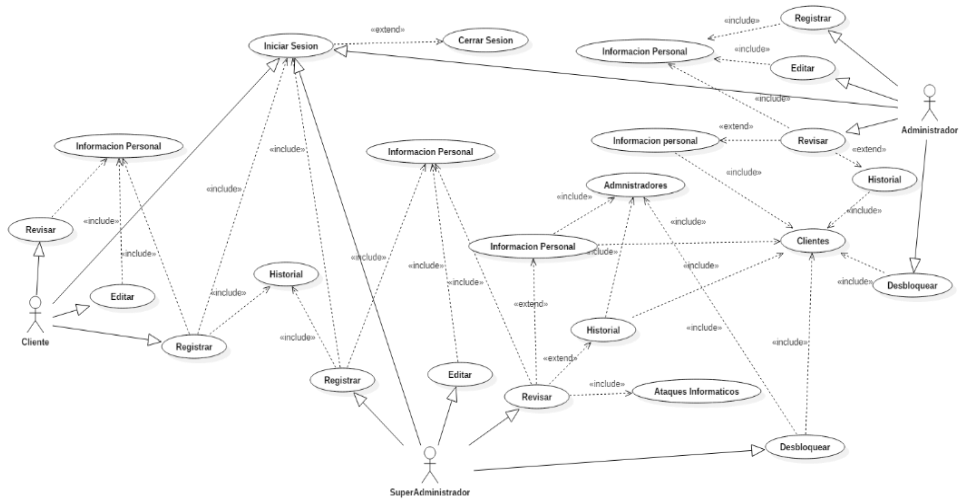

Figura 20: Diagrama de Casos de Uso

- **Modelo de Base de Datos**

El modelo Final de Datos se lo evidencia en el siguiente modelo, la cual consta con las relaciones ya aplicadas, los datos con los que se desarrolló el módulo de seguridad

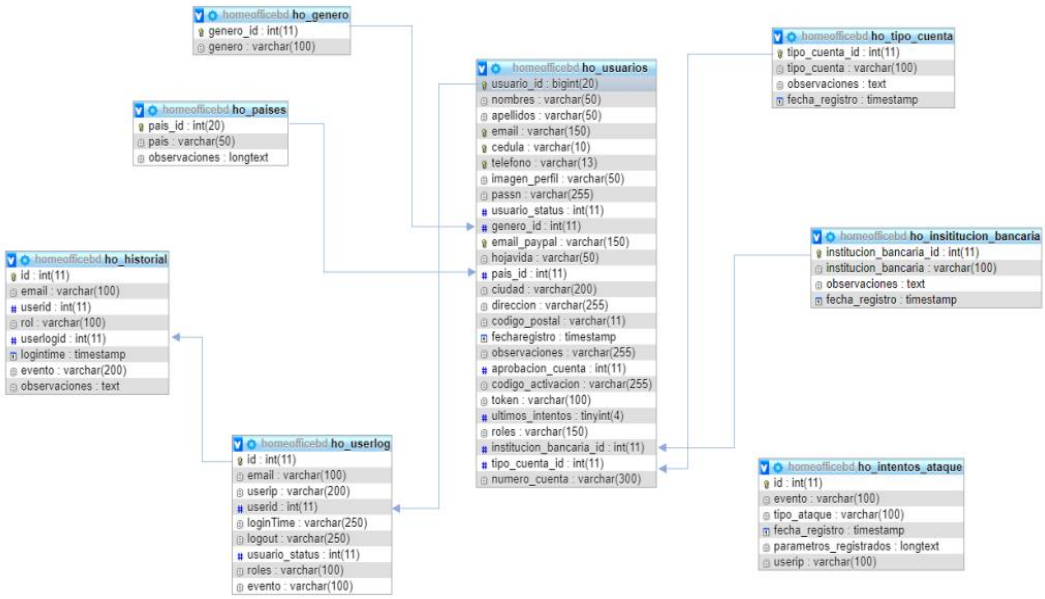

Figura 21: Modelo de Base de Datos

- **Diccionario de Datos**

Para el detalle de cada una de las tablas de la base de datos se establecen las tablas que se muestran a continuación, en las cuales cada una tienen el objetivo de dar a conocer la estructura de las tablas de la base de datos del Módulo de seguridad.

Tabla 15: Tabla ho_genero

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_genero
Descripción de la Tabla: La tabla contiene la información sobre el género de un usuario

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_genero_001	genero_id	Integer	11	Codigo de Autentificación del Genero	Si	Codigo Auto incrementable
ho_genero_002	genero	Varchar	100	Nombre del Genero	Si	

Tabla 16: Tabla ho_institucion_bancaria

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_institucion_bancaria
Descripción de la Tabla: La tabla contiene la información sobre la institución bancaria de un usuario

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_institucion_bancaria_001	institucionbancaria_id	Integer	11	Codigo de Autentificación de la Institución Bancaria	Si	Codigo Auto incrementable
ho_institucion_bancaria_002	institución_bancaria	Varchar	100	Nombre de la Institución Bancaria	Si	
ho_institucion_bancaria_003	observaciones	Text		Observaciones sobre la Institución Bancaria	No	
ho_institucion_bancaria_004	fecha_registro	TimeStamp		Fecha de registro de la Institución Bancaria	Si	Automático al darse un registro

Tabla 17: Tabla ho_paises

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_paises
Descripción de la Tabla: La tabla contiene la información sobre el pais de un usuario

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_paises_001	pais_id	Integer	11	Codigo de Autentificación del Pais	Si	Codigo Auto incrementable
ho_paises_002	país	Varchar	100	Nombre del Pais	Si	
ho_paises_003	observaciones	Text		Observaciones del Pais	No	

Tabla 18: Tabla ho_tipo_cuenta

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_tipo_cuenta
Descripción de la Tabla: La tabla contiene la información sobre el tipo de cuentas que puede tener un usuario

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_tipo_cuenta_001	tipo_cuenta_id	Integer	11	Codigo de Autentificación del Tipo de Cuenta	Si	Codigo Auto incrementable
ho_tipo_cuenta_002	tipo_cuenta	Varchar	100	Nombre del Tipo de Cuenta	Si	
ho_tipo_cuenta_003	observaciones	Text		Observaciones sobre del Tipo de Cuenta	No	
ho_tipo_cuenta_004	fecha_registro	TimeStamp		Fecha de registro del Tipo de Cuenta	Si	Automático al darse un registro

Tabla 19: Tabla ho_intentos_ataque

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_intentos_ataque
Descripción de la Tabla: La tabla contiene la información sobre los ataques detectados y neutralizados

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_intentos_ataque _001	id	Integer	11	Codigo de Autentificación de los Ataques Informáticos	Si	Codigo Auto incrementable
ho_intentos_ataque _002	evento	Varchar	100	Evento que se detectó en el ataque	Si	
ho_intentos_ataque _003	tipo_ataque	Varchar	100	Nombre del Tipo de Ataque detectado	Si	
ho_intentos_ataque _004	fecha_registro	TimeStamp		Fecha de registro del Ataque detectado	Si	Automático al darse un registro
ho_intentos_ataque _005	parámetros_registrados	LongText		Parámetros usados para realizar el ataque informático	Si	
ho_intentos_ataque _006	userip	Varchar	100	Ip de donde se trató de realizar el ataque	Si	

Tabla 20: Tabla ho_usuarios

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_usuarios
Descripción de la Tabla: La tabla contiene la información sobre los usuarios del sistema

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_usuarios _001	usuario_id	Integer	11	Codigo de Autentificación del Usuario	Si	Codigo Auto incrementable
ho_usuarios _002	nombres	Varchar	50	Nombre del Usuario	No	
ho_usuarios _003	apellidos	Varchar	50	Apellidos del Usuario	No	

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_usuarios_004	email	Varchar	150	Correo Electrónico del Usuario	Si	Atributo Único
ho_usuarios_005	cedula	Varchar	10	Cedula de Identidad del Usuario	Si	Atributo Único
ho_usuarios_006	teléfono	Varchar	10	Teléfono del Usuario	No	Atributo Único
ho_usuarios_007	imagen_perfil	Varchar	50	Dirección de Almacenamiento de la imagen de Perfil	No	
ho_usuarios_008	passn	Varchar	255	Contraseña del Usuario	Si	
ho_usuarios_009	usuario_status	Integer	11	Estatus del Usuario	Si	Utilizado para el acceso del usuario, activación y registro
ho_usuarios_010	genero_id	Integer	11	identificador de la Tabla ho_genero	Si	Clave Foránea
ho_usuarios_011	email_paypal	Varchar	150	Correo Electrónico destinado para PayPal	No	
ho_usuarios_012	hojavida	Varchar	50	Dirección de Almacenamiento del archivo de la hoja de vida del Usuario	No	
ho_usuarios_013	país_id	Integer	11	Identificador de la Tabla ho_paises	Si	Clave Foránea
ho_usuarios_014	ciudad	Varchar	200	Ciudad de Residencia del Usuario	No	
ho_usuarios_015	dirección	Varchar	255	Dirección de Residencia del Usuario	No	
ho_usuarios_016	codigo_postal	Varchar	11	Codigo Postal del Usuario	No	

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_usuarios_017	fecharegistro	TimeStamp		Fecha de Registro del Usuario	Si	Automático al registrarse
ho_usuarios_018	observaciones	Varchar	255	Observaciones del Usuario	No	
ho_usuarios_019	aprobación_cuenta	Integer	11	Codigo Ocupada para la recuperación de cuenta	No	
ho_usuarios_020	codigo_activacion	Integer	11	Codigo de Activación de Cuenta de Usuario	Si	
ho_usuarios_021	token	Varchar	100	Codigo Encriptado para reconocer usuario	Si	
ho_usuarios_022	últimos_intentos	Integer	4	Contador de Intentos Permitidos al momento de Ingresar al Sistema	Si	Cambiante constantemente por el usuario
ho_usuarios_023	roles	Varchar	150	Rol asignado a cada usuario del Sistema	Si	
ho_usuarios_024	institución_bancaria_id	Integer	11	Identificación de la Tabla ho_institucion_bancaria	Si	Clave Foránea
ho_usuarios_025	tipo_cuenta_id	Integer	11	Identificación de la Tabla ho_institucion_bancaria	Si	Clave Foránea
ho_usuarios_026	numero_cuenta	Varchar	300	Número de Cuenta del Usuario	No	

Tabla 21: Tabla ho_userlog

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_userlog
Descripción de la Tabla: La tabla contiene la información sobre las sesiones realizadas por el usuario

Id	*Nombre*	*Tipo de Dato*	*Tamaño (Max.)*	*Descripción*	*Obligatorio*	*Observaciones*
ho_userlog_001	id	Integer	11	Codigo de Autentificación de la Sesión	Si	Codigo Auto incrementable
ho_userlog_002	email	Varchar	100	Correo Electrónico del Usuario	Si	
ho_userlog_003	userip	Varchar	100	Dirección Ip del usuario desde el que ingreso	Si	
ho_userlog_004	userid	Integer	11	Identificación de la Tabla ho_usuarios	Si	Clave Foránea
ho_userlog_005	loginTime	Varchar	250	Fecha del Ingreso al Sistema	Si	
ho_userlog_006	logout	Varchar	250	Fecha de Cierre de Sesión	Si	
ho_userlog_007	usuario_status	Integer	11	Estado de la Sesión al Cerrarse	Si	
ho_userlog_008	roles	Varchar	100	Rol del Usuario al momento de Iniciar la sesión	Si	
ho_userlog_009	evento	Varchar	100	Evento al momento de Cerrar Sesión el sistema	Si	

Tabla 22: Tabla *ho_historial*

Nombre del Módulo: Seguridad
Nombre de la Tabla: ho_historial
Descripción de la Tabla: La tabla contiene la información sobre las acciones realizadas por el usuario

Id	***Nombre***	***Tipo de Dato***	***Tamaño (Max,)***	***Descripción***	***Obligatorio***	***Observaciones***
ho_historial_001	id	Integer	11	Codigo de Autentificación del Historial	Si	Codigo Auto incrementable
ho_historial_002	email	Varchar	100	Correo Electrónico del Usuario	Si	
ho_historial_003	userid	Integer	11	Identificación de la Tabla ho_usuarios	Si	Clave Foránea
ho_historial_004	rol	Varchar	100	Rol del Usuario	Si	
ho_historial_005	userlogid	Integer	11	Identificación de la Tabla ho_userlog	Si	
ho_historial_006	logintime	TimeStamp		Fecha y Hora de la acción realizada	Si	
ho_historial_007	evento	Varchar	200	Accion realizada por el Usuario	Si	
ho_historial_008	observaciones	Text		Observaciones de la acción realizada por el Usuario	Si	

ANEXO III. MODELO DE ENCUESTA DE CALIDAD DE SOFTWARE

TEST DE EVALUACION DE CALIDAD DE SOFTWARE

EMPRESA: Home Office S.A.S.

Departamento: Desarrollo

Modulo: Seguridad

Fecha:

Tipo de Usuario:

Rol:

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Adecuación Funcional:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Según su rol definido al usar el módulo de Seguridad obtuvo algún tipo de problema?		
P2	¿Según su rol definido por la base de datos y políticas de la empresa usted cumplió con acceso a todas las funcionalidades?		
P3	¿Según su rol se cumple con todos los requerimientos definidos en el documento de requerimientos?		

Eficiencia de desempeño:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Malo**	**Bueno**	**Excelente**
P4	Califique el tiempo de respuesta entre las acciones específicas realizadas			
P5	Califique la funcionalidad en general de todas las acciones realizadas dentro del Módulo de seguridad			
P6	Califique la capacidad que cuenta el Módulo de Seguridad al momento de ingresar o editar algún tipo de parámetro dentro del Formulario			

Compatibilidad

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P7	¿Cuenta el Módulo de Seguridad con algún tipo de Software exterior independiente?		
P8	¿El Módulo de Seguridad cuenta con componentes que guardan información en común?		

Usabilidad:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Fácil**	**Normal**	**Difícil**
P9	Califique la facilidad que tiene el Módulo de Seguridad para reconocer su adecuación			
P10	Califique la facilidad que tiene el Módulo de Seguridad en ser aprendido			
P11	Califique la facilidad que tiene el Módulo de Seguridad en ser usado de manera correcta			
P12	Califique la facilidad que tiene el sistema para prever errores de parte del usuario			
P13	Califique la facilidad que tiene el usuario en entender la interfaz grafica			
P14	Califique la facilidad que tiene el usuario en acceder a determinadas características y capacidades			

Fiabilidad:

Donde 1 es mínimo y 3 es máximo

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**1**	**2**	**3**
P15	Califique la capacidad que tiene el Módulo de Seguridad para satisfacer las necesidades de fiabilidad en condiciones normales			
P16	Califique la capacidad que posee el Módulo de Seguridad en estar accesible cuando se lo requiera			
P17	Califique la capacidad del Módulo de Seguridad para operar según lo previsto en presencia de fallos de software			
P18	Califique la capacidad que tiene el Módulo de Seguridad para operar bajo presencia a fallos			
P19	Califique la capacidad del Módulo de Seguridad para recuperar los datos directamente afectados en caso de un fallo			

ANEXO IV. ENCUESTA APLICADA AL EQUIPO DE DESARROLLO DE LA EMPRESA HOME OFFICE S.A.S

TEST DE EVALUACION DE CALIDAD DE SOFTWARE

EMPRESA: Home Office S.A.S.

Departamento: Desarrollo

Modulo: Seguridad

Fecha: 26/12/2020

Tipo de Usuario: Desarrollador

Rol: Super Administrador

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Adecuación Funcional:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Según su rol definido al usar el módulo de Seguridad obtuvo algún tipo de problema?		X
P2	¿Según su rol definido por la base de datos y políticas de la empresa usted cumplió con acceso a todas las funcionalidades?	X	
P3	¿Según su rol se cumple con todos los requerimientos definidos en el documento de requerimientos?	X	

Eficiencia de desempeño:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Malo**	**Bueno**	**Excelente**
P4	Califique el tiempo de respuesta entre las acciones especificas realizadas			X
P5	Califique la funcionalidad en general de todas las acciones realizadas dentro del Módulo de seguridad			X
P6	Califique la capacidad que cuenta el Modulo de Seguridad al momento de ingresar o editar algún tipo de parámetro dentro del Formulario			X

Compatibilidad

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P7	¿Cuenta el Módulo de Seguridad con algún tipo de Software exterior independiente?	X	
P8	¿El Módulo de Seguridad cuenta con componentes que guardan información en común?	X	

Usabilidad:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Fácil**	**Normal**	**Dificil**
P9	Califique la facilidad que tiene el Módulo de Seguridad para reconocer su adecuación	X		
P10	Califique la facilidad que tiene el Modulo de Seguridad en ser aprendido	X		
P11	Califique la facilidad que tiene el Modulo de Seguridad en ser usado de manera correcta	X		
P12	Califique la facilidad que tiene el sistema para prever errores de parte del usuario	X		
P13	Califique la facilidad que tiene el usuario en entender la interfaz grafica	X		
P14	Califique la facilidad que tiene el usuario en acceder a determinadas caracteristicas y capacidades	X		

Fiabilidad:

Donde 1 es mínimo y 3 es máximo

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**1**	**2**	**3**
P15	Califique la capacidad que tiene el Módulo de Seguridad para satisfacer las necesidades de fiabilidad en condiciones normales			X
P16	Califique la capacidad que posee el Modulo de Seguridad en estar accesible cuando se lo requiera			X
P17	Califique la capacidad del Modulo de Seguridad para operar según lo previsto en presencia de fallos de software			X
P18	Califique la capacidad que tiene el Modulo de Seguridad para operar bajo presencia a fallos			X
P19	Califique la capacidad del Modulo de Seguridad para recuperar los datos directamente afectados en caso de un fallo			X

TEST DE EVALUACION DE CALIDAD DE SOFTWARE

EMPRESA: Home Office S.A.S.
Departamento: Desarrollo
Modulo: Seguridad
Fecha: 26/12/2020
Tipo de Usuario: Desarrollador
Rol: Cliente

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Adecuación Funcional:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Según su rol definido al usar el módulo de Seguridad obtuvo algún tipo de problema?		X
P2	¿Según su rol definido por la base de datos y politicas de la empresa usted cumplió con acceso a todas las funcionalidades?	X	
P3	¿Según su rol se cumple con todos los requerimientos definidos en el documento de requerimientos?	X	

