

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



“Diseño e implementación de un sistema de autogestión de campañas de phishing para la concientización de la ciberseguridad”

MATÍAS ANDRE RAMÍREZ GONZÁLEZ

**MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA**

Profesor Guía: Francklin Rivas
Profesor Correferente: Xavier Bonnaire

MAYO - 2021

DEDICATORIA

A mi familia y amigos que me apoyaron durante toda mi etapa como estudiante.

AGRADECIMIENTOS

En primer lugar, agradecer al Departamento de Informática por permitir desarrollar la memoria mediante esta modalidad multidisciplinaria, ya que entrega grandes herramientas en la formación de los estudiantes en competencias transversales, el fomento de la innovación, el emprendimiento y la vinculación con la industria.

En segundo lugar, agradecer con mucho cariño a mis compañeros de equipo durante el PMM, Jose Catalán y Esteban Jara, ambos de Ingeniería Civil Telemática. Gracias por estar siempre dentro y fuera del horario de clases.

En tercer lugar, también dar las gracias a los ayudantes Arlette Arancibia y Alejandro Carvallo, quienes son parte del PMM y desempeñaron una tremenda labor para apoyarnos en otras áreas relacionadas al proyecto como son el diseño y el área comercial.

En cuarto lugar, agradecer infinitamente a los profesores guía que estuvieron presente en todo momento, apoyando cuando las cosas no salen como se esperan.

Por último, agradecer a mi familia por todos estos años que han estado apoyándome en todo sentido para que sea un profesional.

¡Gracias a todos!

RESUMEN

Resumen—En esta memoria, se presenta el diseño e implementación de una plataforma web de autogestión de campañas de *phishing*, en el marco de la concientización de la ciberseguridad. El objetivo de la solución es que las organizaciones puedan usar la herramienta para poner a prueba a su personal con simulaciones de envíos masivos de *phishing* y así, mediante los resultados en tiempo real que se generen, tomar acciones correctivas a tiempo.

El proyecto de memoria se realizó como parte del desafío presentado por una empresa especializada en ciberseguridad, en el marco del Programa de Memorias Multidisciplinarias 2020 que incentiva que estudiantes de último año de diversas carreras resuelvan problemáticas de la industria.

Palabras Clave—ingeniería social, campañas de *phishing*, ciberseguridad, concientización en ciberseguridad, plataforma web

ABSTRACT

Abstract—This work presents the design and implementation of a self-management phishing campaigns web platform in the context of cyber security awareness. The goal of the solution is that organizations can use the system to test their staff with phishing simulations, and with the results that generates take remedial actions in time.

This capstone project was done as part of the challenge presented by a specialized cybersecurity company at 'Memorias Multidisciplinarias' Program 2020 that encourages last year university students to solve industrial problems.

Keywords—Social engineering, phishing campaigns, cybersecurity, cybersecurity awareness, web platform.

GLOSARIO

API: Application Programming Interface (Interfaz de programación de aplicaciones)

APWG: Anti-Phishing Working Group

AWS: Amazon Web Services

CSIRT: Computer Security Incident Response Team (Equipo de Respuesta ante Incidencias de Seguridad Informáticas)

CSV: Comma Separated Values (Valores separados por coma)

DOM: Document Object Model (Modelo de Objetos del Documento)

ENISA: European Union Agency for Cybersecurity

PMM: Programa de Memorias Multidisciplinarias

PMV: Producto Mínimo Viable

REST: Representational State Transfer (Transferencia de estado representacional)

SaaS: Software-as-a-Service (Software como servicio)

SMS: Short Message Service (Servicio de mensajes cortos)

SMTP: Simple Mail Transfer Protocol (Protocolo para transferencia simple)

SPA: Single Page Application (Aplicación de página única)

SQL: Structured Query Language (Lenguaje de consulta estructurada)

TI: Tecnologías de la Información

URL: Uniform Resource Locator (Localizador de recursos uniforme)

