Desarrollo de la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la comandancia de la Fuerza Aérea Ecuatoriana.

López Villalba, Daniel Rodrigo y Murillo Lucio, Jipson Yair

Departamento de Eléctrica y Electrónica

Carrera de Ingeniería en Software

Trabajo de titulación previo a la obtención del título de Ingeniero en Software

Ing. Álvarez Veintimilla, Rolando Marcelo, Mgs.

Latacunga, 31 de agosto 2021

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN SOFTWARE

CERTIFICACIÓN

Certifico que el trabajo de unidad de integración curricular, "Desarrollo de La plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la comandancia de la Fuerza Aérea Ecuatoriana." fue realizado por los señores López Villalba, Daniel Rodrigo y Murillo Lucio, Jipson Yair el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga 31 de agosto del 2021

ROLANDO MARCELO ALVAREZ VEINTIMILLA

Firmado digitalmente por ROLANDO MARCELO ALVAREZ VEINTIMILLA
Fecha: 2021.08.31 16:39:56 -05'00'

Ing. Álvarez Veintimilla, Rolando Marcelo, Mgs

C.C.: 0502519051

Curiginal

Document Information

Analyzed document	DOCUMENTO DE TESIS- FINAL_V2.pdf (D111854754)
Submitted	8/31/2021 3:24:00 AM
Submitted by	Lorena Ibarra
Submitter email	loretaibarra@yahoo.es
Similarity	8%
Analysis address	lorenadibarra.uta@analysis.urkund.com

Sources included in the report

W	URL: https://repositorio.espe.edu.ec/bitstream/21000/13115/1/T-ESPEL-SOF-0015.pdf Fetched: 12/27/2019 4:41:05 AM	2
W	URL: https://docplayer.es/55354255-Analisis-diseno-e-implementacion-del-sistema-web-para-control-de-personal-por-medio-de-cedulas-inteligentes-utilizando-radio-frecuencia-id-rfid.html Fetched: 11/26/2020 9:13:44 PM	3
W	URL: https://www.significados.com/colaboracion/#:~:text=Qu%C3%A9%20es%20Colaboraci%C3%B3n%253A,que%20significa%20%2527trabajar%20juntos%2527. Fetched: 8/31/2021 3:25:00 AM	1
W	URL: https://rockcontent.com/es/blog/plataformas-digitales/ Fetched: 8/31/2021 3:25:00 AM	2
SA	**Tesis Final Final (1).docx** Document Tesis Final Final (1).docx (D57270726)	5
W	URL: https://docplayer.es/7003822-Escuela-politecnica-nacional.html Fetched: 3/23/2020 9:50:00 PM	4
W	URL: https://www.slideshare.net/edwinpila/analisis-de-sistemas-53224273 Fetched: 2/7/2020 3:25:01 PM	1
W	URL: https://www.slideshare.net/uni_fcys_sistemas/uwe-129633253 Fetched: 12/19/2019 9:25:36 PM	1
W	URL: https://www.npmjs.com/package/ml Fetched: 8/31/2021 3:25:00 AM	1
W	URL: https://www.ccffaa.mil.ec/ Fetched: 8/31/2021 3:25:00 AM	1
SA	**UNIVERSIDAD TECNICA DE AMBATO / Tesis_MoretaLissette.docx** Document Tesis_MoretaLissette.docx (D111426426) Submitted by: hf.naranjo@uta.edu.ec Receiver: hf.naranjo.uta@analysis.urkund.com	16
	URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019	

ROLANDO MARCELO ALVAREZ VEINTIMILLA
Firmado digitalmente por ROLANDO MARCELO ALVAREZ VEINTIMILLA
Fecha: 2021.08.31 16:36:58 -05'00'

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN SOFTWARE

AUTORÍA DE RESPONSABILIDAD

Nosotros, **López Villalba, Daniel Rodrigo** y **Murillo Lucio, Jipson Yair** declaramos que el contenido, ideas y criterios del trabajo de titulación: **"Desarrollo de la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la comandancia de la Fuerza Aérea Ecuatoriana."** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas. Consecuentemente el contenido de la investigación mencionada es veraz.

Latacunga 27 de agosto del 2021

López Villalba, Daniel Rodrigo

C.C.: 1751580976

Murillo Lucio, Jipson Yair

CC: 1721829693

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN SOFTWARE

AUTORIZACIÓN

Nosotros, **López Villalba, Daniel Rodrigo** y **Murillo Lucio, Jipson Yair** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Desarrollo de la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la comandancia de la Fuerza Aérea Ecuatoriana."** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Latacunga 27 de agosto del 2021

López Villalba, Daniel Rodrigo

C.C.: 1751580976

Murillo Lucio, Jipson Yair

CC: 1721829693

Dedicatoria

Quiero dedicar este trabajo a mi madre, quien supo inculcarme tanto sus valores como sus principios y es gracias a ella que me encuentro en el lugar en donde estoy ahora, y desde que tengo memoria siempre me ha apoyado en todas las decisiones que he tomado a lo largo de mi vida. A mis hermanos porque de una u otra manera me brindaron su apoyo. Y también a todos los maestros que confiaron en mí y formaron parte de mi formación como profesional

Daniel

Dedicatoria

El presente trabajo de titulación quiero dedicar con mucho cariño a mi madre Myrian Lucio, mi padre Victoriano Murillo a mis hermanos Víctor, Merly y Tatiana que gracias a ellos que día a día me dieron ánimos, motivación y mucha ayuda para continuar en esta etapa académica de mi vida.

Jipson

Agradecimientos

Quiero agradecer a mi compañero y amigo Jipson Murillo por la paciencia, esfuerzo y dedicación que demostró en la realización de este trabajo y a lo largo de la carrea.

Al capitán Marcelo Araujo, quien supo brindarnos todas las facilidades para la realización nuestro trabajo de titulación

A nuestro tutor, el ingeniero Marcelo Álvarez, por guiarnos en la realización nuestro trabajo de titulación

A mis amigos con quienes nos estuvimos apoyando mutuamente en la realización de nuestros trabajos de investigación y en el resto de nuestra formación como ingenieros en software convirtiéndose en parte de mi familia, y no se necesita nada más cuando se tiene a la familia.

Daniel

Agradecimientos

En primer lugar, quiero agradecer a Dios por dejarme tener una familia que siempre me apoyo a en todas mis decisiones. A mi compañero y amigo Daniel López que desde un comienzo en mi vida universitaria hemos compartido buenos momentos tanto académicos como personales, gracias a él, su perseverancia y constancia, logramos la culminación del presente trabajo de titulación.

A demás quiero agradecer capitán Marcelo Araujo, quien nos supo ayudar, brindar facilidades en la comandancia de la Fuerza Aérea Ecuatoriana. A nuestro tutor el ingeniero Marcelo Álvarez quien nos supo guiar en el presente trabajo.

Por último, a todos mis amigos quienes estuvieron apoyándome a continuar en esta etapa de mi vida.

Jipson

Tabla de contenidos

Índice de figuras

Índice de tablas

Resumen

El presente proyecto está enfocado en el desarrollo de una plataforma web para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana. El sistema contempla cuatro etapas principales. La primera etapa consta de la formulación del marco teórico asociado a la ingeniería Social y sus métodos de prevención. La segunda etapa trata el diseño y desarrollo del envío de correos para entrenamiento al portal institucional Zimbra de la Comandancia de la Fuerza Aérea Ecuatoriana, haciendo uso de una metodología UWE (UML-Based Web Engineering). En la tercera etapa se propondrá un algoritmo inteligente supervisado para la recomendación de temas efectivos dentro del contexto de los correos enviados para el entrenamiento del personal basándonos en el algoritmo: k-nn nearest neighbour, el cual se utiliza en sistemas de recomendación, búsqueda semántica y detección de anomalías, siendo un clasificador robusto y versátil que a menudo se usa como un punto de referencia para clasificadores más complejos como las redes neuronales artificiales y vectores de soporte (SVM). La cuarta etapa consiste en implantar la propuesta en la Comandancia de la Fuerza Aérea Ecuatoriana, además de validar el sistema y los datos obtenidos por el mismo mediante pruebas de funcionalidad.

Palabras clave:

- **PROGRAMACIÓN WEB**
- **SEGURIDAD INFORMÁTICA**
- **ALGORITMOS DE RECOMENDACIÓN**

Abstract

This This project is focused on the development of a web platform for counseling, awareness and training in social engineering attack prevention techniques for military and civilian personnel of the Ecuadorian Air Force Command. The system includes four main stages. The first stage consists of the formulation of the theoretical framework associated with social engineering and its prevention methods. The second stage deals with the design and development of the mailing of training emails to the institutional portal Zimbra of the Ecuadorian Air Force Command, using a UWE (UML-Based Web Engineering) methodology. In the third stage we will propose a supervised intelligent algorithm for the recommendation of effective topics within the context of the emails sent for personnel training based on the algorithm: k-nn nearest neighbor, which is used in recommendation systems, semantic search and anomaly detection, being a robust and versatile classifier that is often used as a benchmark for more complex classifiers such as artificial neural networks and support vectors (SVM). The fourth stage consists of implementing the proposal in the Command of the Ecuadorian Air Force, in addition to validating the system and the data obtained by it through functionality tests.

Keywords:

- **WEB PROGRAMMING**
- **COMPUTER SECURITY**
- **RECOMMENDATION ALGORITHMS**

CAPÍTULO I

1. Presentación del problema

1.1. Planteamiento del problema

En el mundo de la seguridad informática sin importar que tan reforzada esté la seguridad de un sistema siempre existirá algún tipo de vulnerabilidad independientemente del mismo, no obstante, hay un aspecto a considerar que se repite en cada caso de seguridad, dentro de las tecnologías de la información TI y se trata de las personas encargadas de administrar dichas tecnologías como sistemas software.

La parte más vulnerable de un sistema sin duda son los usuarios, debido a que a través de ellos se puede acceder de la manera rápida y segura, tomando en cuenta esto, con el tiempo se han desarrollado diversas técnicas de fraude que forman parte de lo que se conoce como ingeniería social, la misma que se basa en obtener información confidencial mediante la manipulación de usuarios legítimos. Cuando se habla de una institución tan importante como es la Fuerza Aérea Ecuatoriana no se puede ser indiferente ante esta situación, por consecuencia es preciso establecer medidas de control para combatir este tipo de ataques y para lograrlo, es necesario realizar un esfuerzo no solo del personal informático sino un esfuerzo conjunto de todo el personal involucrado con información relevante perteneciente a la institución.

Dentro de la Comandancia de la Fuerza Aérea Ecuatoriana existe personal militar y civil que hacen uso de plataformas, sistemas e infraestructura tecnológica de la institución, manejando información que en muchos es confidencial. Según versiones del Capitán Guillermo Escobar ex jefe del departamento de seguridad y defensa de la FAE, se conoce que gran parte de estas personas no cuentan con el conocimiento de lo que implica la ingeniería social y actualmente la institución no cuenta con ningún tipo de sistema o plataforma que pueda ayudar a generar conciencia y brindar conocimientos al respecto, en consecuencia la misma no está tomando ninguna medida para capacitar a dichas personas en estos aspectos, convirtiéndolos en potenciales víctimas de ataques de

ingeniería social, poniendo en riesgo no solo sus datos personales sino también la información de la institución.

En caso de que la institución sea objetivo de algún ataque de ingeniería social, debido a lo mencionado anteriormente, su personal no estaría en capacidad de contrarrestar este tipo de ataque y se constituiría en el acceso a todo tipo de información confidencial de la misma.

1.2. Formulación de problema

De acuerdo con lo descrito anteriormente se formula el siguiente problema: ¿Cómo asesorar, concientizar y entrenar al personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana en técnicas de prevención de ataques de ingeniería social?

1.3. Justificación e importancia

Según el informe de Digiware Ecuador ocupa la cuarta posición en la lista de países que más ataques cibernéticos recibe en Latinoamérica con un 11,22%. A esto se suma el aumento de amenazas del 1 al 30% de ataques de Ingeniería Social (Digiware, 2016).

La nueva realidad con la llegada del COVID-19 (COVID-19, enfermedad respiratoria que afronta el mundo como pandemia) ha traído consigo el aumento de nuevos ataques cibernéticos debido a la transformación digital obligatoria, algunas de estas tecnologías no están completamente implementadas y los ciberdelincuentes están poniendo a prueba las defensas de los países (Digiware, 2020). El 2020 es el año donde la sociedad experimentó una transformación drástica en su vida cotidiana, creando un sentido de urgencia en torno a la seguridad de la información.

En la actualidad las instituciones tanto públicas como privadas han sido forzadas a recurrir al teletrabajo, el problema es que muchas de estas instituciones no están conscientes de los riesgos que puede suponer compartir información a través de internet y optar por opciones como el teletrabajo, tomando en cuenta la cantidad inmensurable de información que se encuentra en el internet tiende a que los usuarios no sean capaces de identificar cuando se trata de información real,

la misma que llega día a día a las bandejas de entrada de sus correos electrónicos convirtiendo a dichos usuarios en blancos perfectos para la ingeniería social. (Semana, 2020).

El gran aumento de la dependencia tecnológica en sociedad es una realidad tangible, siendo necesario para una buena administración de los Estados, sus Fuerzas y Cuerpos de Seguridad y sus infraestructuras. Esta dependencia seguirá aumentando en el futuro. Las tecnologías de la información hacen posible casi todo lo que la FAE necesita: apoyo logístico, mando y control de sus fuerzas, información de inteligencia en tiempo real, entre otras. Todas estas funciones dependen de sus comunicaciones y redes informáticas. En menos de una generación, las TIC en el entorno militar han pasado de ser una simple herramienta para mejorar la productividad administrativa a un entorno estratégico. (Durán, 2011)

Al mismo tiempo, la dependencia tecnológica, la globalización y la facilidad de acceso a la tecnología hacen que hoy en día la probabilidad de sufrir ataques informáticos o ciberataques sea muy alta. (Durán, 2011)

Los protagonistas de un ciberataque buscan principalmente el error humano para acceder a las instituciones, vulnerando a cualquier usuario. Es importante conocer y educar a los potenciales usuarios vulnerables, especialmente para que sepan qué herramientas o ingeniería social utiliza el atacante y cuáles son los tipos de ataques más comunes a los que se puede enfrentar el usuario si desconocen de la materia. El conocimiento de ciberseguridad en el usuario será un gran aporte en la motivación, ya que actuará de manera más segura con la tecnología en lo personal y laboral como primera línea de defensa (Lisboa, 2020).

Ante lo expuesto se ha decidido proponer el presente proyecto cuya finalidad consiste tanto en la investigación, análisis, diseño, implementación de la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social.

Los beneficiarios del proyecto serán el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana. A través de la plataforma las personas involucradas podrán identificar los usuarios más vulnerables a sufrir ciberataques con esto la plataforma podrá dar una retroalimentación de temas comunes de ingeniería social como spear phishing, whaling, angler phishing entre otros.

1.4. Objetivos

1.4.1. Objetivo general

Desarrollar la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.

1.4.2. Objetivos específicos

- Formular el marco teórico asociado a la ingeniería social y sus métodos de prevención.
- Diseñar e implementar una plataforma web SafeSecure basado en la metodología UWE (UML-Based Web Engineering).
- Diseñar y desarrollar un algoritmo inteligente supervisado basado en el algoritmo: k-nn nearest neighbour para la recomendación de temas efectivos dentro del contexto de los correos enviados para el entrenamiento.
- Integrar el algoritmo inteligente en la plataforma web SafeSecure.
- Implantar la propuesta en la Comandancia de la Fuerza Aérea Ecuatoriana.
- Validar los resultados obtenidos del sistema mediante pruebas unitarias, de integración, sistema, aceptación.

1.5. Hipótesis

Si se desarrolla la plataforma web SafeSecure entonces se contribuirá al asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.

1.6. Variables de la investigación

1.6.1. Variable dependiente

Se contribuye al asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.

1.6.1.1. Conceptualización Variable Dependiente. La contribución se denomina acción y efecto de colaborar. El significado de colaborar es trabajar junto a otras personas con la finalidad de realizar una obra o alcanzar un objetivo. La palabra, como tal, deriva de colaborar, que a su vez proviene del latín collaborāre, que significa 'trabajar juntos' (Significados,2015).

1.6.2. Variable independiente

Se desarrolla la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.

1.6.2.1. Conceptualización Variable Independiente. **"**Las plataformas digitales o plataformas virtuales son espacios en Internet que permiten la ejecución de diversas aplicaciones o programas en un mismo lugar para satisfacer distintas necesidades" (Giraldo, V. 2021).

1.7. Indicadores

- Porcentajes de progreso del entrenamiento en Ingeniería Social representando un aumento mínimo de 80 por ciento.
- Nivel de efectividad de los nuevos temas o contextos recomendados por el algoritmo inteligente.
- Cantidad de correos de simulación abiertos durante cada periodo de entrenamiento.
- Frecuencia de uso del sistema en la creación de entrenamientos de simulación.

CAPÍTULO II

2. Marco teórico

2.1. Antecedentes históricos

2.1.1. Primera etapa - Ingeniería social sin prevención (1791-1970)

Los dispositivos computacionales han existido, si no en uso práctico, desde los días de Charles Babbage (1791-1871).

El término ingeniería social fue utilizado por primera vez por el industrial holandés J.C. Van Marken en 1894. Van Marken sugirió que los especialistas eran necesarios para atender los desafíos humanos, además de los técnicos (J.M.H, 2018).

En 1911, Edward L. Earp escribió a la Ingeniería Social como una manera de alentar a las personas a manejar las relaciones sociales de manera similar a cómo abordan las máquinas.

El término "Cyber Age" hoy connota más que solo dispositivos computacionales, sino el uso público de dichos dispositivos dentro de un contexto en el que están conectados entre sí para formar una red. La informática en red trae consigo consideraciones de seguridad inmediatas que los dispositivos informáticos autónomos, como el motor diferencial de Babbage, no tienen. Como tal, mientras que la era cibernética comenzó a fines de la década de 1960 y principios de la de 1970, con el advenimiento de la Red de Agencias de Proyectos de Investigación Avanzada (ARPANET), la "ingeniería social", tal y como la entendemos hoy en el contexto de la ciberseguridad, comenzó con el fenómeno del "phreaking telefónico" de finales de los años 50 y principios de los 70, que fue anterior a la creación de ARPANET. Ambos desarrollos tempranos vendrían a dar forma al contexto en el que el concepto de ingeniería social encontró su expresión (J.M.H, 2018). Por lo tanto, es importante comprender el entorno social en el que nació esta época.

Los años sesenta y setenta fueron un período de rápido desarrollo tecnológico en la tecnología informática y, al mismo tiempo, las oportunidades para explotar las vulnerabilidades que

surgieron a partir de ellas (J.M.H, 2018). La computación interactiva, el tiempo compartido, la autenticación de usuarios, el intercambio de archivos a través de estructuras de archivos jerárquicas y los prototipos de utilidades informáticas fueron parte de una ola de innovaciones técnicas en la década de 1960. Junto a esta ola, se implementaron herramientas de seguridad relativamente simples como controles de acceso y contraseñas (J.M.H, 2018). La próxima década vio el comienzo de las redes de área local (LAN), las redes de paquetes (ARPANET) y el diseño orientado a objetos, protegidos por una ola de aplicaciones criptográficas, como la criptografía de clave pública, la verificación de seguridad, los protocolos criptográficos y el hash criptográfico.

2.1.2. Segunda etapa - Prevención por ciberseguridad privatizada (1991-1995)

América Online (AOL) fue uno de los mayores proveedores de servicios de Internet en 1994-1995, con un aumento constante de usuarios. En ese momento, la seguridad de Internet solo se consideraba importante a nivel gubernamental y las empresas privadas rara vez invirtieron en ciberseguridad. Debido a esto, AOL terminó siendo víctima de un ataque de phishing (Inteligencia, 2020).

En 1994, un hacker llamado “Da Chronic” creó una aplicación automatizada llamada “AOHell”. Una de sus características era un conjunto de herramientas de phishing que se utilizaba para explotar el sistema de mensajería de AOL (Inteligencia, 2020). Al enviar un mensaje directo a otros usuarios, el pirata informático obtuvo acceso a credenciales personales. El mensaje era como ser un representante de AOL, necesitando una contraseña y un nombre de usuario para verificar la cuenta. Los usuarios enviaron su información personal sin sospechas y se convirtieron en víctimas del ataque de phishing.

Pronto, los piratas informáticos apuntaron a usuarios más valiosos, haciendo amenazas para verificar rápidamente su información de facturación; de lo contrario, su cuenta sería eliminada. Como resultado, los atacantes lograron obtener la cuenta bancaria de la víctima y detalles de la tarjeta de pago junto con sus credenciales de AOL.

Luego, AOL actualizó su sistema de ciberseguridad. Se han implementado nuevas medidas para eliminar las cuentas asociadas con el phishing.

2.1.3. Tercera etapa - Prevención y concientización gracias a empresas afectadas (1997-actualidad)

Las fugas de datos son un concepto importante. Empresas como Google y Facebook pudieron invertir dinero en ciberseguridad, pero aun así sufrieron violaciones de datos durante más de un año.

Myspace y Armor Games experimentaron fugas de datos y la información se transfirió a la web profunda. Actualmente, más de dos mil millones de las credenciales filtradas están siendo vendidas abiertamente por piratas informáticos.

En las últimas décadas, sólo han mejorado las tecnologías involucradas, es decir, software para suplantación de correo electrónico que se utiliza para enviar correos electrónicos a una gran cantidad de usuarios y la calidad del contenido generado mediante el uso de algoritmos simples (Inteligencia, 2020). Por otro lado, la formación en ciberseguridad no ha mejorado y existe una falta de conocimiento profundo sobre el tema, por lo tanto, hay una falta de profesionales en la materia. Esto ha llevado a empresas afectadas tales como Google y Facebook a realizar diversas campañas de concientización hacia sus usuarios y empleados con el fin de poder mitigar en gran parte los ataques de ingeniería social.

2.2. Antecedentes conceptuales y referenciales

2.2.1. Ingeniería social

El objetivo principal de la ingeniería social dentro de Internet consiste en obtener la colaboración de los usuarios legítimos de los sistemas para activar métodos de hackeo, o bien envolverlos rápidamente en alguna estafa irremediable (Cortez Hernandez, 2019).

El engaño puede llevarse a cabo mediante un sólo medio (un correo electrónico, por ejemplo) con algún tipo de historia para que el usuario revele o entregue información sensible o

ingrese a un enlace sospechoso que proceda a ejecutar códigos maliciosos. Pero también puede ser puesto en marcha haciendo uso de historias y acciones que involucran la interacción de múltiples plataformas como: WhatsApp, mensajes SMS, redes sociales, pagos electrónicos, tarjetas prepago o depósitos bancarios, que a medida se conectan, vulneran más a la víctima (Computer World México, 2017).

2.2.1.1. Phishing. El phishing es una técnica de ingeniería social que utilizan los delincuentes cuyo objetivo principal es obtener información personal como nombres de usuario, contraseñas y datos de tarjetas de crédito, haciéndose pasar por una entidad legítima o de confianza.

El entorno del Phishing comúnmente va de la mano a la capacidad de imitar una página web con el fin de hacer creer a sus visitantes que se encuentra en el sitio web original. El engaño suele empezar por medio de correos electrónicos que comúnmente contienen enlaces a un sitio web falso que trata de imitar a un sitio legítimo. Una vez en el sitio falso los usuarios desprevenidos son engañados para que introduzcan sus datos confidenciales, lo que da a los delincuentes un amplio margen para realizar estafas y fraudes con la información obtenida. Principalmente el engaño se lleva a cabo enviando spam (correo basura) e incitando a los usuarios a acceder a páginas señuelo. La finalidad del engaño es obtener información confidencial de los usuarios como: contraseñas, tarjetas de crédito o datos financieros y bancarios. Con frecuencia estos correos electrónicos llegan a la bandeja de entrada disfrazados, simulando que provienen de los departamentos de tecnología, recursos humanos o de áreas de negocio relacionadas con las transacciones financieras (Sgu-info, 2005).

2.2.1.2. Vishing. "El vishing son llamadas telefónicas mediante las que se buscan engañar a la víctima suplantando a compañías de servicios o de gobierno para que revele información privada." (Rodríguez Rincón).

2.2.1.3. Baiting. El Baiting se basa en abandonar dispositivos de almacenamiento extraíble (USB, CD, DVD) infectados en lugares que se puedan encontrar a simple vista (por ejemplo, baños públicos, ascensores, aceras, etc.), con el fin de que alguien los recoja y conecte a su dispositivo para posteriormente instalar un software malicioso y permitir que el hacker obtenga los datos personales del usuario (Fernandez M., 2019).

2.2.1.4. Quid pro quo. El quid pro quo es ofrecer un beneficio a cambio de información. En el caso más común de este ataque el atacante se hace pasar por personal de IT, solicitando ciertos datos confidenciales al usuario con el motivo de resolver un conflicto o brindando algún malware disfrazado de una actualización de seguridad. (Garcia Romero).

2.2.2. Metodologías para el desarrollo de aplicaciones web

2.2.2.1. Rmm relationship management methodology. Rmm es una metodología enfocada en el desarrollo de aplicaciones de hipermedia que tiene definida una estructura regular a través de entidades y sus respectivas relaciones. Los modelos de RMM son denominados Modelo de Datos de Administración de Relaciones (Relationship Management Data Model, RMDM).

El modelado de la navegación se lleva a cabo a través de enlaces unidireccional, bidireccionales, y estructuras de acceso; las cuales pueden ser índices, visitas guiadas, índice-visita-guiada y grupos.

La Metodología de Gestión de Relaciones (RMM) brinda una metodología de diseño estructurada centrado en el desarrollo de una gran clase de aplicaciones hipermedia, haciendo más sencillo su diseño, desarrollo y mantenimiento. Esta gran clase se basa en aplicaciones de dificultad moderada a alta que poseen componentes reutilizables. “La RMM se utiliza actualmente en instituciones financieras (por ejemplo, Merrill Lynch), editoriales (por ejemplo, M.E. Sharpe, Inc.), instituciones de investigación (por ejemplo, Bellcore) e instituciones educativas (Pace University in NY; SYRECOS consortium in Luxembourg, Staffordshire University in the UK)”. (Sakowitz, 1995)

Los objetos del dominio se definen con la ayuda de entidades, atributos y relaciones asociativas, sus principales características son:

- Aproximación para el diseño de sitios web, bajo una aproximación centrada en la información.
- Lenguaje de modelado de sitios web a nivel lógico (dominio de información + estructuras de navegación + elementos de presentación).
- Integrado en una metodología de desarrollo.
- Facilitar la estructuración de páginas web complejas que contienen elementos de distintas entidades (vistas múltiples).
- Permitir la reutilización de elementos en el diseño (vistas jerárquicas).
- Diseño de enlaces más potentes y versátiles.
- Mantener el contexto durante la navegación.

2.2.2.2. Oohdm object oriented hypermedia design method. "OOHDM propone el desarrollo de aplicaciones hipermedia a través de un proceso compuesto por cuatro etapas: diseño conceptual, diseño navegacional, diseño de interfaces abstractas e implementación." (Mariño, 2017)

2.2.2.2.1. Diseño conceptual. En el diseño conceptual se desarrolla un esquema representado por los objetos del dominio, las relaciones y colaboraciones existentes establecidas entre ellos. (Rand, 2021)

Se puede utilizar un modelo de datos semántico estructural en las aplicaciones con componentes de hipermedia que no son modificados durante la ejecución. En ocasiones se necesitará enriquecer el comportamiento del modelo de objetos esto cuando la información base pueda cambiar dinámicamente o se intenten ejecutar cálculos complejos. (Silva, 2001).

2.2.2.2.2. Diseño navegacional. En OOHDM, la navegación se considera un paso crítico en el diseño de un Aplicación hipermedia. Un modelo de navegación se construye como una vista sobre un modelo conceptual permitiendo así la construcción de diferentes modelos según diferentes

perfiles de usuarios. Cada modelo de navegación proporciona una Visión "subjetiva" del modelo conceptual. (Schwabe, 1998)

El diseño de navegación es expresado en dos esquemas: el esquema de clases navegacionales y el esquema de contextos navegacionales. (Schwabe, 1998)

En OOHDM, de manera similar a HDM y RMD existe un conjunto de tipos predefinidos de clases de navegación: nodos, enlaces y estructuras de acceso. La semántica de nodos y enlaces es la habitual en las aplicaciones hipermedia, y las estructuras de acceso, como índices y visitas guiadas, representan posibles formas de acceder a los nodos. (Schwabe, 1998)

La especificación de transformaciones de navegación describe la dinámica de la aplicación, mostrando la forma en que cambia el espacio de navegación cuándo navega el usuario, es decir, qué nodos están activados y cuáles desactivado cuando se sigue un enlace. La semántica de navegación predeterminada en OOHDM es que cuando se sigue un enlace, el nodo de origen se desactiva y el nodo objetivo activado. (Schwabe, 1998)

2.2.2.2.3. Diseño de interfaz abstracta. "En OOHDM se utiliza el diseño de interfaz abstracta para describir la interfaz del usuario de la aplicación de hipermedia." (Silva, 2001).

En OOHDM, se utiliza el enfoque de diseño Abstract Data View (ADV) para describir la interfaz de usuario de una aplicación hipermedia. (Schwabe, 1998)

Las ADV son objetos en el sentido de que tienen un estado y una interfaz, donde la interfaz se puede ejercitar a través de mensajes (en particular, eventos externos generados por el usuario). Los ADV son abstractos en el sentido de que solo representan la interfaz y el estado, y no la implementación. (Schwabe, 1998)

Los ADV se han utilizado para representar interfaces entre dos medios diferentes, como un usuario, una red o un dispositivo (un temporizador, por ejemplo) o como una interfaz entre dos o más datos abstractos. (Schwabe, 1998)

2.2.2.2.4. Implementación. En la fase de implementación, el responsable del diseño deberá encargarse de implementar el diseño. Ya que todos los modelos fueron construidos de manera independiente a la plataforma de implementación; en este punto se tiene presente el entorno particular en donde se va a ejecutar la aplicación. El primer paso que el diseñador debe llevarse a cabo en esta fase es definir los ítems de información que forman parte del dominio de la problemática., también debe identificar como estos son organizados acorde con el perfil del usuario y su tarea, además se encargara de decidir qué interfaz debería visualizar y cómo debería comportarse. Con la finalidad de implementar todo en un entorno web, la persona encargada del diseño tiene la tarea de decidir qué información debe ser almacenada (Silva, 2001).

2.2.2.3. Uwe - uml-based web engineering. UWE es una metodología para el desarrollo de aplicaciones web que se enfoca en el Proceso Unificado y UML. Su proceso de desarrollo está conformado por tres fases principales: la captura de requisitos, el análisis y diseño y la implementación.

La metodología UWE define modelos como el modelo de navegación y el modelo de presentación que son vistas especiales representadas por diagramas en UML.

Los diagramas pueden ser adaptados basandoce en estereotipos que proporciona UML como mecanismos de extensión, los mismos que UWE utiliza para definir estereotipos que serán utilizados en las vistas especiales para el modelado de aplicaciones Web. Consiguiendo, una notación UML adecuada para un dominio específico conocida como “Perfil UML” (Rossi G. 2008).

“Un perfil de UML consiste en una jerarquía de estereotipos y un conjunto de restricciones.” (Narváez A., 2012).

Fases de la UWE

- Captura, análisis y especificación de requisitos; se adquieren, reúnen y especifican las características funcionales y no funcionales que deberá cumplir la aplicación web.

- Diseño del Sistema; se basa en la especificación de requisitos producido por el análisis de los requerimientos (fase de análisis), el diseño define como estos requisitos se cumplirán, la estructura que debe darse a la aplicación web.

- Codificación del software, durante esta etapa se realizan las tareas que comúnmente se conocen como programación; que consiste, esencialmente en llevar a código fuente, en el lenguaje de programación elegido, todo lo diseñado en la fase anterior.