Eficiencia de desempeño:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Malo**	**Bueno**	**Excelente**
P4	Califique el tiempo de respuesta entre las acciones especificas realizadas	X		
P5	Califique la funcionalidad en general de todas las acciones realizadas dentro del Módulo de seguridad		X	
P6	Califique la capacidad que cuenta el Modulo de Seguridad al momento de ingresar o editar algún tipo de parámetro dentro del Formulario			X

Compatibilidad

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P7	¿Cuenta el Módulo de Seguridad con algún tipo de Software exterior independiente?	X	
P8	¿El Módulo de Seguridad cuenta con componentes que guardan información en común?		X

Usabilidad:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Fácil**	**Normal**	**Dificil**
P9	Califique la facilidad que tiene el Módulo de Seguridad para reconocer su adecuación		X	
P10	Califique la facilidad que tiene el Modulo de Seguridad en ser aprendido		X	
P11	Califique la facilidad que tiene el Modulo de Seguridad en ser usado de manera correcta	X		
P12	Califique la facilidad que tiene el sistema para prever errores de parte del usuario	X		
P13	Califique la facilidad que tiene el usuario en entender la interfaz grafica	X		
P14	Califique la facilidad que tiene el usuario en acceder a determinadas caracteristicas y capacidades		X	

Fiabilidad:

Donde 1 es mínimo y 3 es máximo

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**1**	**2**	**3**
P15	Califique la capacidad que tiene el Módulo de Seguridad para satisfacer las necesidades de fiabilidad en condiciones normales		X	
P16	Califique la capacidad que posee el Modulo de Seguridad en estar accesible cuando se lo requiera			X
P17	Califique la capacidad del Modulo de Seguridad para operar según lo previsto en presencia de fallos de software			X
P18	Califique la capacidad que tiene el Modulo de Seguridad para operar bajo presencia a fallos			X
P19	Califique la capacidad del Modulo de Seguridad para recuperar los datos directamente afectados en caso de un fallo			X

TEST DE EVALUACION DE CALIDAD DE SOFTWARE

EMPRESA: Home Office S.A.S.
Departamento: Desarrollo
Modulo: Seguridad
Fecha: 26/12/2020
Tipo de Usuario: Desarrollador
Rol: Administrador

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Adecuación Funcional:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Según su rol definido al usar el módulo de Seguridad obtuvo algún tipo de problema?		X
P2	¿Según su rol definido por la base de datos y políticas de la empresa usted cumplió con acceso a todas las funcionalidades?	X	
P3	¿Según su rol se cumple con todos los requerimientos definidos en el documento de requerimientos?	X	

Eficiencia de desempeño:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Malo**	**Bueno**	**Excelente**
P4	Califique el tiempo de respuesta entre las acciones específicas realizadas		X	
P5	Califique la funcionalidad en general de todas las acciones realizadas dentro del Módulo de seguridad			X
P6	Califique la capacidad que cuenta el Modulo de Seguridad al momento de ingresar o editar algún tipo de parámetro dentro del Formulario			X

Compatibilidad

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P7	¿Cuenta el Módulo de Seguridad con algún tipo de Software exterior independiente?	X	
P8	¿El Módulo de Seguridad cuenta con componentes que guardan información en común?	X	

Usabilidad:

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**Fácil**	**Normal**	**Dificil**
P9	Califique la facilidad que tiene el Módulo de Seguridad para reconocer su adecuación		X	
P10	Califique la facilidad que tiene el Modulo de Seguridad en ser aprendido	X		
P11	Califique la facilidad que tiene el Modulo de Seguridad en ser usado de manera correcta		X	
P12	Califique la facilidad que tiene el sistema para prever errores de parte del usuario	X		
P13	Califique la facilidad que tiene el usuario en entender la interfaz grafica	X		
P14	Califique la facilidad que tiene el usuario en acceder a determinadas características y capacidades		X	

Fiabilidad:

Donde 1 es mínimo y 3 es máximo

CUESTIONARIO		Respuesta		
ID	**PREGUNTAS**	**1**	**2**	**3**
P15	Califique la capacidad que tiene el Módulo de Seguridad para satisfacer las necesidades de fiabilidad en condiciones normales		X	
P16	Califique la capacidad que posee el Modulo de Seguridad en estar accesible cuando se lo requiera			X
P17	Califique la capacidad del Modulo de Seguridad para operar según lo previsto en presencia de fallos de software			X
P18	Califique la capacidad que tiene el Modulo de Seguridad para operar bajo presencia a fallos			X
P19	Califique la capacidad del Modulo de Seguridad para recuperar los datos directamente afectados en caso de un fallo		X	

ANEXO V. VISTAS DEL MODULO DE SEGURIDAD

Vista Principal

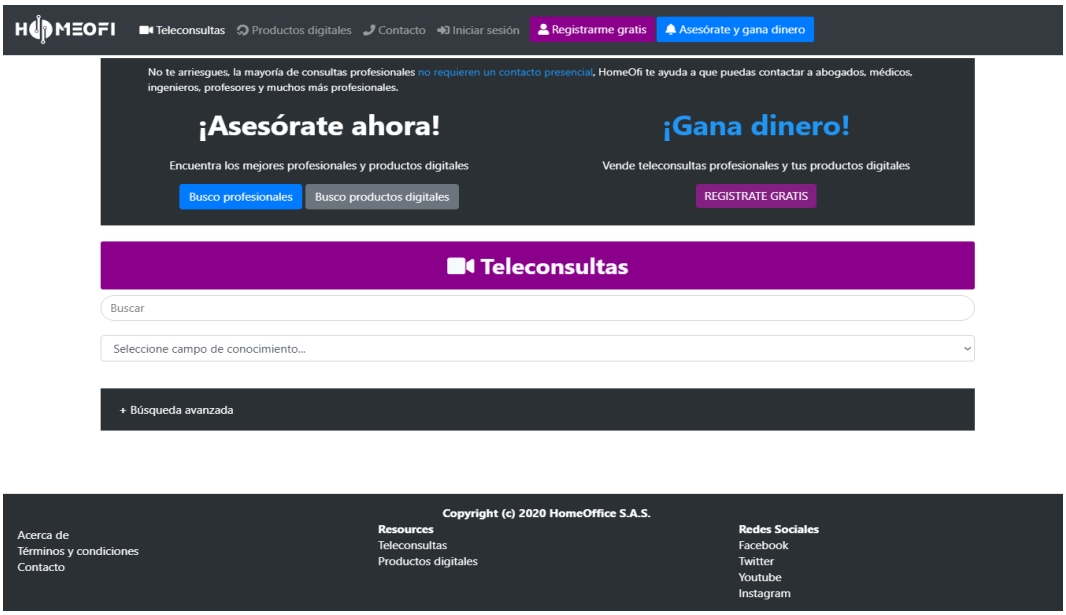

Figura 22: Vista Principal del Sistema

El módulo de seguridad se encuentra implementado al Sistema General de la página HomeOfi.com el mismo que pertenece a la empresa Home Office S.A.S., el cual cuenta con su propio servidor. el cual se puede acceder mediante el enlace www.homeofi.com

Vista de Registro de Cliente

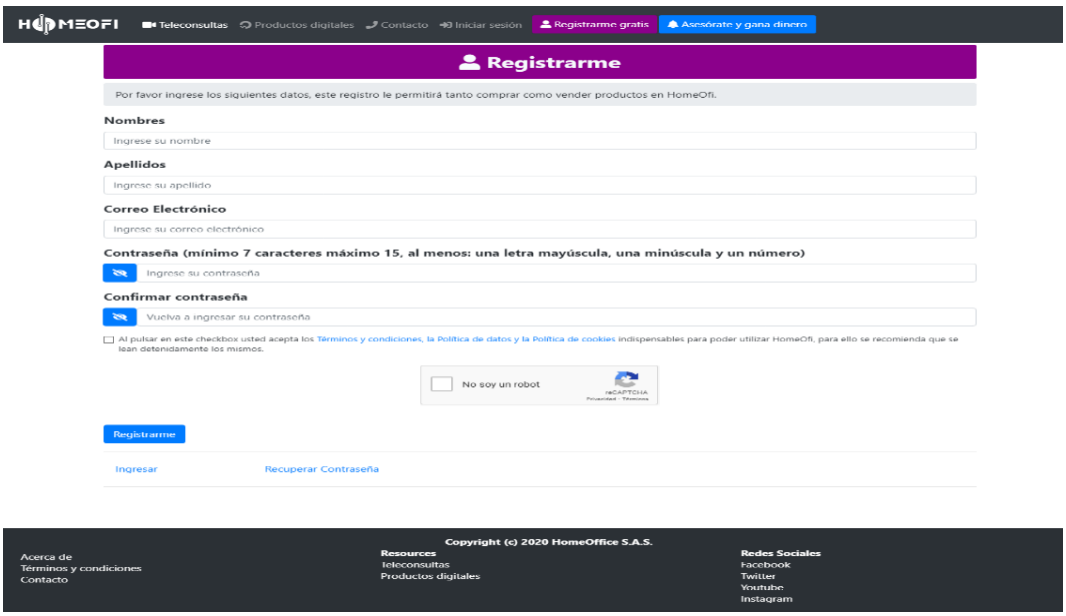

Figura 23: Vista de Registro de Cliente (Vacía)

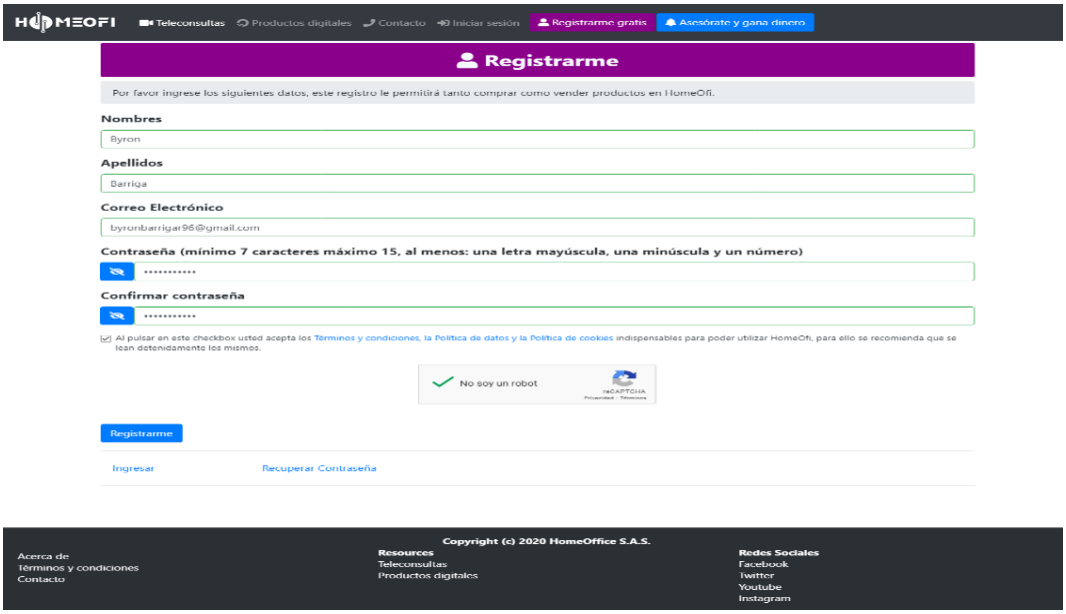

Figura 24: Vista de Registro Cliente (Llena)

En la Figura 31 se observa el registro de un cliente, el cual cuenta con la incorporación del Captcha y validaciones de Javascript en los datos, y en la Figura 32 se muestra la manera correcta del ingreso y validación de datos para llevar acabo un registro exitoso.

Vista del Registro Exitoso en el Sistema

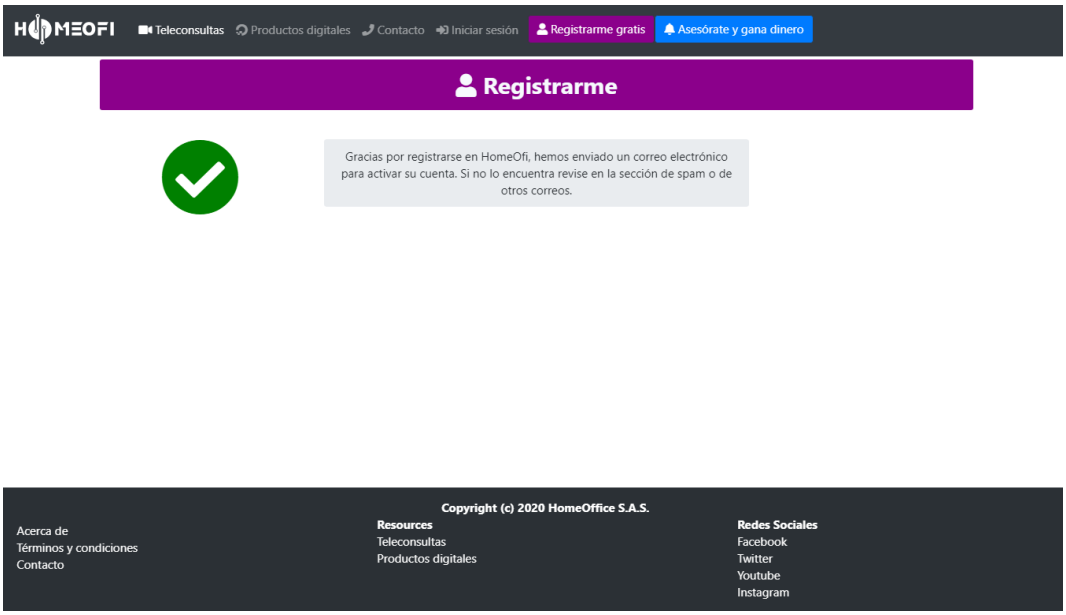

Figura 25: Vista de Registro Exitoso de Cliente

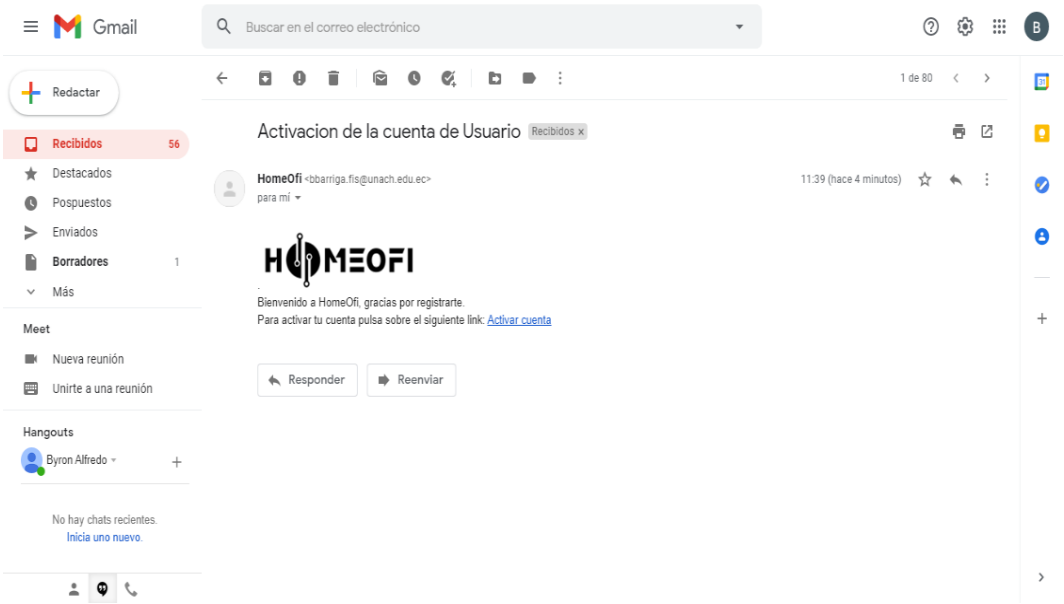

Figura 26: Email enviado al Correo Electrónico

En la Figura 33 se muestra la vista del correcto registro del cliente, con un respectivo mensaje de validación del registro, y en la Figura 34 se muestra el link de activación de la cuenta mediante el correo electrónico registrado.

Vista de la Activación de la Cuenta de Usuario

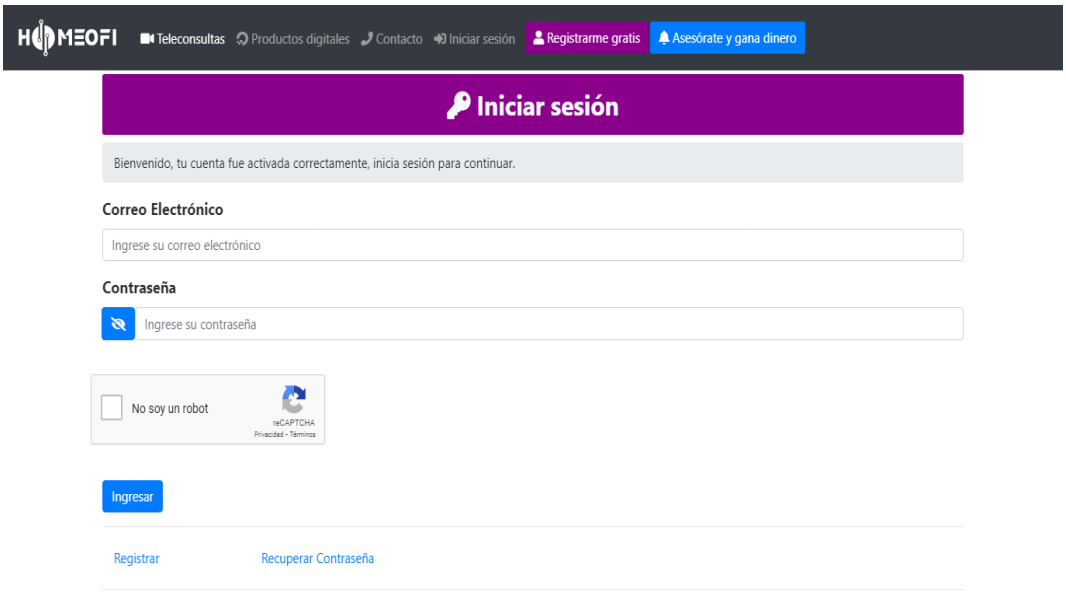

Figura 27: Activación de Cuenta de Cliente

En la Figura 35 se muestra la vista luego de que el cliente pulso el link de activación de la cuenta enviado al correo electrónico registrado, el cual manda el token y el codigo de activación encriptado.