ÍNDICE DE CONTENIDOS

RESUMEN	4
ABSTRACT	4
GLOSARIO	4
ÍNDICE DE CONTENIDOS	6
ÍNDICE DE FIGURAS	9
ÍNDICE DE TABLAS	10
INTRODUCCIÓN	11
Contexto	11
Programa de Memorias Multidisciplinarias	11
CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA	13
1.1 El Phishing	13
1.2 La Empresa y su desafío	17
1.3 Problemas y oportunidades	17
1.4 Objetivos	18
1.4.1 Objetivo general	18
1.4.2 Objetivos específicos	18
CAPÍTULO 2: MARCO CONCEPTUAL	20
2.1 Estado del Arte: Soluciones existentes	20
2.1.1 Conclusiones de las soluciones existentes	21
2.2 Herramientas de trabajo	21
2.2.1 Frontend	22
2.2.2 Backend	24
2.2.3 Gophish	26

2.2.4 AWS	27
2.2.5 Postman	27
CAPÍTULO 3: PROPUESTA DE SOLUCIÓN	29
3.1 Descripción de la solución	29
3.1 Usuarios del sistema	29
3.2 Requisitos del sistema	30
3.2.1 Lanzamiento de campañas	30
3.2.2 Visualización de resultados	31
3.2.3 Gestión de usuarios	32
3.2.4 Registro de actividad	33
3.2.5 Lanzamiento de campañas personalizadas	33
3.2.6 Sugerencias educativas	33
3.2.7 Integración vishing, smishing, phishing por Whatsapp	33
3.2.8 Autenticación de dos pasos	34
3.2.9 Resumen de requisitos	34
3.3 Arquitectura del sistema	35
3.3.1 Descripción de componentes y tecnologías	36
3.3.2 División del trabajo	36
3.5 Diseño de interfaces usuarias	36
CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN	39
4.1 Prototipo funcional	39
4.1.1 Contexto general del prototipo	39
4.1.2 Cumplimiento de requisitos	39
CAPÍTULO 5: CONCLUSIONES	49
5.1 Conclusiones generales	49
5.2 Cumplimiento de objetivos	49

5.3 Trabajo futuro	50
5.4 Trabajo multidisciplinario	51
REFERENCIAS BIBLIOGRÁFICAS	52
ANEXOS	54
Anexo A. Diagrama Funcional, plataforma Cliente	54
Anexo B. Diagrama Funcional, plataforma Super Admin/Consultor (La Empresa)	56
Anexo C. Landing page para la validación de la solución.	58

ÍNDICE DE FIGURAS

Figura 1: Actividad de phishing entre tercer trimestre 2019 y tercer trimestre...	13
Figura 2: Alertas informadas a la ciudadanía por medio del CSIRT....	14
Figura 3: Sectores de la industria más atacados, tercer trimestre...	14
Figura 4: Ejemplo de landing page de phishing. Fuente:...	16
Figura 5: Ejemplo de correo de phishing. Fuente: WeLiveSecurity...	16
Figura 6: Desglose de usuarios de la plataforma. Fuente:...	30
Figura 7: Diagrama de arquitectura. Fuente: Elaboración Equipo Multidisciplinario...	35
Figura 8: Sketching y retroalimentación de parte de La Empresa....	37
Figura 9: Mockup plataforma en Adobe XD. Vista de campañas...	38
Figura 10: Estructura de carga de material de phishing por medio...	40
Figura 11: Formulario de grupo objetivo. Nombre grupo objetivo....	41
Figura 12: Formulario de grupos objetivos. Carga de archivos....	41
Figura 13: Formulario de grupos objetivos. Confirmar envío de datos...	42
Figura 14: Listado de grupos objetivos en la plataforma Cliente....	42
Figura 15: Formulario de nueva campaña. Información Básica. Fuente...	43
Figura 16: Formulario de nueva campaña. Elección de temática de...	44
Figura 17: Formulario de nueva campaña. Calendarización de campaña....	44
Figura 18: Listado de campañas activas. Campaña Seleccionada. Fuente...	45
Figura 19: Resultados de campaña específica. Fuente: Equipo Multidisciplinario...	45
Figura 20: Formulario de Nueva Organización. Fuente: Equipo Multidisciplinario...	46
Figura 21: Listado de Organizaciones. Fuente: Equipo Multidisciplinario...	46
Figura 22: Formulario de Nueva Cuenta Organización (Admin o Viewer...	47
Figura 23: Cuentas asociadas a una organización específica. Fuente:...	47
Figura 24: Perfil de organización (Owner). Fuente: Equipo...	48
Figura 25: Actualizar Perfil de organización (Owner). Fuente:...	48