- Pruebas; se utilizan para asegurar el correcto funcionamiento de secciones de código.

- Fase de Implementación; es el proceso por el cual los programas desarrollados son transferidos apropiadamente al computador destino, inicializados y eventualmente, configurados. Todo ello con el propósito de ser utilizados por el usuario final.

- Mantenimiento; es el proceso de control, mejora y optimización del software ya desarrollado e instalado, que también incluye depuración de errores y defectos que puedan haberse filtrado de la fase de pruebas de control (Casas H., 2014).

2.2.3. Infraestructura del sistema

2.2.3.1. Infraestructura backend

2.2.3.1.1. Backend como servicio (baas). Un Backend como servicio con sus siglas en inglés (Baas) o móvil (MBaas), es un servicio que proporciona a los desarrolladores de aplicaciones web y móviles una forma para vincular sus aplicaciones con el almacenamiento en la nube del backend y al mismo tiempo proporcionar características como gestión de usuarios, almacenamiento, hosting para nombrar algunos servicios (BitHeads C.S.D.).

Descrita por los analistas tecnológicos como una infraestructura de encendido, en inglés (turn-on infrastructure), un BaaS es básicamente una categoría de computación en la nube que se compone de empresas que facilitan a los desarrolladores la configuración, el uso y la operación de un backend en la nube para sus dispositivos móviles, tabletas y aplicaciones web conectando sus

aplicaciones a dispositivos remotos y / o locales almacenamiento en la nube backend a través de servicios proporcionados a través del kit de desarrollo de software (SDK) y un conjunto de rutinas, protocolos y herramientas para construir software y aplicaciones, también conocida como interfaz de programación de aplicaciones con sus siglas en inglés (API).

Un proveedor BaaS proporciona un puente entre el backend en la nube con el frontend a través de API o SDK.

El enfoque BaaS basado en API proporcionará servicios de terceros como una función de backend, con los usuarios creando aplicaciones específicas de la plataforma sobre una base reutilizable (Weber, J.). Los servicios reutilizables proporcionados por BaaS aportan varias ventajas sobre el desarrollo frontend tradicional como:

- Detiene el desarrollo innecesario de la pila.
- Permite más accesibilidad.
- Descarta tareas repetitivas y centra su esfuerzo en aportar el mayor valor a su software.
- Escalabilidad de la aplicación.
- Sin problemas de infraestructura.
- Centrarse en el desarrollo frontend.

2.2.3.1.2. Firebase. Firebase es una plataforma de desarrollo de aplicaciones móviles, propiedad de Google. Firebase se encuentra disponible para las diferentes plataformas como lo son Android, iOS y Web. Firebase es una plataforma utilizada en la Nube (Cloud), lo que permite acceder a la información desde cualquier dispositivo (Zamora, 2016)

Firebase se considera una plataforma de aplicaciones web. Ayuda a los desarrolladores a crear aplicaciones de alta calidad. Almacena los datos en formato JavaScript Object Notation (JSON)

que no utiliza consultas para insertar, actualizar, eliminar o agregar datos. (Khawas, C., & Shah, P. 2018).

Firebase es una herramienta muy útil para los proyectos que deben ser realizados en un tiempo limitado gracias a que posee su propia API (Interfaz de Programación de Aplicaciones) que resulta intuitiva y es sostenida en un SDK (Kit de Desarrollo de Software) y es una herramienta ágil debido a que se pueden integrar API de terceras partes a una aplicación, por ejemplo, Google Maps (Sanz, 2017).

- **Firebase Analytics:** Proporciona una visión profunda sobre el uso de la aplicación por parte de los usuarios. La función de análisis se registra automáticamente cuando un desarrollador aplica otras funciones de Firebase. El compositor de notificaciones se activa para enviar mensajes a los clientes. Más acciones, si necesita realizar análisis personalizados o unir sus datos con otras fuentes, puede vincular sus datos de Analytics a BigQuery, que permite realizar análisis más complejos como la consulta de grandes conjuntos de datos y la unión de múltiples fuentes de datos.

- **Firebase Cloud Messaging:** La aplicación recibe notificaciones a través de la mensajería en la nube. la notificación se utiliza para enviar mensajes de datos o determinar el estado actual de sus códigos. La notificación se envía a uno o varios dispositivos. Los sujetos son datos, fechas de vencimiento, sonido o prioridades dependiendo del control del cliente. Firebase Cloud Messaging (FCM) es un canal fiable para enviar mensajes de la aplicación al servidor. Ahora la supervisión del panel de control está más detallada mediante la integración de FCM con Firebase Analytics. Además, también se pueden unir las pruebas A/B, ya que las notificaciones de sus varias versiones pueden ayudar al desarrollador a investigar el rendimiento. (Google 2019.)

- **Firebase Auth:** Firebase permite utilizar proveedores, como pueden ser Twitter, Facebook, teléfono, correo/contraseña, o el propio Google mediante correo electrónico. Con dicha

funcionalidad se puede gestionar y dar un servicio de más calidad y utilidad al usuario. Es importante resaltar que en la nube se guardan los datos de forma segura y la experiencia de usuario es la misma independientemente el dispositivo. Firebase Authentication se integra estrechamente en otros servicios de Firebase y aprovecha los estándares de la industria como OAuth 2.0 OpenID Connect.

- **Realtime Database:** Firebase Realtime Database es una base de datos alojada en la nube. Los datos son almacenanados en un archivo tipo JSON y son sincronizados en tiempo real con cada cliente conectado.

- **Firebase Storage:** Es un servicio muy potente de almacenamiento de objetos simple y rentable construido para la escala de Google. Los SDK de Google agregan la seguridad de Google a las operaciones de carga y descarga de archivos. Sin importar la calidad de la red, estos archivos pueden ser fotos, videos, u otros tipos de archivos. (Cardiel Altemir, G. 2019)

- **Firebase Firestore:** Es una base de datos NoSQL, aunque presenta diversas diferencias. Su organización se encuentra en forma de agrupaciones de documentos como colecciones en donde se puede incluir campos de diversos tipos (números, cadenas de texto, referencias a la misma base de datos, puntos geográficos, booleanos, arrays, marcas de tiempo, e incluso objetos propios) u otras subcolecciones.(Firebase, 2018.)

- **Hosting:** Con una colección de estáticos (o de archivos que han pasado ya el proceso de build) podemos subir una aplicación y esta automáticamente contará con SSL y HTTP2. (Firebase, 2018.)

2.2.3.2. Infraestructura frontend

2.2.3.2.1. Angular. Es una plataforma y un marco para crear aplicaciones cliente de una sola página mediante HTML y TypeScript. Angular está escrito en TypeScript. Implementa la funcionalidad básica y opcional como un conjunto de bibliotecas de TypeScript[1], Angular incluye:

- Un marco basado en componentes para crear aplicaciones web escalables
- Una colección de bibliotecas bien integradas que cubren una amplia variedad de características, incluyendo enrutamiento, administración de formularios, comunicación cliente-servidor.
- Un conjunto de herramientas de desarrollo para ayudarle a desarrollar, compilar, probar y actualizar el código.

Con Angular, está aprovechando una plataforma que puede escalar desde proyectos de un solo desarrollador a aplicaciones de nivel empresarial. Angular está diseñado para hacer que la actualización sea lo más fácil posible, para que pueda aprovechar los últimos desarrollos con un mínimo de esfuerzo. (Angular, 2021)

Arquitectura: La arquitectura de una aplicación Angular se basa en ciertos conceptos fundamentales. Los bloques de construcción básicos del marco angular son componentes angulares que se organizan en NgModules. NgModules recopilan código relacionado en conjuntos funcionales; una aplicación Angular se define mediante un conjunto de NgModules (Angular, 2021). Una aplicación siempre tiene al menos un módulo raíz que permite el arranque y, por lo general, tiene muchos más módulos de características.

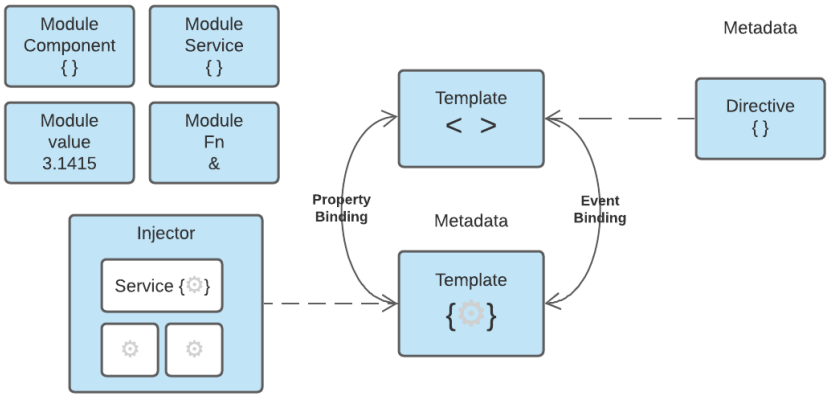
Los módulos, componentes y servicios son clases que utilizan decoradores. Estos decoradores marcan su tipo y proporcionan metadatos que indican a Angular cómo usarlos.

[1] TypeScript es un superconjunto de JavaScript que agrega capacidades de tipado estático. Esto nos da la ventaja de poder tipar cosas como variables, funciones, devoluciones, además de poder crear Interfaces. TypeScript también nos da la capacidad de usar enumerators, modules, namespaces, decorators y generics.

- Los metadatos de una clase de componente lo asocian a una plantilla que define una vista. Una plantilla combina HTML normal con directivas Angular y marcado de enlace que permiten a Angular modificar el HTML antes de representarlo para su presentación.

- Los metadatos de una clase de servicio proporcionan la información que Angular necesita para que esté disponible para los componentes a través de la inserción de dependencias (DI).

Figura 1.
Arquitectura Angular



Módulos: Angular NgModules difiere y complementa a los módulos de JavaScript (ES2015). NgModule declara un contexto de compilación para un conjunto de componentes dedicado a un dominio de aplicación, un flujo de trabajo o un conjunto de funciones estrechamente relacionado (Angular, 2021). Un NgModule puede asociar sus componentes con código relacionado, como servicios, para formar unidades funcionales.

Organizar el código en módulos funcionales distintos ayuda a administrar el desarrollo de aplicaciones complejas y a diseñar para la reutilización. Además, esta técnica le permite aprovechar la carga diferida (es decir, cargar módulos a petición) para minimizar la cantidad de código que debe cargarse en el inicio.

Componentes: Cada aplicación Angular tiene al menos un componente, el componente raíz que conecta una jerarquía de componentes con el modelo de objetos de documento de página

(DOM). Cada componente define una clase que contiene datos y lógica de la aplicación, y está asociada a una plantilla HTML que define una vista que se va a mostrar en un entorno de destino (Angular, 2021).

El decorador[2] identifica la clase inmediatamente debajo de ella como un componente y proporciona la plantilla y los metadatos específicos del componente relacionados @Component().

Plantillas, directivas y enlace de datos: Una plantilla combina HTML con marcado Angular que puede modificar elementos HTML antes de que se muestren (Angular, 2021). Las directivas de plantilla proporcionan lógica de programa y el marcado de enlace conecta los datos de la aplicación y el DOM. Hay dos tipos de enlace de datos:

- El enlace de eventos permite a la aplicación responder a los datos proporcionados por el usuario en el entorno de destino mediante la actualización de los datos de la aplicación.
- El enlace de propiedades permite interpolar los valores que se calculan a partir de los datos de la aplicación en el código HTML.

Servicios e inserción de dependencias: Para los datos o la lógica que no está asociada a una vista específica y que desea compartir entre componentes, cree una clase de servicio (Angular, 2021). Una definición de clase de servicio va precedida inmediatamente por el decorador. El decorador proporciona los metadatos que permiten que otros proveedores se inyecten como dependencias en la clase @Injectable().

La inserción de dependencias (DI) le permite mantener las clases de componentes ágiles y eficientes. No obtienen datos del servidor, no validan la entrada del usuario ni registran directamente en la consola; delegan estas tareas en los servicios.

[2] Los decoradores son funciones que modifican las clases de JavaScript. Angular define varios decoradores que adjuntan tipos específicos de metadatos a las clases, para que el sistema sepa lo que significan esas clases y cómo deben funcionar.

Enrutamiento: Angular NgModule proporciona un servicio que permite definir una ruta de navegación entre los diferentes estados de aplicación y jerarquías de vista de la aplicación (Angular, 2021). Se basa en las convenciones de navegación del explorador conocidas Router.

El router asocia rutas url-como a las vistas en vez de a las páginas. Cuando un usuario realiza una acción, como hacer clic en un vínculo, que cargaría una nueva página en el explorador, el enrutador intercepta el comportamiento del explorador y muestra u oculta las jerarquías de vista.

2.2.3.3. Algoritmo inteligente. Lo que buscan los sistemas inteligentes es comprender las características de la inteligencia humana, para poder agregar a las máquinas características de organismos biológicos con el fin de volverlas más inteligentes. La inteligencia artificial(lA) es el estudio de la inteligencia en pensamiento y acción. “La lA propone y desarrolla algoritmos que emulan características de los sistemas inteligentes, el propósito es transferir estas características a sistemas artificiales, robots, para elevar la calidad de vida de los seres humanos.” (Delgado A., 1999).

Los algoritmos inteligentes consisten fundamentalmente en redes neuronales, lógica difusa, neuro difusa, algoritmos evolutivos, algoritmos genéticos, algoritmos de enjambre de partículas, juegan un papel significativo para resolver problemas, porque son capaces de manipular problemas no estructurados con la propagación del error, las incertidumbres y la imprecisión en la medición. Son sistemas que apoyan a las decisiones que reúnen los recursos intelectuales de los individuos con las capacidades de las computadoras con el objetivo de mejorar la calidad de las decisiones. (OAS, 2018)

Hay tres clases principales de aprendizaje automático

2.2.3.3.1. Aprendizaje supervisado. **“**En el aprendizaje supervisado, el conjunto de entrenamiento consta de pares de entrada y salida, y el objetivo es aprender un mapeo entre los espacios de entrada y salida.” (Simeone, 2018).

2.2.3.3.2. Aprendizaje no supervisado. Las técnicas de aprendizaje no supervisado funcionan sin resultados ni observaciones conocidas, es decir, estas técnicas no intentan predecir ningún resultado específico. En cambio, las técnicas no supervisadas intentan descubrir patrones dentro de los conjuntos de datos. El aprendizaje no supervisado es un enfoque útil para los problemas que no tienen suficientes datos de salida o de ejemplo para entrenar un modelo supervisado. (C3.ia, 2021)

2.2.3.3.3. Aprendizaje por refuerzo. Se encuentra, en cierto sentido, entre el aprendizaje supervisado y no supervisado.

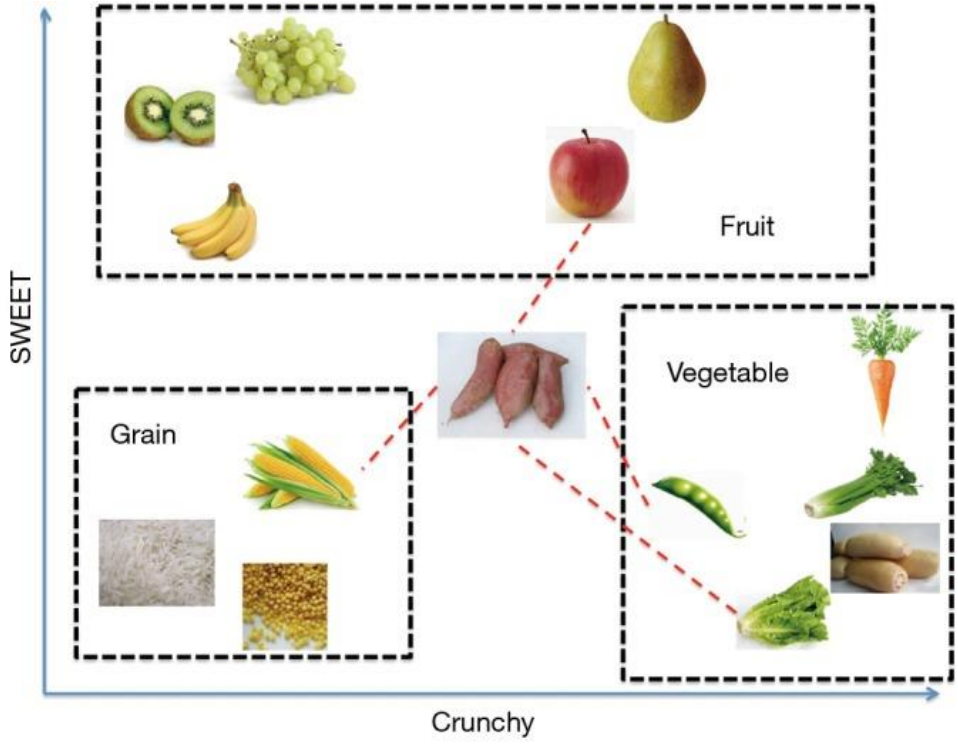
A diferencia del aprendizaje no supervisado existe una forma de supervisión, pero esto no viene en forma de especificación de una salida deseada para cada entrada en los datos. En cambio, un algoritmo de aprendizaje de refuerzo recibe retroalimentación del entorno solo después de seleccionar una salida para una determinada entrada u observación. La retroalimentación indica el grado en el que el resultado, conocido como acción en el aprendizaje por refuerzo, cumple los objetivos del aprendedor.

El aprendizaje por refuerzo se aplica a problemas secuenciales de toma de decisiones en los que el aprendedor interactúa con un entorno tomando acciones secuencialmente - los resultados - sobre la base de sus observaciones -sus aportaciones, mientras recibe retroalimentación sobre cada acción seleccionada. (Simeone, 2018)

2.2.3.3.4. K-nearest neighbor. El clasificador kNN sirve para clasificar las observaciones no etiquetadas asignándolas a la clase de los ejemplos etiquetados más similares. Las características de las observaciones se recopilan tanto para el entrenamiento como para el conjunto de datos de prueba. Por ejemplo, las frutas, verduras y cereales se pueden distinguir por su crujiente y dulzura (Figura 2). Con el fin de mostrarlos en una gráfica de dos dimensiones, solo se emplean dos características. En realidad, puede haber cualquier número de predictores y el ejemplo se puede ampliar para incorporar cualquier número de características. En general, las frutas son más dulces

que las verduras. Los cereales no son crujientes ni tampoco dulces. Nuestro trabajo es determinar a qué categoría pertenece la batata. En este ejemplo, elegimos los cuatro tipos de alimentos más cercanos: manzana, judía verde, lechuga y maíz. Como la verdura tiene mayor número de votos, la batata es asignada a la clase de verdura.

Figura 2.
Modelo Knn



El método para calcular la distancia entre la batata y otros tipos de alimentos. De forma predeterminada, la función knn () emplea la distancia euclidiana que se puede calcular con la ecuación (1)

$$\boldsymbol{D(p,q) = \sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots + (p_n - q_n)^2}} \text{ (1)}$$

donde p y q son sujetos a comparar con n características. (Demey, 2011).

El parámetro k que decide cuántos vecinos se elegirán para el algoritmo kNN. La elección adecuada de k tiene un impacto significativo en el rendimiento diagnóstico del algoritmo kNN. Una k

grande reduce el impacto de la varianza causada por un error aleatorio, pero corre el riesgo de ignorar un patrón pequeño pero importante. (Zhang, 2016)

2.2.3.3.5 ml.js. La biblioteca ML es una recopilación de las herramientas desarrolladas en la organización mljs.

Se mantiene principalmente para su uso en el navegador. Si se trabaja con Node.js, es posible que se prefiera agregar a sus dependencias solo las bibliotecas que se necesiten, ya que normalmente se publican en npm con más frecuencia.
Se prefijan todos sus nombres de paquetes npm con (por ejemplo, ml-matrix) para que sean fáciles de encontrar.

La lista de librerías que incluye son:

- Aprendizaje no supervisado
    - Análisis de componentes principales (PCA): ML.PCA.
    - Agrupación en clústeres jerárquica: ML.HClust.
    - Agrupación en clústeres K-means: ML.KMeans.
- Aprendizaje supervisado
    - Bayes ingenuo: ML.NaiveBayes.
    - K-Vecino más cercano (KNN): ML.KNN.
    - Mínimos cuadrados parciales (PLS): ML.PLS.
    - K-OPLS: ML.KOPLS.
    - Validación cruzada: ML.CrossValidation.
    - Matriz de confusión: ML.ConfusionMatrix.

  - Clasificador de árbol de decisión: ML.DecisionTreeClassifier.
  - Clasificador de bosque aleatorio: ML.RandomForestClassifier.

- Redes neuronales artificiales (ANN)
  - Redes neuronales feedforward: ML.FNN.
  - Mapa autoorganizado / redes Kohonen: ML.SOM.

- Regresión
  - Regresión lineal simple: ML.SimpleLinearRegression.
  - Regresión polinómica: ML.PolynomialRegression.
  - Regresión lineal multivariante: ML.MultivariateLinearRegression.
  - Regresión de potencia: ML.PowerRegression.
  - Regresión exponencial: ML.ExponentialRegression.
  - Regresión de Theil-Sen: ML.TheilSenRegresión.
  - Regresión polinómica robusta: ML.RobustPolynomialRegression.
  - Regresión del árbol de decisión: ML.DecisionTreeRegression.
  - Regresión de bosque aleatorio: ML.RandomForestRegression.

- Optimización
  - Levenberg-Marquardt: ML.levenbergMarquardt.
  - Mínimos cuadrados no negativos combinatorios rápidos: ML.FCNNLS.

- Matemática
  - Matrix: ML.Matrix (clase Matrix).

- Descomposición de valores singulares (SVD): ML.SVD.
- Descomposición del valor propio (EVD): ML.EVD.
- Descomposición de Cholesky: ML.CholeskyDescomposición.
- Descomposición lu: ML.LuDescomposición.
- Descomposición QR: ML.QrDescomposición.
- Matriz dispersa: ML.SparseMatrix.
- Kernels: ML.Kernel.
- Funciones de distancia: ML.Distance.
- Funciones de similitud: ML.Similarity.
- Matriz de distancia: ML.distanceMatrix.
- XORShift-add RNG: ML.XSadd.
- análisis morfológico generalizado no negativo de componentes ML.nGMCA

- ML.Array
  - ML.Array.min.
  - ML.Array.max.
  - ML.Array.median.
  - ML.Array.mean
  - ML.Array.mode.
  - ML.Array.normed.
  - ML.Array.rescale.

- ML.Array.sequentialFill.
- ML.Array.standardDeviation.
- ML.Array.variance.

- ML.ArrayXY
  - ML.ArrayXY.weightedMerge:Combinar valores de abscisas en ordenadas similares y ponderar el grupo de abscisas.
  - ML.ArrayXY.maxMerge:Combinar valores de abscisas en ordenadas similares y mantiene la abscisa con un valor de ordenada mayor.
  - ML.ArrayXY.closestX:Obtener el punto más cercano para un valor de abscisa específico.
  - ML.ArrayXY.centroidsMerge:combinar valores de abscisas si el valor de ordenada está en una lista de centroides.
  - ML.ArrayXY.sortX:Ordenar un conjunto de puntos en función de los valores de abscisas.
  - ML.ArrayXY.maxY:Ordenar un conjunto de puntos en función de los valores de abscisas.
  - ML.ArrayXY.uniqueX:asegúrese de que los valores x son únicos.

- Estadística
  - Rendimiento (curva ROC): ML.Performance
  - procesamiento de datos
  - Análisis de componentes principales (PCA): ML.PCA

- Filtro Savitzky-Golay: ML.savitzkyGolay
- Deconvolución espectral global (GSD): ML.GSD

- Utilidad
  - Operaciones de matriz de bits: ML.BitArray
  - Tabla hash: ML.HashTable
  - Matriz de pad: ML.padArray
  - Búsqueda binaria: ML.binarySearch
  - Funciones de comparación de números para ordenar: ML.numSort
  - Generación de números aleatorios: ML.Random. (npm:,2021, 10 junio)

2.2.3.4. Chatbot. Es un programa informático que simula y procesa la conversación humana (ya sea escrita o hablada), permitiendo a los humanos interactuar con dispositivos digitales como si se estuvieran comunicando con una persona real. Los chatbots pueden ser tan simples como los programas rudimentarios que responden a una consulta simple con una respuesta de una sola línea, o tan sofisticados como los asistentes digitales que aprenden y evolucionan para ofrecer niveles crecientes de personalización a medida que recopilan y procesan información.

Sin embargo, es un complemento para mejorar un servicio nunca puede sustituir el servicio de una persona.

Enfoques

- **IA.** Ventaja: Trato más natural.
  - **Hándicap:** Necesario mucho aprendizaje.
- **Mixto.** Ventaja: Consenso entre naturalidad y automatización.

- **Hándicap:** Trato menos personal.

- **Dirigido.** Ventaja: Menos errores.

    - **Hándicap:** restringido a contexto y a flujo predefinido. (Ortega M,2018)

2.2.3.4.1. Dialogflow. "Es una plataforma con comprensión del lenguaje natural que te facilita el diseño de una interfaz de usuario de conversación y su integración a tu aplicación para dispositivos móviles, aplicación web, dispositivo, bot." (Dialogflow, 2021).

Dialogflow tiene soporte para múltiples tipos de entradas, incluidas entradas de audio o texto. Además de igual manera también puede responder a través de texto o con voz sintética (Dialogflow, 2021).

Arquitectura de DialogFlow

Agente: Dialogflow es un agente virtual que maneja las conversaciones con los usuarios finales. Es un módulo encargado del entendimiento e interpretación del lenguaje natural que comprende los matices del lenguaje humano. Durante una conversación Dialogflow traduce la entrada del usuario final a datos estructurados para el entendimiento otras aplicaciones y servicios (Dialogflow, 2021). Un agente de Dialogflow se crea y diseña con la finalidad de controlar los tipos de conversaciones que puede requerir un sistema.

Intent: Un intent se encarga de clasificar la intención del usuario final en turnos de conversación. Para cada agente se definen varios intents; los intents combinados son capaces de simular una conversación completa. Cuando un usuario final interactúa se denomina como una expresión de usuario final, Dialogflow hace coincidir la expresión del usuario final con el intent más adecuado del agente. La coincidencia de un intent es conocida como clasificación de intent (Dialogflow, 2021).

Entidades: Dialogflow brinda varias entidades del sistema predefinidas que pueden coincidir con tipos de datos comunes como: horas, fechas, colores, direcciones de correo electrónico, etcétera. También existe la posibilidad de crear entidades propias y personalizadas para detectar coincidencias en datos personalizados. (Dialogflow, 2021).

Contexto: Similares a los contextos del lenguaje natural para que Dialogflow maneje una expresión de usuario final, por ejemplo, cuando se dice "es de color naranja", se necesita contexto para saber de quien se habla. En DialogFlow es necesario proporcionarse un contexto con el objetivo decoincidir de forma correcta con un intent (Dialogflow, 2021).

2.2.3.4.2. Kommunicate. Kommunicate es una plataforma inteligente de comunicación con el cliente para un soporte en tiempo real, proactivo y personalizado para empresas en crecimiento. Kommunicate es una solución integral para todos los problemas de atención al cliente.

2.3. Antecedentes contextuales

El comando conjunto de las Fuerzas Armadas es una institución de más alto nivel de credibilidad; sistemáticamente integrada, con capacidades conjuntas e interoperabilidad, personal profesional, ético y moralmente calificado, para enfrentar los cambios y nuevos escenarios, que garanticen la paz, seguridad y el bienestar de la nación.

Dentro del comando conjunto se encuentran, la Fuerza Terrestre Fuerza Aérea y Fuerza Naval. (C.C.F.F.A.A)

La Comandancia de la Fuerza Aérea Ecuatoriana hace uso de diferentes servicios informáticos internos como: El Sistema de Gestión Documental “CHASQUI”, El Correo Institucional “ZIMBRA”, El Sistema de Gestión Integral, El Sistema de Gestión Institucional SIGEIN, La Intranet Comando Conjunto, y el Sistema de auditoría de proyectos. (F.A.E)

2.4. Metodología de desarrollo del proyecto

2.4.1. Tipo de investigación

- **Investigación Documental.** El presente proyecto implementará la investigación documental, basado en la recolección de diferentes tipos de información disponible tanto en publicaciones, artículos científicos y proyectos asociados.

2.4.2. Métodos

- **Teórico.** Para el cumplimiento de las actividades se utilizarán distintos tipos de métodos teóricos.
    - **Método Histórico Lógico:** El método histórico lógico se utilizará para determinar los antecedentes históricos sobre la evolución de la ingeniería social y sus métodos de prevención.
    - **Método Hipotético Deductivo:** El método hipotético deductivo es usado desde el inicio de la investigación cuando se determinó la situación problemática.
    - **Método de Modelación:** El método de modelación será utilizado para determinar el enfoque y alcance del sistema.
- **Empírico.** El proyecto es práctico así que se utilizará el método empírico Experimental.
    - **Método Experimental:** La experimentación permite verificar el comportamiento del proyecto bajo diferentes configuraciones que se enfocan a mejorar la experiencia de usuario, con lo cual permite aumentar la calidad del sistema.

CAPÍTULO III

3. Desarrollo del sistema

En este capítulo se desarrolla la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana., utilizando como base la metodología web UWE.

Para desarrollar la plataforma SafeSecure, se va a seguir los pasos que propone la metodología Web UWE.

3.1. Gestión y análisis de requisitos.

Empezando con la fase de captura, análisis y especificación de requisitos propuesta por la metodología Web UWE se realizó la elicitación de requisitos del sistema, la misma que fue culminada en un total de 2 reuniones con las autoridades del departamento de seguridad informática de la Comandancia de la Fuerza Aérea Ecuatoriana, y posteriormente plasmada en forma de historias de usuario.

3.1.1. Documento ERS.

3.1.1.1. Historias De Usuario. Yo teniente Marcelo Araujo **Como** jefe del departamento de seguridad de la información **Quiero** una plataforma web que se encargue de concientizar y entrenar al personal militar, civil y terceros que hacen uso de las plataformas, sistemas e infraestructura tecnológica de la Fuerza Aérea Ecuatoriana, sobre las vulnerabilidades a las que están expuestos en el ciberespacio a través de técnicas de ingeniería social.

Para proteger la confidencialidad, integridad, disponibilidad y el no repudio de la información institucional.

- Cargar información de los departamentos que están conformados por la institución (nombre del departamento, jefe del departamento, cantidad de empleados, ...).

- Gestionar información de los departamentos que están conformados por la institución.
- Cargar datos de trabajadores de la institución (Nombre, Correo, Cargo, Departamento, Fecha de Nacimiento).
- Gestionar información de los trabajadores de la institución.
- Cargar información de plantillas mensajes de correo electrónico (Nombre, Asunto, Contenido, Categoría, Enlaces).
- Gestionar información de plantillas mensajes de correo electrónico.
- Cargar plantillas HTML para vincular a los mensajes de correo electrónico (Código HTML).
- Crear y Personalizar plantillas HTML para vincular a los mensajes de correo electrónico.
- Gestionar plantillas HTML para vincular a los mensajes de correo electrónico.
- Envío de ataque de simulación (nombre, fecha_creacion, fecha_envio, estado, mail(remitente_nombre,remitente_email,plantilla), destinatario(coleccion de trabajadores)).
- Gestionar ataques de simulación.
- Generar reportes de ataque de simulación por fecha de envío.
- Generar reportes de ataque de simulación por departamento.
- Generar reportes de ataque de simulación por categoría de mail.
- Generar recomendaciones de asuntos para nuevos contenidos de correos electrónicos a través de un algoritmo inteligente basado en los resultados de los ataques enviados.
- Consultar información de ingeniería social a través de un chatbot.
- Visualizar información básica sobre ingeniería social
- Llevar un control del personal que visualiza y se capacita con la información básica sobre la ingeniería social, con los campos (Nombre, Correo, Cargo, Departamento, Fecha de Nacimiento, tiempo uso, utilidad (Se capacito o no))
- Generar reportes con la información del personal capacitado.