Vista de Ingreso al Sistema (Login de Usuarios)

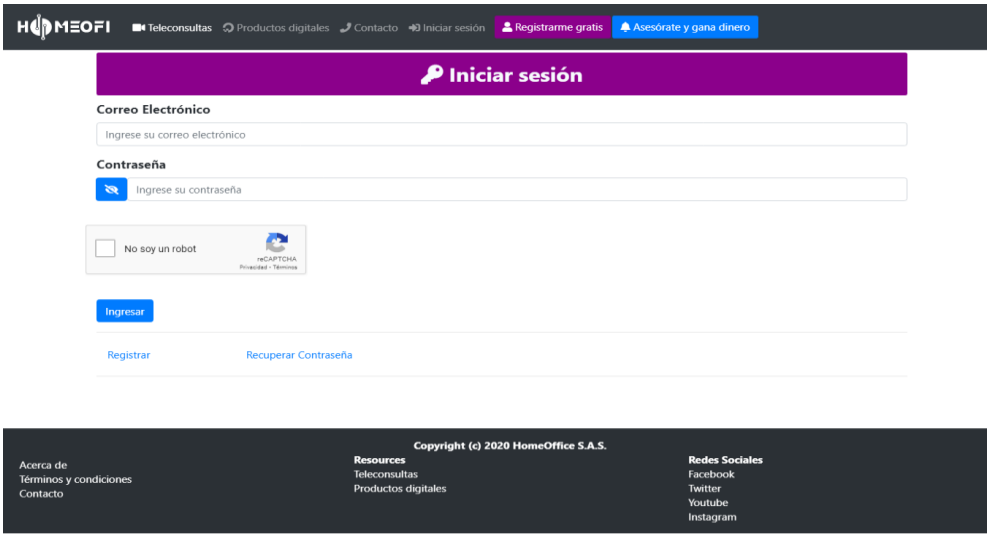

Figura 28: Vista de Login

En la Figura 36 se muestra la vista de todos los usuarios para ingresar al sistema, cabe destacar que tiene incorporado el captcha en el momento del ingreso para la verificación, dando una protección extra al momento del ingreso del sistema

Vistas de la Autentificación por Doble Factor

- **Cliente**

Figura 29: Vista Autentificación Doble Factor Cliente

Figura 30: Codigo de la App Google Authenticator del Cliente

- **Administrador**

Figura 31: Vista Autentificación Doble Factor Administrador

Figura 32: Codigo de la App Google Authenticator del Administrador

- **SuperAdministrador**

Figura 33: Vista Autentificación Doble Factor SuperAdministrador

Figura 34: Codigo de la App Google Authenticator del SuperAdministrador

En las Figuras 37, 39 y 41 se muestra la Autentificación para el cliente, administrador y superadministrador respectivamente, en el cual incluye el nombre del usuario y el rol al que pertenece, los links para descargar la aplicación de Google Authenticator y el codigo QR para el ingreso del sistema y en las Figuras 38, 40 y 42 se muestra el codigo generado al escanear el codigo QR con la aplicación Google Authenticator.

Vista del Aviso de Inicio de Sesión

- **Cliente**

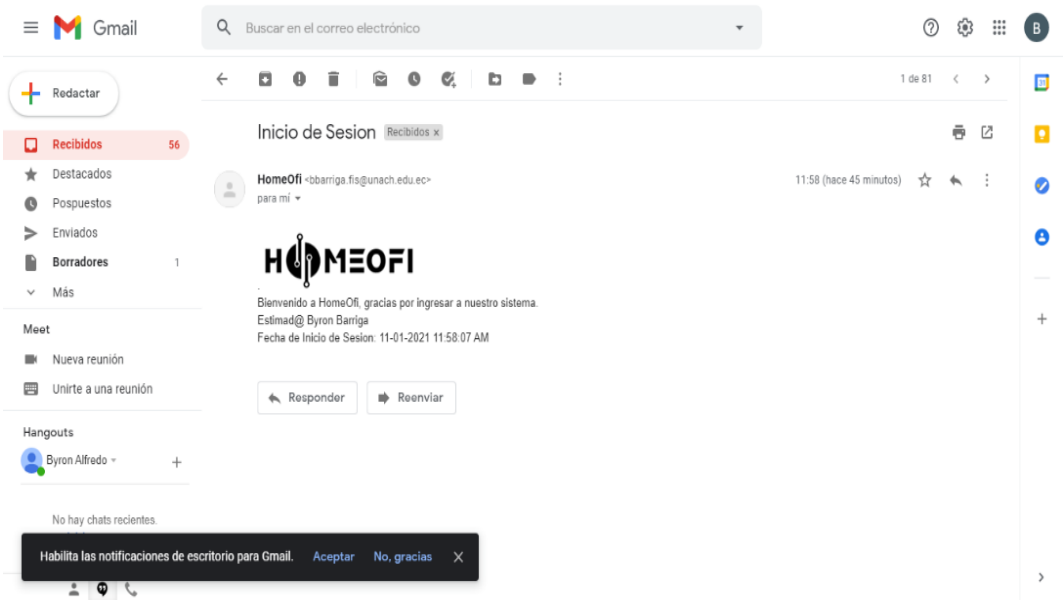

Figura 35: Email enviado del inicio de sesión de usuario (Gmail)

- **Administrador**

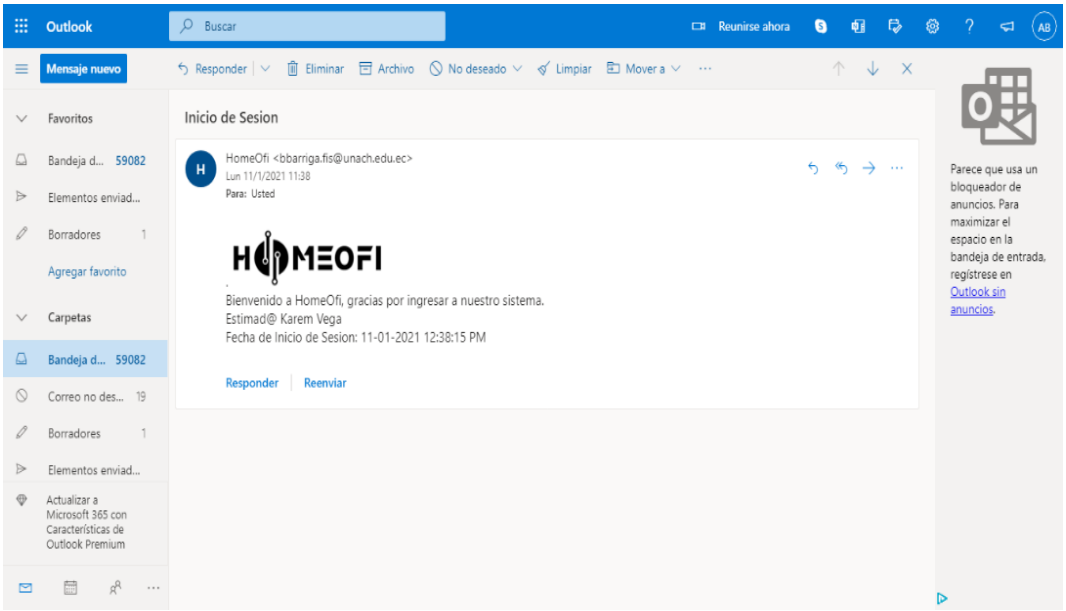

Figura 36: Email enviado del inicio de sesión de usuario (Outlook)

En las Figuras 43 y 44 se muestra la notificación al correo electrónico al momento del ingreso al sistema, mostrando datos como el nombre y fecha del inicio de sesión.

Vista del Cliente del Módulo de Seguridad (Panel Principal)

Figura 37: Panel Principal del Cliente

En la Figura 45 se muestra el panel principal del Cliente registrado, cabe destacar que el caso del módulo de seguridad, solo tiene vigente las opciones de Cambio de Contraseña y Acceso a la edición de su propio perfil del sistema.

Vista del Cambio de Contraseña del Cliente

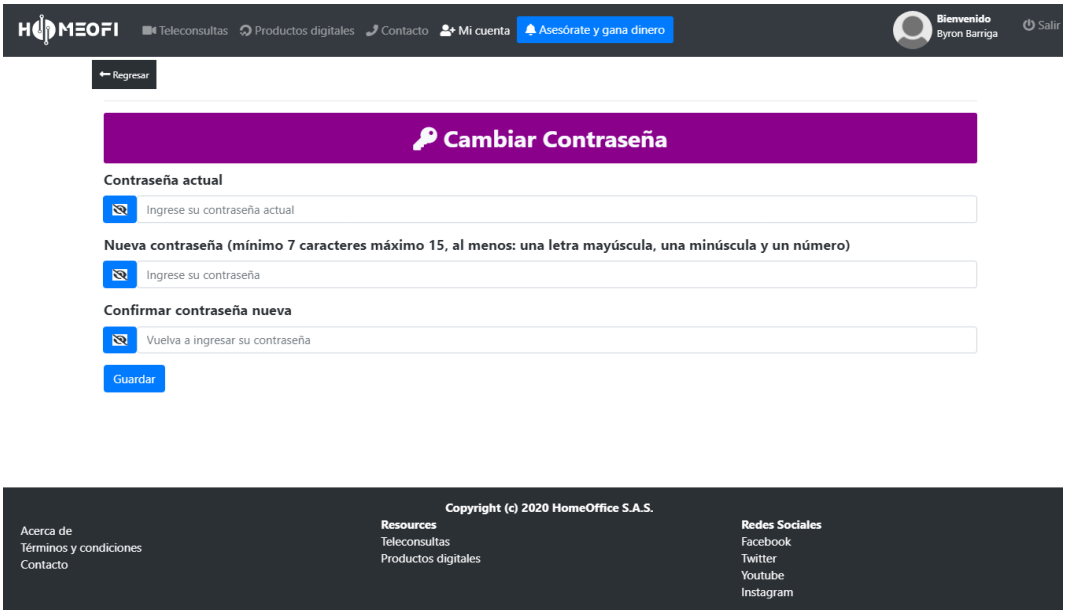

Figura 38: Vista del cambio de contraseña del usuario

En la Figura 46 se muestra la vista para el cambio de contraseña del cliente manteniendo siempre las validaciones con JavaScript y bloqueando en el caso de 5 veces ingresar de manera incorrecta la contraseña actual.

Vista del Perfil Personal del Cliente (Datos Generales)

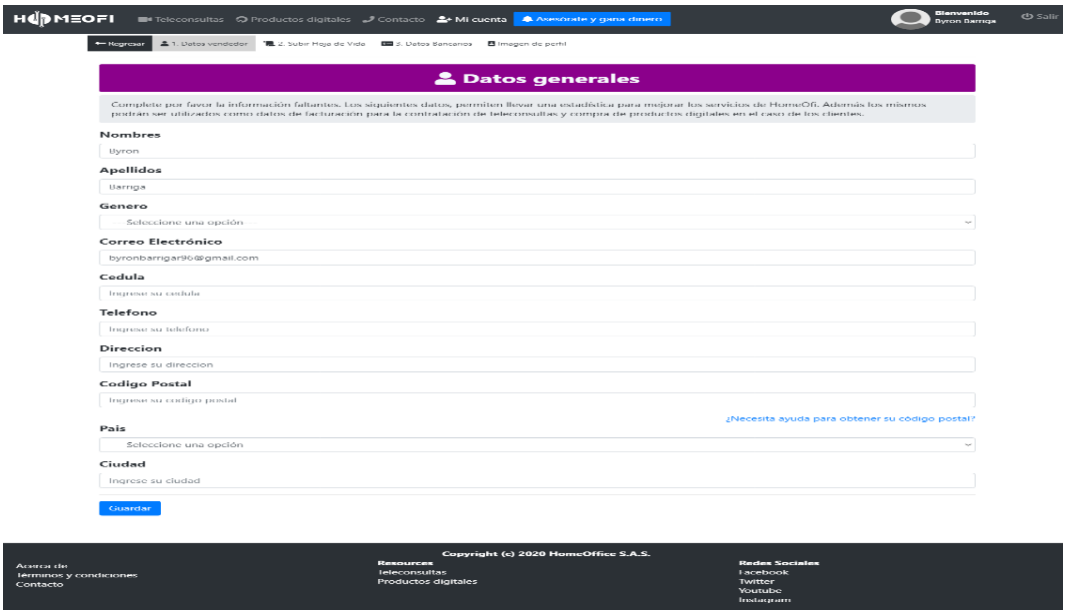

Figura 39: Vista del Perfil del Cliente

En la Figura 47 se muestra los datos generales del cliente los mismos que fueron ingresados al momento del registro, en esta vista se puede realizar la actualización de la información, además de ser la vista principal de la Información del Cliente divido en un panel donde puede ingresar los datos faltantes

Vista del Perfil Personal del Cliente (Hoja de Vida)

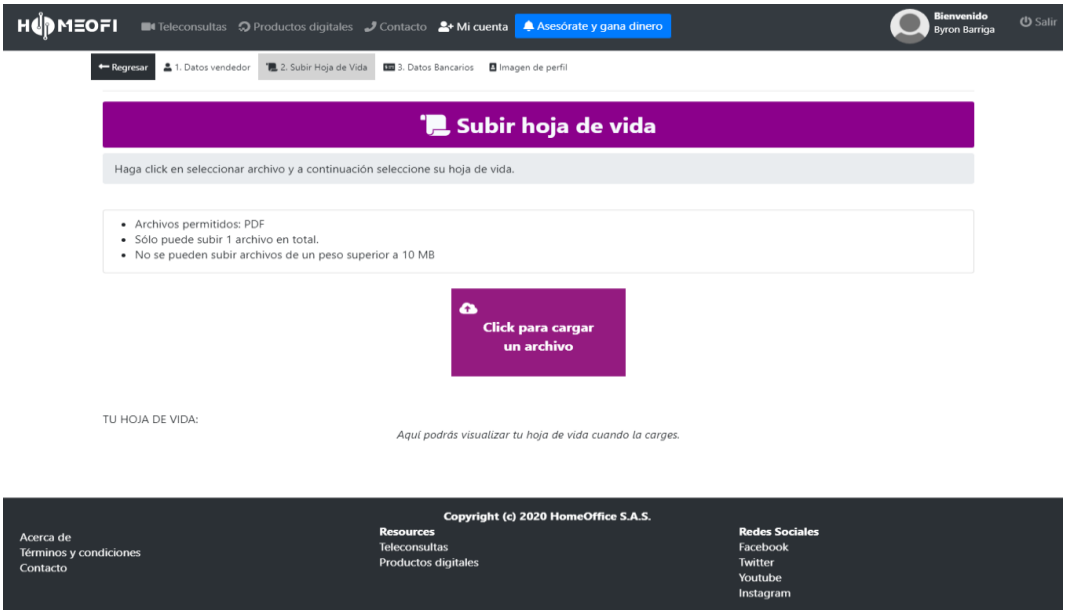

Figura 40: Vista de la Hoja de Vida del Cliente

En la Figura 48 se muestra la vista para poder subir y visualizar el archivo de la hoja de vida del cliente, el cual debe de estar en formato pdf.

Vista del Perfil Personal del Cliente (Datos Bancarios)

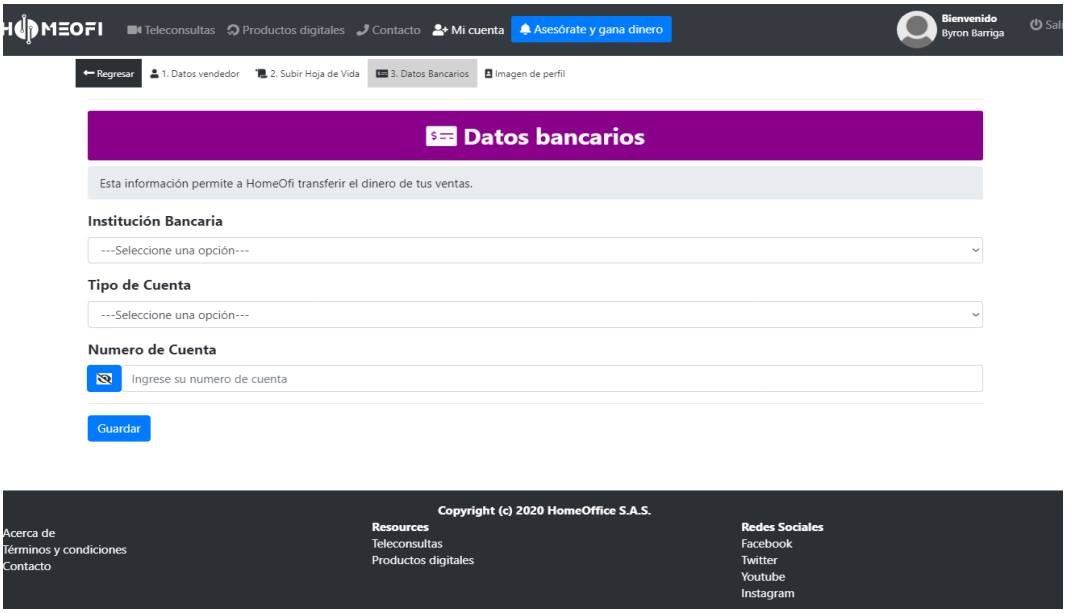

Figura 41: Vista de los Datos Bancarios del Cliente

En la Figura 49 se muestra los datos bancarios del cliente los cuales deben ser actualizados para cualquier tipo de transacción monetaria, tiene validaciones con Javascript y cuenta con la mayoría de entidades bancarias registradas del país.