ÍNDICE DE TABLAS

Tabla 1: Actores identificados. Fuente: Equipo Multidisciplinario	18
Tabla 2: Evaluación de frameworks de frontend. Fuente: Adaptado...	22
Tabla 3: Evaluación de frameworks de backend. Fuente: Adaptado...	24
Tabla 4: Perfiles de Usuario. Fuente: Elaboración Propia	29
Tabla 5: Tabla resumen de requisitos por usuario. Fuente:...	34

INTRODUCCIÓN

Contexto

Actualmente, el mundo enfrenta cambios enormes dado el gran avance de la tecnología y el acceso a la información. Tanto para las personas como también para las organizaciones los beneficios de la era digital son cuantiosos, sin embargo, como un sin fin de cosas también trae diversos riesgos.

Para las organizaciones que han apostado por la transformación digital, es realmente importante la ciberseguridad. El alto volumen de información que algunas manejan y el valor que representan, hace necesario estar bien protegidos para evitar pérdidas económicas, de reputación, operacionales y de información relevante.

Durante el período 2019-2020, según el resumen anual de ENISA [1], las principales amenazas cibernéticas la conformaron el *malware*, los ataques basados en la web, ataques a aplicaciones web, el *phishing*, el ataque de denegación de servicio (DoS), spam, *botnets*, entre otros.

Para el año 2021, y según señala Eset en su informe de tendencia de ciberseguridad para 2021 [2], las principales amenazas cibernéticas se darán con mayor frecuencia dado el auge del uso de la tecnología debido a la pandemia por COVID-19.

Esta memoria se enfoca en el *phishing*, una técnica que es parte de la ingeniería social, que consiste en engañar o manipular a personas usando habilidades sociales, para obtener información confidencial o infectar sistemas informáticos. En específico, se expone el diseño e implementación de una plataforma web que permita la autogestión de campañas de *phishing*, con el fin de concientizar a las organizaciones.

Estar en conocimiento de la práctica del *phishing* es de suma importancia, sobre todo en organizaciones, donde los más propensos a caer ante estas situaciones es el propio personal.

Programa de Memorias Multidisciplinarias

El proyecto se realizó en el marco del Programa de Memorias Multidisciplinarias 2020, el cual incentiva que estudiantes de último año de diversas carreras resuelvan problemáticas de impacto real en la industria.

El avance en el trabajo sigue la metodología ágil SCRUM, la cual se caracteriza por ciclos cortos de desarrollo para favorecer la interacción continua entre los integrantes del equipo, los profesores guías y representantes de la organización proponente del desafío.

El documento tiene la siguiente estructura: la definición del problema (Capítulo 1); el marco conceptual (Capítulo 2); la propuesta de solución (Capítulo 3); la validación de la solución (Capítulo 4); y conclusiones (Capítulo 5).

CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA

1.1 El Phishing

El *phishing* es una forma de la ingeniería social, en la cual un atacante intenta de manera fraudulenta adquirir información sensible de una víctima haciéndose pasar por un tercero de confianza [3]. Comúnmente, las víctimas de este ataque reciben un correo electrónico o mensaje que los incentiva a acceder a un sitio web, imitación de uno legítimo, y registrar sus credenciales, como correo electrónico y contraseña.