***3.1.1.1.1. Roles*.**

- **Administrador.** Tiene acceso a todo el sistema
- **Trabajador.** Tiene acceso solo al contenido de visualización de ingeniería social

3.1.1.1.2. Fichas de historias de usuario

Tabla 1.
Cargar Información de Departamentos

	HISTORIAS DE USUARIO
NÚMERO: 1	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Cargar Información de Departamentos	
PRIORIDAD DE NEGOCIO: Alta	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 2	**ITERACIÓN ASIGNADA:** 2
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere poder cargar/subir la información de departamentos conformados por la institución con los datos: • Nombre del departamento • Jefe del departamento • Cantidad de empleados • .... • Nombre de las Direcciones - Modelo (nombre) El sistema brindará una plantilla en la que deben presentarse los datos a subir para poder ser procesados. Los datos podrán ser cargados de manera individual o en glosa.	
VALIDACIÓN: El administrador puede cargar/subir la información de departamento requerida.	

Tabla 2.
Gestionar información de departamentos

	HISTORIAS DE USUARIO
NÚMERO: 2	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Gestionar información de departamentos	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Bajo

PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 1
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere gestionar la información de los departamentos que están conformados por la institución guardados en el sistema. • Agregar departamentos • Modificar departamentos • Eliminar departamentos	
VALIDACIÓN: El administrador puede gestionar la información de departamentos	

Tabla 3.
Cargar datos de trabajadores

	HISTORIAS DE USUARIO
NÚMERO: 3	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Cargar datos de trabajadores	
PRIORIDAD DE NEGOCIO: Alta	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 2	**ITERACIÓN ASIGNADA:** 2
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere cargar/subir los datos de trabajadores de la institución con los datos: • Nombre • Correo • Cargo • Departamento • Fecha de Nacimiento El sistema brindará una plantilla en la que deben presentarse los datos a subir para poder ser procesados. Los datos podrán ser cargados de manera individual o en glosa.	
VALIDACIÓN: El administrador puede cargar/subir los datos de trabajadores de la institución	

Tabla 4.
Gestionar información de los trabajadores

HISTORIAS DE USUARIO

NÚMERO: 4	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Gestionar información de los trabajadores	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 1
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere gestionar la información de los trabajadores de la institución guardados en el sistema. • Agregar nuevo trabajador • Modificar trabajador • Eliminar trabajador	
VALIDACIÓN: El administrador podrá gestionar la información de trabajadores de la institución guardados en el sistema.	

Tabla 5.
Cargar información de plantillas

	HISTORIAS DE USUARIO
NÚMERO: 5	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Cargar información de plantillas	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 2	**ITERACIÓN ASIGNADA:** 2
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere subir/cargar información de plantillas mensaje de correo electrónico con los datos: • Nombre • Asunto • Contenido • Categoría • Enlaces	
VALIDACIÓN: El administrador podrá cargar información de plantillas mensajes de correo electrónico.	

Tabla 6.
Gestionar información de plantillas de mensajes

	HISTORIAS DE USUARIO
NÚMERO: 6	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Gestionar información de plantillas de mensajes	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 2	**ITERACIÓN ASIGNADA:** 1
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere gestionar la información de plantillas mensajes de correo electrónico guardadas en el sistema como: • Agregar plantillas de mensaje • Modificar plantillas de mensaje • Eliminar plantillas de mensaje	
VALIDACIÓN: El administrador podrá gestionar información de plantillas de mensajes de correo electrónico guardadas en el sistema.	

Tabla 7.
Cargar plantillas HTML

	HISTORIAS DE USUARIO
NÚMERO: 7	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Cargar plantillas HTML	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 3
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere subir/cargar plantillas HTML con los siguientes datos: • Nombre • Archivo HTML Las plantillas HTML podrán ser vinculadas a los mensajes de correo electrónico dentro de los ataques de simulación.	
VALIDACIÓN: El administrador podrá subir/cargar plantillas HTML y podrá vincularlos a los mensajes de correo electrónico dentro de los ataques de simulación. .	

Tabla 8.
Crear y Personalizar plantillas HTML

	HISTORIAS DE USUARIO
NÚMERO: 8	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Crear y Personalizar plantillas HTML	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 3
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere poder crear y personalizar plantillas HTML que podrán ser vinculadas a los mensajes de correo electrónico dentro de los ataques de simulación.	
VALIDACIÓN: El administrador podrá crear y personalizar plantillas HTML y podrá vincularlos a los mensajes de correo electrónico dentro de los ataques de simulación.	

Tabla 9.
Gestionar plantillas HTML

	HISTORIAS DE USUARIO
NÚMERO: 9	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Gestionar plantillas HTML	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 3
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere gestionar la información de las plantillas HTML guardadas en el sistema. • Agregar plantillas HTML • Modificar • Eliminar	
VALIDACIÓN: El administrador podrá gestionar plantillas HTML guardadas en el sistema.	

Tabla 10.
Envío de ataque de simulación

	HISTORIAS DE USUARIO
NÚMERO: 10	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Envío de ataque de simulación	
PRIORIDAD DE NEGOCIO: Alta	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA: 3**
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	

DESCRIPCIÓN: Se requiere poder realizar el envío de ataques de simulación en una fecha determinada con datos como:
• nombre del ataque
• fecha creación
• fecha envió
• estado (estado del ataque enviado o pendiente)
• mail
  o nombre del remitente.
  o email del remitente.
  o plantilla del correo electrónico.
  o email del destinatario.
• destinatario
  o Lista de los trabajadores para enviar.	

VALIDACIÓN: El administrador podrá enviar ataques de simulación a trabajadores de la institución.	

Tabla 11.
Gestionar ataques de simulación

	HISTORIAS DE USUARIO
NÚMERO: 11	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Gestionar ataques de simulación	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Medio
PUNTOS ESTIMADOS: 3	**ITERACIÓN ASIGNADA:** 2

PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO
DESCRIPCIÓN: Se requiere gestionar ataques de simulación guardados en el sistema. • Agregar ataque • Modificar ataque • Eliminar ataque
VALIDACIÓN: El administrador podrá gestionar ataques de simulación.

Tabla 12.
Generar reportes de ataque de simulación por fecha de envío

		HISTORIAS DE USUARIO
NÚMERO: 12	**USUARIO:** Administrador	
NOMBRE DE LA HISTORIA: Generar reportes de ataque de simulación por fecha de envío		
PRIORIDAD DE NEGOCIO: Media		**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 2		**ITERACIÓN ASIGNADA:** 2
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO		
DESCRIPCIÓN: Se requiere generar reportes de ataque de simulación por fecha de envío.		
VALIDACIÓN: El administrador podrá solicitar la generación de reportes de ataque de simulación por fecha de envío.		

Tabla 13.
Generar reportes de ataque de simulación por departamento

		HISTORIAS DE USUARIO
NÚMERO: 13	**USUARIO:** Administrador	
NOMBRE DE LA HISTORIA: Generar reportes de ataque de simulación por departamento.		
PRIORIDAD DE NEGOCIO: Media		**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 2		**ITERACIÓN ASIGNADA:** 2
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO		
DESCRIPCIÓN: Se requiere generar reportes de ataque de simulación por departamento.		
VALIDACIÓN: El administrador podrá solicitar la generación de reportes de ataque de simulación por departamento.		

Tabla 14.
Generar reportes de ataque de simulación por categoría de mail

	HISTORIAS DE USUARIO
NÚMERO: 14	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Generar reportes de ataque de simulación por categoría de mail	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 2	**ITERACIÓN ASIGNADA:** 2
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere generar reportes de ataque de simulación por categoría de mail	
VALIDACIÓN: El administrador podrá solicitar al sistema la generación de reportes de ataque de simulación por categoría de mail.	

Tabla 15.
Cargar datos de trabajadores

	HISTORIAS DE USUARIO
NÚMERO: 15	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Generar recomendaciones de asuntos de correos electrónicos.	
PRIORIDAD DE NEGOCIO: Baja	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 1
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere poder generar recomendaciones de asuntos para nuevos contenidos de correos electrónicos a través de un algoritmo de recomendación algoritmo k-Nearest Neighbor basado en los resultados de los ataques enviados.	
VALIDACIÓN: El administrador podrá solicitar al sistema asuntos para nuevos contenidos de correos.	

Tabla 16.
Consultar información de ingeniería social a través de un chatbot

HISTORIAS DE USUARIO

NÚMERO: 16	**USUARIO:** Trabajador
NOMBRE DE LA HISTORIA: Consultar información de ingeniería social a través de un chatbot.	
PRIORIDAD DE NEGOCIO: Media	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 2	**ITERACIÓN ASIGNADA:** 2
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere consultar información de ingeniería social a través de un chatbot, que pueda responder preguntas como: • ¿Qué es ingeniería social? • ¿Qué es Phishing? • ¿Cómo identificar un ataque de Phishing? • ¿Por qué se realizó este tipo de simulación? • etc.	
VALIDACIÓN: El trabajador podrá consultar información de ingeniería social a través de un chatbot.	

Tabla 17.
Visualizar información básica sobre ingeniería social

	HISTORIAS DE USUARIO
NÚMERO: 17	**USUARIO:** Trabajador
NOMBRE DE LA HISTORIA: Visualizar información básica sobre ingeniería social.	
PRIORIDAD DE NEGOCIO: Baja	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 1
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere poder visualizar información básica sobre ingeniería social como: • ¿Qué es ingeniería social? • ¿Qué es Phishing? • ¿Cómo identificar un ataque de Phishing? • ¿Por **qué** se realizó este tipo de simulación? • etc.	
VALIDACIÓN: El trabajador podrá visualizar información básica sobre ingeniería social.	

Tabla 18.
Llevar un control del personal que visualiza y se capacita con la información

HISTORIAS DE USUARIO	
NÚMERO: 18	**USUARIO:** Trabajador
NOMBRE DE LA HISTORIA: Llevar un control del personal que visualiza y se capacita con la información.	
PRIORIDAD DE NEGOCIO: Alta	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 1
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	
DESCRIPCIÓN: Se requiere poder llevar un control del personal que visualiza y se capacita con la información básica sobre la ingeniería social, con los campos: • Nombre • Correo • Cargo • Departamento • Fecha de Nacimiento • Tiempo uso • Utilidad (Se capacito o no)	
VALIDACIÓN: El Trabajador podrá registrar sus datos acerca de la visualización de información de capacitación.	

Tabla 19.
Generar reportes del personal capacitado

HISTORIAS DE USUARIO	
NÚMERO: 19	**USUARIO:** Administrador
NOMBRE DE LA HISTORIA: Generar reportes del personal capacitado	
PRIORIDAD DE NEGOCIO: Alta	**RIESGO EN EL DESARROLLO:** Bajo
PUNTOS ESTIMADOS: 1	**ITERACIÓN ASIGNADA:** 1
PROGRAMADOR RESPONSABLE: DANIEL LOPEZ – JIPSON MURILLO	

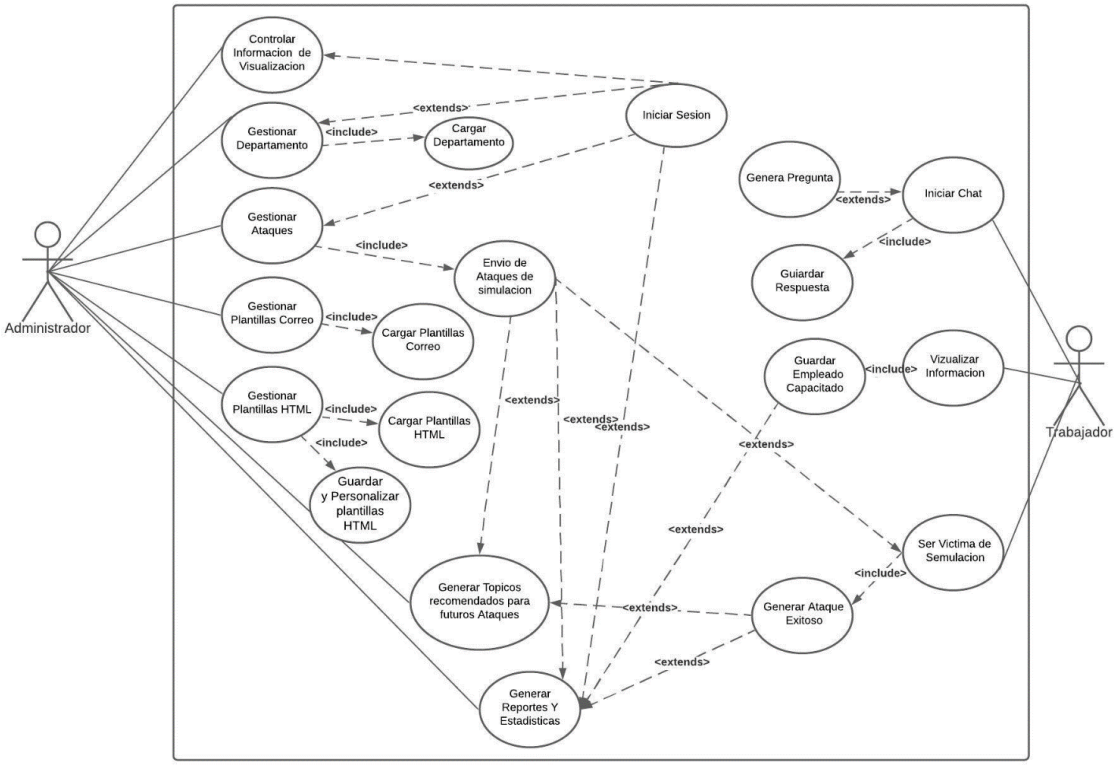
DESCRIPCIÓN: Se requiere generar reportes con la información del personal capacitado.
VALIDACIÓN: El administrador podrá generar reportes con la información del personal capacitado.

3.2. Diseño Conceptual, de Navegación y de Presentación

Continuando a la fase de diseño se realizaron los modelos de Casos de Uso, Contenido y Presentación, propuestos por la metodología UWE además de la realización de diagramas de secuencia sustituyendo al Modelo de Procesos.

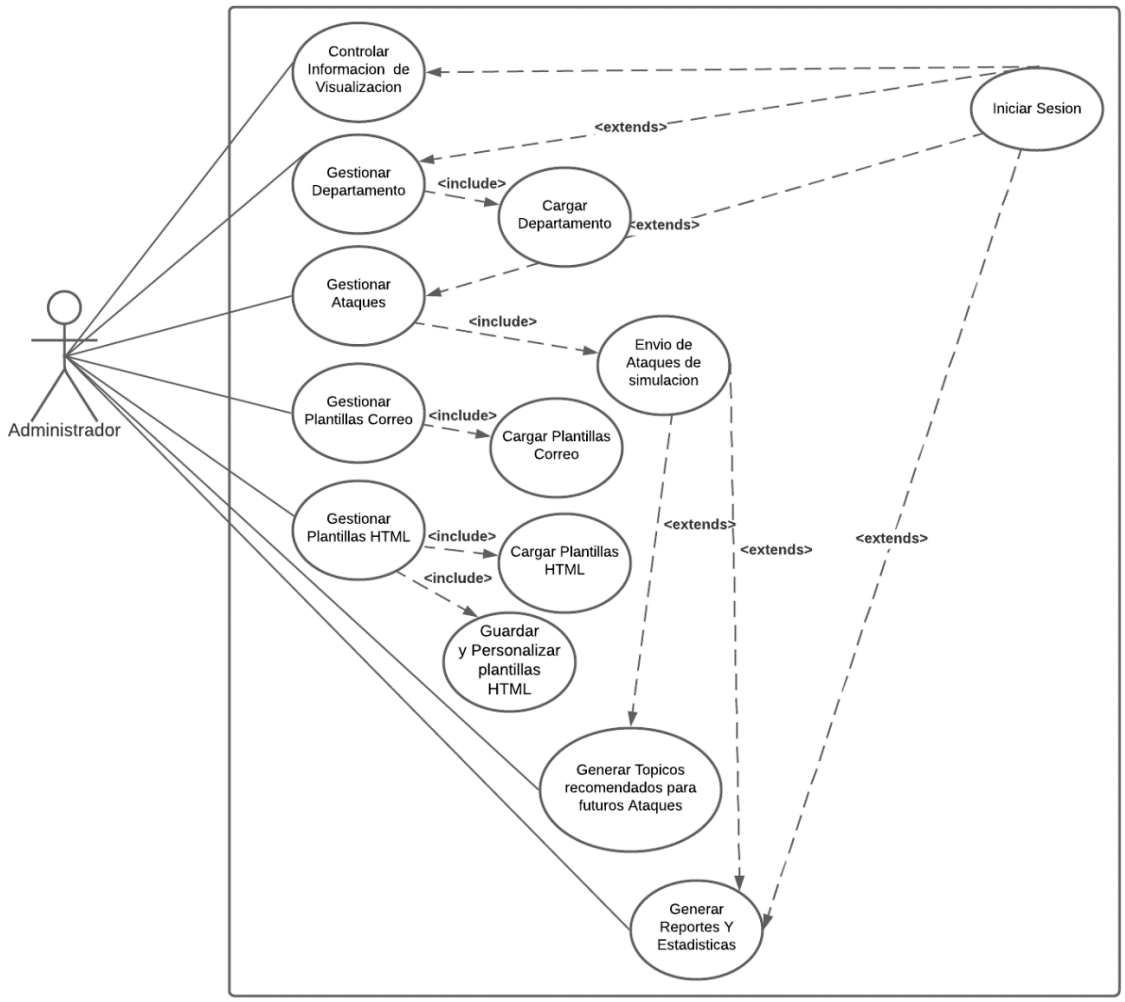
3.2.1. Descripción de Casos de Uso

Figura 3.
Diagrama de caso de uso - General



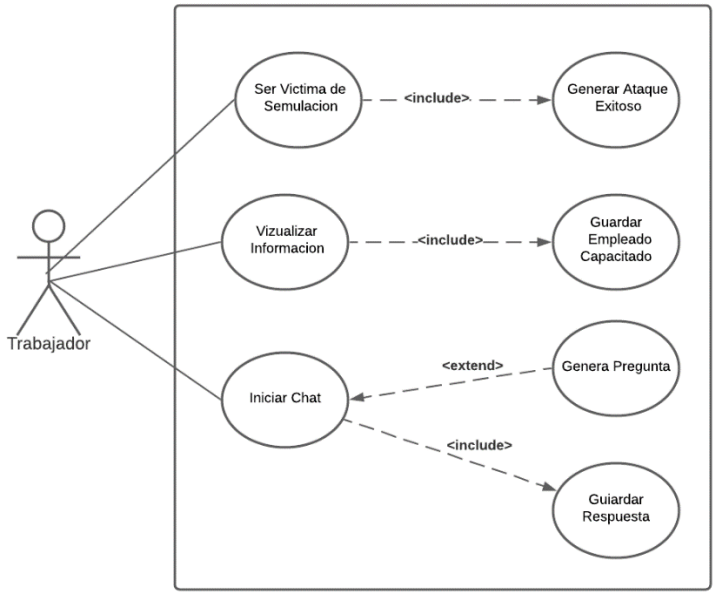
Nota. En la figura muestra el diagrama de casos de uso general del sistema en donde se representa las actividades que pueden realizar los diferentes actores dentro de la plataforma SafeSecure.

Figura 4.
Diagrama de casos de uso - Usuario administrador



Nota. En la figura se muestra el diagrama de casos de uso del administrador del sistema, en donde se representa las actividades que puede realizar el administrador dentro de la plataforma web SafeSecure.

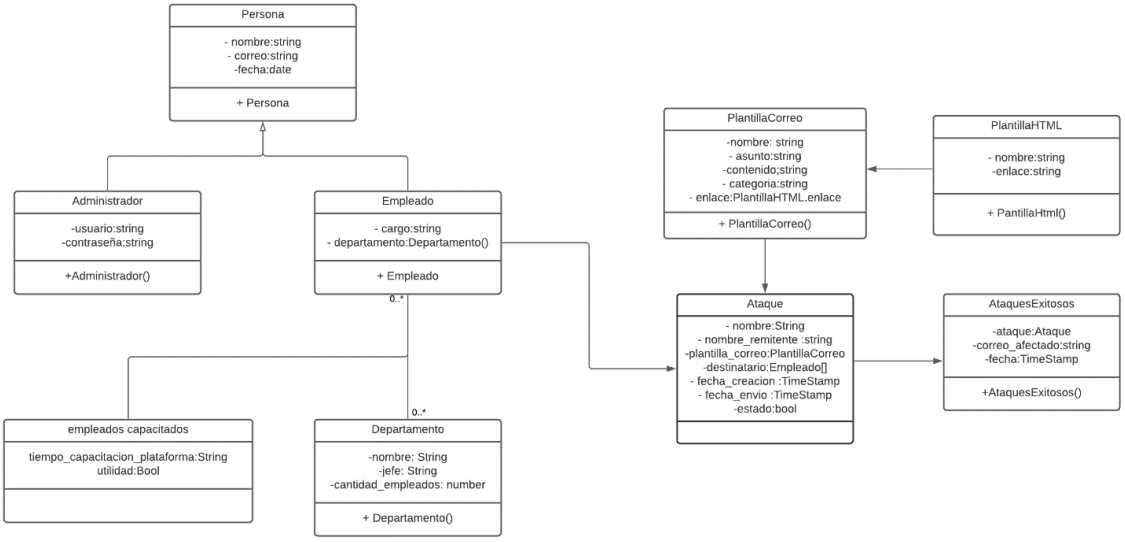
Figura 5.
Diagrama de casos de uso - Usuario trabajador



Nota. En la figura se muestra el diagrama de casos de uso del trabajador en donde se representa las actividades que puede realizar el trabajador dentro de la plataforma web SafeSecure.

3.2.2. Modelo de Contenido

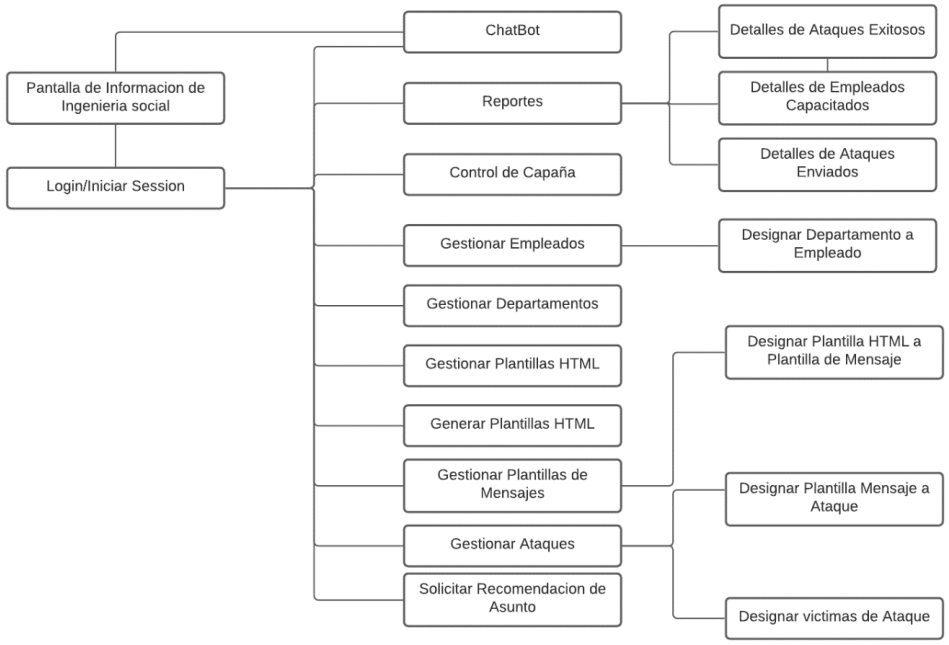
Figura 6.
Diagrama de contenido - SafeSecure



Nota. En la Figura se representa el diagrama de contendió en donde se muestra las distintitas clases que forman parte del sistema con sus respectivos atributos.

3.2.3. Modelo de Navegación

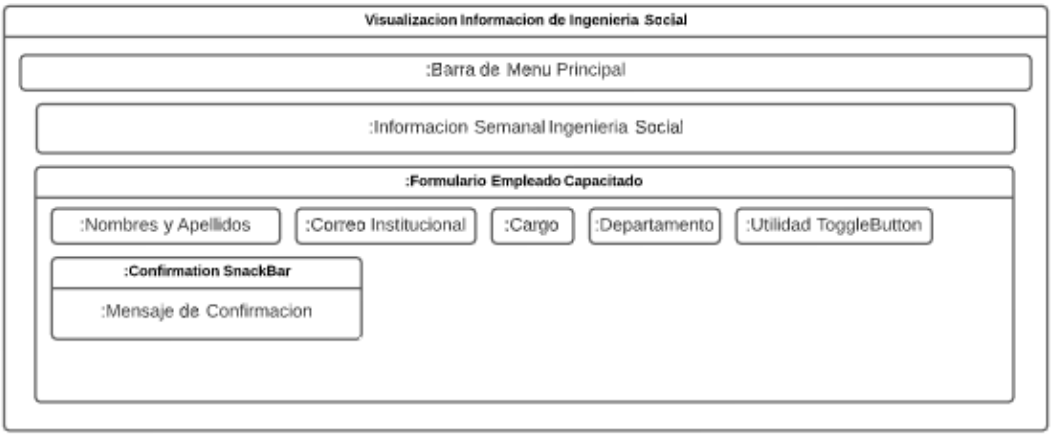
Figura 7.
Diagrama de navegación - SafeSecure



Nota. En la figura se representa el diagrama de navegación en el cual se visualiza la navegación del usuario dentro de la plataforma SafeSecure.

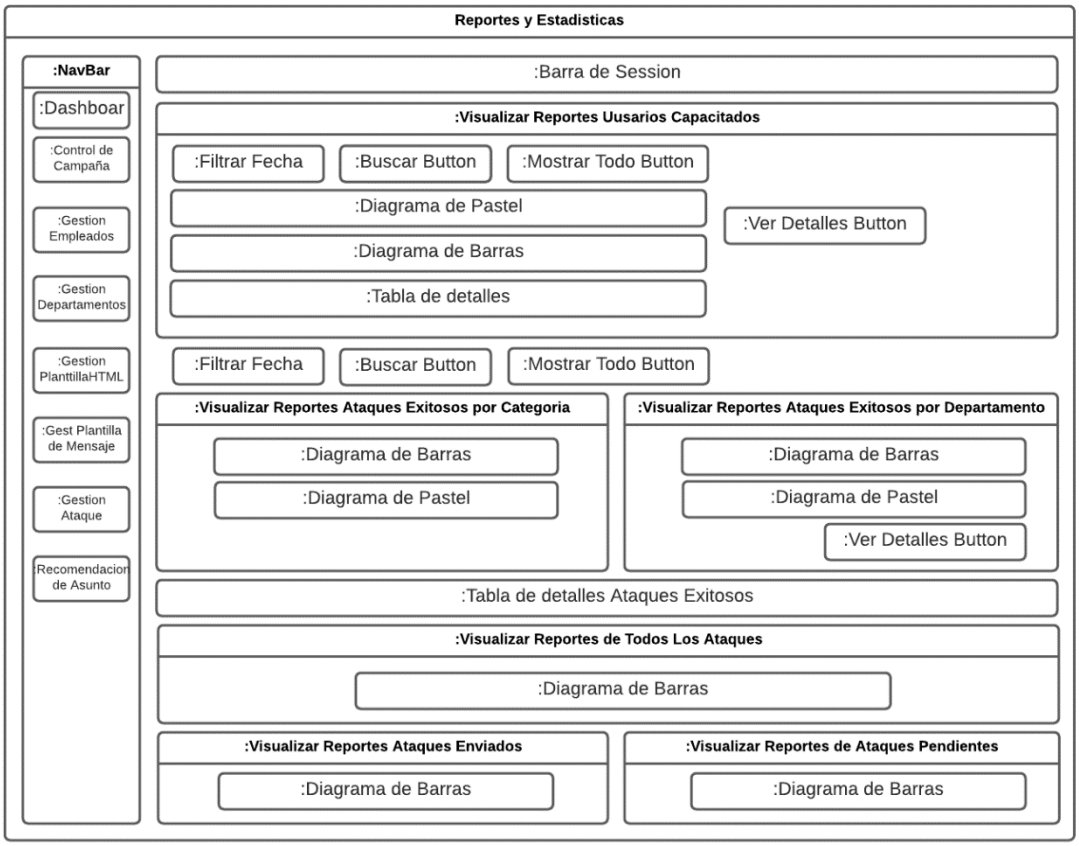
3.2.4. Modelo de Presentación

Figura 8.
Modelo de presentación - Visualizar información de ingeniería social



Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "*Visualizar información de ingeniería social*"

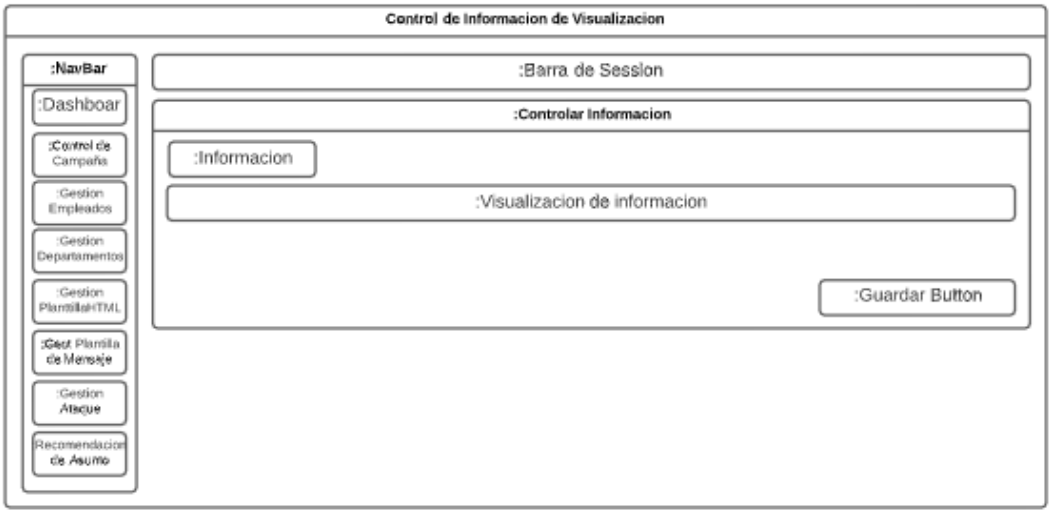
Figura 9.
Modelo de presentación - Generar reportes y estadísticas



Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "*Generar reportes y estadísticas*"

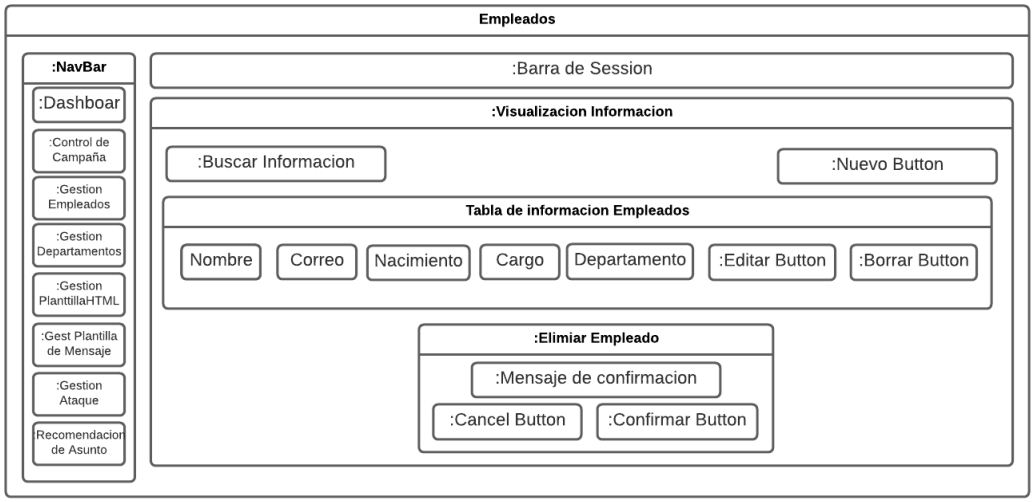
Figura 10.