Vista del Perfil Personal del Cliente (Imagen de Perfil)

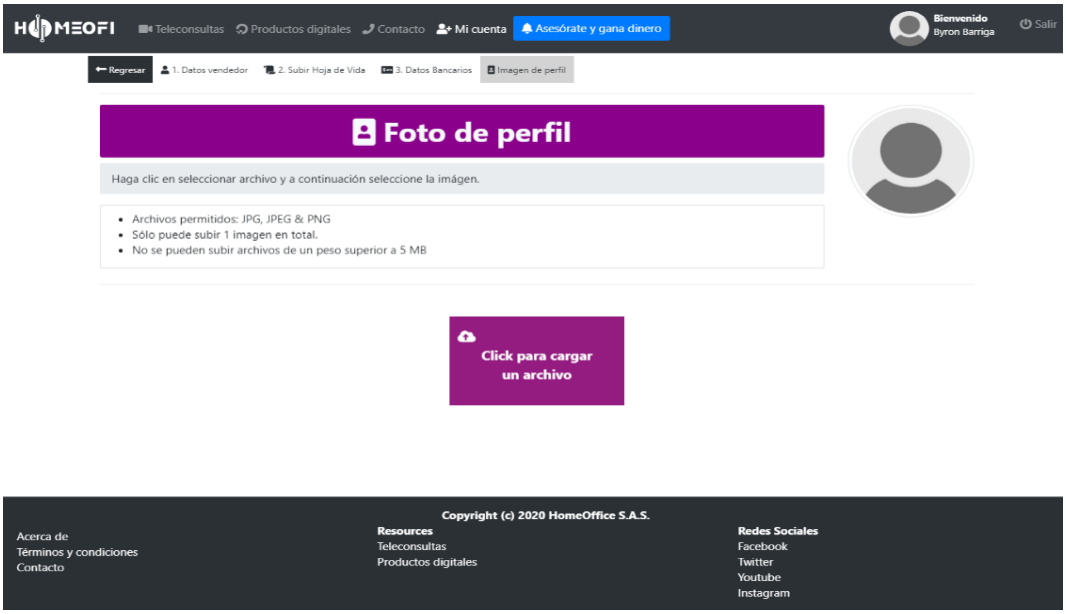

Figura 42: Vista de la Imagen de Perfil del Cliente

En la Figura 50 se muestra la vista para poder subir y visualizar la imagen de perfil del cliente el cual al cambiar se actualizará automáticamente en todas las vistas, además el archivo debe estar en formato png, jpg o jpeg.

Vista del Panel Principal del Administrador

Figura 43: Vista Principal del Panel del Administrador

En la Figura 51 se muestra la vista del Panel Principal para cualquier administrador en el cual tiene las opciones de cambiar su contraseña, revisar el Panel de los Clientes registrados por el sistema, e ir al panel de los usuarios con problemas.

Vista del Perfil del Administrador

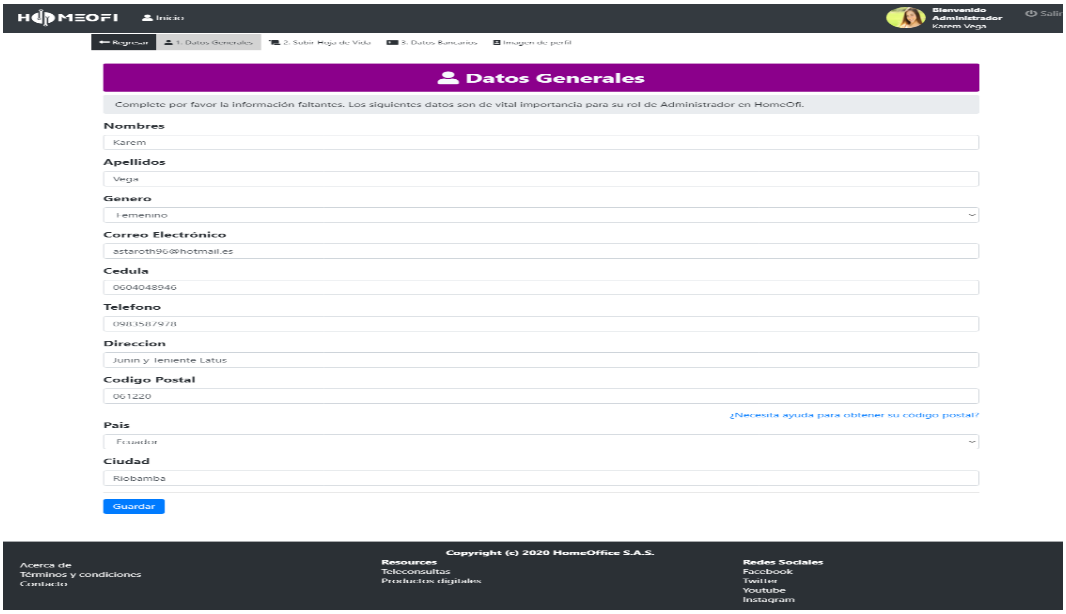

Figura 44: *Vista de* Datos Generales del Administrador

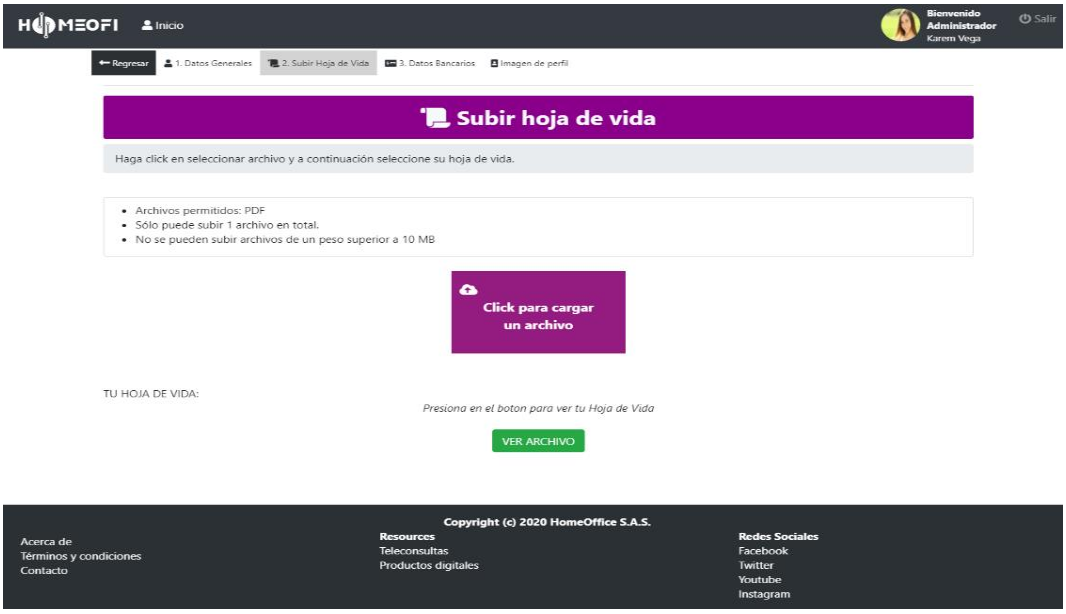

Figura 45: Vista de Hoja de Vida del Administrador

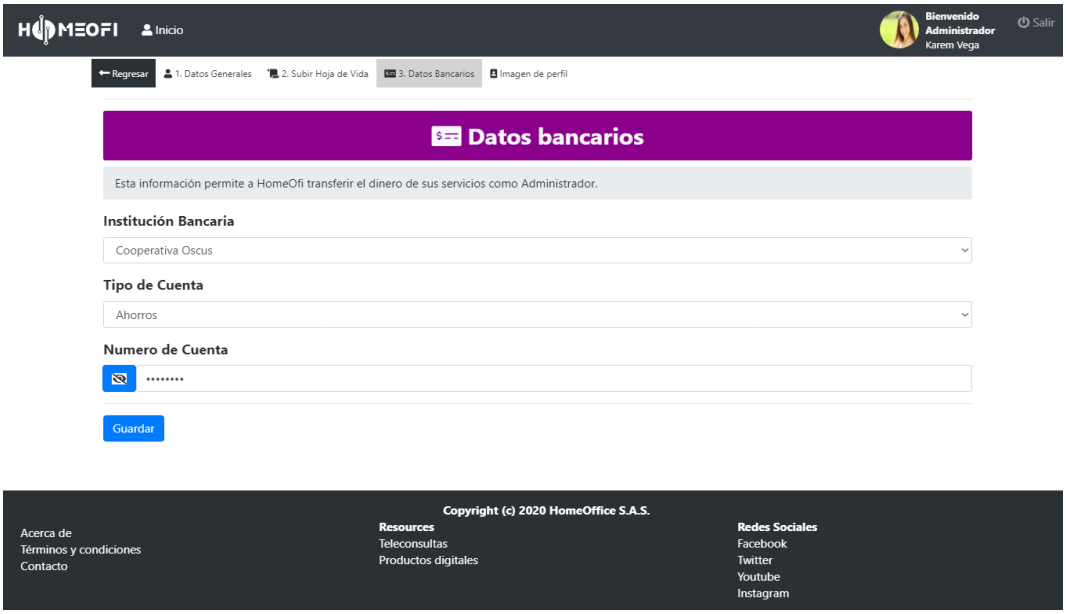

Figura 46: Vista de Datos Bancarios del Administrador

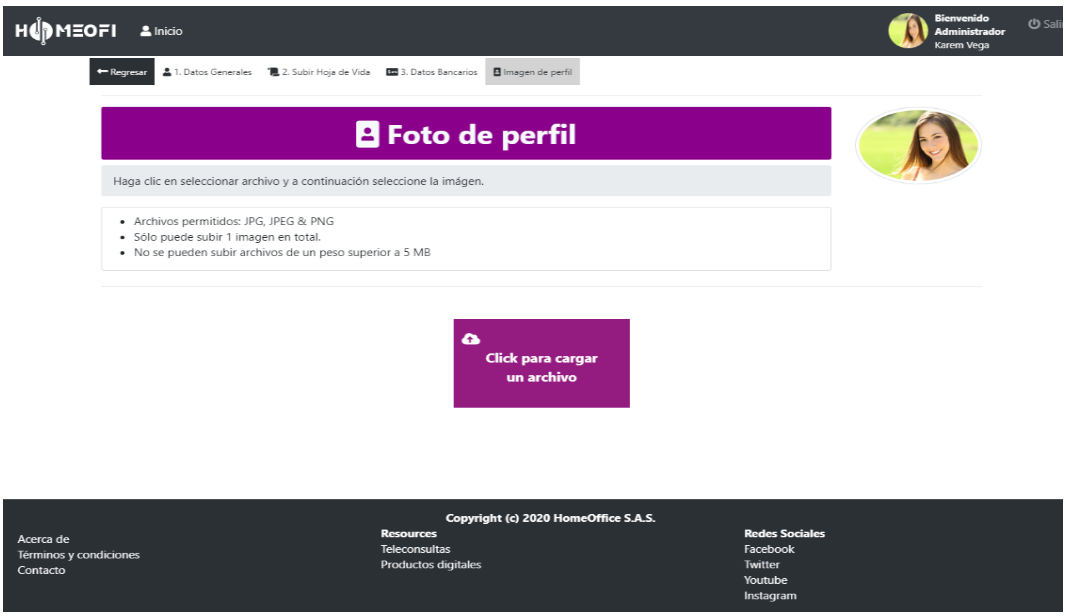

Figura 47: Vista de la Imagen Perfil del Administrador

En las Figuras desde la 52 hasta la 55 se muestra el Perfil del Administrador de misma manera que el Cliente se puede realizar la actualización de cada uno de sus apartados, descritos anteriormente, siendo la misma funcionalidad que el perfil del Cliente.

Vista de los Clientes Registrados y sin ningún tipo de Problema

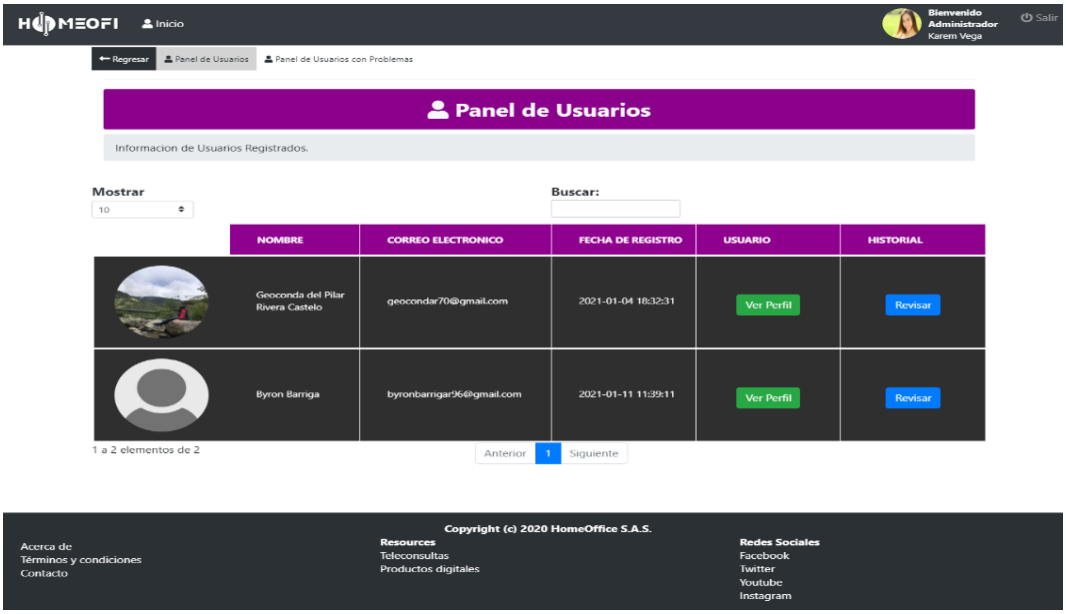

Figura 48: Vista de Clientes

En la Figura 56 se muestra el panel de los usuarios registrados y sin ningún tipo de problema, en el cual se puede revisar el historial realizado por el cliente registrado y ver el perfil con los datos personales del cliente.