ENISA, en su informe anual de amenazas 2020, incluye al *phishing* en el tercer lugar de amenazas en el periodo 2019-2020, siendo superada solo por los ataques por *malware* y los ataques basados en web, mostrando una tendencia a la alza a futuro [1].

Como muestra la [Figura 1](#), el tercer trimestre de 2020 se vio una gran aumento en la actividad de *phishing*, que se ve reflejado en los incrementos en las URLs fraudulentas detectadas a nivel mundial, y los asuntos de email únicos que reflejan la variedad en los ataques.

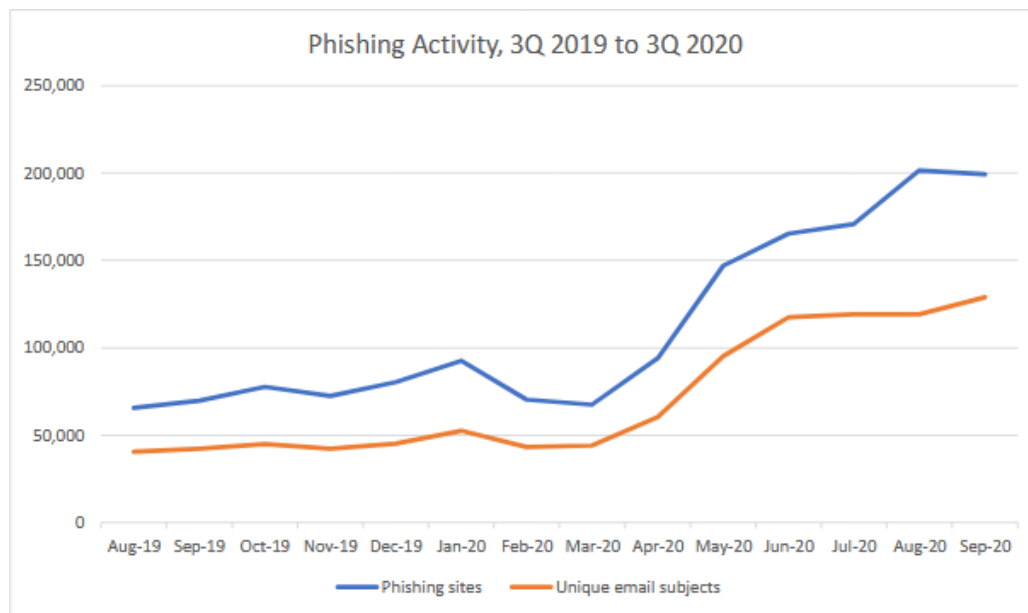


Figura 1: Actividad de phishing entre tercer trimestre 2019 y tercer trimestre 2020. Fuente: APWG

A nivel local, en Chile se notificaron 267 campañas de phishing en 2020, de un total de 1.297 alertas informadas por el CSIRT. En la [Figura 2](#) se aprecia que el *phishing* abarca el 21% de las alertas.