Modelo de presentación - Controlar información de visualización



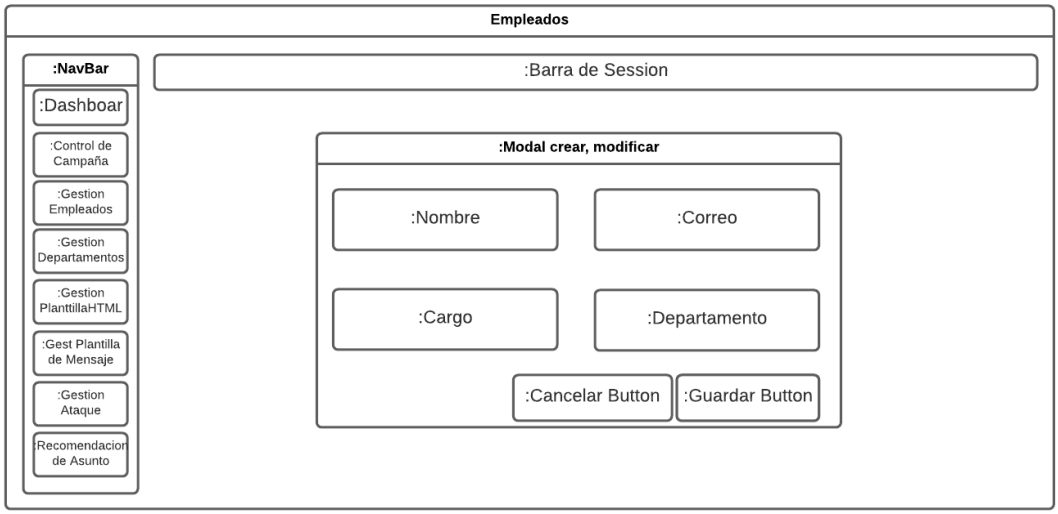
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "*Controlar información de visualización*"

Figura 11.
Modelo de presentación - Gestionar empleados



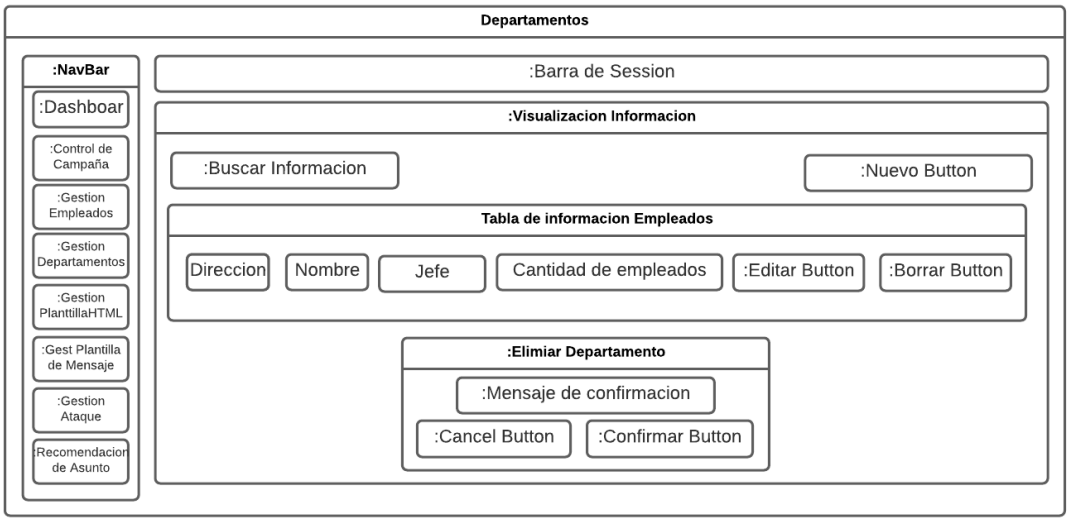
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de “Gestionar empleados”

Figura 12.
Modelo de presentación - Agregar/Modificar empleados



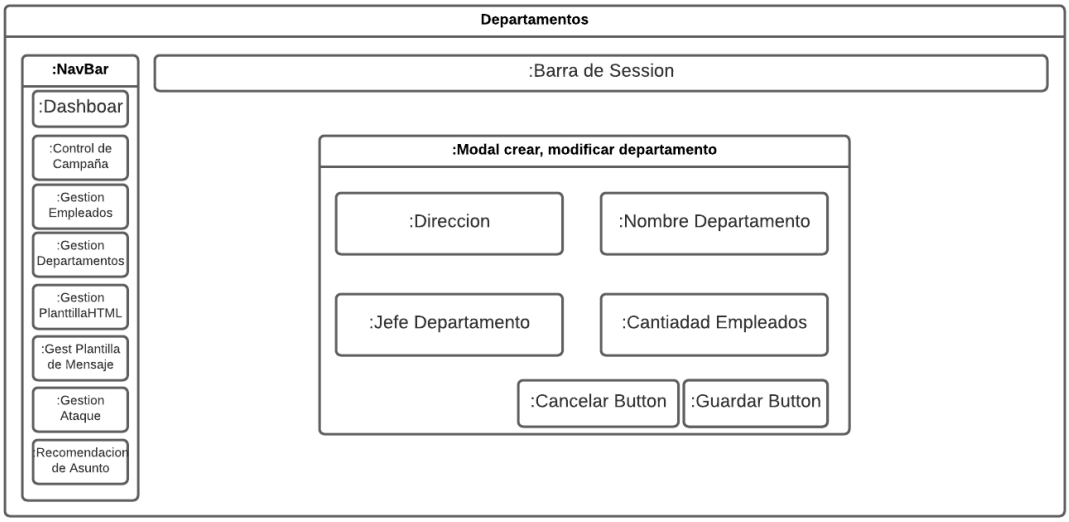
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de “Agregar/Modificar empleados”

Figura 13.
Modelo de presentación - Gestión departamento



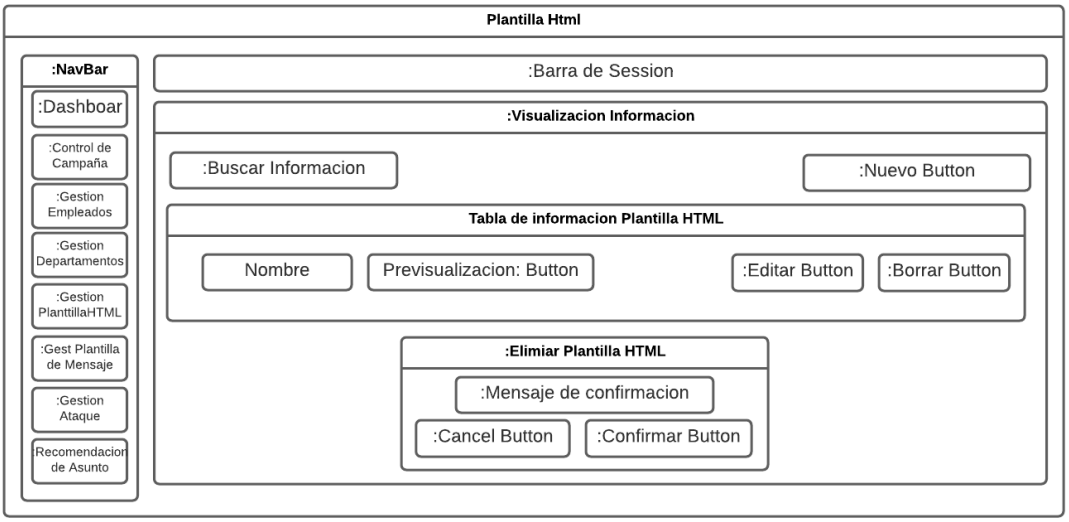
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de “Gestión departamento”

Figura 14.
Modelo de presentación - Agregar/Modificar departamento



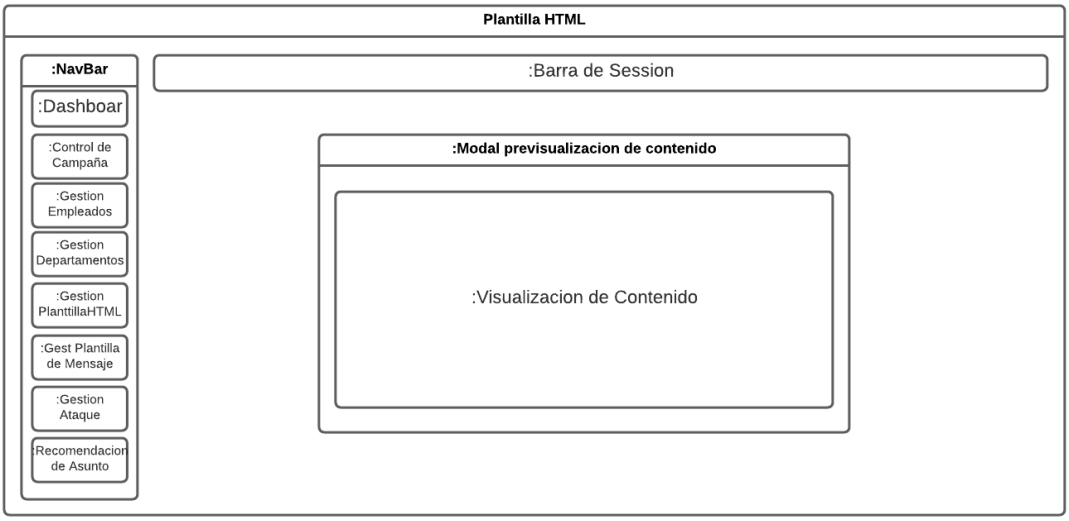
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "Agregar/Modificar departamento"

Figura 15.
Modelo de presentación - Gestión plantilla HTML



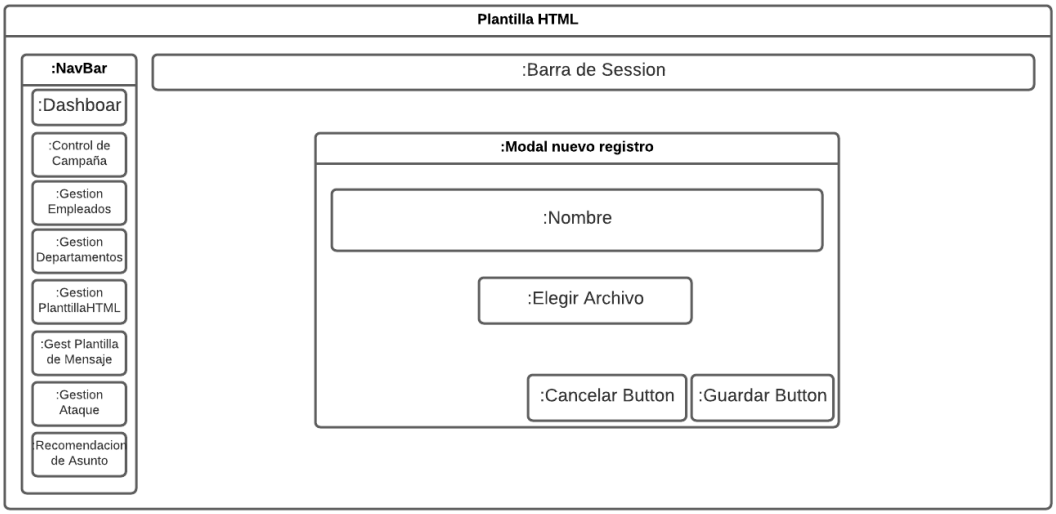
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "Gestión plantilla HTML"

Figura 16.
Modelo de presentación - Previsualización contenido HTML



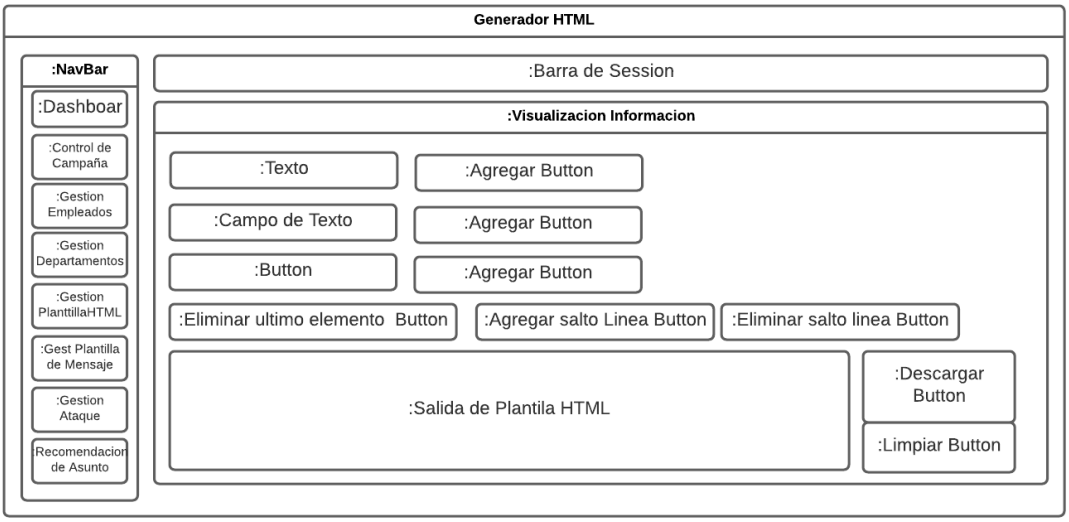
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "Previsualización contenido HTML"

Figura 17.
Modelo de presentación - Nuevo registro Plantilla HTML



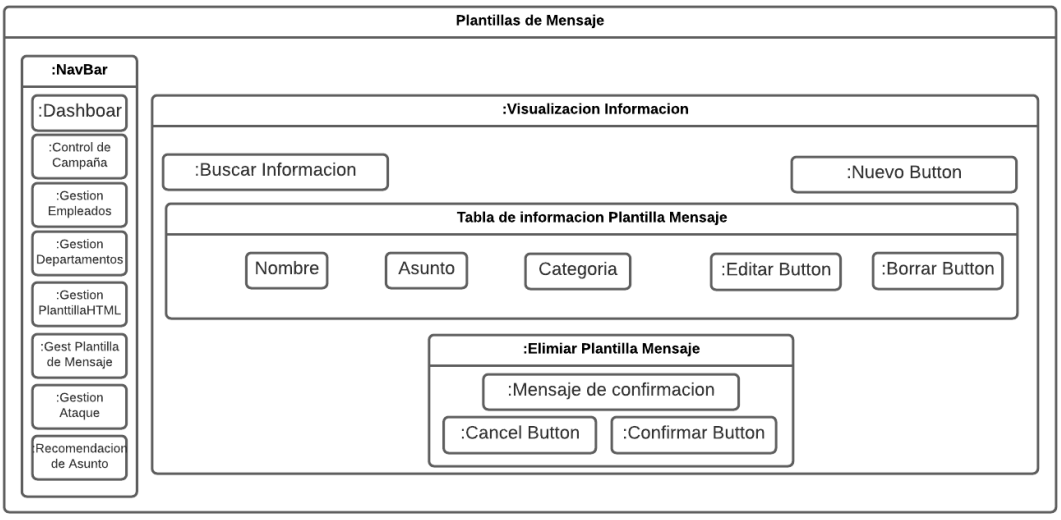
Nota. En la Figura se muestra como están distribuidos los elementos en la ventana de "Nuevo registro Plantilla HTML"

Figura 18.
Modelo de presentación - Generador HTML



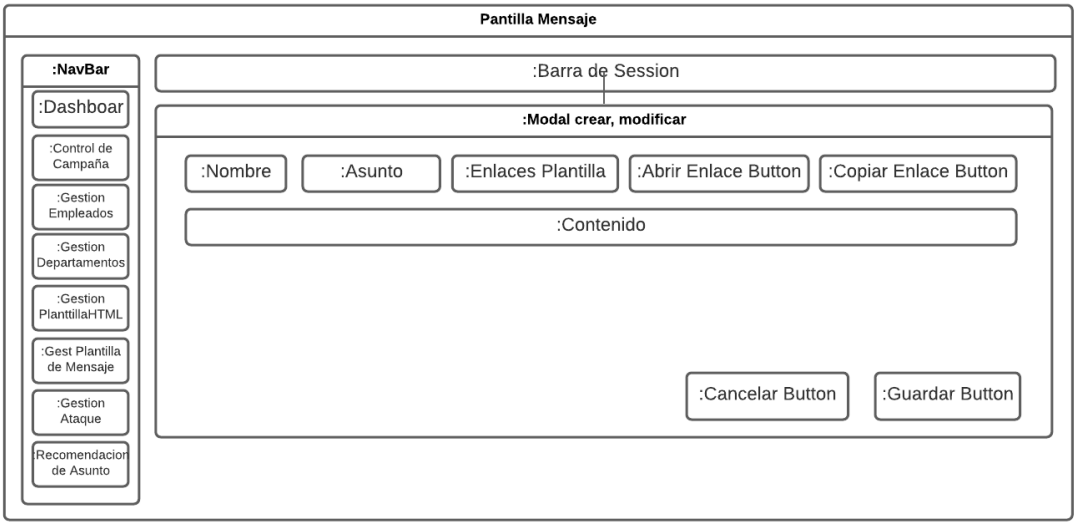
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "Generador HTML"

Figura 19.
Modelo de presentación - Gestionar Plantilla de Mensajes



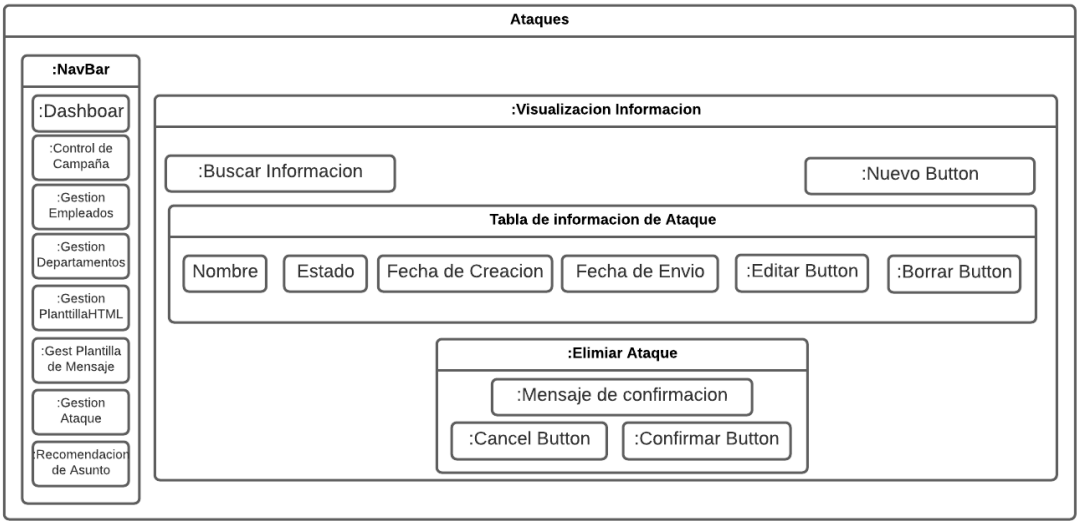
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "Gestionar Plantilla de Mensajes"

Figura 20.
Modelo de presentación - Agregar/Modificar plantilla de mensajes



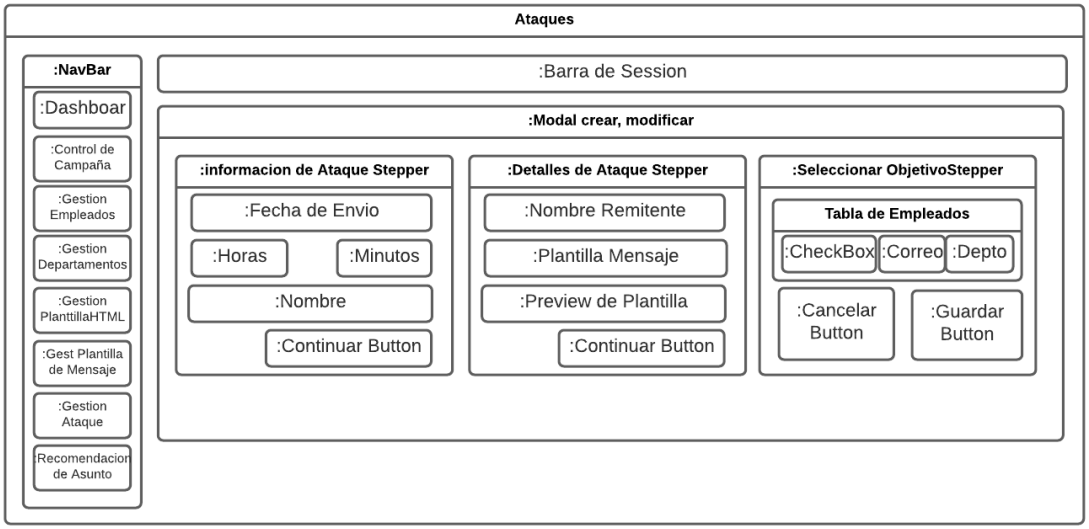
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "Agregar/Modificar plantilla de mensajes"

Figura 21.
Modelo de presentación - Gestionar ataques



Nota. En la figura se muestra como están distribuidos los elementos en la ventana de "Gestionar ataques"

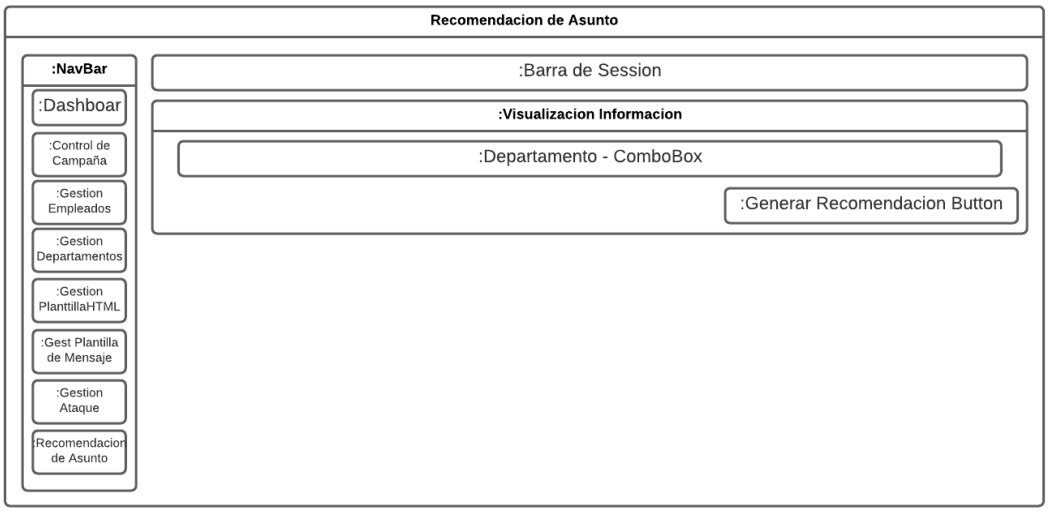
Figura 22.
Modelo de Presentación - Agregar/Modificar ataques



Nota. En la figura se muestra como están distribuidos los elementos en la ventana de

"Agregar/Modificar ataques"

Figura 23.
Modelo de presentación - Recomendación de asunto



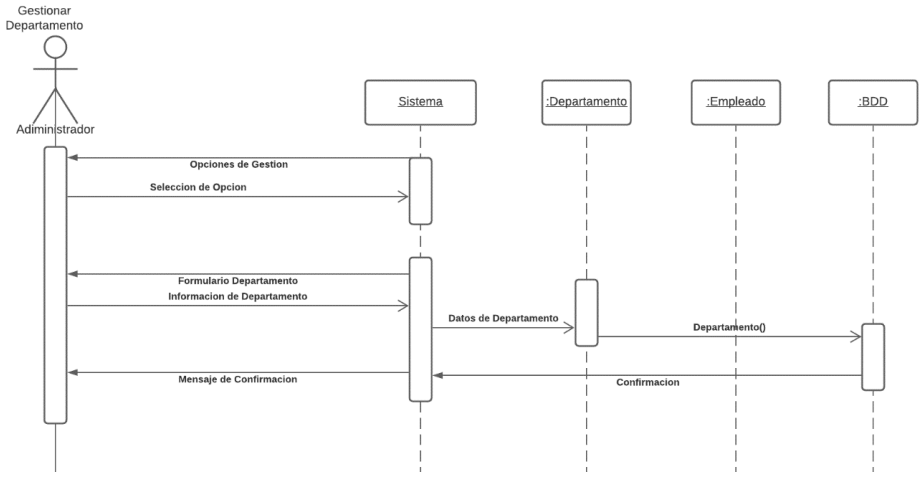
Nota. En la figura se muestra como están distribuidos los elementos en la ventana de

"Recomendación de asunto"

3.2.5. Diagramas de secuencia.

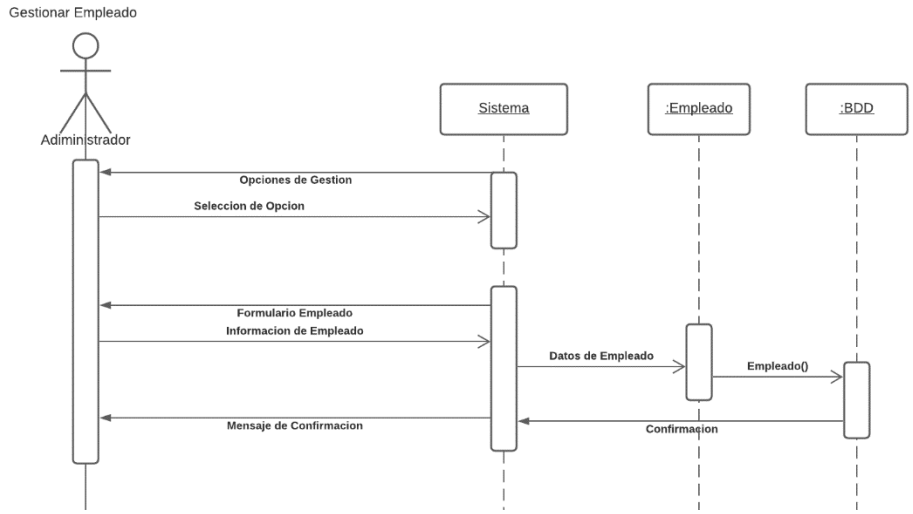
Se decidió optar por sustituir al modelo de procesos por diagramas de secuencias con la finalidad de que los diagramas puedan especificar con mayor claridad y completitud las actividades que va a realizar el sistema.

Figura 24.
Diagrama de secuencia - Gestionar departamentos



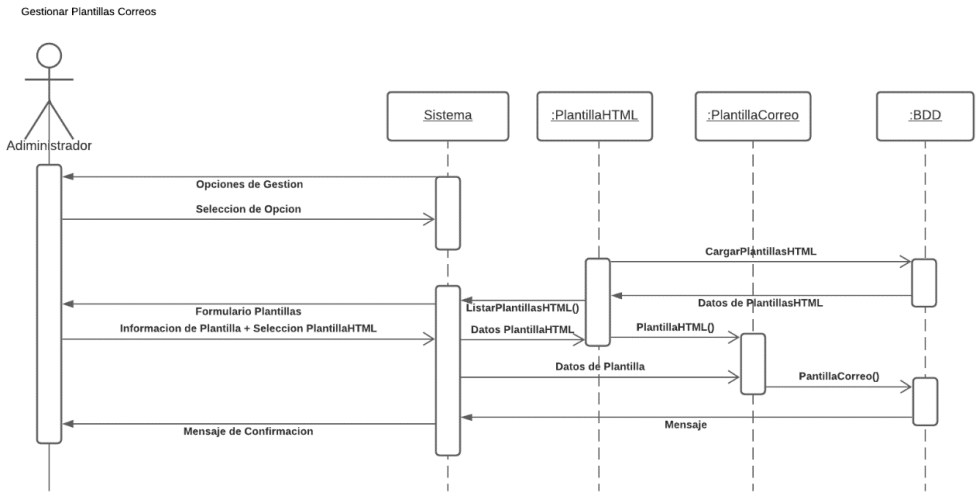
Nota. En la figura se visualiza un diagrama de secuencia de como el administrador podrá gestionar los departamentos, el sistema visualizará una serie de opciones entre ellas la crear departamento el administrador llenará un formulario donde el controlador departamento se encarga de validar datos para proceder enviarlos a una base de datos la misma que devolverá un mensaje de confirmación.

Figura 25.
Diagrama de secuencia - Gestionar empleados



Nota. En la figura se visualiza un diagrama de secuencia como el administrador podrá gestionar los datos empleados, el sistema visualizará una serie de opciones entre ellas crear empleado el administrador llenará un formulario donde el controlador empleado se encarga de validar datos para proceder enviarlos a una base de datos la misma que devolverá un mensaje de confirmación.

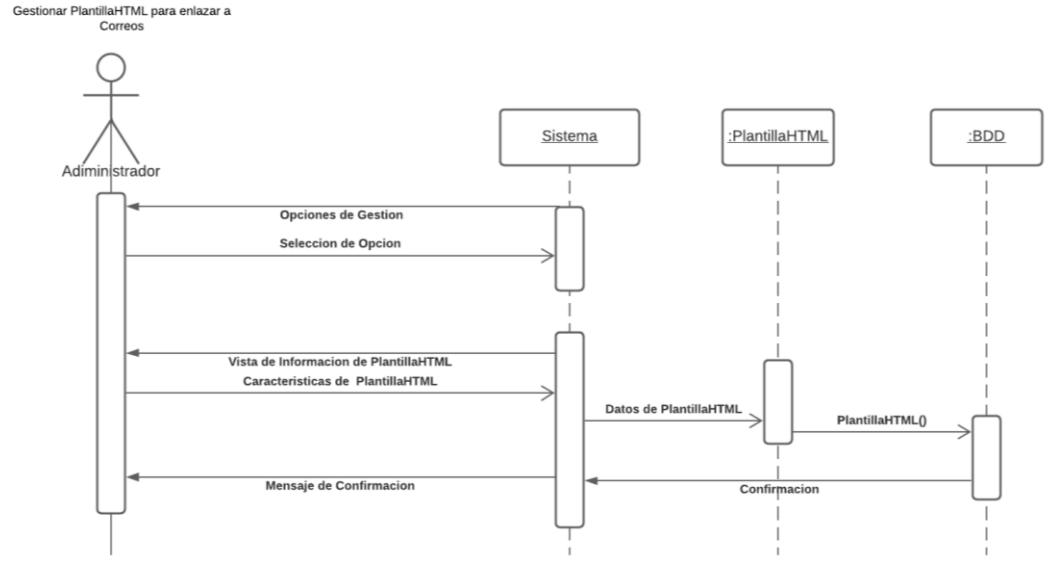
Figura 26.
Diagrama de secuencia - Gestionar plantillas de mensajes



Nota. En la figura se visualiza un diagrama de secuencia de como el administrador podrá gestionar las plantillas de mensajes, el sistema visualizará una serie de opciones entre ellas crear nueva plantilla de mensaje el administrador llenará un formulario donde el controlador plantilla correo es

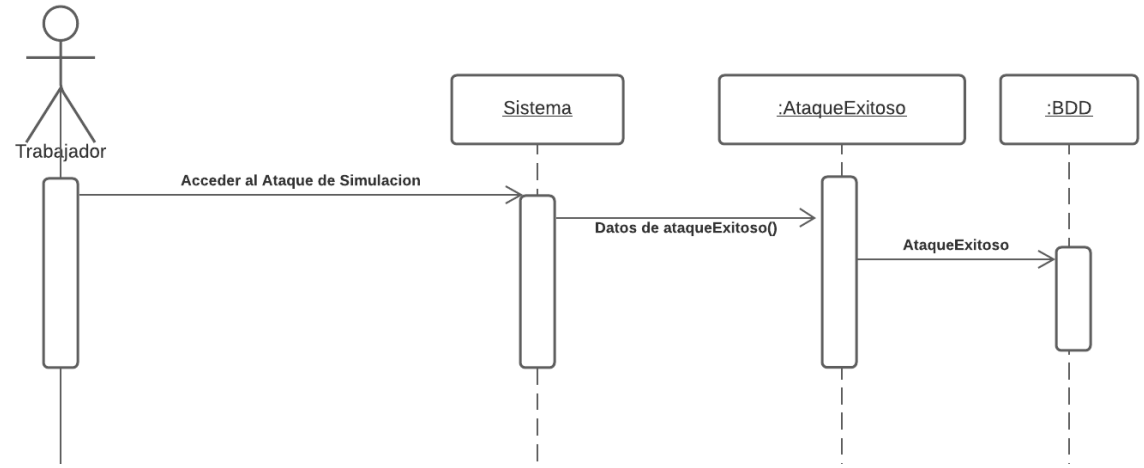
el encargado de obtener las plantilla HTML alojadas en la base de datos para anexarlo dentro de las plantillas correo donde el controlador plantilla correo se encarga de validar datos para proceder enviarlos a una base de datos la misma que devolverá un mensaje de confirmación.