Vista de Información Personal del Cliente registrado

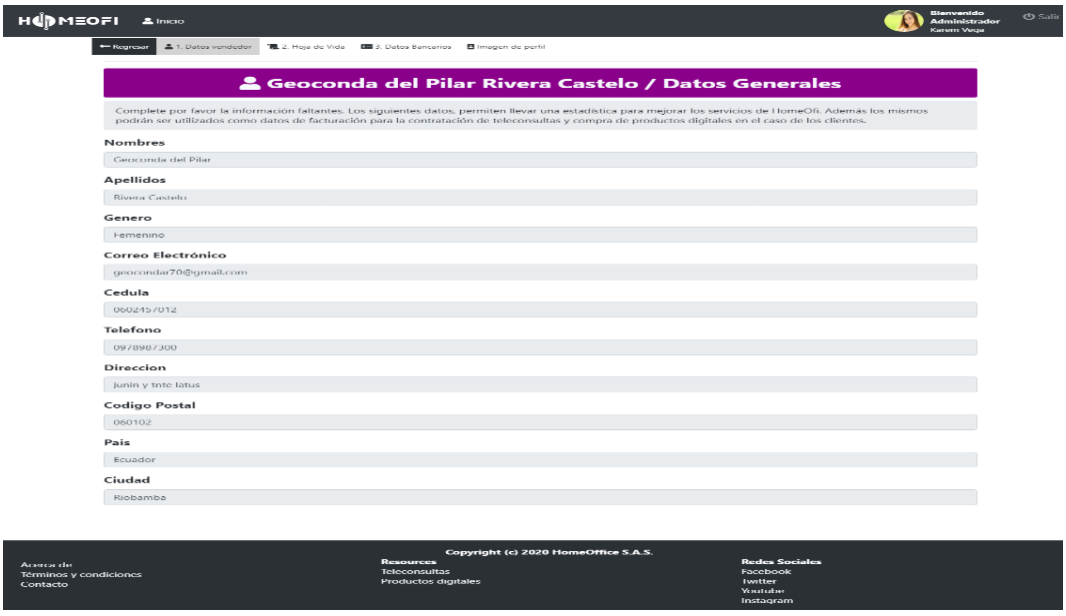

Figura 49: Datos Generales del Cliente Registrado

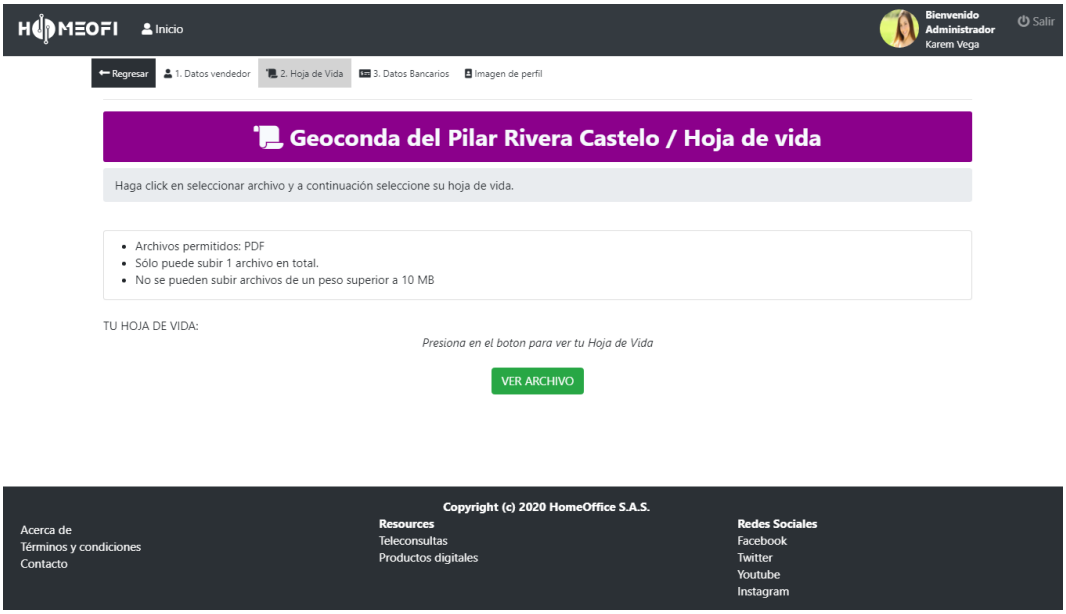

Figura 50: Hoja de Vida del Cliente Registrado

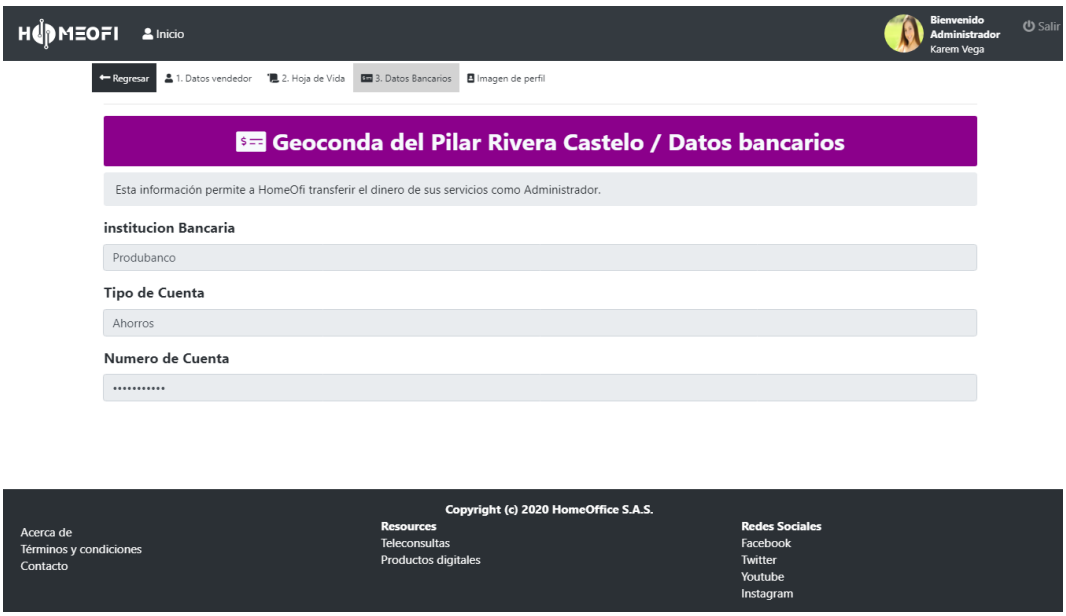

Figura 51: Datos Bancarios del Cliente Registrado

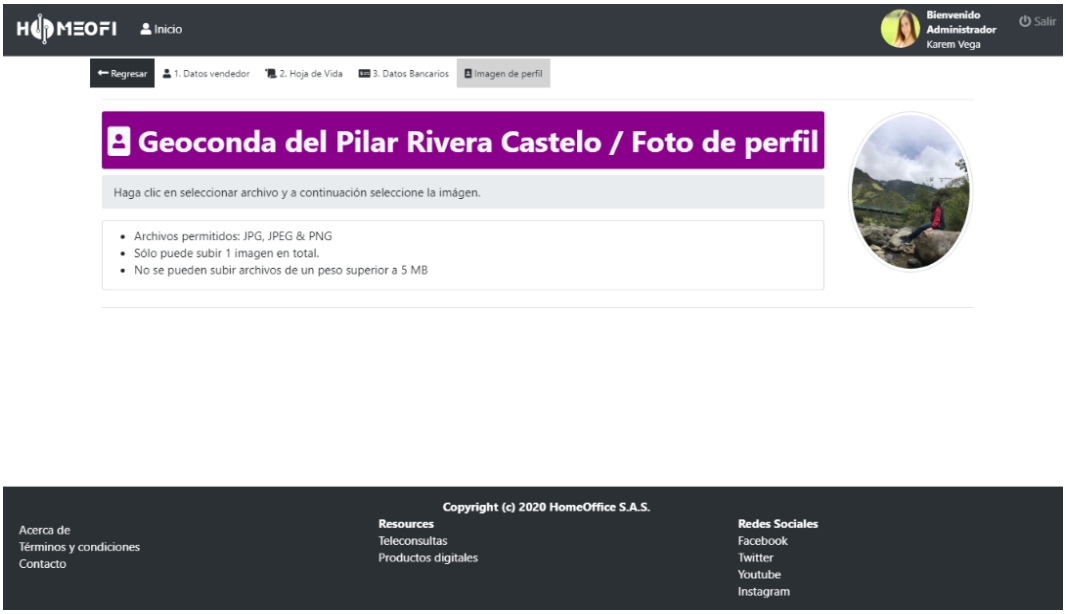

Figura 52: Imagen de Perfil del Cliente Registrado

En las Figuras desde la 51 hasta la 60 se muestra el perfil del cliente seleccionado el cual no tiene ningún tipo de bloqueo por el sistema, dicha información es inalterable por lo que solamente se puede visualizar, pero no editar por parte del Administrador.

Vista del historial de un cliente registrado

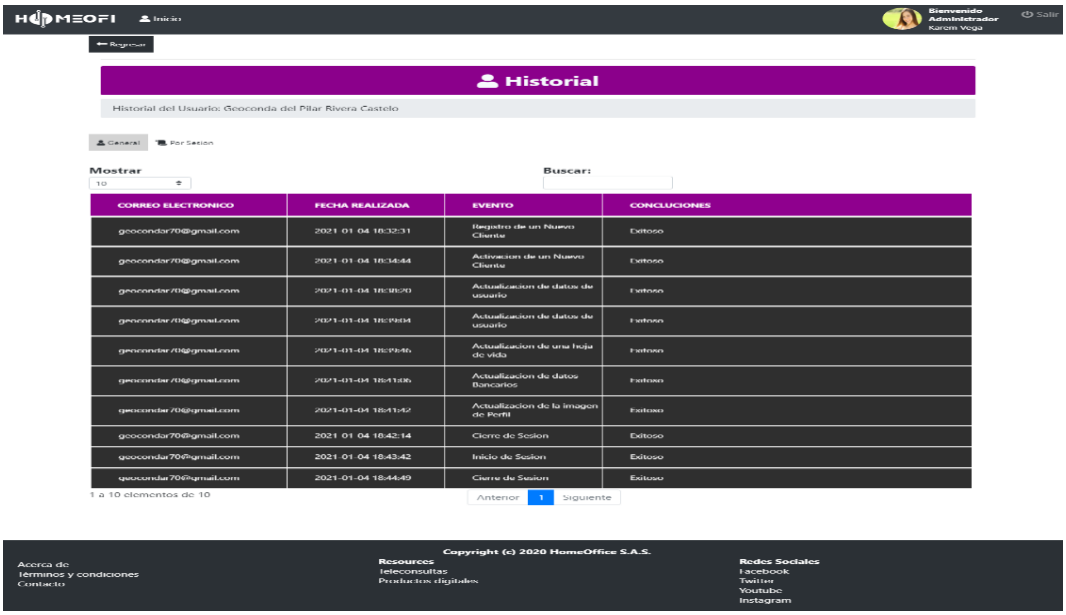

Figura 53: Historial del Cliente Registrado

En la Figura 61 se muestra el historial general de todas las acciones realizadas por el cliente seleccionado en el cual se puede revisar por sesión y de manera general.

Vista del historial de un cliente registrado por sesión

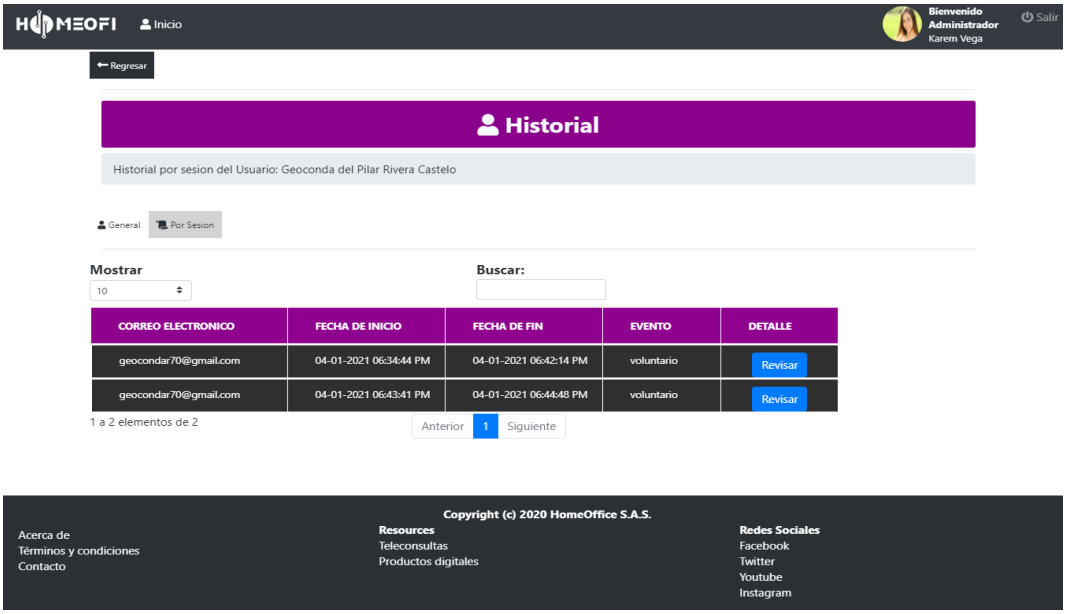

Figura 54: Historial por Sesión del Cliente Registrado

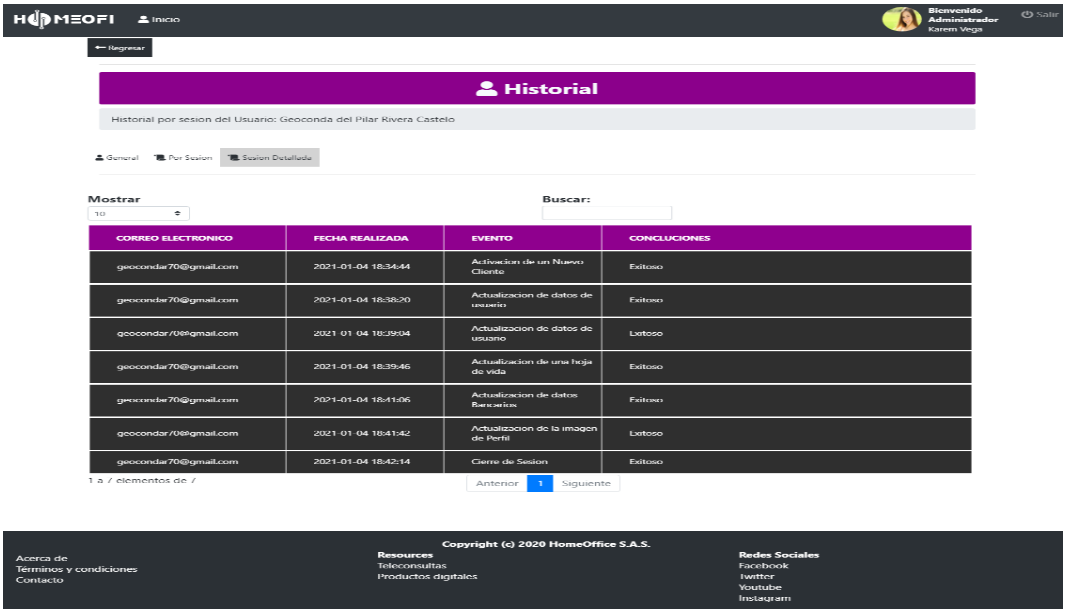

Figura 55: Historial detallado de la Sesión del Cliente Registrado

En la Figura 61 se muestra el historial de acciones organizado por sesiones realizadas por el cliente, y en la Figura 63 se muestra el historial de cada una de las acciones realizadas en cada una de sus respectivas sesiones.

Vista de clientes bloqueados o con problemas

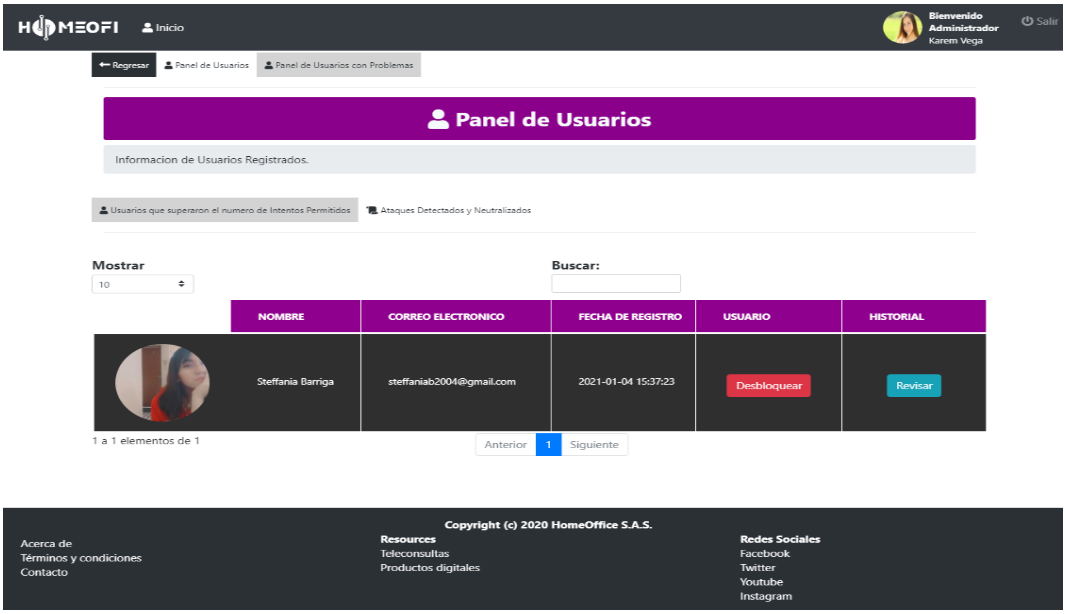

Figura 56: Vista de los Clientes Bloqueados

En la Figura 64 se muestra una lista de usuarios bloqueados los cuales en su mayoría son por superar los intentos permitidos al momento de Logueo o en el cambio de contraseña, en esta vista da la opción de desbloquear a dicho usuario y ver el historial del mismo.

Vista de Ataques detectados y neutralizados por el Módulo de Seguridad

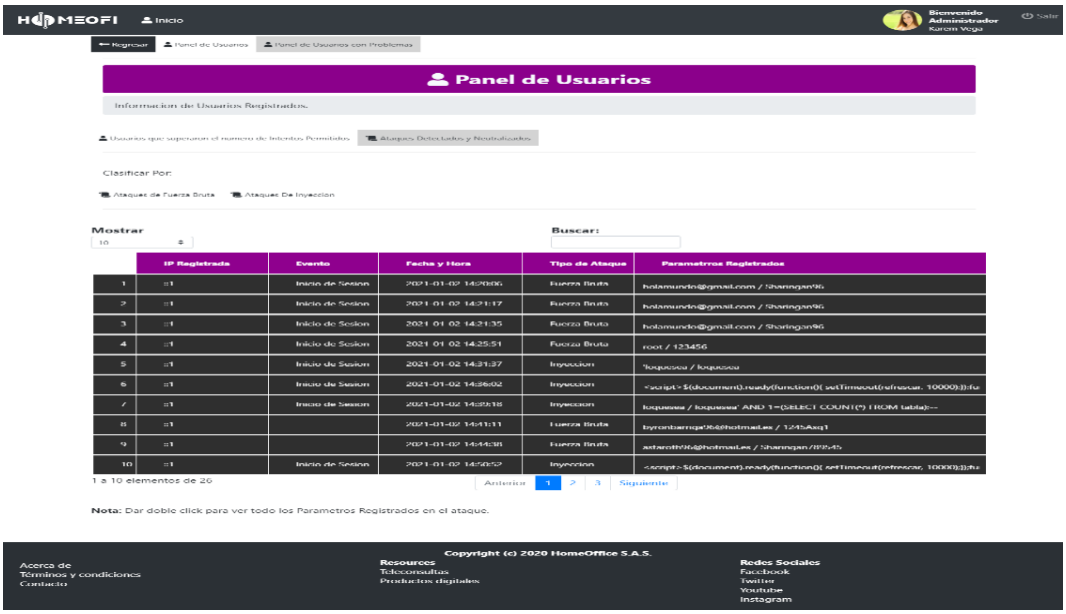

Figura 57: Vista de los Ataques Informáticos realizados al sistema

En la Figura 65 se muestra una lista de ataques realizados hacia el sistema, clasificados por ataques de inyección o de fuerza bruta, en dicha lista se evidencia la ip desde la que fue realizada, el tipo de ataque y los parámetros utilizados para realizar el ataque informático.

Vista del Panel principal del SuperAdministrador

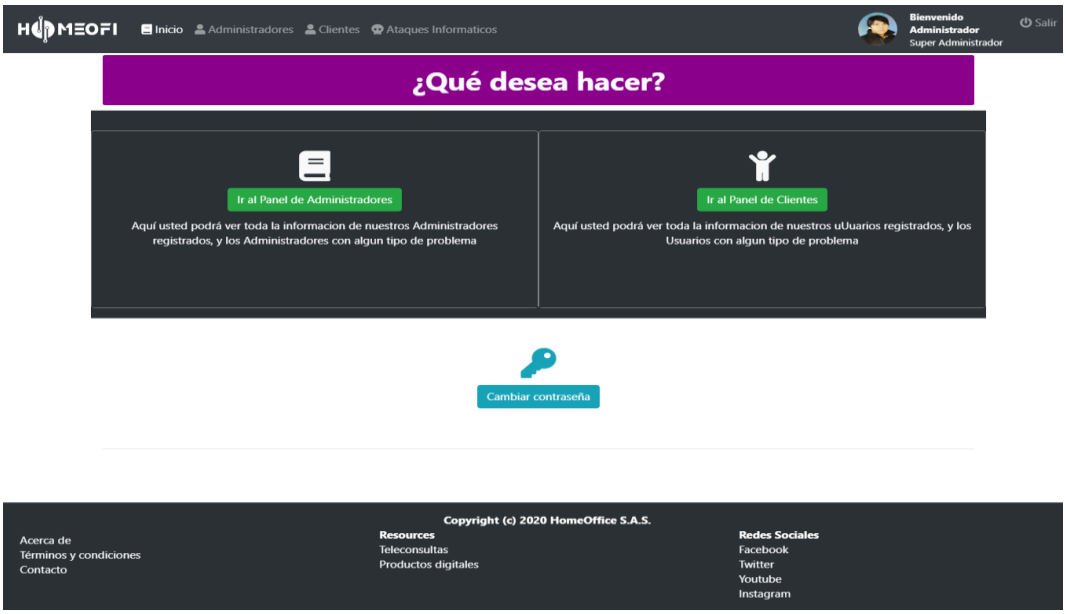

Figura 58: Vista del Panel Principal del SuperAdministrador

En la Figura 66 se muestra el panel principal de acceso al módulo de seguridad por parte del SuperAdministrador en el cual tiene las opciones de ir al panel de Administradores o Clientes, además de poder realizar el cambio de la contraseña, se puede también acceder al panel de datos personales y al panel de ataques informáticos detectados y neutralizados.