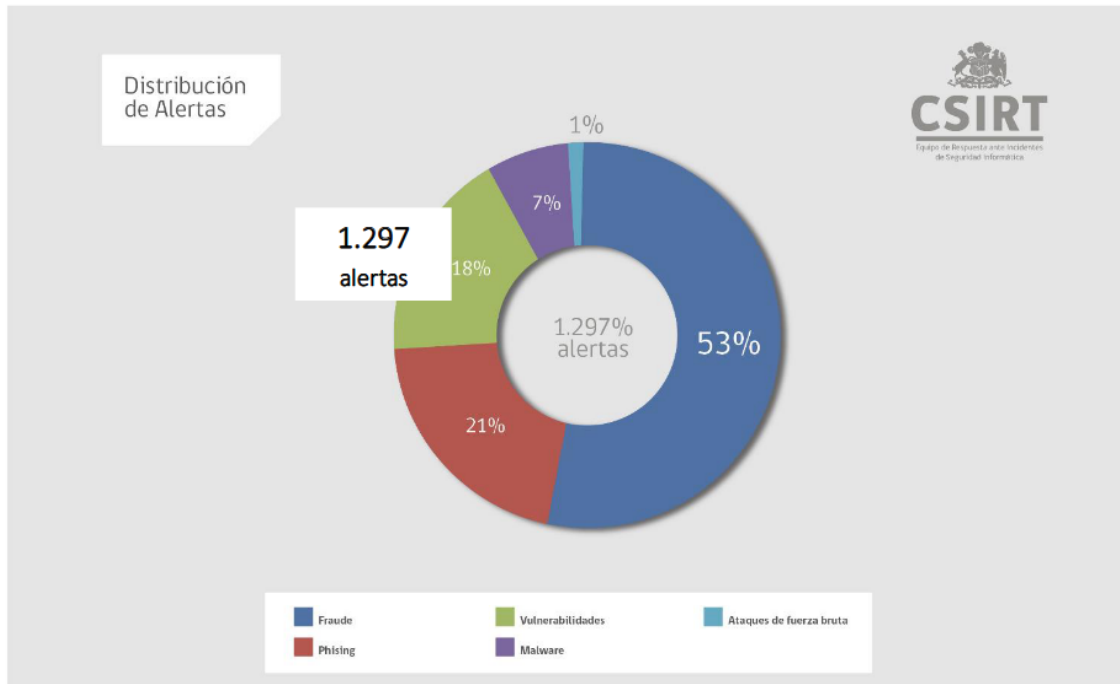


Figura 2: Alertas informadas a la ciudadanía por medio del CSIRT. Fuente: CSIRT Chile [4]

Además, como se observa en la [Figura 3](#), en el mismo tercer trimestre del 2020, el SaaS y sitios *webmail* fueron los objetivos más frecuentes para el *phishing* con el 31.4% del total, seguido por las instituciones financieras con un 19.2 %.

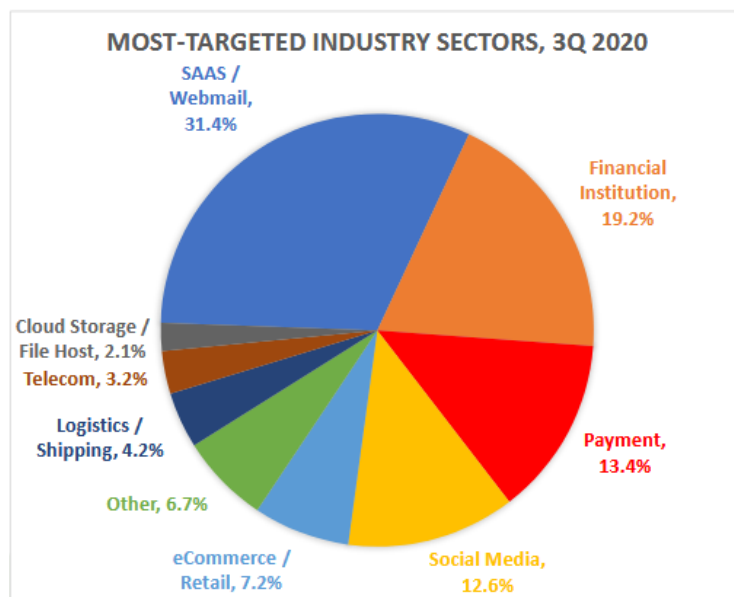


Figura 3: Sectores de la industria más atacados, tercer trimestre 2020. Fuente: APWG

Las fases del proceso de phishing son las siguientes [5] :