Figura 27.
Diagrama de secuencia gestionar plantillas HTML



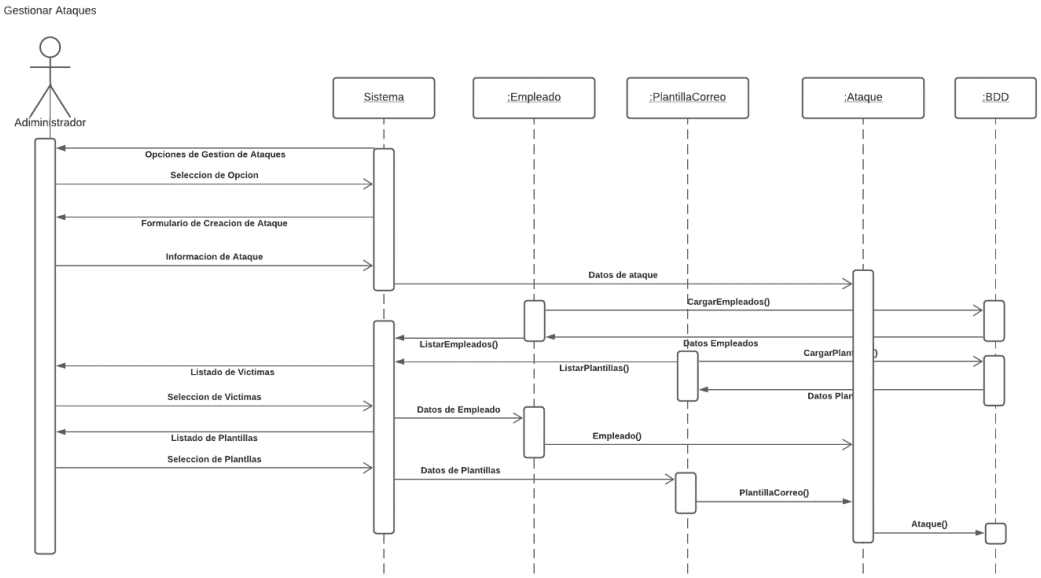
Nota. En la figura se visualiza un diagrama de secuencia de como el administrador podrá gestionar las plantillas HTML, el sistema visualizará una serie de opciones entre ellas subir plantilla de mensaje al subir una plantilla HTML se podrá ver una previsualización de la plantilla de mensaje para forma posterior el controlador plantilla HTML guarde la plantilla HTML en la base de datos.

Figura 28.
Diagrama de secuencia de guardar ataque exitoso



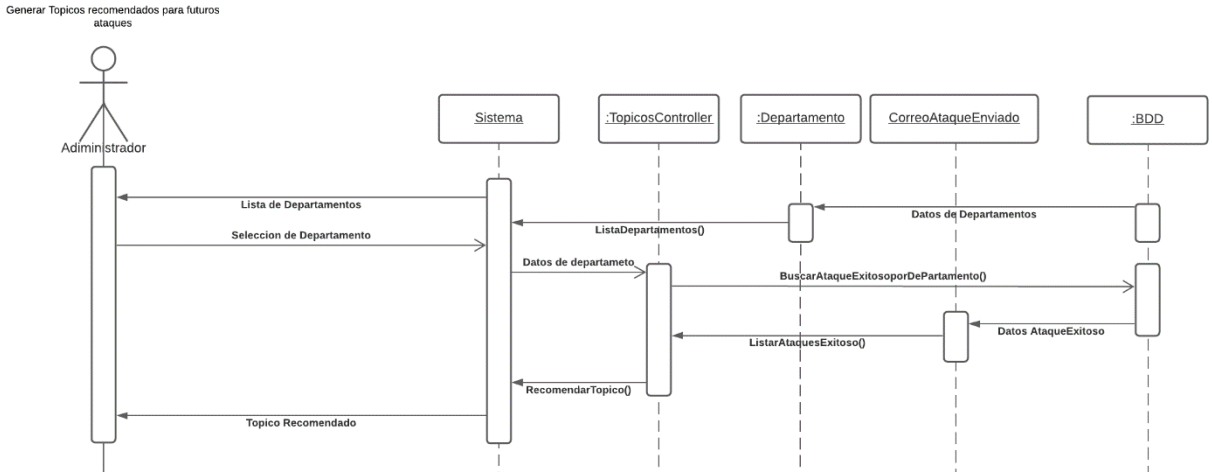
Nota. En la figura se visualiza un diagrama de secuencia de como el sistema guardara la información de los ataques exitoso de un trabajador, el trabajador accede a la simulación y le controlador captura la información del ataque y procede a guardarlos en la base de datos.

Figura 29.
Diagrama de secuencia de gestionar ataques



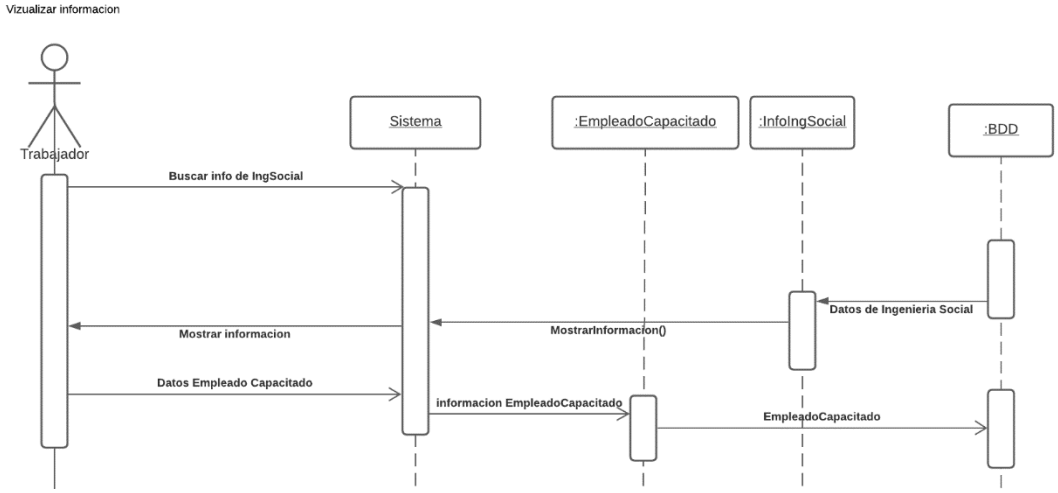
Nota. En la figura se visualiza un diagrama de secuencia de como el administrador podrá gestionar los ataques de simulación, el sistema mostrará una serie de opciones como: crear, modificar o eliminar ataques en donde dependiendo la opción elegida se deberá llenar diferentes datos.

Figura 30.
Diagrama de secuencia de generar recomendación de asuntos de mensajes



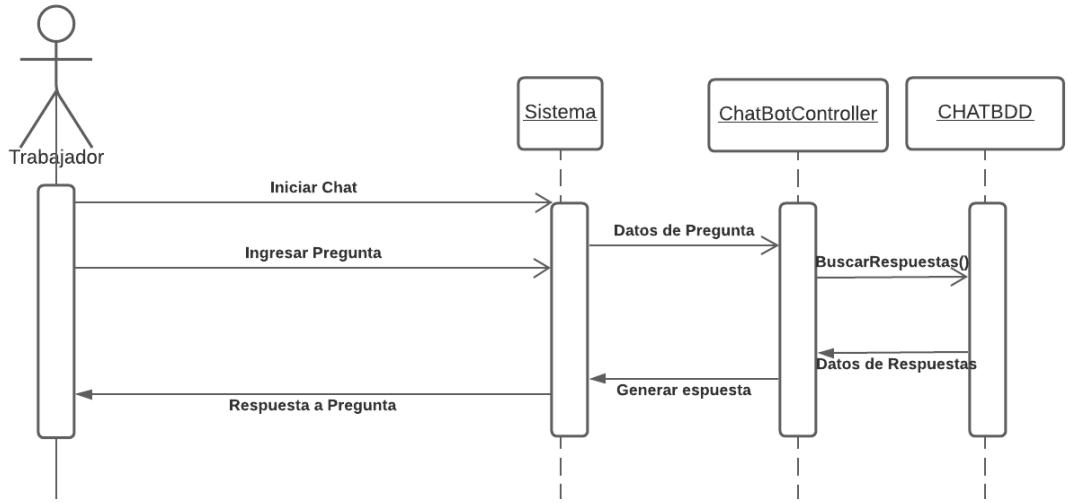
Nota. En la figura se muestra un diagrama de secuencia de como el administrador podrá solicitar al sistema recomendaciones de asuntos para usarlos en las plantillas de mensajes.

Figura 31.
Diagrama de secuencia de visualizar información de ingeniería social



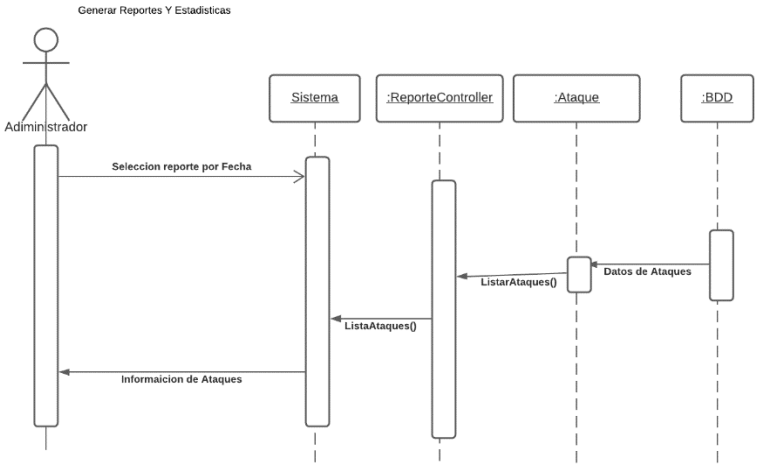
Nota. En la figura se muestra un diagrama de secuencia de como el trabajador podrá visualizar la información de ingeniería social elegida previamente por el administrador.

Figura 32.
Diagrama de Secuencia de Interacción con el ChatBot



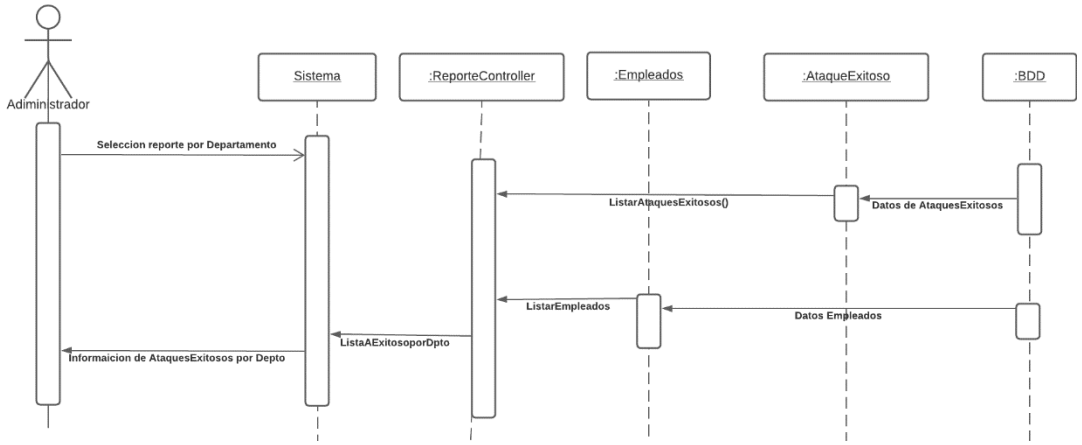
Nota. En la figura se muestra un diagrama de secuencia de como el trabajador podrá interactuar con el ChatBot que responderá preguntas acerca de la ingeniería social.

Figura 33.
Diagrama de Secuencia de Generar Reportes por Ataque



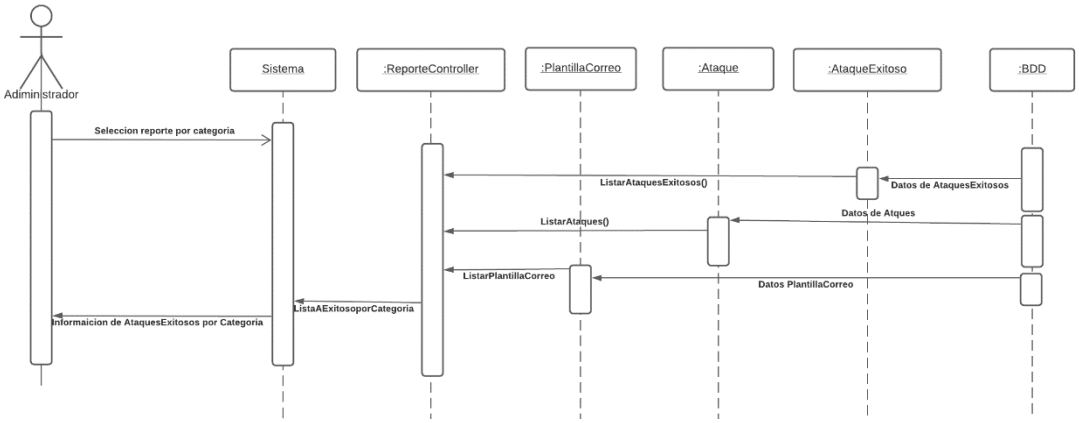
Nota. En la figura se visualiza un diagrama de secuencia de como el administrador podrá visualizar los reportes de los ataques exitosos clasificados por fecha de envió de los ataques.

Figura 34.
Diagrama de Secuencia de Generar Reportes por Departamento



Nota. En la figura se visualiza un diagrama de secuencia de como el administrador podrá visualizar los reportes de los ataques exitosos clasificados por departamento de los empleados.

Figura 35.
Diagrama de Secuencia de Generar Reportes por Categoría



Nota. En la figura se muestra un diagrama de secuencia de como el administrador podrá visualizar los reportes de los ataques exitosos clasificados por categoría de la plantilla de mensaje de los ataques.

3.3. Esquema de base de datos NoSQL

Figura 36.
Esquema de base de datos NoSQL

Nota. Esquema de base de datos NoSQL: La representación de base de datos SafeSecure está basada en documentos, los datos son específicos y tienen esquemas flexibles, realizar base de datos no relacionales son ampliamente reconocidas por su facilidad de desarrollo, funcionalidad y el rendimiento a escala.

3.4. Implementación de la Plataforma “SafeSecure”

3.4.1. Consultas de información básica sobre ingeniería Social

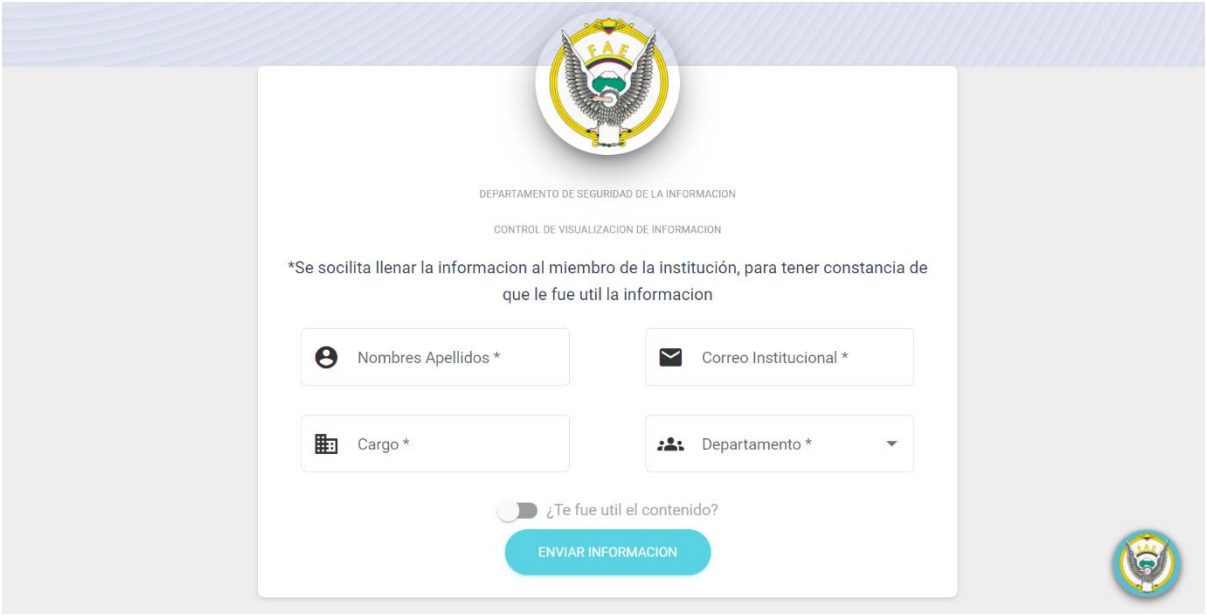
Figura 37.
Gestión de contenido a visualizar

Nota. En la figura se muestra la pantalla de control de información de campaña, en donde se puede observar como el administrador de la plataforma es capaz de elegir la información que van a visualizar los empleados en la ventana principal, dentro de la figura también se puede observar la barra de navegación o barra de menú del administrador con la cual puede acceder a las diferentes funcionalidades del sistema y está presente en todas las pantallas del administrador.

Figura 38.
Ventana Principal

Nota. En la figura se muestra la pantalla principal tanto para el administrador como para los trabajadores, en dicha pantalla se encuentra la información de campaña de concientización sobre ingeniería social que puede ser controlada por el administrador en la pantalla de control tal como se muestra en la **figura 37**. Además de la información de campaña es importante mencionar que esta sección se complementa con un chatBot el cual se puede observar en la parte inferior derecha con el logo de las Fuerza Aérea Ecuatoriana, dicho chatBot será explicado posteriormente.

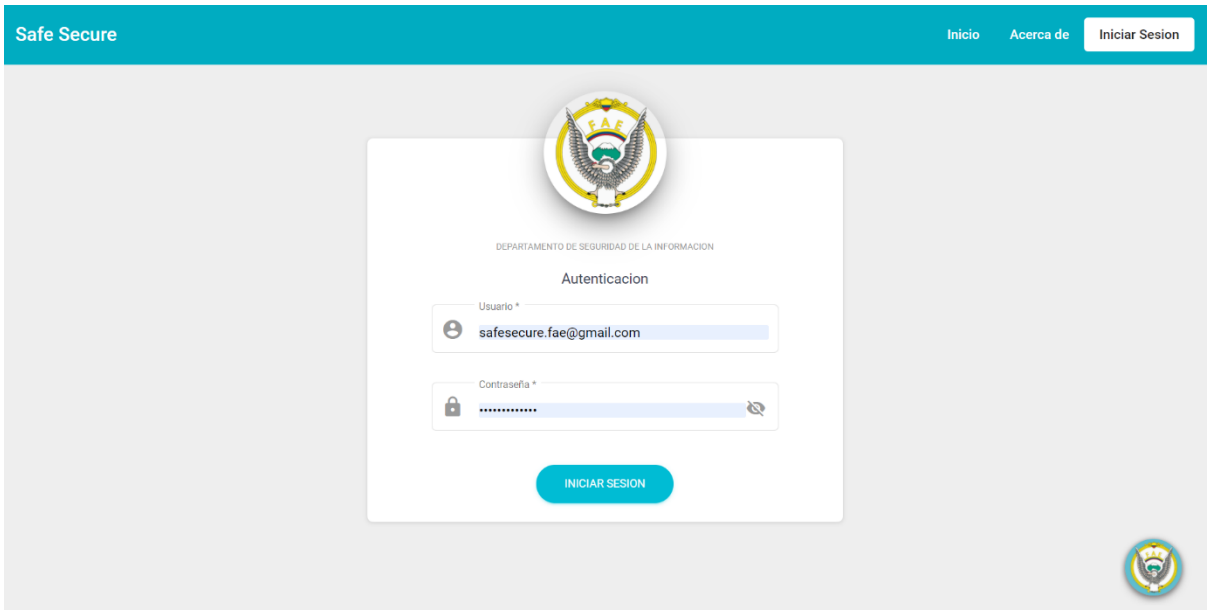
Figura 39.
Control de Visualización



Nota. En la figura se encuentra el formulario de empleados capacitados que es parte de la pantalla principal mostrada en la **figura 38.** Este formulario permite a los empleados guardar su información después de haber leído la información de ingeniería social, con el fin de que el administrador tenga un control de los empleados que están haciendo uso del sistema para capacitarse en temas de ingeniería social.

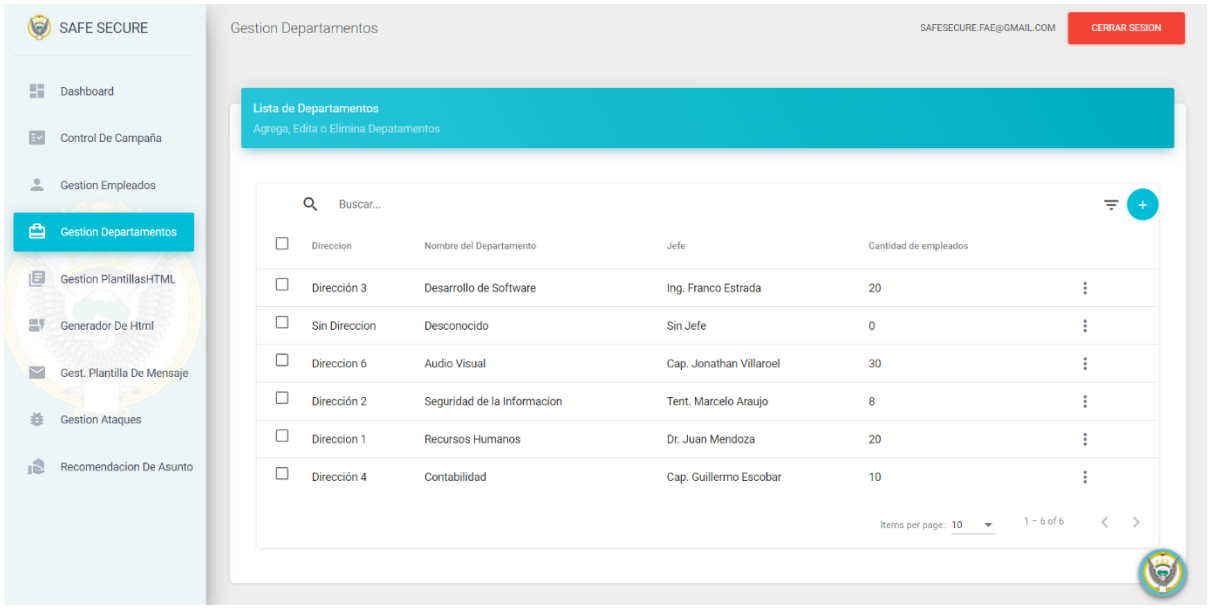
3.4.2. Envío de correos de Entrenamiento

Figura 40.
Autenticación de usuario



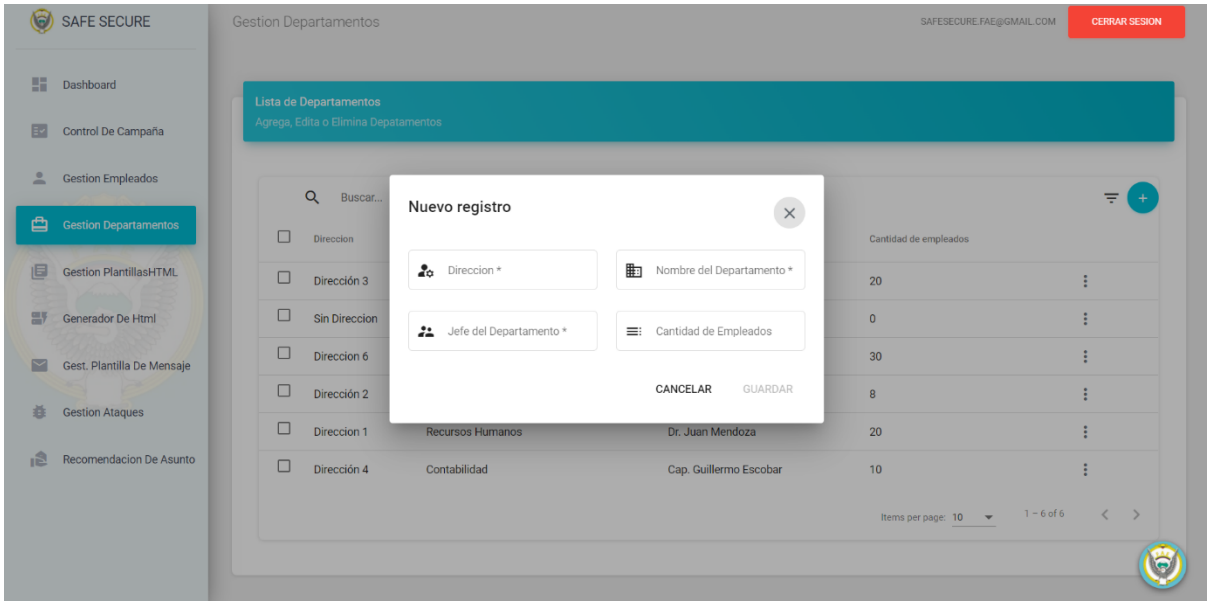
Nota. La figura se trata del ingreso de credenciales del administrador para tener acceso a sus funciones dentro del sistema.

Figura 41.
Gestionar departamentos



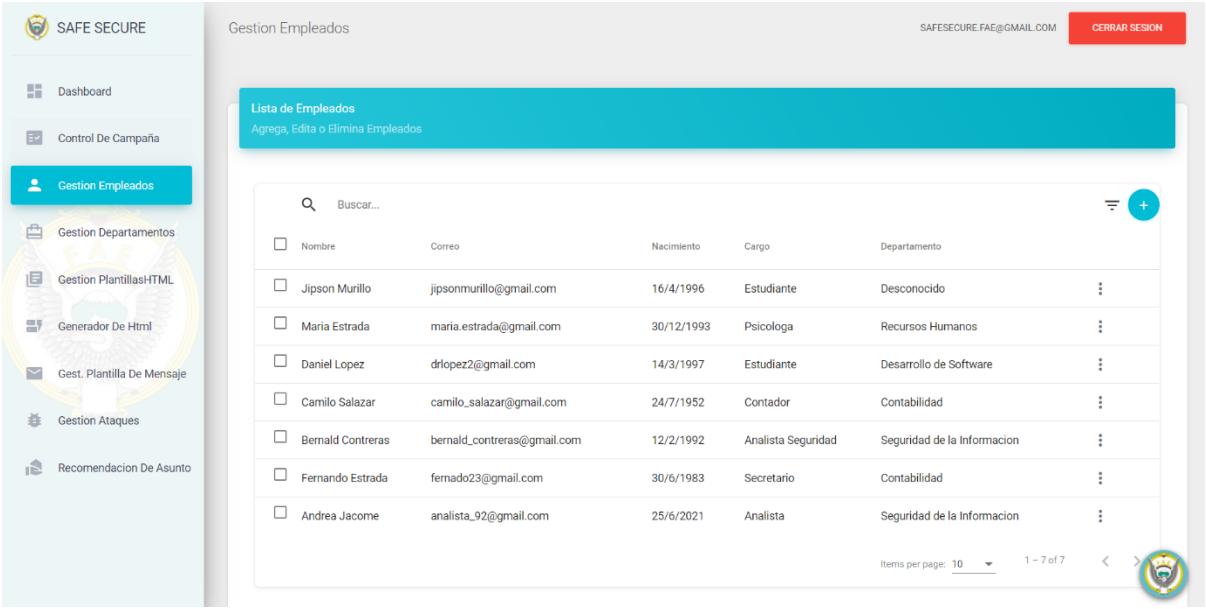
Nota. En la figura se muestra la pantalla de Gestión de departamentos donde el administrador puede alimentar al sistema con departamentos acorde como desee trabajar, además de visualizar la lista de departamentos existentes en el sistema.

Figura 42.
Registrar/Modificar departamento



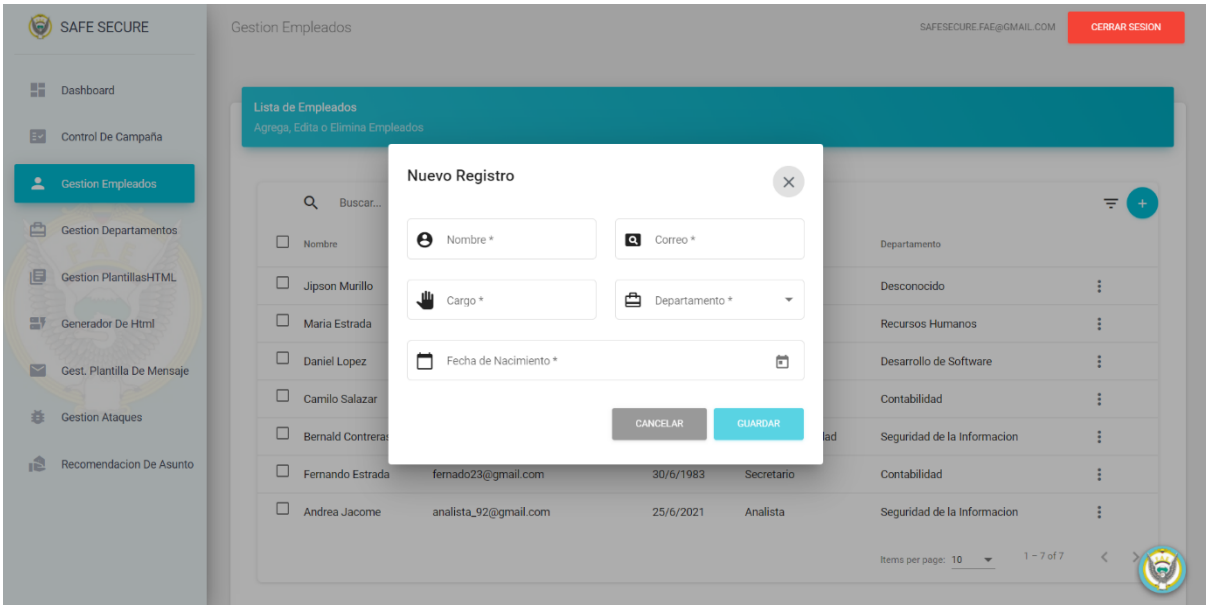
Nota. En la figura se puede observar el formulario de registro de los departamentos.