Vista del Panel de Información Personal del Super Administrador

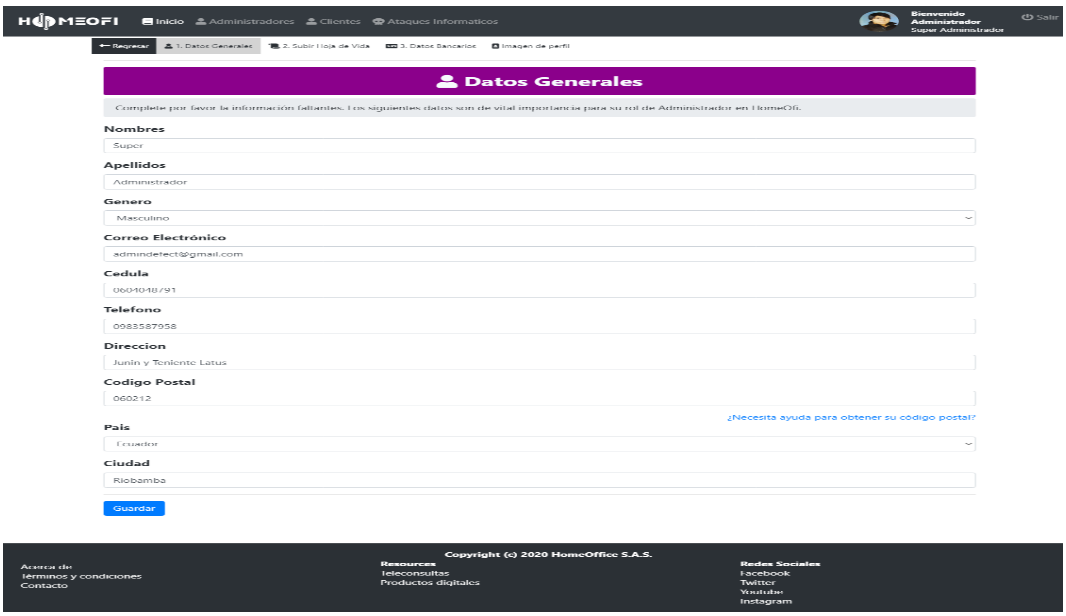

Figura 59: Vista de Datos Generales del SuperAdministrador

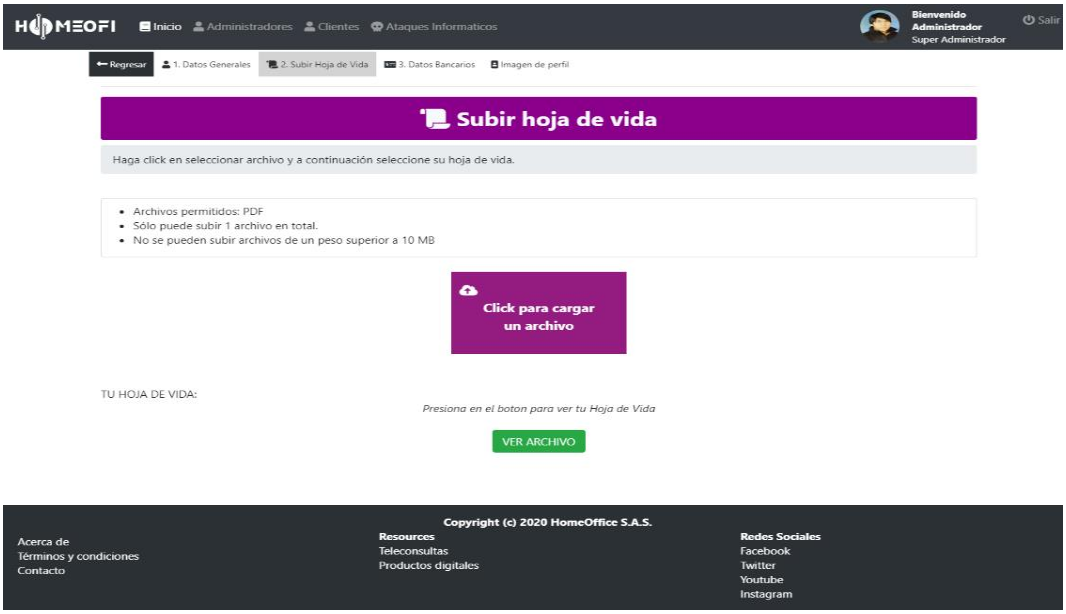

Figura 60: Vista de la Hoja de Vida del SuperAdministrador

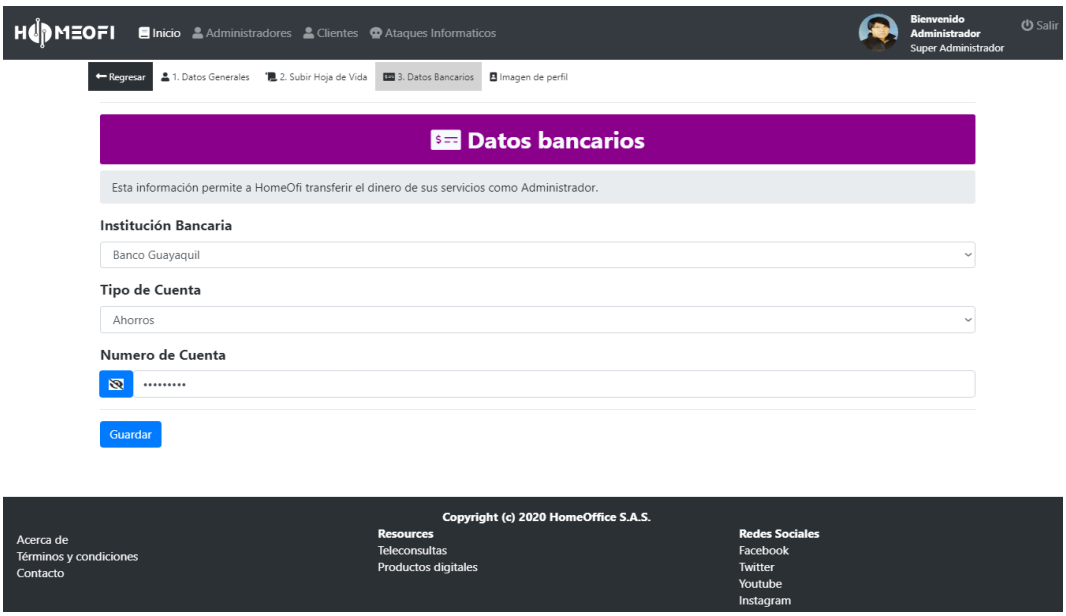

Figura 61: Vista de Datos Bancarios del SuperAdministrador

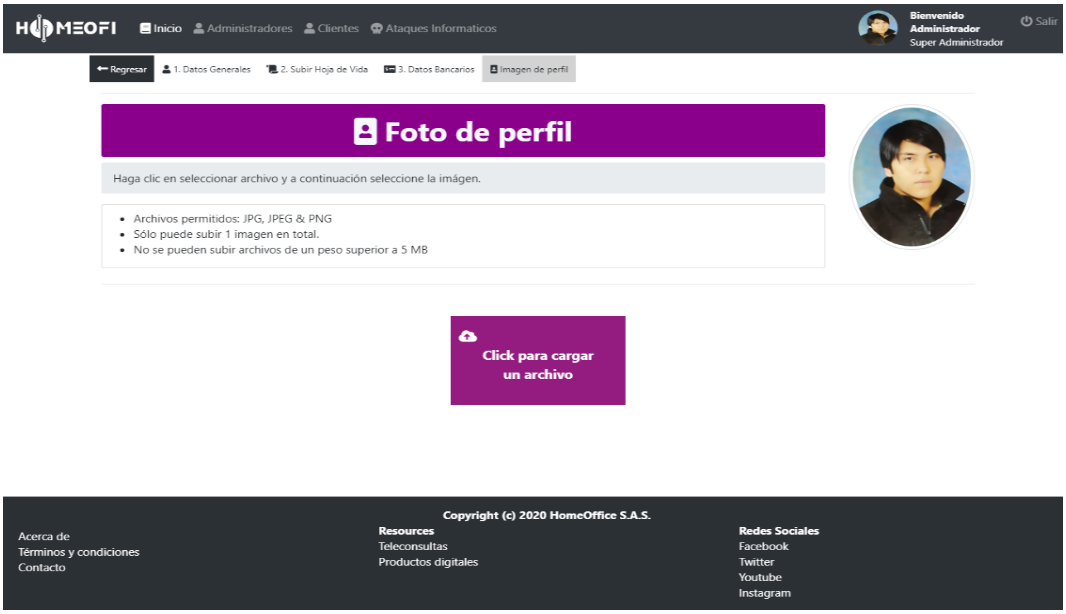

Figura 62: Vista de la Imagen de Perfil del SuperAdministrador

En las Figuras desde la 67 hasta la 70 se muestra la información personal del SuperAdministrador, la misma que tiene la misma funcionalidad que las vistas de información personal de Administradores como de Clientes.

Vista del Panel Principal de Administradores

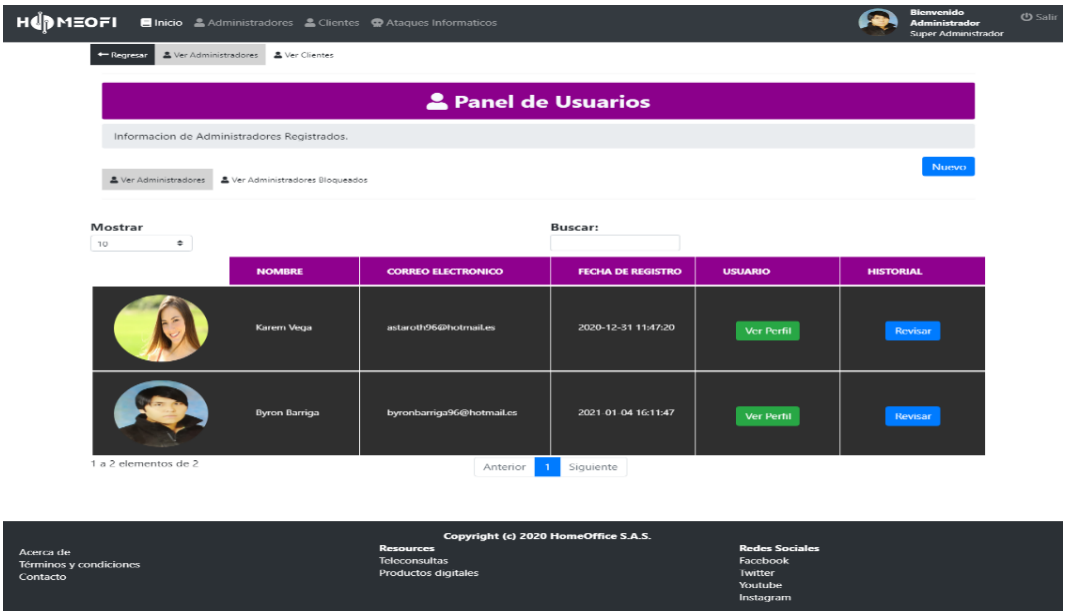

Figura 63: Vista de Administradores

En la Figura 71 se muestra un listado de todos los Administradores registrados en el Sistema, además de un botón para agregar un nuevo Administrador, la clasificación de los Administradores se lo realiza en 2 grupos, Administradores con y sin problemas, en la presente vista se muestra los Administradores sin problemas.

Vista del Registro de un nuevo Administrador

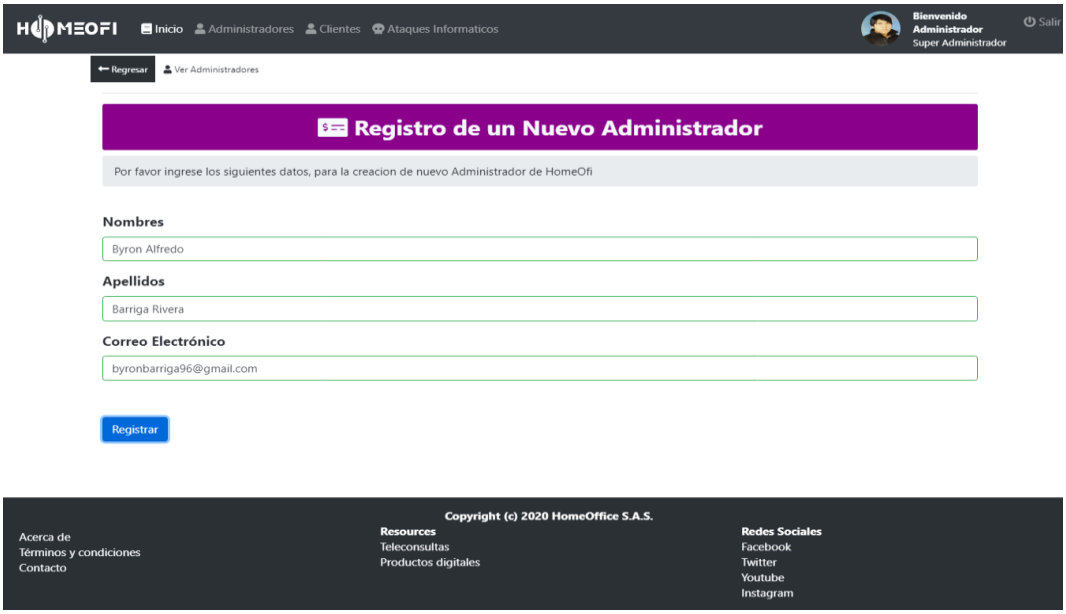

Figura 64: *Vista de Registro de un Administrador*

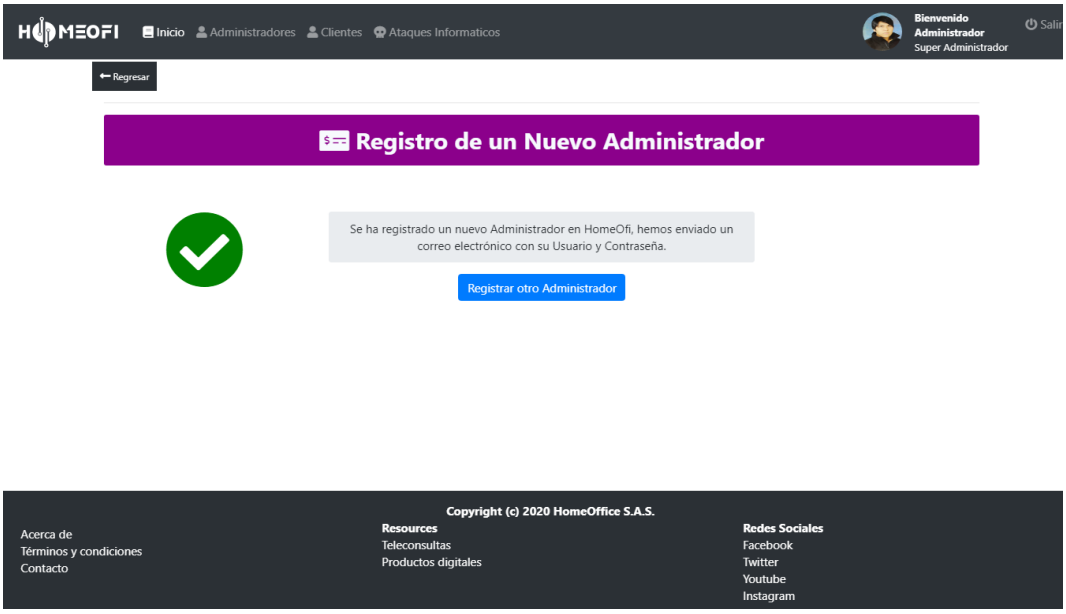

Figura 65: Vista de un Administrador Registrado de manera correcta

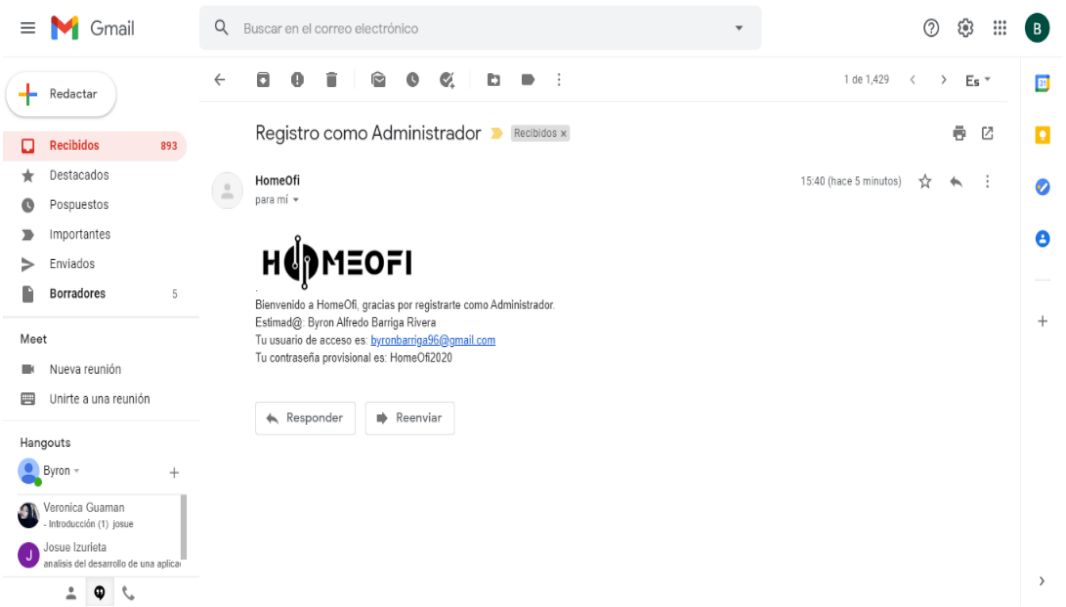

Figura 66: Email enviado al Administrador

En las Figuras 72, 73 y 74 muestra el proceso de registro de un nuevo Administrador, desde el ingreso de los datos por parte del superadministrador y finalmente el sistema generando la clave provisional del Administrador registrado y enviándola por medio del correo electrónico registrado.