Figura 43.
Gestionar Empleados



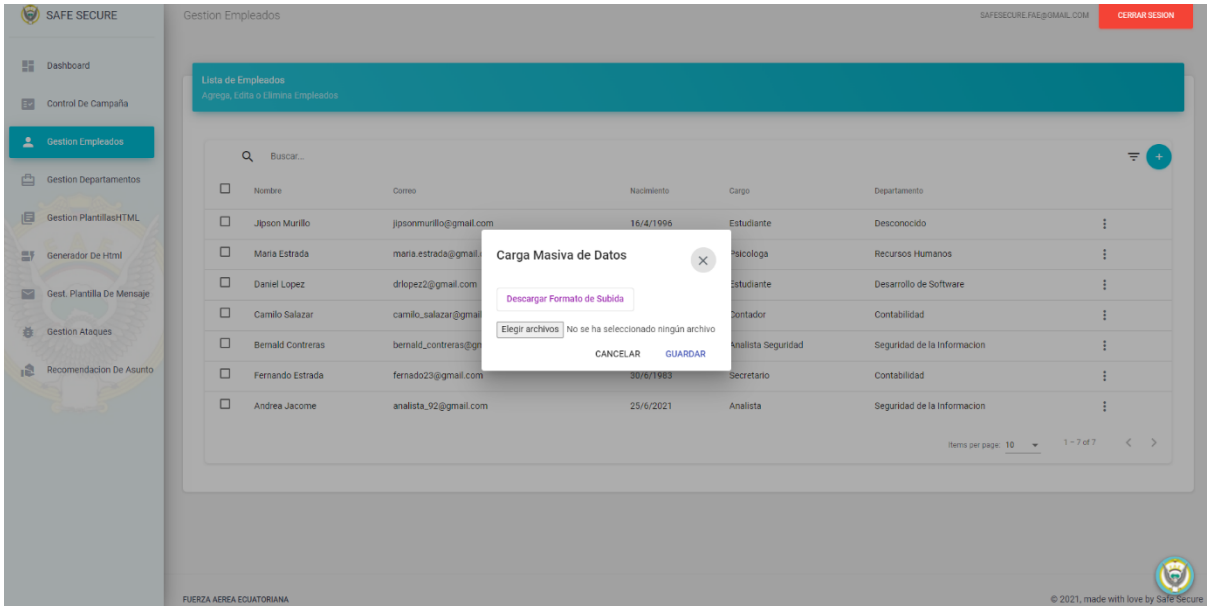
Nota. En La figura se muestra la pantalla de Gestión de empleados donde el administrador puede alimentar al sistema con los empleados a quienes va a seleccionar como objetivo de algún ataque de simulación, además de visualizar la lista de empleados previamente cargados en el sistema.

Figura 44.
Registrar/Modificar Empleado



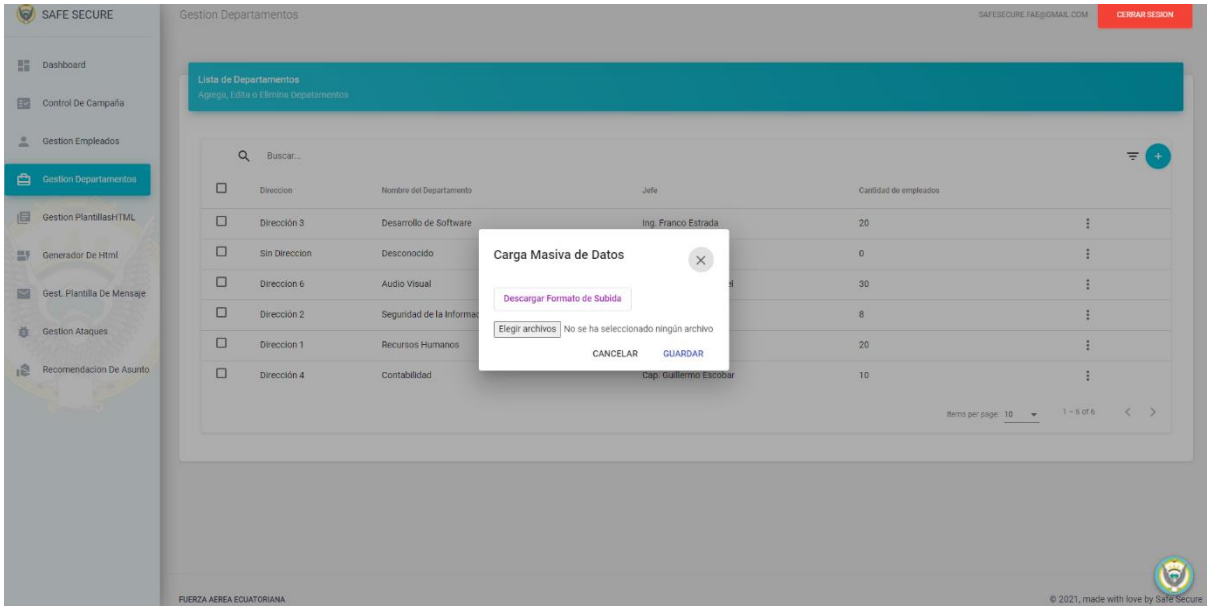
Nota. La figura contiene el formulario de registro de empleados en donde se debe asignar a cada uno un departamento cagado en la f**igura 41**.

Figura 45.
Registro masivo de Empleados



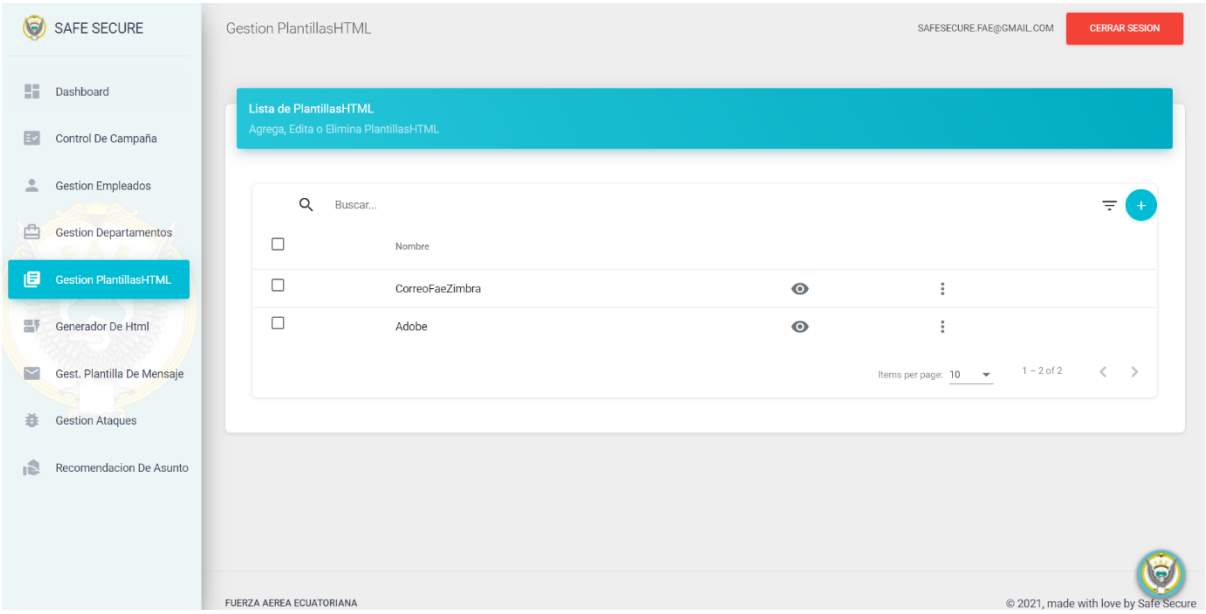
Nota. La figura es un complemento de la **figura 43** esta pantalla se visualiza otra opción de cargar información de empleados, la carga masiva de empleados para utilizar esta funcionalidad el sistema proporciona un documento tipo xls con un formato para que el usuario llene la información correspondiente del empleado y proceder a subir los datos de los empleados al sistema.

Figura 46.
Registro masivo departamentos



Nota. La figura es un complemento de la **figura 41** esta pantalla se visualiza otra opción de cargar información de departamento, la carga masiva de departamento para utilizar esta funcionalidad el sistema proporciona un documento tipo xls con un formato para que el usuario llene la información correspondiente de departamentos y proceder a subir los datos de los departamentos al sistema.

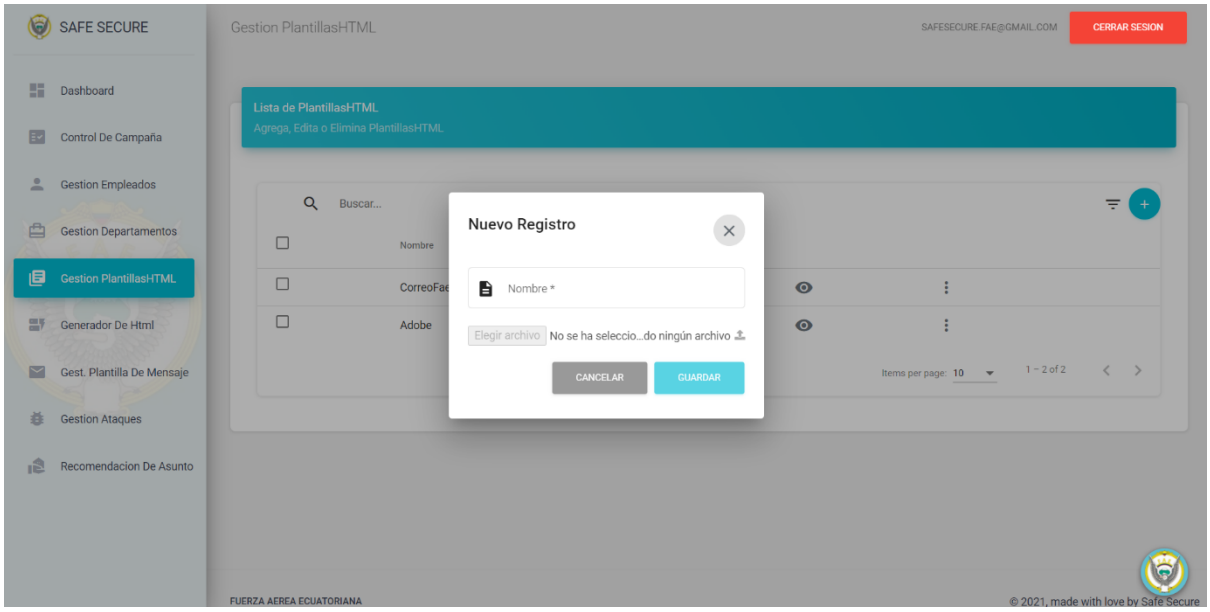
Figura 47.
Gestionar Plantilla HTML



Nota. En la figura se muestra la pantalla de Gestión de Plantilla HTML donde el administrador puede alimentar al sistema con información como las plantillas HTML las cuales pueden ser seleccionadas dentro de la **figura 52**, además de visualizar la lista de plantillas HTML previamente cargadas en el sistema.

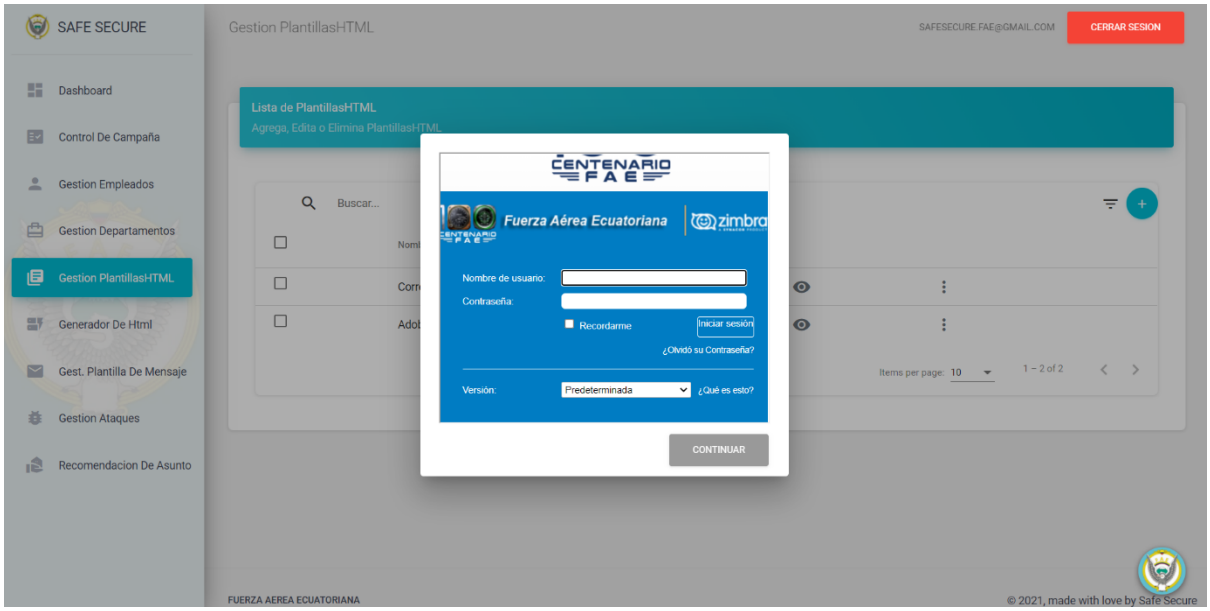
Figura 48.

Guardar/Modificar Plantilla HTML



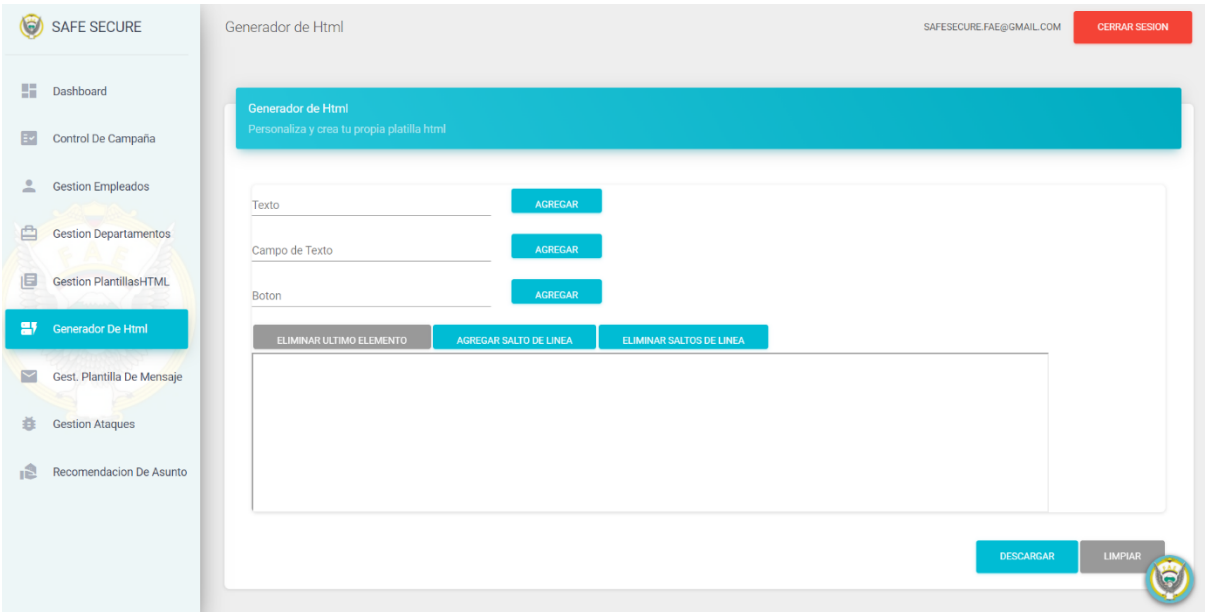
Nota. En la figura se muestra un formulario de nuevo registro donde el administrador puede asignar un nombre a la plantilla HTML y subir un archivo con formato .html al sistema

Figura 49.
Previsualización de Plantilla HTML



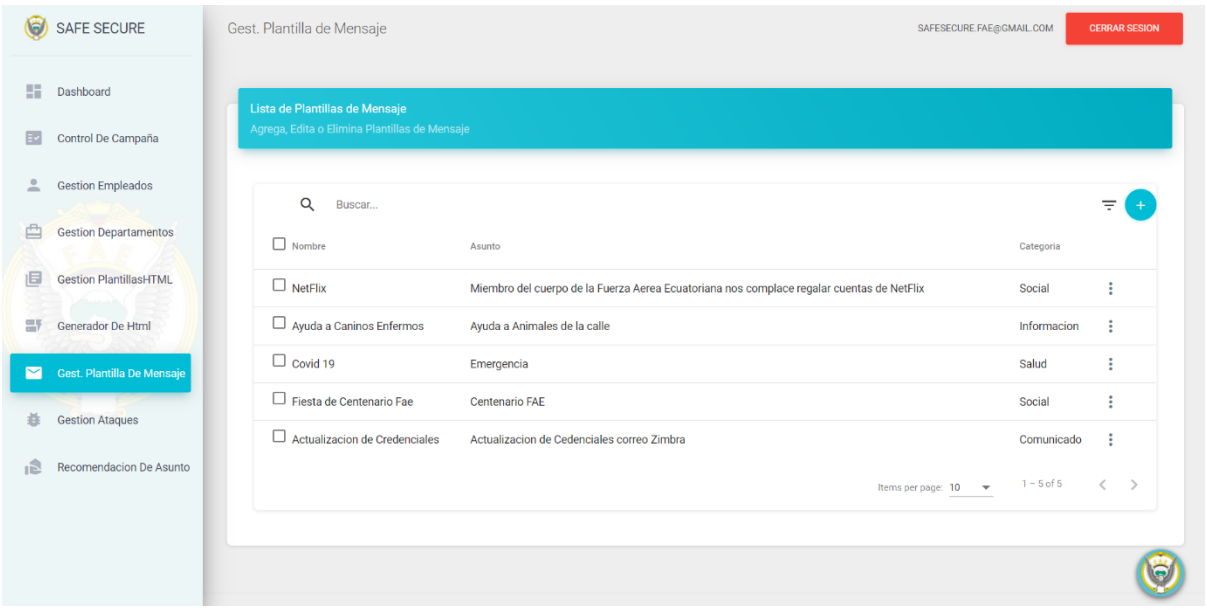
Nota. En la figura se muestra la pantalla previsualización de plantilla HTML esta opción está disponible en la **figura 47** cuando el administrador presiona el icono de ojo, se muestra la previsualización.

Figura 50.
Generador HTML



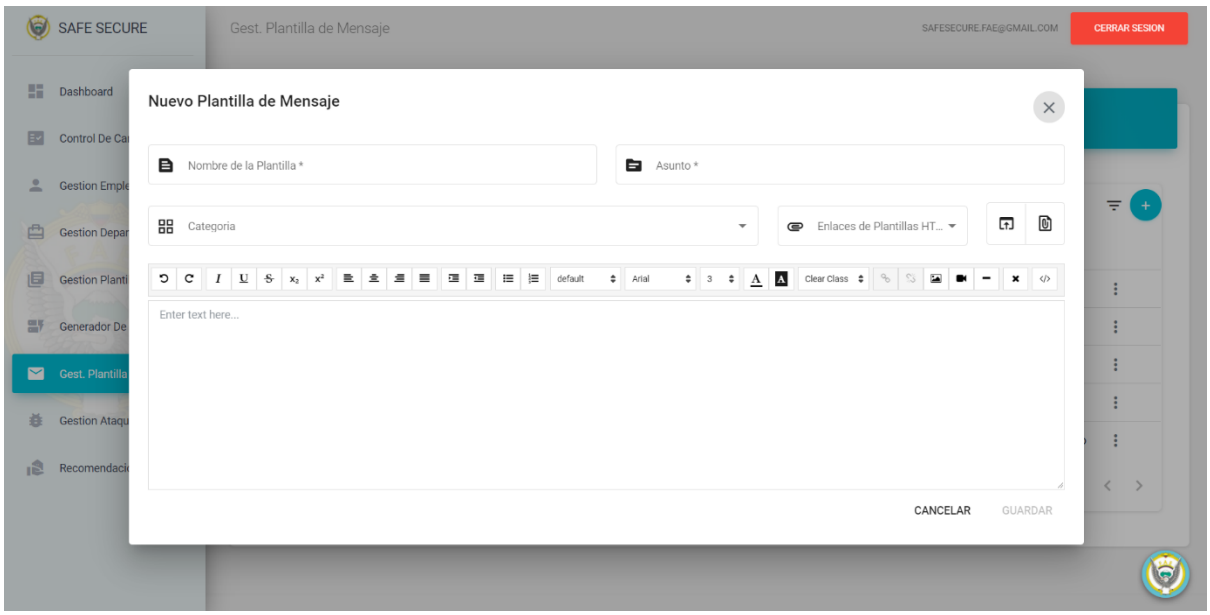
Nota. En la figura se muestra la pantalla generadora de HTML el administrador puede realizar acciones como agregar campos de texto, texto y botones. Las acciones se verán reflejadas en un iframe además cuenta con tres acciones adicionales como eliminar último elemento, agregar santo de línea y eliminar santos de línea el administrador termine de editar puede descargar en formato en un archivo .html

Figura 51.
Gestionar plantillas de mensaje



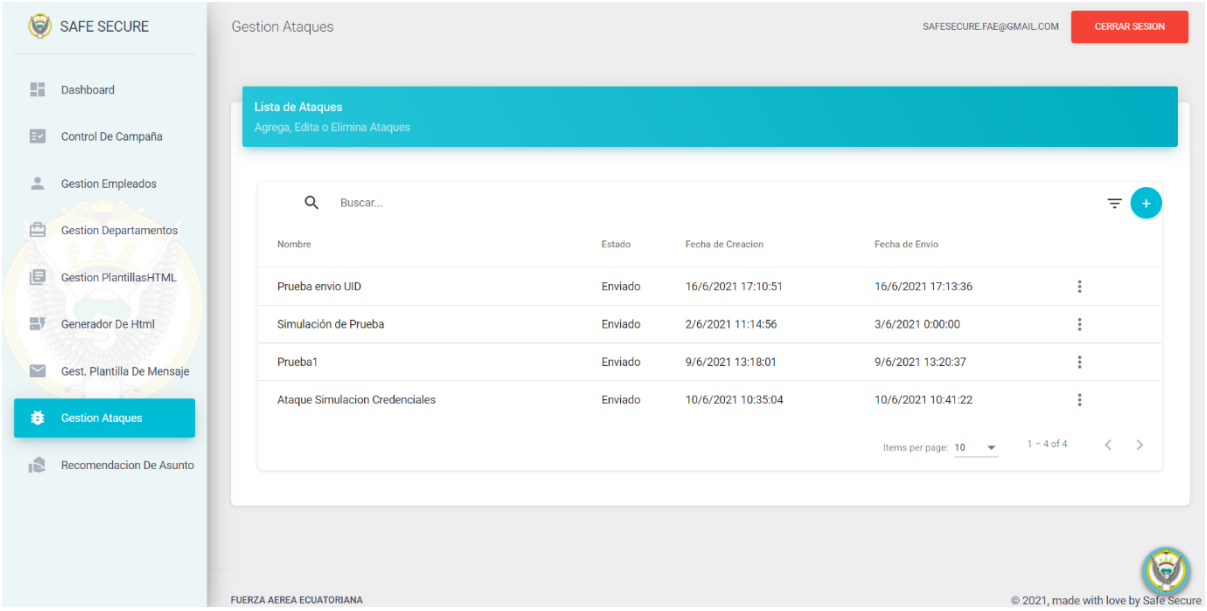
Nota. En la figura se muestra la pantalla de gestión de plantilla de mensaje donde el administrador puede alimentar al sistema con información como la plantilla de mensaje las cuales pueden ser seleccionadas dentro de la **figura 55**, además de visualizar una lista de plantilla mensaje previamente cargadas en el sistema.

Figura 52.
Crear/Modificar plantilla mensaje



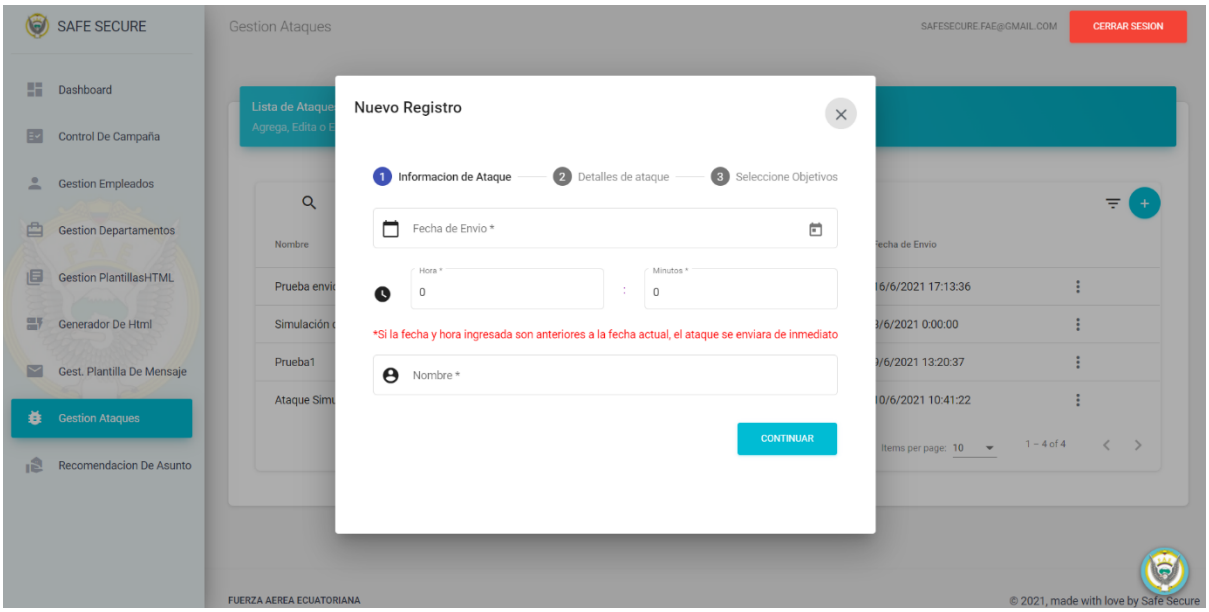
Nota. En la figura se muestra la pantalla crear/modificar plantilla mensaje este formulario el administrador puede crear plantilla de mensaje que serán utilizadas cuando se realice un ataque en la **figura 55**, se puede asignar un nombre, asunto, categoría, contenido y el enlace de la plantilla HTML que se requiere para realizar el ataque.

Figura 53.
Gestionar Ataques



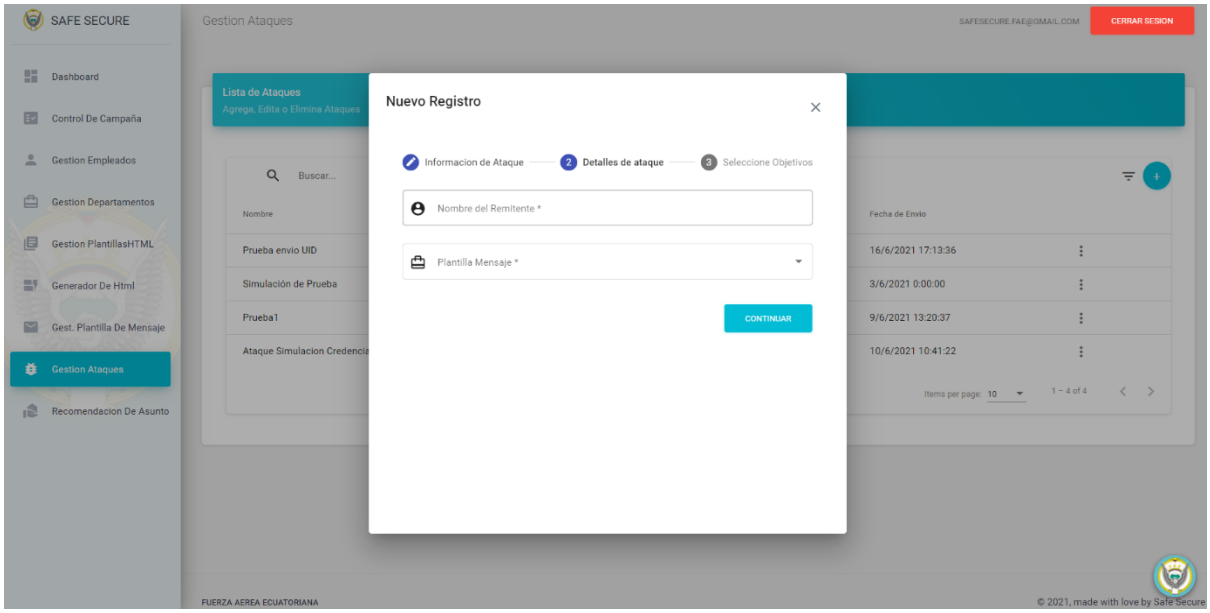
Nota. En la figura se muestra la pantalla de gestión de ataques donde el administrador puede alimentar al sistema con información como ataque, además de visualizar una lista de ataques previamente realizadas en el sistema.

Figura 54.
Crear/Modificar ataque – Información de ataque



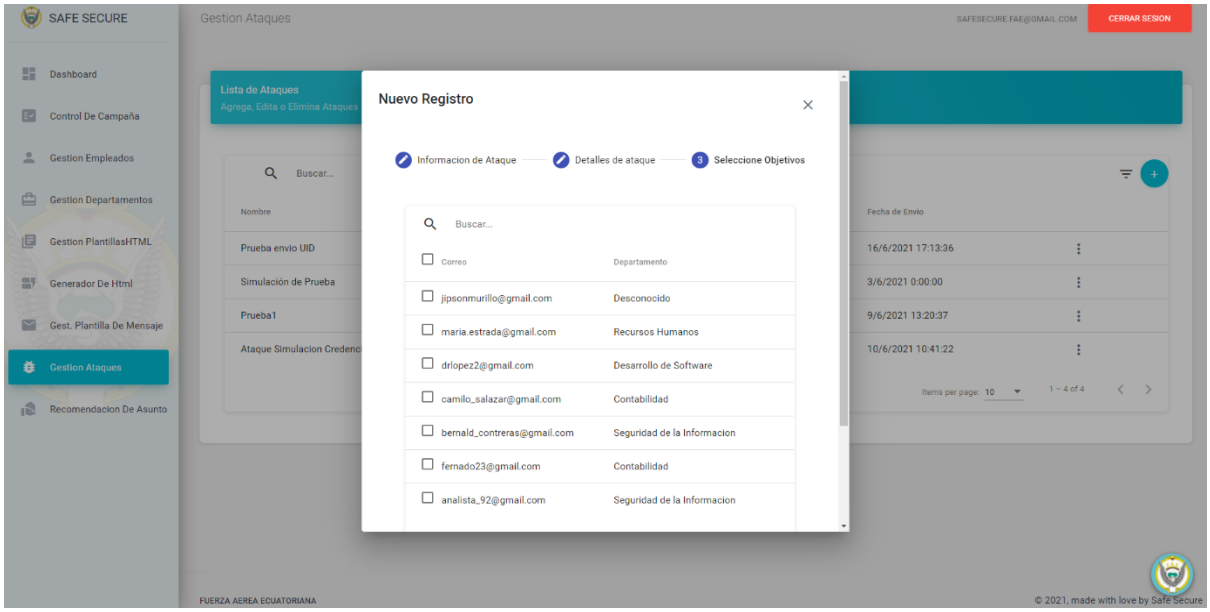
Nota. En la figura se muestra la pantalla de crear o modificar ataque sección, información de ataque es un formulario donde el administrador puede agendar la fecha de ataque, hora de ataque y un nombre al ataque.

Figura 55.
Crear/Modificar ataque – Detalle de ataque



Nota. En la figura se muestra la pantalla de crear o modificar ataque sección, detalle de ataque que es el siguiente paso de la **figura 54.** Es un formulario donde el administrador puede agregar un nombre de remitente, una plantilla de mensaje de la lista de plantilla mensaje de la **figura 51.**

Figura 56.
Crear/Modificar ataque – Selección de objetivos



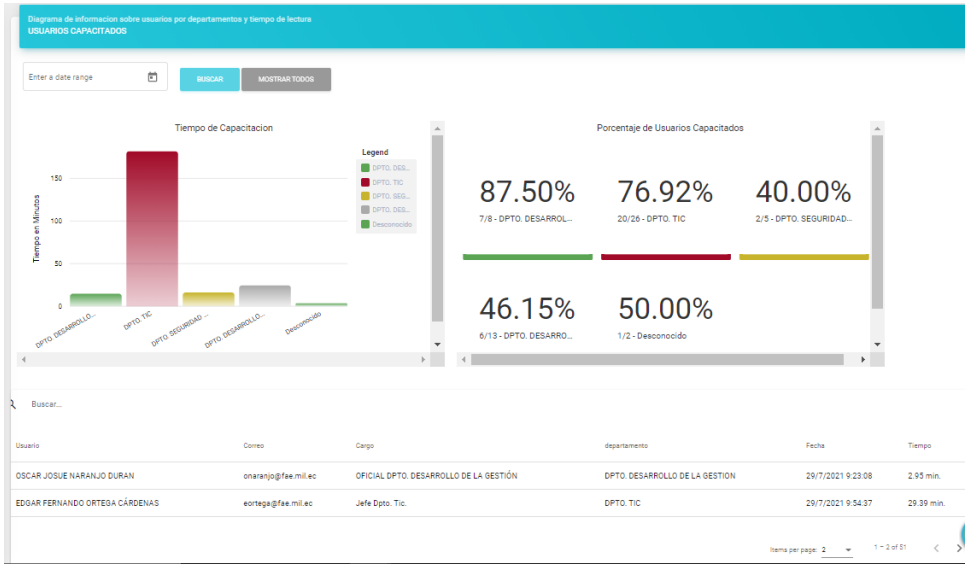
Nota. En la figura se muestra la pantalla de crear o modificar ataque sección, selección de objetivos que es el siguiente paso de la **figura 55.** Es una tabla donde el administrador puede seleccionar a los objetivos, los objetivos son los empleados creados en la **figura 43** luego de seleccionar los objetivos el sistema agenda el ataque correspondiente con la información añadida en la **figura (54, 55)**.

3.4.3. Seguimiento de entrenamiento

Figura 57.
Ataques exitosos por categoría de mensaje y departamento

Nota. La figura muestra un conjunto de gráficos porcentuales y un gráfico de barras con la información de los ataques exitosos centrándose en la categoría de los mensajes y el departamento al que pertenecen los afectados.

Figura 58.
Empleados capacitados, clasificados por departamentos y tiempo



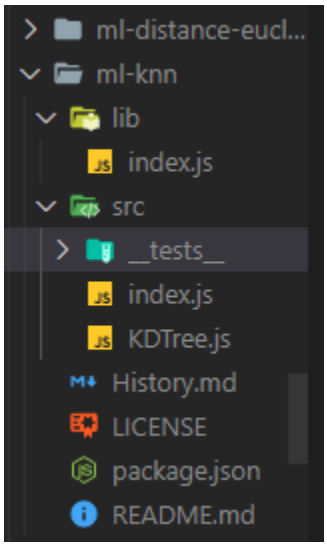
Nota. La figura muestra un conjunto de gráficos porcentuales y un gráfico de barras con la información de los empleados capacitados centrándose en el departamento al que pertenecen y la cantidad de tiempo invertida en la pantalla de visualización de información de capacitación.

Figura 59.
Visualización de ataques seccionados por ataques enviados y pendientes

Nota. La figura muestra tres gráficos de barras con la cantidad por fecha de los ataques totales, enviados y pendientes

3.4.4. Inteligencia Artificial

Figura 60.
Modulo Knn de la librería ML



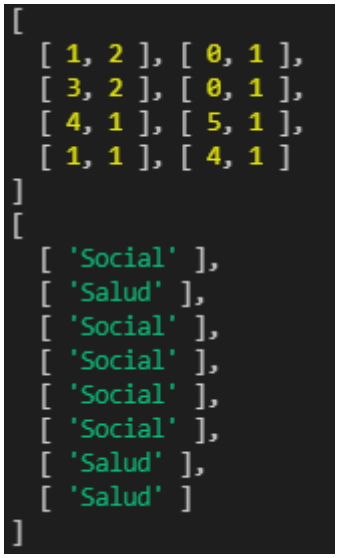
Nota. En la figura se puede observar el módulo de ML-Knn del paquete ML.js que permite realizar machine learning en node y dicho modulo como su nombre indica es el encargado del algoritmo K-Neigth Neigthbour.

Figura 61.
DataSet de Entrenamiento obtenido de la base de datos de ataque exitoso

```
[
  {
    tema: 'Miembro del cuerpo de la Fuerza Aerea Ecuatoriana nos complace regalar cuentas de NetFlix',
    departamento: 'Desconocido',
    categoria: 'Social',
    cantidad: 2
  },
  {
    tema: 'Emergencia ',
    departamento: 'Desarrollo de Software',
    categoria: 'Salud',
    cantidad: 1
  },
  {
    tema: 'Miembro del cuerpo de la Fuerza Aerea Ecuatoriana nos complace regalar cuentas de NetFlix',
    departamento: 'Seguridad de la Informacion',
    categoria: 'Social',
    cantidad: 2
  },
  {
    tema: 'Miembro del cuerpo de la Fuerza Aerea Ecuatoriana nos complace regalar cuentas de NetFlix',
    departamento: 'Desarrollo de Software',
    categoria: 'Social',
    cantidad: 1
  },
  {
    tema: 'Miembro del cuerpo de la Fuerza Aerea Ecuatoriana nos complace regalar cuentas de NetFlix',
    departamento: 'Recursos Humanos',
    categoria: 'Social',
    cantidad: 1
  },
  {
    tema: 'Miembro del cuerpo de la Fuerza Aerea Ecuatoriana nos complace regalar cuentas de NetFlix',
    departamento: 'Contabilidad',
    categoria: 'Social',
    cantidad: 1
  },
  {
    tema: 'Emergencia ',
    departamento: 'Desconocido',
    categoria: 'Salud',
    cantidad: 1
  },
  {
    tema: 'Emergencia ',
    departamento: 'Recursos Humanos',
    categoria: 'Salud',
    cantidad: 1
  }
]
```

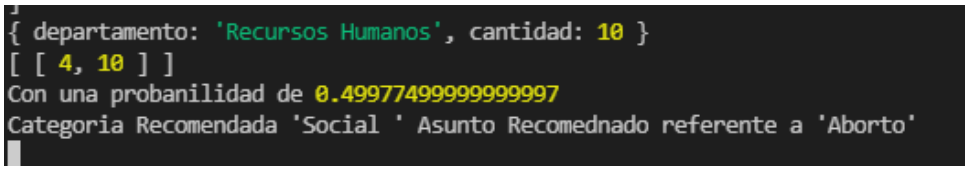

Nota. En la figura se encuentra un dataset de entrenamiento obtenido de los ataques exitosos previos.

Figura 62.
Data set representado en valores números



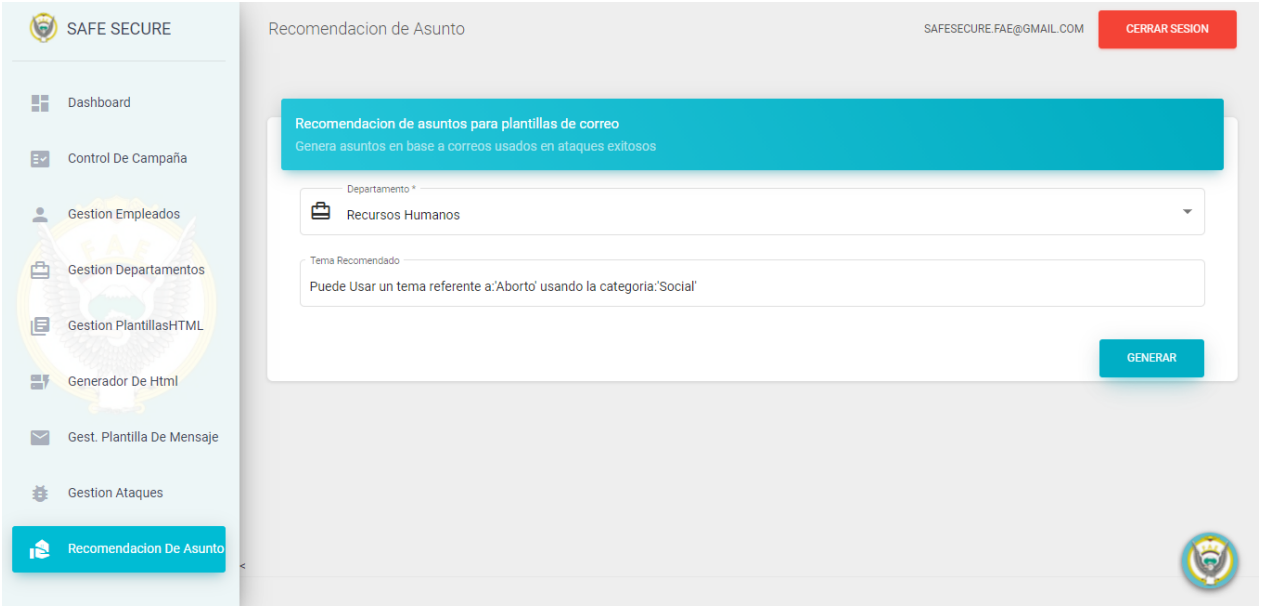
Nota. En la figura se encuentra la representación del dataset de entrenamiento de manera numera, en donde el primer número es el valor de los departamentos que toma su valor numérico de su posición en la base de datos y el segundo valor es la cantidad de ataques exitosos dirigidos a cada departamento.

Figura 63.
Recomendación en tiempo real



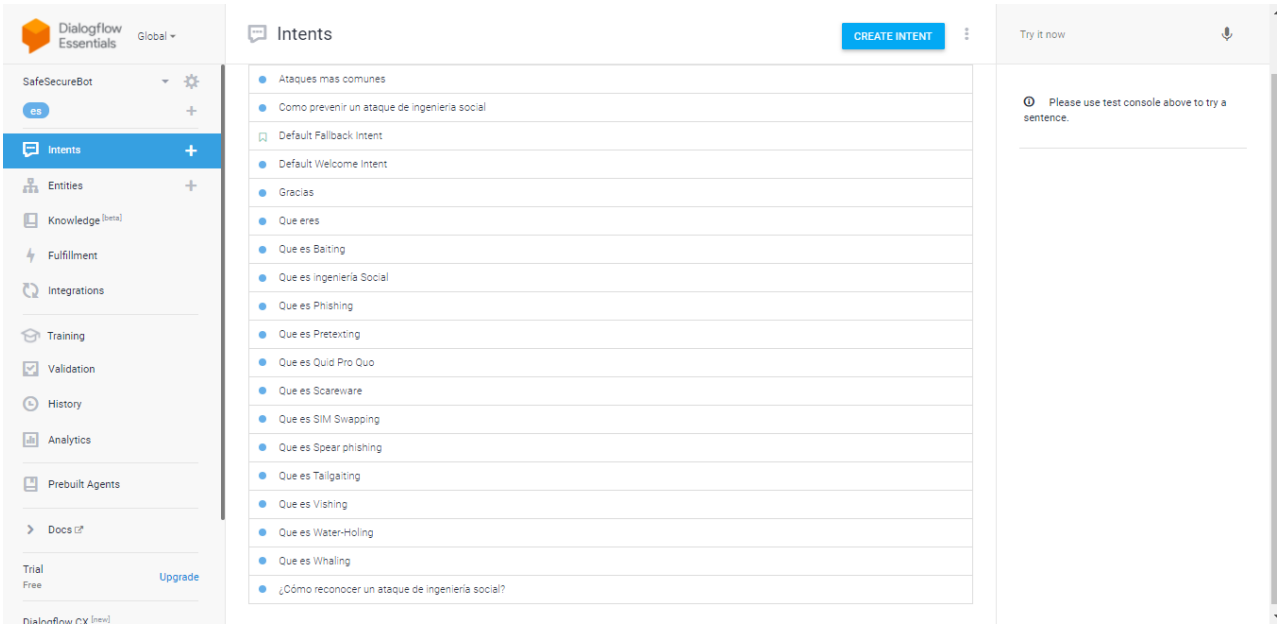
Nota. En la figura se puede observar **l**a recomendación de un asunto en tiempo real para la plantilla de correo de un ataque dirigido al departamento de “Recursos Humanos”

Figura 64.
Recomendación de Asunto para plantilla de correo



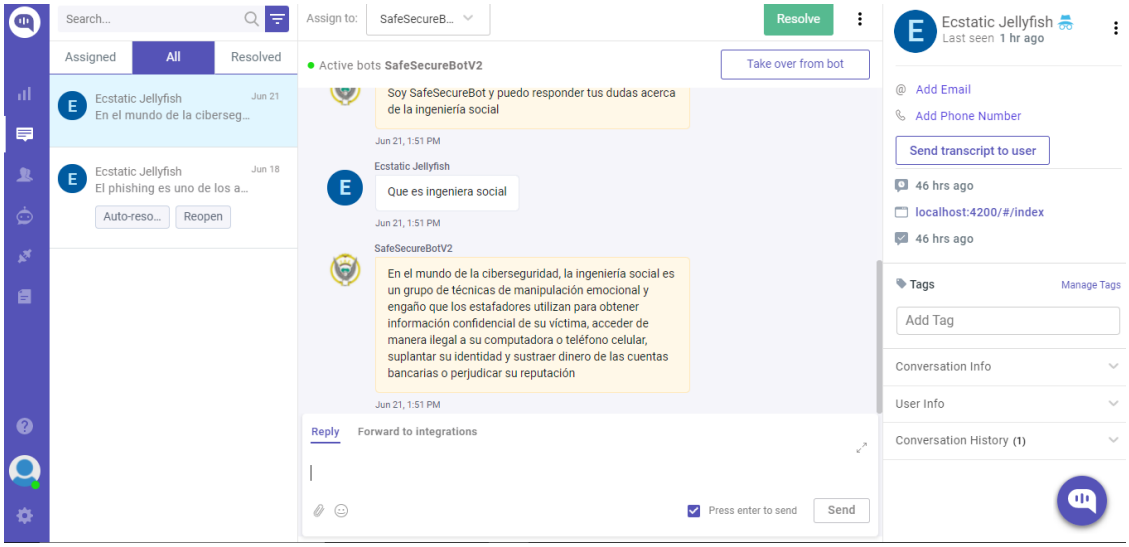
Nota. La figura muestra la integración del algoritmo de recomendación dentro del sistema.

Figura 65.
Infraestructura del Chatbot



Nota. En La figura se puede observar la creación de los diferentes intents del ChatBot que responde preguntas concretas acerca de la ingeniería social, dentro de la plataforma de DialogFlow.

Figura 66.
Kommunicate.io Administrador de Conversaciones del ChatBot



Nota. La figura muestra la plataforma Kommunicate.io en donde se vinculó el ChatBot creado en DialogFlow para poder contar con un panel de administración y realizar la integración con la plataforma SafeSecure.

Figura 67.
Chat Bot integrado

Nota. En la parte inferior derecha de la figura se muestra el ChatBot ya implementado en el sistema con el cual el personal de la Fuerza Aérea podrá realizar preguntas concretas acerca de la ingeniería social.

CAPÍTULO IV

Validación del Sistema

4.1. Pruebas

4.1.1. Pruebas Unitarias.

Tabla 20.
Verificar el funcionamiento del control del contenido de visualización

Prueba No.	**1**
Descripción	Verificar el funcionamiento del control del contenido de visualización
Objetivos	Verificar si la información mostrada en la pantalla principal es la misma que la seleccionada por el administrador en la pantalla de control.
Condiciones	Seleccionar la información a mostrar en la pantalla de control
Resultados Esperados	La información mostrada en la pantalla principal concuerda con la seleccionada en la pantalla de control
Resultados Obtenidos	La prueba fue aprobatoria la información mostrada en la pantalla principal si concuerda con la seleccionada en la pantalla de control

Tabla 21.
Verificar la información de departamentos

Prueba No.	**2**
Descripción	Verificar la información de departamentos
Objetivos	Verificar si la visualización de información de departamentos es la misma que se agregó en la base de datos.
Condiciones	Seleccionar un departamento y verificar la información.
Resultados Esperados	La información de un departamento concuerda con la información guardada en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria la información de un departamento concuerda con la información guarda en la base de datos.

Tabla 22.
Verificar el funcionamiento de crear nuevo departamento

Prueba No.	**3**

Descripción	Verificar el funcionamiento de crear nuevo departamento
Objetivos	Verificar que la información creada de departamento no contenga campos vacíos.
Condiciones	Crear departamento con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá crear departamentos con campos incompletos del formulario. El sistema permitirá crear departamentos con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite crear departamentos con campos incompletos del formulario además el sistema permite crear departamentos con los campos completos del formulario

Tabla 23.
Verificar el funcionamiento de modificar departamento

Prueba No.	4
Descripción	Verificar el funcionamiento de modificar departamento
Objetivos	Verificar que la información modificada de departamento no contenga campos vacíos.
Condiciones	Modificar departamento con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá modificar departamentos con campos incompletos del formulario. El sistema permitirá modificar departamentos con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite modificar departamentos con campos incompletos del formulario además el sistema permite modificar departamentos con los campos completos del formulario

Tabla 24.
Verificar el funcionamiento de eliminar departamento

Prueba No.	5
Descripción	Verificar el funcionamiento de eliminar departamento
Objetivos	Verificar que el departamento eliminado se elimine de la base de datos.

Condiciones	Eliminar departamento simple o selección múltiple de departamentos.
Resultados Esperados	El sistema permitirá eliminar departamentos de forma simple. El sistema permitirá eliminar departamentos de forma múltiple. Las acciones deberán ser reflejadas en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria el sistema permite eliminar departamentos de forma simple, múltiple las acciones si se vieron reflejada en la base de datos.

Tabla 25.
Verificar la información de empleados

Prueba No.	6
Descripción	Verificar la información de empleados
Objetivos	Verificar si la visualización de información de empleados es la misma que se agregó en la base de datos.
Condiciones	Seleccionar un empleado y verificar la información.
Resultados Esperados	La información de empleados concuerda con la información guardada en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria la información de empleados concuerda con la información guarda en la base de datos.

Tabla 26.
Verificar el funcionamiento de crear nuevo empleado

Prueba No.	**7**
Descripción	Verificar el funcionamiento de crear nuevo empleado
Objetivos	Verificar que la información creada de empleado no contenga campos vacíos.
Condiciones	Crear empleado con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá crear empleados con campos incompletos del formulario. El sistema permitirá crear empleados con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite crear empleados con campos incompletos del formulario además el sistema permite crear empleados con los campos completos del formulario

Tabla 27.
Verificar el funcionamiento de modificar empleado

Prueba No.	**8**
Descripción	Verificar el funcionamiento de modificar empleado
Objetivos	Verificar que la información modificada de empleado no contenga campos vacíos.
Condiciones	Modificar empleado con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá modificar empleados con campos incompletos del formulario. El sistema permitirá modificar empleados con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite modificar empleados con campos incompletos del formulario además el sistema permite modificar empleados con los campos completos del formulario

Tabla 28.
Verificar el funcionamiento de eliminar empleados

Prueba No.	**9**
Descripción	Verificar el funcionamiento de eliminar empleados
Objetivos	Verificar que el empleado eliminado se elimine de la base de datos.
Condiciones	Eliminar empleado simple o selección múltiple de empleados.
Resultados Esperados	El sistema permitirá eliminar empleados de forma simple. El sistema permitirá eliminar empleados de forma múltiple. El sistema no permitirá eliminar empleados si tienen ataques agendados. Las acciones deberán ser reflejadas en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria el sistema permite eliminar empleados de forma simple, múltiple y no permite eliminar empleados con ataques agendados las acciones si se vieron reflejada en la base de datos.

Tabla 29.
Verificar la información de plantillas HTML

Prueba No.	**10**
Descripción	Verificar la información de plantillas HTML
Objetivos	Verificar si la visualización de información de plantillas HTML es la misma que se agregó en la base de datos.
Condiciones	Seleccionar una plantilla HTML y verificar la información.
Resultados Esperados	La información de plantillas HTML concuerda con la información guardada en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria la información de plantillas HTML concuerda con la información guarda en la base de datos.

Tabla 30.
Verificar el funcionamiento de cargar nueva plantilla HTML

Prueba No.	**11**
Descripción	Verificar el funcionamiento de cargar nueva plantilla HTML
Objetivos	Verificar que la información creada de plantilla HTML no contenga campos vacíos.
Condiciones	Cargar plantilla HTML con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá cargar plantillas HTML con campos incompletos del formulario. El sistema permitirá cargar plantillas HTML con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite cargar plantillas HTML con campos incompletos del formulario además el sistema permite cargar plantillas HTML con los campos completos del formulario

Tabla 31.
Verificar el funcionamiento de modificar plantillas HTML

Prueba No.	**12**
Descripción	Verificar el funcionamiento de modificar plantillas HTML
Objetivos	Verificar que la información modificada de una plantilla HTML no contenga campos vacíos.

Condiciones	Modificar plantilla HTML con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá modificar plantillas HTML con campos incompletos del formulario. El sistema permitirá modificar plantillas HTML con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite modificar plantillas HTML con campos incompletos del formulario además el sistema permite modificar plantillas HTML con los campos completos del formulario

Tabla 32.
Verificar el funcionamiento de eliminar plantillas HTML

Prueba No.	**13**
Descripción	Verificar el funcionamiento de eliminar plantillas HTML
Objetivos	Verificar que la plantilla HTML eliminada se elimine de la base de datos.
Condiciones	Pulsar el botón Eliminar plantilla HTML
Resultados Esperados	El sistema permitirá eliminar plantillas HTML de forma simple. Las acciones deberán ser reflejadas en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria el sistema permite eliminar plantillas HTML, las acciones si se vieron reflejada en la base de datos.

Tabla 33.
Verificar la información de plantilla mensaje

Prueba No.	**14**
Descripción	Verificar la información de plantilla mensaje
Objetivos	Verificar si la visualización de información de plantilla mensaje es la misma que se agregó en la base de datos.
Condiciones	Seleccionar una plantilla mensaje y verificar la información.
Resultados Esperados	La información de una plantilla mensaje concuerda con la información guardada en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria la información de una plantilla mensaje concuerda con la información guarda en la base de datos.

Tabla 34.
Verificar el funcionamiento de crear nueva plantilla mensaje

Prueba No.	**15**
Descripción	Verificar el funcionamiento de crear nueva plantilla mensaje
Objetivos	Verificar que la información creada de plantilla mensaje no contenga campos vacíos.
Condiciones	Crear plantilla mensaje con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá crear plantilla mensaje con campos incompletos del formulario. El sistema permitirá crear plantilla mensaje con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite crear plantilla mensaje con campos incompletos del formulario además el sistema permite crear plantilla mensaje con los campos completos del formulario.

Tabla 35.
Verificar el funcionamiento de modificar plantilla mensaje

Prueba No.	**16**
Descripción	Verificar el funcionamiento de modificar plantilla mensaje
Objetivos	Verificar que la información modificada de plantilla mensaje no contenga campos vacíos.
Condiciones	Modificar plantilla mensaje con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá modificar plantilla mensaje con campos incompletos del formulario. El sistema permitirá modificar plantilla mensaje con los campos completos del formulario.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite modificar plantilla mensaje con campos incompletos del formulario además el sistema permite modificar plantilla mensaje con los campos completos del formulario

Tabla 36.
Verificar el funcionamiento de eliminar plantilla mensaje

Prueba No.	**17**
Descripción	Verificar el funcionamiento de eliminar plantilla mensaje
Objetivos	Verificar que la plantilla mensaje eliminado se elimine de la base de datos.
Condiciones	Eliminar plantilla mensaje simple o selección múltiple de plantilla mensaje.
Resultados Esperados	El sistema permitirá eliminar plantilla mensaje de forma simple. El sistema permitirá eliminar plantilla mensaje de forma múltiple. El sistema no permitirá eliminar plantilla mensaje que estén siendo utilizadas en ataques. Las acciones deberán ser reflejadas en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria el sistema permite eliminar plantilla mensaje de forma simple, múltiple y no permite eliminar plantilla mensaje que estén siendo utilizadas en ataques las acciones si se vieron reflejada en la base de datos.

Tabla 37.
Verificar la información de Ataque

Prueba No.	**18**
Descripción	Verificar la información de Ataque
Objetivos	Verificar si la visualización de información de Ataque es la misma que se agregó en la base de datos.
Condiciones	Seleccionar un Ataque y verificar la información.
Resultados Esperados	La información de Ataque concuerda con la información guardada en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria la información de Ataque concuerda con la información guarda en la base de datos.

Tabla 38.
Verificar el funcionamiento de crear nuevo Ataque

Prueba No.	**19**
Descripción	Verificar el funcionamiento de crear nuevo Ataque
Objetivos	Verificar que la información creada de Ataque no contenga campos vacíos. Verificar que se realice el ataque en la fecha especificada
Condiciones	Crear Ataque con campos incompletos y campos completos Crear Ataque con una fecha y hora anterior al actual
Resultados Esperados	El sistema no permitirá crear Ataques con campos incompletos del formulario. El sistema permitirá crear Ataques con los campos completos del formulario. El sistema enviara correos a los objetivos seleccionados.
Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite crear Ataques con campos incompletos del formulario, permite crear Ataques con los campos completos del formulario y realiza él envió de correos a los objetivos en la fecha especificada seleccionados además si la fecha es anterior a la actual el sistema enviara el correo en ese instante.

Tabla 39.
Verificar el funcionamiento de modificar Ataques

Prueba No.	**20**
Descripción	Verificar el funcionamiento de modificar Ataques
Objetivos	Verificar que la información modificada de un ataque no contenga campos vacíos. Verificar que un ataque realizado no se pueda modificar.
Condiciones	Modificar ataque con campos incompletos y campos completos
Resultados Esperados	El sistema no permitirá modificar ataques realizados. El sistema no permitirá modificar ataques pendientes con campos incompletos del formulario. El sistema permitirá modificar ataques pendientes con los campos completos del formulario.

Resultados Obtenidos	La prueba fue aprobatoria el sistema no permite modificar ataques realizados ni ataques pendientes con campos incompletos del formulario además el sistema permite modificar ataques pendientes con los campos completos del formulario.

Tabla 40.
Verificar el funcionamiento de eliminar ataques

Prueba No.	**21**
Descripción	Verificar el funcionamiento de eliminar ataques
Objetivos	Verificar que el ataque eliminado se elimine de la base de datos.
Condiciones	Pulsar el botón Eliminar Ataque.
Resultados Esperados	El sistema permitirá eliminar Ataque. Las acciones deberán ser reflejadas en la base de datos.
Resultados Obtenidos	La prueba fue aprobatoria el sistema permite eliminar Ataques, las acciones si se vieron reflejada en la base de datos.

Tabla 41.
Verificar el funcionamiento de generar plantillas HTML

Prueba No.	**22**
Descripción	Verificar el funcionamiento de generar plantillas HTML
Objetivos	Verificar que el sistema genere plantillas HTML
Condiciones	Agregar elementos a la plantilla HTML y pulsar el botón guardar
Resultados Esperados	La plantilla HTML se genera y se guarda en el computador.
Resultados Obtenidos	La prueba fue aprobatoria el sistema permite generar plantillas HTML y guardarlas en el computador.

Tabla 42.
Verificar el funcionamiento de recomendación de asunto

Prueba No.	**23**
Descripción	Verificar el funcionamiento de recomendación de asunto
Objetivos	Verificar que el sistema mediante un algoritmo inteligente recomiende un asunto dependiendo por departamento.

Condiciones	Seleccionar un departamento y generar un asunto.
Resultados Esperados	El asunto generado depende a los ataques realizados si envía un departamento, y dentro de los ataques realizados existen personas que corresponden a dicho departamento el algoritmo de recomendación será más eficaz.
Resultados Obtenidos	La prueba fue aprobatoria la recomendación de asunto generado es eficaz.

Tabla 43.
Verificar el funcionamiento de generar reportes de ataques por fecha

Prueba No.	**24**
Descripción	Verificar el funcionamiento de generar reportes de ataques por fecha
Objetivos	Verificar que el sistema genere reportes de ataques por fecha.
Condiciones	Entrar a la pantalla de reportes.
Resultados Esperados	El sistema muestra información de los ataques por fecha
Resultados Obtenidos	La prueba fue aprobatoria el sistema muestra reportes de los todos los ataques, ataques pendientes y ataques enviados según fecha de creación.

Tabla 44.
Verificar el funcionamiento de generar reportes de ataques exitosos por categoría de plantilla mensaje

Prueba No.	**25**
Descripción	Verificar el funcionamiento de generar reportes de ataques exitosos por categoría de plantilla mensaje
Objetivos	Verificar que el sistema genere reportes de ataques exitosos por categoría de plantilla mensaje.
Condiciones	Entrar a la pantalla de reportes y pulsar el botón más detalles en la sección de ataques exitosos por categoría.
Resultados Esperados	El sistema muestra información de los ataques exitosos por categoría de plantilla mensaje
Resultados Obtenidos	La prueba fue aprobatoria el sistema muestra reportes de los ataques exitosos clasificándolos por categoría de plantilla de mensaje.

Tabla 45.
Verificar el funcionamiento de generar reportes de ataques exitosos por departamento de empleado

Prueba No.	**26**
Descripción	Verificar el funcionamiento de generar reportes de ataques exitosos por departamento de empleado
Objetivos	Verificar que el sistema genere reportes de ataques exitosos por departamento de empleado.
Condiciones	Entrar a la pantalla de reportes y pulsar el botón más detalles en la sección de ataques exitosos por departamento.
Resultados Esperados	El sistema muestra información de los ataques exitosos por departamento de empleado.
Resultados Obtenidos	La prueba fue aprobatoria el sistema muestra reportes de los ataques exitosos clasificándolos por departamento de empleados afectados.

Tabla 46.
Verificar el funcionamiento de generar reportes de empleados capacitados

Prueba No.	**27**
Descripción	Verificar el funcionamiento de generar reportes de empleados capacitados
Objetivos	Verificar que el sistema genere reportes de empelados capacitados.
Condiciones	Entrar a la pantalla de reportes y pulsar el botón más detalles en la sección de empleados capacitados.
Resultados Esperados	El sistema muestra información de los empleados capacitados.
Resultados Obtenidos	La prueba fue aprobatoria el sistema muestra reportes de los empleados capacitados clasificándolos por departamentos.

Tabla 47.
Verificar el funcionamiento de guardar información de empleados capacitados

Prueba No.	**28**
Descripción	Verificar el funcionamiento de guardar información de empleados capacitados

Objetivos	Verificar que el sistema guarde información de empleados capacitados.
Condiciones	Entrar al índex de la página al final de la sección el usuario tiene un formulario donde tiene que llenar información si el contenido de la página es de utilidad o no.
Resultados Esperados	El sistema guardara información de los usuarios capacitados.
Resultados Obtenidos	La prueba fue aprobatoria el sistema guarda información de los usuarios capacitados.