Vista del Perfil del Administrador

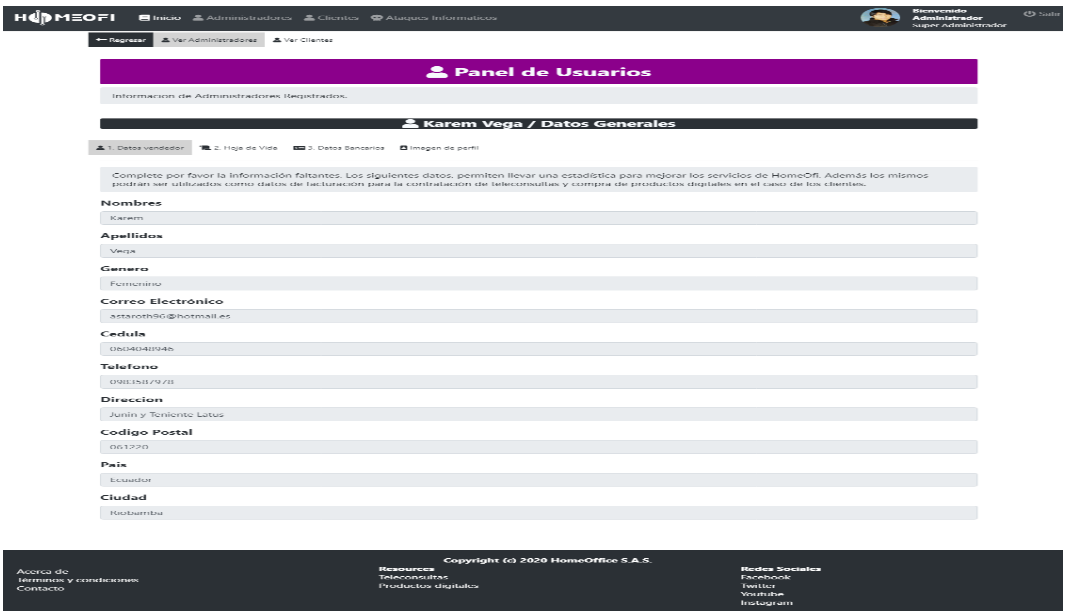

Figura 67: Datos Generales del Administrador Registrado

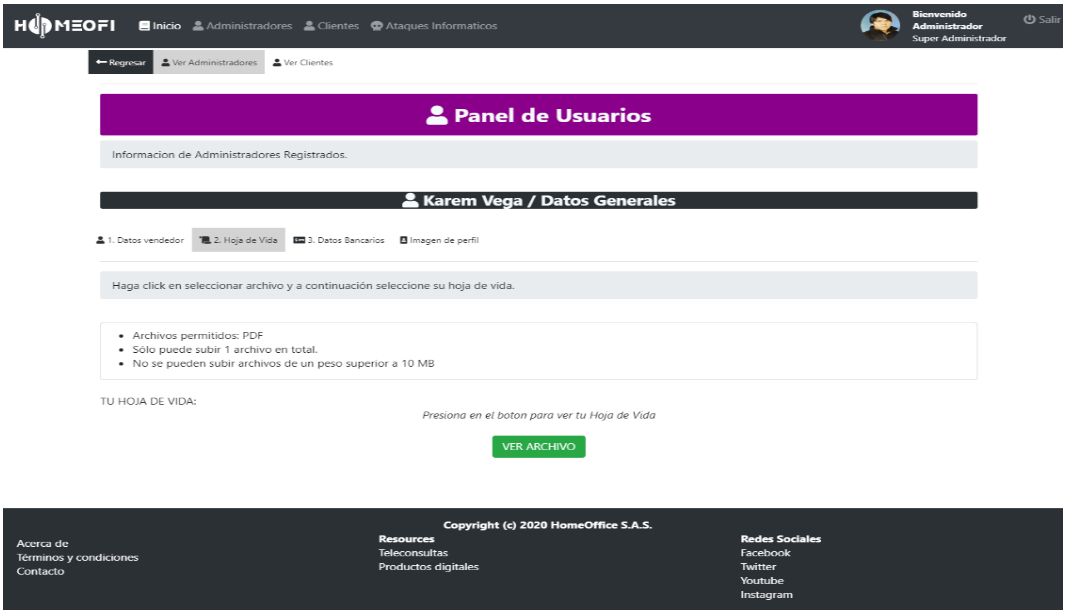

Figura 68: Hoja de Vida del Administrador Registrado

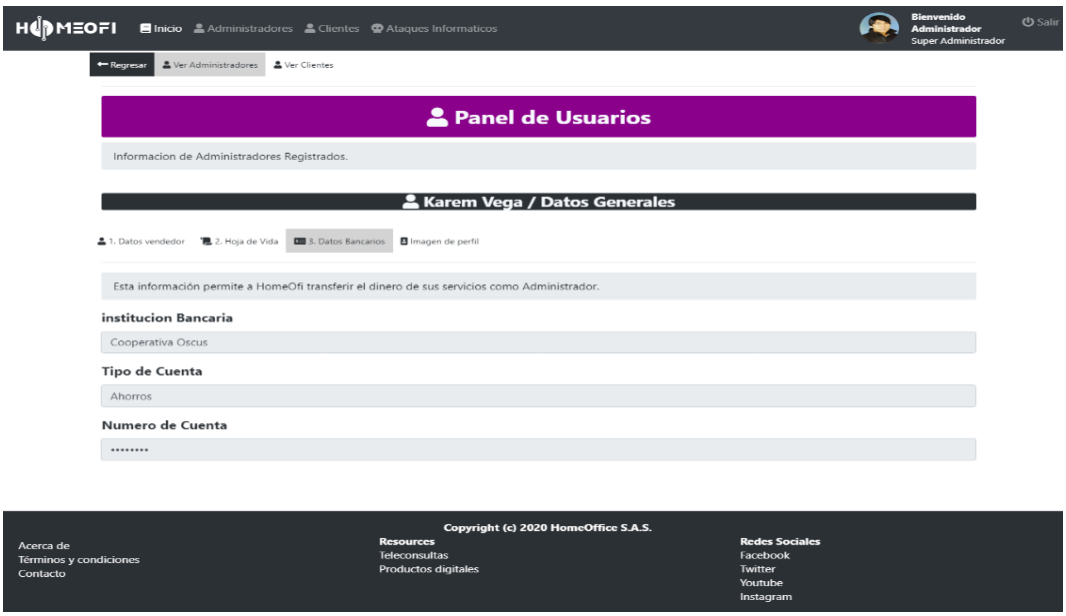

Figura 69: Datos Bancarios del Administrador Registrado

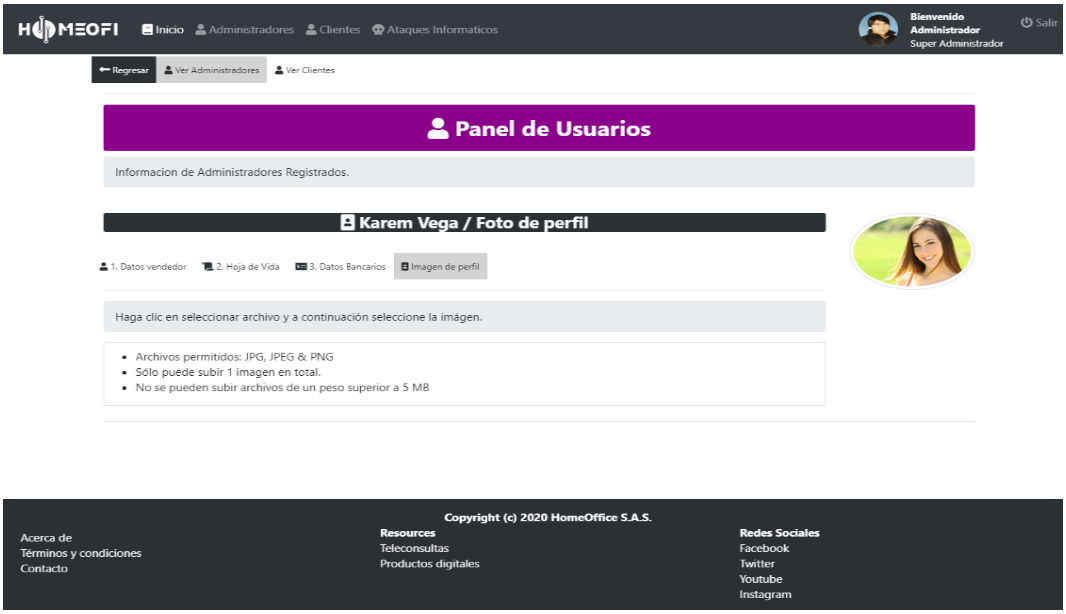

Figura 70: Imagen de Perfil del Administrador Registrado

En las Figuras desde la 75 hasta la 78 se muestra todo el perfil personal del Administrador seleccionado, el mismo que al igual que el Administrador con el Cliente solo puede ser revisado, pero no puede ser modificado.

Vista del Historial del Administrador

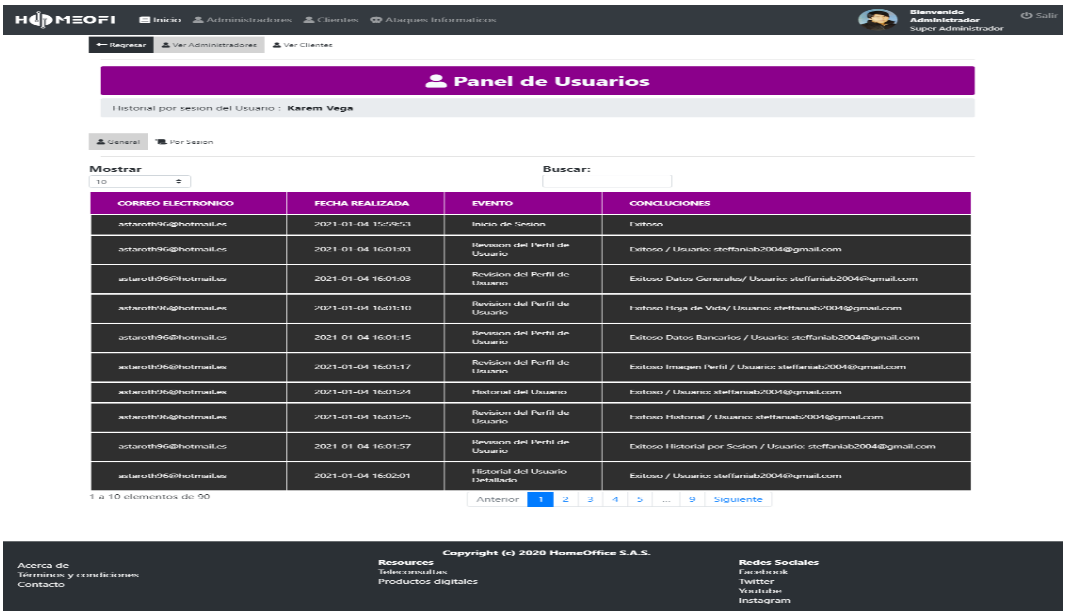

Figura 71: Historial del Administrador Registrado

En la Figura 79 se muestra todo el historial realizado por el Administrador seleccionado, siendo, teniendo de este la información por sesiones y en general igual que el del cliente revisado con anterioridad.

Vista del Panel de Administradores Bloqueados

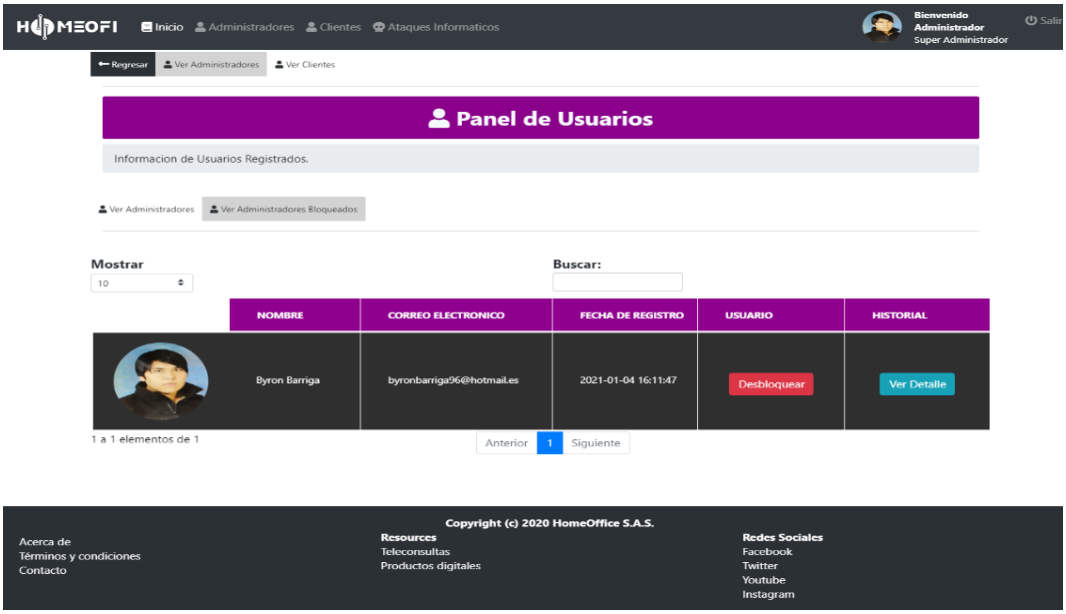

Figura 72: Vista de Administradores Bloqueados

En la Figura 80 se muestra una lista con todos los Administradores bloqueados por el sistema por super el intento de cambio de contraseña o de intentos de ingreso permitido, se muestra un botón para desbloquearlo además de revisar su historial.

Vista del Panel de Clientes Registrados

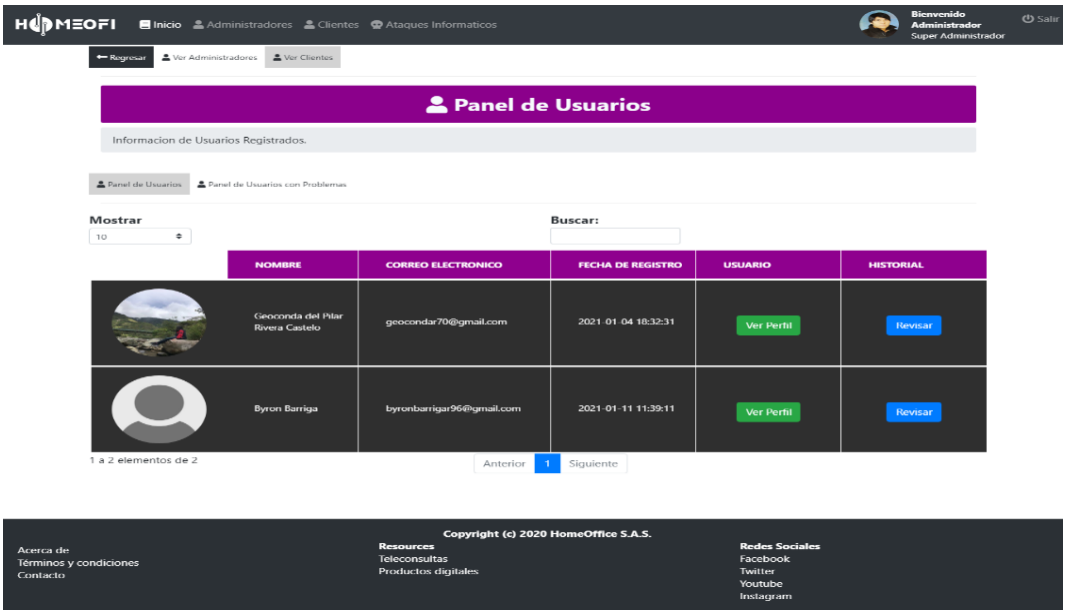

Figura 73: Vista de los Clientes Registrados

En la Figura 81 se muestra los clientes registrados y que no tengan ningún problema, funcionando tal cual revisa la información de los clientes por parte del Administrador.
Nota: Las Vistas de revisión del Perfil e Historial son exactamente las mismas que las vistas del Administrador, motivo por la que no se repetirá

Vista del Panel de Clientes Bloqueados

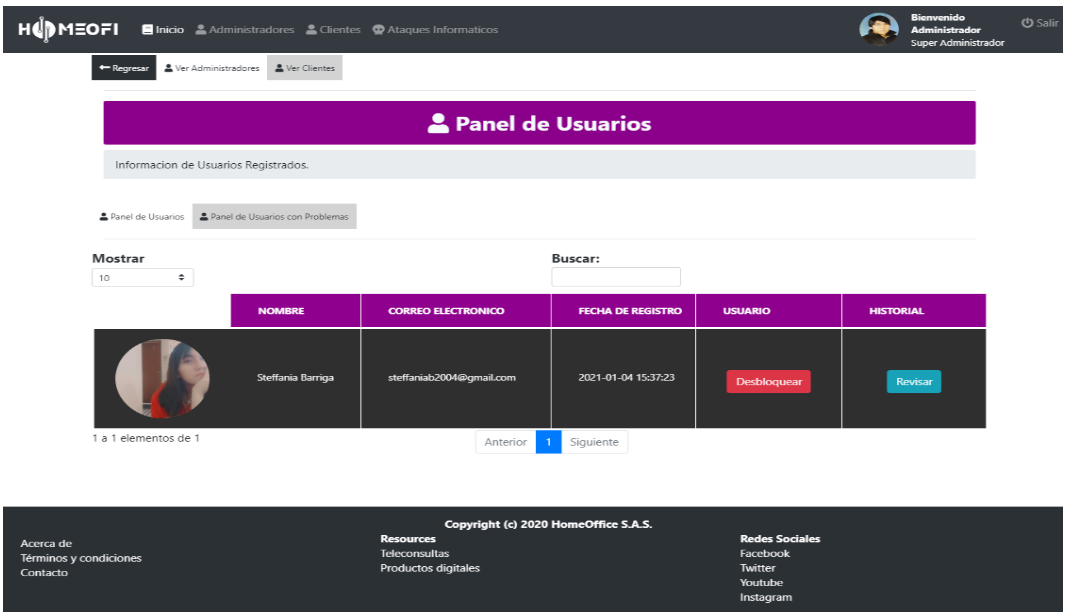

Figura 74: Vista de los Clientes Bloqueados

En la Figura 82 se muestra una lista de clientes bloqueados, el SuperAdministrador tiene la opción de desbloquear a dicho cliente o de revisar su historial.