4.1.2. Pruebas de integración

Tabla 48.
Pruebas de integración

No.	Descripción	Cumple
1	Integración de Firebase con Angular	Si
2	Integración de DialogFlow en Kommunicate.io	Si
3	Integración de Kommunicate en Angular	Si
4	Integración de NodeMail	Si

4.1.3. Pruebas de Sistema

Tabla 49.
Pruebas de sistema

No.	**Requisito**	**Cumple**
1	Cargar información de los departamentos que están conformados por la institución.	Si
2	Gestionar información de los departamentos que están conformados por la institución.	Si
3	Cargar datos de trabajadores de la institución, Gestionar información de los trabajadores de la institución.	Si
4	Cargar información de plantillas mensajes de correo electrónico.	Si
5	Gestionar información de plantillas mensajes de correo electrónico.	Si

6	Cargar plantillas HTML para vincular a los mensajes de correo electrónico.	Si
7	Crear y Personalizar plantillas HTML para vincular a los mensajes de correo electrónico.	Si
8	Gestionar plantillas HTML para vincular a los mensajes de correo electrónico.	Si
9	Envío de ataque de simulación.	Si
10	Gestionar ataques de simulación.	Si
11	Generar reportes de ataque de simulación por fecha de envío.	Si
12	Generar reportes de ataque de simulación por departamento.	Si
13	Generar reportes de ataque de simulación por categoría de mail.	Si
14	Cargar información de los departamentos que están conformados por la institución.	Si
15	Generar recomendaciones de asuntos para nuevos contenidos de correos electrónicos a través de un algoritmo inteligente basado en los resultados de los ataques enviados.	Si
16	Consultar información de ingeniería social a través de un chatbot.	Si
17	Visualizar información básica sobre ingeniería social	Si
18	Llevar un control del personal que visualiza y se capacita con la información básica sobre la ingeniería social.	Si
19	Generar reportes con la información del personal capacitado.	Si

4.1.4. Pruebas de Aceptación

Para las pruebas de aceptación se realizó una encuesta al usuario final para conocer su nivel de satisfacción de cada requisito.

Tabla 50.
Pruebas de aceptación

No.	Pregunta	Nivel de Satisfacción
1	Cargar información de los departamentos que están conformados por la institución.	Alto
2	Gestionar información de los departamentos que están conformados por la institución.	Alto
3	Cargar datos de trabajadores de la institución, Gestionar información de los trabajadores de la institución.	Alto
4	Cargar información de plantillas mensajes de correo electrónico.	Alto
5	Gestionar información de plantillas mensajes de correo electrónico.	Alto
6	Cargar plantillas HTML para vincular a los mensajes de correo electrónico.	Alto
7	Crear y Personalizar plantillas HTML para vincular a los mensajes de correo electrónico.	Bajo
8	Gestionar plantillas HTML para vincular a los mensajes de correo electrónico.	Alto
9	Envío de ataque de simulación.	Alto
10	Gestionar ataques de simulación.	Alto
11	Generar reportes de ataque de simulación por fecha de envío.	Alto
12	Generar reportes de ataque de simulación por departamento.	Alto
13	Generar reportes de ataque de simulación por categoría de mail.	Alto
14	Cargar información de los departamentos que están conformados por la institución.	Alto
15	Generar recomendaciones de asuntos para nuevos contenidos de correos electrónicos a través de un algoritmo inteligente basado en los resultados de los ataques enviados.	Medio

16	Consultar información de ingeniería social a través de un chatbot.	Alto
17	Visualizar información básica sobre ingeniería social	Alto
18	Llevar un control del personal que visualiza y se capacita con la información básica sobre la ingeniería social.	Alto
19	Generar reportes con la información del personal capacitado.	Alto

4.2. Recolección de datos

Los datos recolectados serán los mismos que hayan sido almacenados en el sistema tanto como de empleados capacitados y de empleados vulnerados los cuales se pueden visualizar en el apartado de reportes del sistema.

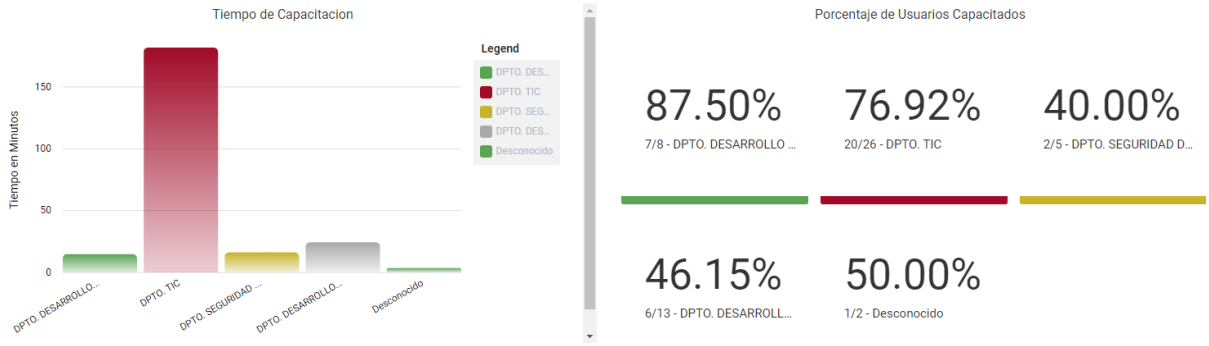
4.3. Resultados

Se recolectaron datos del uso del sistema dentro de un periodo de 2 semanas. En donde, al inicio de la primera semana se compartió el sistema con 59 empleados de la Comandancia de la Fuerza Aérea Ecuatoriana quienes tendrán a su disposición la pantalla principal y el ChatBot del sistema SafeSecure con el fin de capacitarlos en los temas comunes de la ingeniería social.

Al finalizar la primera semana se envió una simulación de ataques de ingeniería social, para verificar si los empleados se capacitaron con la información que se compartió en el transcurso de la semana.

Una vez culminada la primera semana se repitió el proceso para la segunda semana usando un asunto recomendado por el sistema dentro de los correos de los ataques simulados, con objetivo de observar progresos en la capacitación y verificar la efectividad del algoritmo de recomendación.

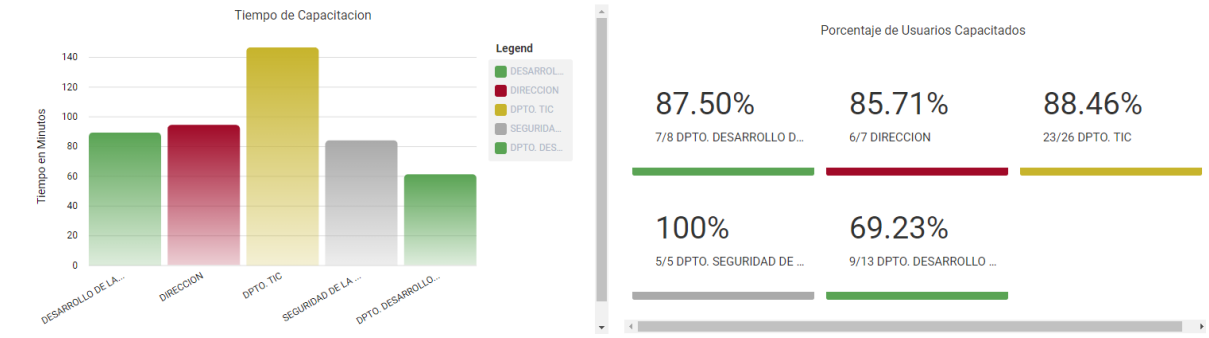
Figura 68.
Datos del número de capacitaciones de la primera semana.



Nota. En la figura se muestra dividido en dos diagramas los datos de las capacitaciones de la primera semana, en donde el grafico de la izquierda muestra el tiempo de visualización de las capacitaciones totales de cada empleado, clasificado por departamentos, mientras que el grafico de la derecha muestra la cantidad de empleados que se capacitaron, de igual forma clasificados por departamento.

Esta información fue recolectada a través del formulario mostrado en la **figura 39.**

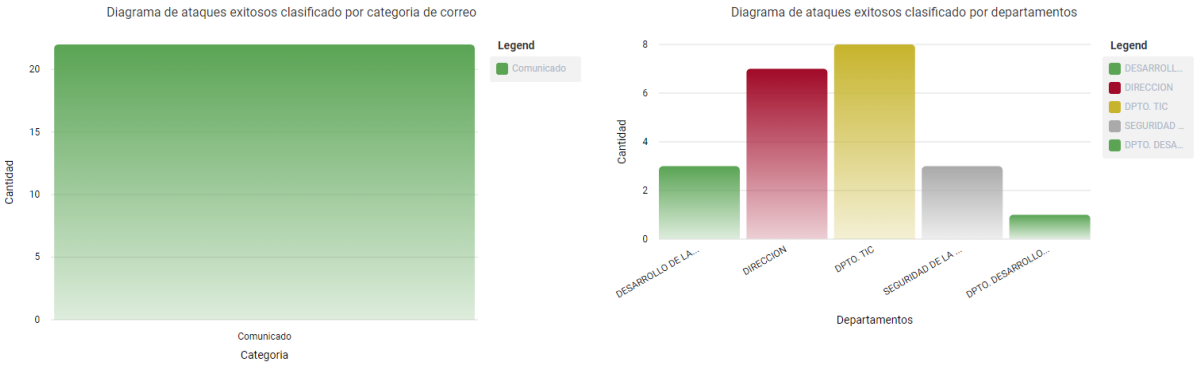
Figura 69.
Datos del número de capacitación de la segunda semana.



Nota. En la figura se muestra dividido en dos diagramas los datos de las capacitaciones de la segunda semana, en donde el grafico de la izquierda muestra el tiempo de visualización de las capacitaciones totales de cada empleado, clasificado por departamentos, mientras que el grafico de la derecha muestra la cantidad de empleados que se capacitaron, de igual forma clasificados por departamento.

Esta información fue recolectada a través del formulario mostrado en la **figura 39.**

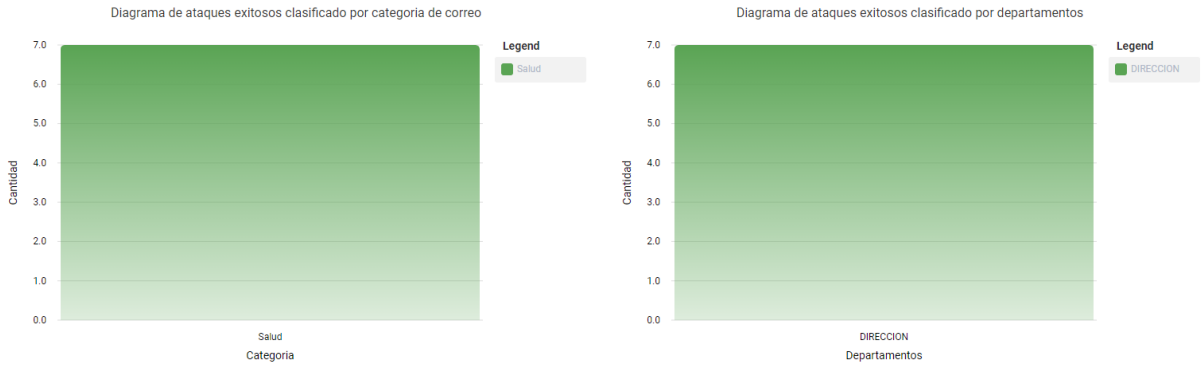
Figura 70.
Datos de los ataques exitosos (correos abiertos y usuarios vulnerados) durante la primera semana.



Nota. En la figura se muestra un diagrama de barras de los ataques exitosos (correos abiertos o usuarios vulnerados) durante la primera semana.

Esta información fue obtenida de la base de datos del sistema SafeSecure después de que un empleado haya sido vulnerado en un ataque simulado.

Figura 71.
Datos de los ataques exitosos (correos abiertos y usuarios vulnerados) durante la semana dos.



Nota. La figura se muestra un diagrama de barras de los ataques exitosos (correos abiertos o usuarios vulnerados) durante la semana dos.

Esta información fue obtenida de la base de datos del sistema SafeSecure después de que un empleado haya sido vulnerado en un ataque simulado.

4.4. Análisis de resultados

En la primera semana se obtuvo un total de treinta y seis empelados capacitados como se muestra en la **figura 68**, mientras que en la segunda semana este número aumento a cincuenta

como se muestra en la **figura 69**. Si se realiza una comparación de los datos de capacitaciones recolectadas en la primera y segunda semana, se puede observar que el número de empleados capacitados aumento en un 23.73%, además de que, el tiempo total invertido en las capacitaciones por los empleados entre las dos semanas, aumento considerablemente de doscientos treinta y cuatro minutos a cuatrocientos setenta y tres minutos visualizados en las **figuras 68,69** respectivamente.

De acuerdo con los datos de ataques exitosos, se puede visualizar que al finalizar la primera semana se obtuvo un total de veintidós ataques exitosos o empleados vulnerados, visualizados en la **figura 70**, mientras que al finalizar la segunda semana solamente se obtuvo un total de siete visualizado en la **figura 71**, logrando disminuir en diecisiete el total de ataques exitosos o empleados vulnerados.

4.5. Discusión de resultados

La hipótesis propuesta es: ¿Si se desarrolla la plataforma web SafeSecure entonces se contribuirá al asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana?; las variables de investigación son:

Variable Dependiente: Se contribuye al asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.

Variable Independiente: Se desarrolla la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.

Los indicadores que se consideran para la validación son:

a) Porcentajes de progreso del entrenamiento en Ingeniería Social representando un aumento mínimo de 80 por ciento.

b) Nivel de efectividad de los nuevos temas o contextos recomendados por el algoritmo inteligente.

c) Cantidad de correos de simulación abiertos durante cada periodo de entrenamiento.

d) Frecuencia de uso del sistema en la creación de entrenamientos de simulación.

Si se habla de capacitaciones, considerando que, de los cincuenta y nueve empleados ninguno de ellos tenía una capacitación registrada al inicio de la semana uno, al finalizar la semana dos se consiguió aumentar el número de empleados capacitados a cincuenta como se muestra en la **figura 69**, logrando así capacitar al 84.745% de los empleados en quienes se aplicó el sistema. Admitiendo así la validación del indicador a).

Para los ataques exitosos si se toma en cuenta los datos de la primera y segunda semana, se puede concluir que, en vista de la reducción de ataques exitosos. Los cuales se visualizan en la **figura 70** "Datos del número de capacitación de la primera semana", con una cantidad de veintidós ataques exitosos y la **figura 71** "Datos del número de capacitación de la segunda semana", con una cantidad de siete ataques exitosos, se comprobó que efectivamente más del 80% de los empleados consiguió capacitarse en ingeniería social y ciberataques. Admitiendo así la validación del indicador a) y c).

Un aspecto por tomar en cuenta es que los ataques enviados al finalizar la segunda semana se realizaron haciendo uso del sistema de recomendación por lo que considerando que de los cincuenta y nueve empleados a quienes se envió un ataque, cincuenta de ellos ya se encontraban capacitados, se puede decir que el asunto recomendado por el algoritmo tuvo una efectividad del 77.78% en empleados no capacitados. Admitiendo así la validación del indicador b).

Dado que el sistema se manejó durante dos semanas tanto por el administrador para gestionar datos y para controlar la información visualizada en la página principal, como por los empleados quienes se capacitaban con la información e interactuaban con el chatbot, se puede

concluir que el sistema fue usado un aproximado de quince días continuos, admitiendo así la validación del indicador d).

La validación de la hipótesis se llevó a cabo haciendo uso de la prueba de independencia chi cuadrado, estableciendo las hipótesis nula y alternativa:

Hipótesis nula ($H0$): ¿Si se desarrolla la plataforma web SafeSecure entonces no se contribuirá al asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana?

Hipótesis alternativa ($H1$): ¿Si se desarrolla la plataforma web SafeSecure entonces se contribuirá al asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana?

En la **Tabla 51** se muestra la tabla de contingencia estableciendo como variables los empleados vulnerados y empleados capacitados al finalizar la segunda semana.

Tabla 51
Tabla de contingencia de empleados capacitados y vulnerados.

Empleados	**Capacitados**	**No Capacitados**	**Total**
Vulnerados	0	7	7
No Vulnerados	50	2	52
Total	50	9	59

Después se procedió a obtener la tabla de frecuencias esperadas aplicando la fórmula 2. (Mendivelso, 2018)

$$fe = \frac{Total\ de\ columna\ x\ Total\ de\ Fila}{Suma\ Total} \quad (2)$$

Tabla 52
Tabla de frecuencias esperadas de empleados capacitados y vulnerados.

Empleados	**Capacitados**	**No Capacitados**

Vulnerados	5,93220339	1,06779661
No Vulnerados	44,06779661	7,93220339

Por último, se calculó el chi cuadrado aplicando la fórmula 3. (Mendivelso, 2018)

$$x^2 = \sum \frac{(fo-fe)^2}{fe} \quad (3)$$

$$x^2 = 44{,}12393162$$

Posteriormente obtenemos el chi cuadrado critico inverso 3,841458821 sabiendo que:

$\alpha = 0.05$

$gl = 1.$

El valor de chi cuadrado obtenido $44{,}12393162$ es mayor al chi cuadrado critico inverso 3,841458821, por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, donde se establece que si se desarrolla la plataforma web SafeSecure entonces se contribuirá al asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.

CAPÍTULO V

Conclusiones y Recomendaciones

5.1. Conclusiones

- Se cumplió con el objetivo principal del proyecto; “Desarrollar la plataforma web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil de la Comandancia de la Fuerza Aérea Ecuatoriana.”

- Gracias a la elaboración del marco teórico se establece la información necesaria sobre la ingeniería social, características y métodos de prevención aplicados en el proyecto.

- Se aplico la metodología UWE en la realización de la plataforma web SafeSecure tal y como se propuso inicialmente ya que, gracias a lo expuesto en el marco teórico, es la más indicada para el desarrollo de sistemas web.

- A pesar de que la metodología UWE brinda una variedad de diagramas para representar de manera detallada el sistema a desarrollar, se optó por cambiar algunos de estos por otros diagramas UML para tener aún más detalles en la interacción de los objetos del sistema.

- Se implemento un algoritmo inteligente supervisado de recomendación de asuntos de correos para las simulaciones de ataques de cada departamento, basado en los asuntos de correos con ataques exitosos enviados previamente.

- El componente de ML.js es de gran ayuda para incorporar Machine Learning en Node y fue una parte fundamental para desarrollar el algoritmo inteligente supervisado de recomendación de asuntos de correos a ser enviados en los entrenamientos.

- Tal y como se muestra en la **figura 64** acompañado de los resultados de la segunda semana mostrados en la **figura 71** se puede concluir que el algoritmo inteligente supervisado de

recomendación fue implementado con éxito en la plataforma web SafeSecure, obtenidos una efectividad del 77.78% en vulnerar empleados no capacitados

- Dentro de la plataforma web SafeSecure, el algoritmo inteligente supervisado de recomendación interactúa con el usuario solicitando un departamento para proceder a recomendarle un tema o asunto potencialmente efectivo para dicho departamento.
- Se implanto el sistema web SafeSecure para el asesoramiento, concientización y entrenamiento en técnicas de prevención de ataques de ingeniería social para el personal militar y civil en la comandancia de la Fuerza Aérea Ecuatoriana.
- Se validó el sistema con pruebas unitarias, de integración, sistemas y aceptación obteniendo resultados muy fieles a los esperados.
- Para validar el sistema con pruebas de aceptación se realizó una encuesta a personal del departamento de seguridad informática de la comandancia de la Fuerza Aérea Ecuatoriana obteniendo como resultado una media de nivel de satisfacción alto tal y como se muestra en la **tabla 50**.
- Para la recolección de resultados se realizó un periodo de pruebas con dos semanas de duración, en 59 empleados de la comandancia de la Fuerza Aérea del Ejercito ecuatoriana.
- En la etapa de pruebas, el sistema se manejó durante dos semanas tanto por el administrador para gestionar datos y para controlar la información visualizada en la página principal, como por los empleados quienes se capacitaban con la información e interactuaban con el chatbot, por lo que se puede concluir que, el sistema fue usado un aproximado de quince días continuos.
- La hipótesis fue exitosa, ya que al culminar la etapa de pruebas se demostró que el uso la plataforma web SafeSecure tuvo un aumento del 84.745% en capacitación de la ingeniería

social en los 59 empleados, además de reducir la cantidad de correos abiertos de la primera a la segunda semana.

5.2. Recomendaciones

- Para desarrollo de sistemas web a la medida se recomienda realizar varias reuniones con el cliente para detallar de manera correcta los requisitos.
- Se recomienda definir una metodología ágil a seguir antes de iniciar cualquier proyecto de desarrollo de software.
- Gracias a la experiencia obtenida en el desarrollo de sistemas web se recomienda utilizar la metodología UWE debido a que la misma se enfoca en el desarrollo de dichos sistemas.
- Se recomienda consultar la documentación respectiva de cada herramienta a utilizar en el desarrollo de un aplicativo web.
- Antes de realizar la fase de pruebas se recomienda analizar los requisitos del sistema software con el fin de reconocer las funcionalidades que se van a probar.
- Se recomienda utilizar herramientas de control de versiones tanto para el desarrollo del software como para su documentación ya que estas herramientas son de gran ayuda para administrar y gestionar cambios.

Bibliografía

Angular. (s. f.). Angular. Recuperado 23 de junio de 2021, de https://angular.io/guide/what-is-angular

Aldawood, Hussain & Skinner, Geoff. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 2019-2020.

Avoiding World Cup scams. (2018, 25 junio). Consumer Information. Recuperado 23 de junio de 2021, de https://www.consumer.ftc.gov/blog/2018/06/avoiding-world-cup-scams.

BitHeads CUSTOM SOFTWARE DEVELOPMENT. (s. f.). A BACKEND-AS-ASERVICE (BAAS) OVERVIEW. https://telusdigital-marketplace-production.s3.amazonaws.com/. Recuperado 12 de enero de 2021, de https://telusdigital-marketplace-production.s3.amazonaws.com/iot/user-content/product/818d-o.pdf

Calvo, A. M., Batista, V. L., & González, G. V. Sistema de recomendación de música basado en etiquetado social. AVANCES EN INFORMÁTICA Y AUTOMÁTICA, 47.

Capterra. (2021, 9 junio). Kommunicate. Recuperado 23 de junio de 2021, de https://www.capterra.ec/software/172677/kommunicate.

Cardiel Altemir, G. (2019). Desarrollo de una aplicación Fitness en el sistema operativo de Android con la plataforma Firebase.

Casas, H. H. (2 de Junio de 2014). UML based Web Engineering (UWE). Recuperado 23 de junio de 2021, de https://prezi.com/vf22m4sunbjq/uml-based-web-engineering-uwe/

CERT-PY :: Ciberejercicios - Simulacro de ciberataque. (2019). Ministerio de Tecnologías de la Información y Comunicación. Recuperado 23 de junio de 2021, de https://cert.gov.py/servicios/ciberejercicios-simulacro-de-ciberataque

Ciberseguridad: los riesgos que puede traer el teletrabajo. (2020, 2 diciembre). Semana.com Ultimas Noticias de Colombia y el Mundo. Recuperado 23 de junio de 2021, de https://www.semana.com/management/articulo/los-riesgos-del-teletrabajo-en-ciberseguridad/284349/

Chequea, E. (2019, 5 diciembre). Ecuador es el tercer país más ciberseguro de la región. CriteriosDigital. Recuperado 23 de junio de 2021, de https://criteriosdigital.com/noticias/ecuador-chequea/ciberseguridad-ecuador/

Chizari, Hassan & Zulkurnain, Ahmad & Hamidy, Ahmad & Husain, Affandi.

Comando Conjunto de las Fuerzas Armadas del Ecuador. (s. f.). Comando Conjunto de las Fuerzas Armadas del Ecuador. Recuperado 1 de marzo de 2021, de https://www.ccffaa.mil.ec/

Cortés Hernández, A. M. (2019). Ingeniería social Phishing y Baiting.

Cyber Security Breaches Survey 2019. (2019, 2 julio). GOV.UK. Recuperado 23 de junio de 2021, de https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

C3.ai. (2021, 3 agosto). C3 AI - Enterprise AI. C3 AI. Recuperado 23 de junio de 2021, de https://c3.ai/

Delgado, A. (1999). Robótica inteligente. Revista de la Facultad de Medicina, 47(1), 32-34.

Demey, J. R., Pla, L., Vicente-Villardón, J. L., Di Rienzo, J., & Casanoves, F. (2011). Medidas de distancia y similitud. Valoración y análisis de la diversidad funcional y su relación con los servicios ecosistémicos, 384, 47-59.

Dialogflow ES basics |. (s. f.). Google Cloud. Recuperado 23 de junio de 2021, de https://cloud.google.com/dialogflow/es/docs/basics.

Digiware. (2016). Contexto de seguridad en Tecnología Operacional. Recuperado 20 de octubre de 2020, de https://www.digiware.net/

Digiware. (2020). Ciberseguridad: Su importancia en la nueva normalidad. Recuperado el 20 de octubre del 2020, de https://www.digiware.net/post/ciberseguridad-su-importancia-en-la-nueva-normalidad

Durán, J. D. D. R. (s. f.). La ciberseguridad en el ámbito militar. Dialnet. Recuperado 22 de marzo de 2021, de https://dialnet.unirioja.es/servlet/articulo?codigo=3837348

El poder de la ingeniería social para realizar estafas en Internet (2017). Recuperado 23 de junio de 2021, de http://computerworldmexico.com.mx/poder-la-ingenieriasocial-realizar-estafas-en-internet/

Estafas que se aprovechan de la Copa del Mundo para engañar a los usuarios. (2018). welivesecurity. Recuperado 23 de junio de 2021, de https://www.welivesecurity.com/la-es/2018/06/06/estafas-aprovechan-copa-mundo-rusia-enganar-usuarios/

Firebase, 2018. Cloud Firestore | Firebase. Recuperado 12 de enero de 2021 de, https://firebase.google.com/docs/firestore/.

Firebase, 2018. Firebase Hosting | Firebase. Recuperado 12 de enero de 2021 de, https://firebase.google.com/docs/hosting/

Fuerza Aérea Ecuatoriana. (s. f.). Fuerza Aérea Ecuatoriana. Recuperado 1 de marzo de 2021, de https://www.fae.mil.ec/

Garcia Romero, J. E. Estudio de metodologías de ingeniería social. (2015). Social Engineering Attack Mitigation. International Journal of Mathematics and Computational Science. 1. 188-198.

Garrido Ortega, M. (2018). Chatbots en educación.

Gil Hernán, A. (2017). Framework orientado a algoritmos de recomendación basados en vecinos cercanos (Bachelor's thesis).

Giraldo, V. (2021, 19 febrero). Plataformas digitales: ¿qué son y qué tipos existen? Rock Content - ES. Recuperado 23 de junio de 2021, de https://rockcontent.com/es/blog/plataformas-digitales/

Google. 2019. Firebase. California: USA. Recuperado 12 de enero de 2021, de https://firebase.google.com/docs/

Hamzaoui, D. Y. (2014). Aplicación de Algoritmos Inteligentes en Problemas de Ingeniería

Ibarra-Báez, L. D., Mota-Carrera, L. C., Rojas-López, V., & Sánchez-Acevedo, M. A. Sistema de Recomendación de Libros.

Inteligencia (2020, 19 octubre). La evolución del ataque de phishing. Inteligencia. Recuperado 23 de junio de 2021, de https://inteligencia.pro/la-evolucion-del-ataque-de-phishing/

Isakowitz, T., Stohr, E., & Balasubramanian, P. (1995). RMM: a methodology

for structured hypermedia design. Common. ACM, 38(8), pp. 34–44.

Jaime López Sánchez. (2019). Métodos y técnicas de detección temprana de casos de phishing

J.M.H. (2018, 1 marzo). Social engineering in cybersecurity: The evolution of a concept. ScienceDirect. Recuperado 23 de junio de 2021, de https://www.sciencedirect.com/science/article/pii/S0167404817302249

Khawas, C., & Shah, P. (2018). Application of firebase in android app development-a study. International Journal of Computer Applications, 179(46), 49-53.

Lisboa Díaz, M. A. (2020). Predicción de áreas con usuarios vulnerables a ciberataques (Doctoral dissertation, Universidad Andrés Bello).

Mariño, S. (2017). Metodología para el Desarrollo WEB. Metodología para el Desarrollo WEB, 1, 1. Recuperado 23 de junio de 2021, de https://issuu.com/yvalos/docs/desarollo_web_3a120d319996d9

Mülchi, S., & Andrés, C. (2016). Estudio del framework angularjs y su uso en el desarrollo web.

M. Fernandez. (2019, May 6). ” Ingeniería Social: ¿qué es el Baiting («cebar», o «poner carnada»)”. Recuperado 23 de junio de 2021, de https://blog.mailfence.com/es/que-esbaiting-ingenieria-social/

Mendivelso, F., & Rodríguez, M. (2018). Prueba Chi-cuadrado de independencia aplicada a tablas 2xN. *Revista Médica Sanitas*, *21*(2), 92-95.

Narváez, A., Baldeón, P., Hinojosa, C., & Martínez, D. (2012). Experiencia de desarrollo de una aplicación Web utilizando la metodología UWE y el lenguaje QVT en la transformación de modelos. vol. I, (1), 1-10.

Operation «Phish Phry». (2009). FBI. Recuperado 27 de octubre del 2020, de https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709

Phishing (2005) Recuperado 23 de junio de 2021, de https://www.sgu-info.com.ar/malware/phising.htm

Rand, P. (s. f.). 3.5.3.5 Diseñar la base de datos. Analisis y diseño orientados a objetos. Recuperado 3 de agosto de 2021, de http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro10/3535_disear_la_base_de_datos.html

Rodríguez Rincón, E. Y. Metodologías de ingeniería social.

Rossi, G. P., Schwabe, O., & D. Olsina, L. (2008). Web Engineering - Modelling and Implementing Web Applications. Londres: Springer Case Studies in the Current Situation.

Sanz, J. (2017). Firebase: Qué Es y Por Qué Integrarlo en Nuestras APPs. Recuperado el 12 de enero de 2021 de: https://javiersanzrozalen.wordpress.com/2017/01/09/firebase-que-es-y- por-que-integrarlo-en-nuestras-apps/

Schwabe D.: An Object Oriented Aproach to Web-Based Application Design. Theory and Practice of Objects Systems 4(4). Willey and Sons, New York. (1998) 1074-3224

Significados (2015, 26 agosto). Significado de Colaboración. Significados. Recuperado 23 de junio de 2021, de https://www.significados.com/colaboracion/#:%7E:text=Qu%C3%A9%20es%20Colaboraci%C3%B3n%3A,que%20significa%20%27trabajar%20juntos%27.

Silva, D. A., & Mercerat, B. (2001). Construyendo aplicaciones web con una metodología de diseño orientada a objetos. Revista Colombiana de Computación, 2(2), 1-21.

Simeone, O. (2018). A Very Brief Introduction to Machine Learning With Applications to Communication Systems.

Sofy, B. (12 de octubre de 2015). Arquitectura multicapa para implementar aplicaciones de tipo empresarial y aplicaciones basadas en la Web. Recuperado 23 de junio de 2021, de https://es.scribd.com/document/284470143/Que-es-JEE

State of Cybersecurity in the Banking Sector in Latin America and the Caribbean. (2018). OAS ORG. Recuperado 23 de junio de 2021, de https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf

Syiemlieh, Phirashisha & Golden, Mary & Khongsit, & Sharma, Ushamary & Sharma, Bobby. (2015). Phishing-An Analysis on the Types, Causes, Preventive Measuresand

Valdiviezo-Díaz, P., & Hernando, A. (2016). Una comprensiva revisión de los métodos de recomendación basados en técnicas probabilísticas. International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC), 3(2), 65-74.

Weber, J. (s. f.). What is Backend as a Service and What Does It Mean for Devs? - CenturyLink Cloud Developer Center. https://www.ctl.io/. Recuperado 12 de enero de 2021, de https://www.ctl.io/developers/blog/post/what-is-backend-as-a-service

Zamora, J. (2016). ¿Qué es Firebase? La Mejorada Plataforma de Desarrollo de Google. Recuperado el 12 de enero de 2021 de: https://elandroidelibre.elespanol.com/2016/05/firebase-plataforma-desarrollo-android-ios-web.html

Zhang, Z. (2016). Introduction to machine learning: k-nearest neighbors. Annals of translational medicine, 4(11).

npm: ml. (2021, 10 junio). NPM. Recuperado 10 de junio de 2021, de https://www.npmjs.com/package/ml

Anexos