Vista del Panel de Ataques Informáticos

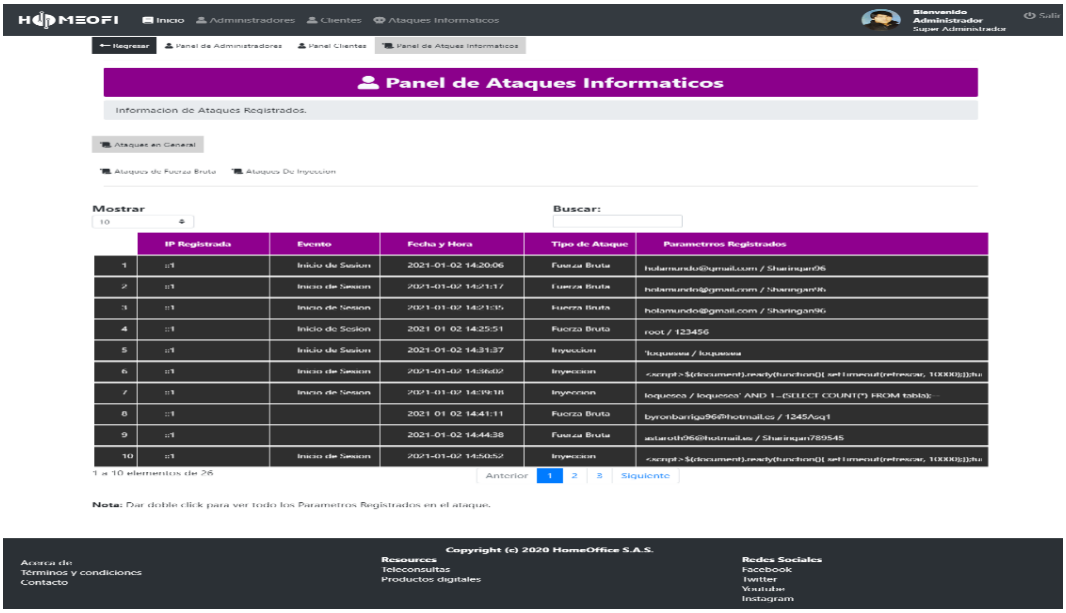

Figura 75: Vista de los Ataques Informáticos

En la Figura 83 se muestra el Panel con una lista de Ataques informáticos detectados y neutralizados por el módulo de seguridad, el mismo que se puede clasificar por ataques de Fuerza Bruta o de Inyección según lo necesite.

Vista de la Pantalla de Errores al acceder al sistema

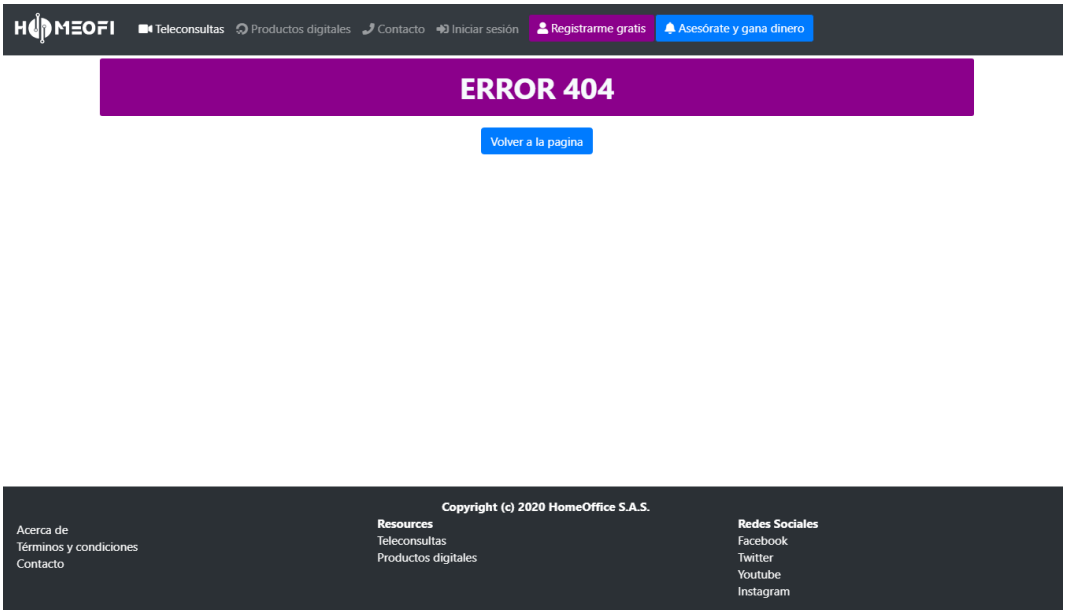

Figura 76: Vista de Errores del Sistema

En la Figura 84 se muestra la vista de los errores al momento de acceder al sistema, estos archivos son válidos mediante al archivo .httaccess.

ANEXO VI. MODELO DE ENCUESTA PARA LA MEDICION DE LA SEGURIDAD DEL MODULO INFORMATICO

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?		
P2	¿Se requiere una contraseña de máximo 15 caracteres?		
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?		
P4	¿Se requiere una contraseña que posea números y letras?		
P5	¿El sistema utiliza conexión segura mediante HTTPS?		
P6	¿La base de datos posee datos encriptados?		
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		
P10	¿Cualquier persona tiene acceso al servidor físico?		
P11	¿Cualquier persona tiene acceso al servidor remoto?		
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?		
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		

ID	PREGUNTAS	V	F
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		
P16	¿El sistema permite inyecciones SQL?		
P17	¿El sistema posee un historial de acciones realizadas?		
P18	¿El sistema posee algoritmos de cifrado de datos?		
P19	¿El sistema posee algoritmos de encriptación de datos?		
P20	¿El sistema verifica los datos antes de realizar una acción?		
P21	¿El sistema permite inyecciones de JavaScript?		
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		
P23	¿El sistema es capaz de detectar y detener ataques informáticos?		
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?		
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?		
P26	¿El sistema informa vía mail del ingreso de sesión?		
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?		
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?		
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		
P30	¿El sistema posee un sistema de verificación de dos pasos?		
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		
P33	¿El sistema realiza una comprobación de identidad mediante código QR?		
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?		
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?		

Nombre:
Cedula de Identidad:
Versión: 00

_____

Firma

ANEXO VII. PRIMERA ENCUESTA APLICADA A EXPERTOS SEGÚN EL METODO DELPHI

- **Primer Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?	X	
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?		X
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?		X
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?		X
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?		X
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?		X
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?		X

Nombre: Ing. Andrés Caina

Cedula de Identidad: 100293593-8

Versión: 1

Firmado electrónicamente por:
ANDRES EDUARDO
CAINA GUAMAN

Firma

- **Segundo Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?	X	
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?		X
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?		X
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?		X
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?		X
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?		X
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?		X
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?		X
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?		X

Nombre: Ing. Cristian Hugo Morales Alarcón, Mgs.

Cedula de Identidad: 0604270223

Versión: 1

CRISTIAN HUGO MORALES ALARCON

Firmado digitalmente por CRISTIAN HUGO MORALES ALARCON
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000482756, cn=CRISTIAN HUGO MORALES ALARCON
Fecha: 2021.01.25 11:59:15 -05'00'

Firma

- **Tercer Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?	X	
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?		X
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?		X
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?		X
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?		X

Nombre: Lic. Silvia Castelo

Cedula de Identidad: 0603914219

Versión: 1

Firma

- **Cuarto Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?	X	
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?		X
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?		X
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?		X
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?		X
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?		X

Nombre: Ing. Lady M. Espinoza

Cedula de Identidad: 0703752345

Versión: 1

.

_____

Firma

- **Quinto Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?		X
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?	X	
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?		X
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?		X
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?		X
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?		X
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?		X
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?		X
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?		X

Nombre: Ing. Efrén Efraín Cajamarca Altamirano

Cedula de Identidad: 0603589862

Versión: 1

Firma

ANEXO VIII. SEGUNDA ENCUESTA APLICADA A EXPERTOS SEGÚN EL METODO DELPHI

- **Primer Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?	X	
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?	X	
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?	X	
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?	X	
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?	X	

Nombre: Ing. Andrés Caina

Cedula de Identidad: 100293593-8

Versión: 2

Firmado electrónicamente por:
ANDRES EDUARDO
CAINA GUAMAN

Firma

- **Segundo Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?	X	
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?	X	
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?	X	
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?	X	
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?	X	

Nombre: Ing. Cristian Hugo Morales Alarcón, Mgs.

Cedula de Identidad: 0604270223

Versión: 2

CRISTIAN HUGO MORALES ALARCON

Firmado digitalmente por CRISTIAN HUGO MORALES ALARCON
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000482756, cn=CRISTIAN HUGO MORALES ALARCON
Fecha: 2021.01.25 11:59:15 -05'00'

Firma

- **Tercer Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?	X	
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?	X	
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?	X	
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?	X	
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?	X	

Nombre: Lic. Silvia Castelo

Cedula de Identidad: 0603914219

Versión: 2

Firma

- **Cuarto Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?	X	
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?	X	
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?	X	
P33	¿El sistema realiza una comprobación de identidad mediante código QR?		X
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?	X	
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?	X	

Nombre: Ing. Lady M. Espinoza

Cedula de Identidad: 0703752345

Versión: 2

.

_____

Firma

- **Quinto Experto**

CUESTIONARIO

Tema de Investigación: Módulo de Seguridad Informática Aplicando la Autentificación de Doble Factor para la empresa Home Office S. A. S

Objetivo del Cuestionario:

El presente cuestionario tiene la finalidad de evaluar la Calidad de la seguridad mediante el estándar de calidad ISO 25010, para lo cual se definieron 35 preguntas para responder con verdadero o falso.

Instrucciones:

Marcar con una X correspondiente en cada pregunta establecida, Verdadero o Falso mostradas con la inicial de cada palabra.

Desarrollo:

CUESTIONARIO		Respuesta	
ID	**PREGUNTAS**	**V**	**F**
P1	¿Se requiere una contraseña de al menos 7 caracteres?	X	
P2	¿Se requiere una contraseña de máximo 15 caracteres?	X	
P3	¿Se requiere una contraseña que posea letras mayúsculas y minúsculas?	X	
P4	¿Se requiere una contraseña que posea números y letras?	X	
P5	¿El sistema utiliza conexión segura mediante HTTPS?	X	
P6	¿La base de datos posee datos encriptados?	X	
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?		X
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?		X
P9	¿El sistema permite que cualquier persona tenga acceso al Código del servidor de la aplicación?		X
P10	¿Cualquier persona tiene acceso al servidor físico?		X
P11	¿Cualquier persona tiene acceso al servidor remoto?		X
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?		X
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?	X	
P14	¿El sistema posee que cualquier persona pueda modificar la base de datos?		X
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?		X
P16	¿El sistema permite inyecciones SQL?		X

ID	PREGUNTAS	V	F
P17	¿El sistema posee un historial de acciones realizadas?	X	
P18	¿El sistema posee algoritmos de cifrado de datos?	X	
P19	¿El sistema posee algoritmos de encriptación de datos?	X	
P20	¿El sistema verifica los datos antes de realizar una acción?	X	
P21	¿El sistema permite inyecciones de JavaScript?		X
P22	¿El sistema permite el acceso al usuario si han superado el número de intentos permitidos para el inicio de sesión?		X
P23	¿El sistema es capaz de detectar y detener ataques informáticos?	X	
P24	¿El sistema posee un registro de parámetros ingresados causantes de posibles ataques informáticos realizados?	X	
P25	¿El sistema posee un cierre forzado al momento de un tiempo sin uso del sistema o luego de finalizado la sesión?	X	
P26	¿El sistema informa vía mail del ingreso de sesión?	X	
P27	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?	X	
P28	¿El sistema registra la dirección IP la cual se intenta acceder al sistema?	X	
P29	¿El sistema realiza una comprobación de identidad mediante un certificado digital?		X
P30	¿El sistema posee un sistema de verificación de dos pasos?	X	
P31	¿El requerida una clave de segundo nivel para el ingreso al sistema?		X
P32	¿El sistema realiza una comprobación de identidad mediante datos biométricos?		X
P33	¿El sistema realiza una comprobación de identidad mediante código QR?	X	
P34	¿El sistema utiliza una aplicación externa para la autentificación de identidad?	X	
P35	¿El sistema hace uso de Captchas para la verificación o autentificación de identidad?	X	

Nombre: Ing. Efrén Efraín Cajamarca Altamirano

Cedula de Identidad: 0603589862

Versión: 2

Firma

ANEXO IX. APLICACIÓN DEL METODO DELPHI HACIA LOS EXPERTOS Y TABULACION DE DATOS

Primer Ciclo de Evaluación

En este primer ciclo de evaluación se tomó el módulo de seguridad sin la implementación de la Autentificación por Doble Factor, en el cual no se implementó ningún factor de autentificación externa al propio modulo ya implementado.

- **Primer Evaluador (Primer Experto)**

Tabla 23: Primera Aplicación de Criterios de Evaluación Primer Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**0**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**0**
A- 14	Comprobaciones adicionales	**1**

Tabla 24: Primera Evaluación de las Métricas de Seguridad Primer Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**0.75**	75%	
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	**85 %**
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**0.5**	50%	

- **Segundo Evaluador (Segundo Experto)**

Tabla 25: Primera Aplicación de Criterios de Evaluación Segundo Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**0**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**

ID	*Nombre*	*Valor Obtenido*
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**0**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**0**
A- 14	Comprobaciones adicionales	**1**

Tabla 26: Primera Evaluación de las Métricas de Seguridad Segundo Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**0.75**	75%	**78.4 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**0.67**	67%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**0.5**	50%	

- **Tercer Evaluador (Tercer Experto)**

Tabla 27: Primera Aplicación de Criterios de Evaluación Tercer Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**1**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**0**
A- 14	Comprobaciones adicionales	**1**

Tabla 28: Primera Evaluación de las Métricas de Seguridad Tercer Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**1**	100%	**90 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**0.5**	50%	

- **Cuarto Evaluador (Cuarto Experto)**

Tabla 29: Primera Aplicación de Criterios de Evaluación Cuarto Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**0**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**0**
A- 14	Comprobaciones adicionales	**1**

Tabla 30: Primera Evaluación de las Métricas de Seguridad Cuarto Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**0.75**	75%	
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	**85 %**
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**0.5**	50%	

- **Quinto Evaluador (Quinto Experto)**

Tabla 31: Primera Aplicación de Criterios de Evaluación Quinto Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**0**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**

ID	*Nombre*	*Valor Obtenido*
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**0**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**0**
A- 14	Comprobaciones adicionales	**1**

Tabla 32: Primera Evaluación de las Métricas de Seguridad Quinto Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**0.75**	75%	**78.4 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**0.67**	67%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**0.5**	50%	

Segundo Ciclo de Evaluación

En este segundo ciclo de evaluación se tomó el módulo de seguridad con la implementación de la Autentificación por Doble Factor, en el cual se implementó autentificaciones con aplicaciones externas y factores extra de autentificación.

- **Primer Evaluador (Primer Experto)**

Tabla 33: Segunda Aplicación de Criterios de Evaluación Primer Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**1**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**1**
A- 14	Comprobaciones adicionales	**1**

Tabla 34: Segunda Evaluación de las Métricas de Seguridad Primer Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**1**	100%	**100 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**1**	100%	

- **Segundo Evaluador (Segundo Experto)**

Tabla 35: Segunda Aplicación de Criterios de Evaluación Segundo Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**1**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**1**
A- 14	Comprobaciones adicionales	**1**

Tabla 36: Segunda Evaluación de las Métricas de Seguridad Segundo Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**1**	100%	**100 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**1**	100%	

- **Tercer Evaluador (Tercer Experto)**

Tabla 37: Segunda Aplicación de Criterios de Evaluación Tercer Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**1**
C-2	Control de Acceso	**1**

ID	*Nombre*	*Valor Obtenido*
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**1**
A- 14	Comprobaciones adicionales	**1**

Tabla 38: Segunda Evaluación de las Métricas de Seguridad Tercer Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**1**	100%	**100 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**1**	100%	

- **Cuarto Evaluador (Cuarto Experto)**

Tabla 39: Segunda Aplicación de Criterios de Evaluación Cuarto Evaluador

ID	*Nombre*	*Valor Obtenido*
C-1	Conexiones Seguras	**1**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**1**
A- 14	Comprobaciones adicionales	**1**

Tabla 40: Evaluación de las Métricas de Seguridad Cuarto Evaluador

Métrica	*Formula*	*Valor*	*Porcentaje (%)*	*Final*

Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**1**	100%	**100 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**1**	100%	

- **Quinto Evaluador (Quinto Experto)**

Tabla 41: Segunda Aplicación de Criterios de Evaluación Quinto Evaluador

ID	***Nombre***	***Valor Obtenido***
C-1	Conexiones Seguras	**1**
C-2	Control de Acceso	**1**
C-3	Encriptación de datos	**1**
C-4	Contraseña de alto nivel	**1**
I-5	Prevención de Accesos	**1**
I-6	Prevención de Modificaciones	**1**
I-7	Confirmación de datos	**1**
NR-8	Operaciones Realizadas	**1**
NR-9	Mecanismo de Cifrado	**1**
NR-10	Verificación de Acciones	**1**
R-11	Registro de Acciones y Datos	**1**
R-12	Detección de Posibles Ataques	**1**
A-13	Comprobación de Identidad	**1**
A- 14	Comprobaciones adicionales	**1**

Tabla 42: Segunda Evaluación de las Métricas de Seguridad Quinto Evaluador

Métrica	***Formula***	***Valor***	***Porcentaje (%)***	***Final***
Confidencialidad	X = (C-1 + C-2 + C-3 + C-4) / 4	**1**	100%	**100 %**
Integridad	X = (I-5 + I-6 + I-7) / 3	**1**	100%	
No Repudio	X = (NR-8 + NR-9 + NR-10) / 3	**1**	100%	
Responsabilidad	X = (R-11 + R-12) / 2	**1**	100%	
Autenticidad	X = (A-13 + A-14) / 2	**1**	100%	

ANEXO X. CERTIFICADO DE IMPLEMENTACION DEL MODULO DE SEGURIDAD POR PARTE DE LA EMPRESA HOMEOFFICE .S.A.S.

Yo, CRISTIAN HUGO MORALES ALARCÓN, en calidad de Gerente de la empresa HomeOffice S. A. S. RUC: 0691779025001

CERTIFICO

Que el señor estudiante **BYRON ALFREDO BARRIGA RIVERA**, CC: 0604048942, ha desarrollado y entregado a la empresa que yo represento, un módulo de seguridad contra ataques informáticos aplicando la autenticación doble factor, como parte de su proyecto de graduación titulado "**MÓDULO DE SEGURIDAD INFORMÁTICA APLICANDO LA AUTENTIFICACIÓN DE DOBLE FACTOR PARA LA EMPRESA HOME OFFICE S. A. S.**".

Es cuanto puedo certificar en honor a la verdad facultando al interesado, la utilización de este documento con fines de graduación.

Riobamba, 25 de enero de 2021.

CRISTIAN HUGO MORALES ALARCON

Firmado digitalmente por CRISTIAN HUGO MORALES ALARCON
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000482756, cn=CRISTIAN HUGO MORALES ALARCON
Fecha: 2021.01.25 12:22:20 -05'00'

Ing. Cristian Morales, Mgs.
CC: 0604270223
GERENTE HOME OFFICE S.A.S.

Figura 77: Certificado de Implementación del Módulo de Seguridad