1. Preparación del ataque
 - a. Selección del medio de comunicación y dispositivos: generalmente se usa el email como medio, sin embargo se ha visto recientemente el uso de *smishing* (*phishing* por SMS) y *vishing* (*phishing* por llamada telefónica).
 - b. Selección de la técnica: existen muchas técnicas de *phishing*, pero generalmente se clasifican en dos tipos, por un lado los *Fake Websites* y *Email Spoofing* (uso remitente falso para divulgar una página web falsa), y por otro lado los relacionados al *Cross Site Scripting* (inyección de código malicioso), *Malware Phishing* (implantación de *malware* por medio de un descargable), *Key Loggers* (*softwares* que registran pulsaciones del teclado), entre otros [6].
 - c. Preparación del material: se busca de forma manual o por medio de kits de *phishing*. Diseño de páginas web, plantillas de correo y scripts son ejemplos de este material. En la [Figura 4](#) y [Figura 5](#) se muestran una plantilla de correo y una página web de ejemplo (comúnmente llamada *landing page*) usada para un ejercicio de *phishing*.
2. Ejecución del ataque
 - a. Distribución del material: se realiza el envío a una o más víctimas.
 - b. Recolección de datos: dependiendo la técnica utilizada y los recursos con los que se cuente, se recogen los resultados a partir de la interacción de la víctima con el material enviado.
 - c. Penetración a recursos: dependiendo de la técnica, se realiza la inyección de scripts o malware para comprometer los sistemas.
3. Aprovechamiento de los resultados del ataque:
 - a. En esta última etapa se usan los datos o recursos penetrados para la actividad que el atacante considere.

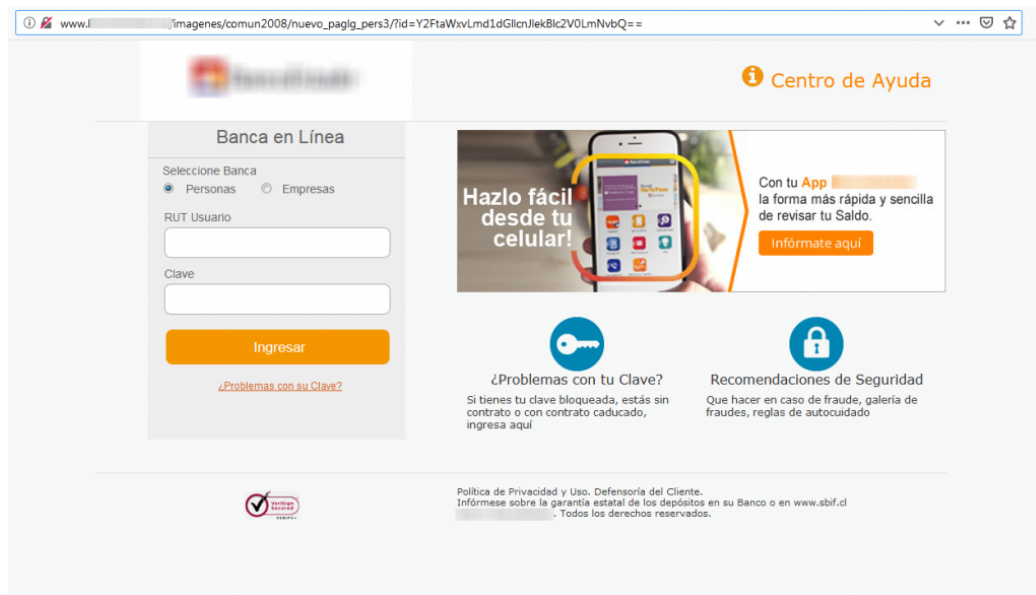


Figura 4: Ejemplo de *landing page* de *phishing*. Fuente: WeLiveSecurity [7]

From: mensajeria@...cl <mensajeria@...cl>
Sent: miércoles, 13 de marzo de 2019 8:04 a. m.
To: [REDACTED]
Subject: [IMPORTANTE] Clave de Transferencia Bloqueada. - (255617475871)

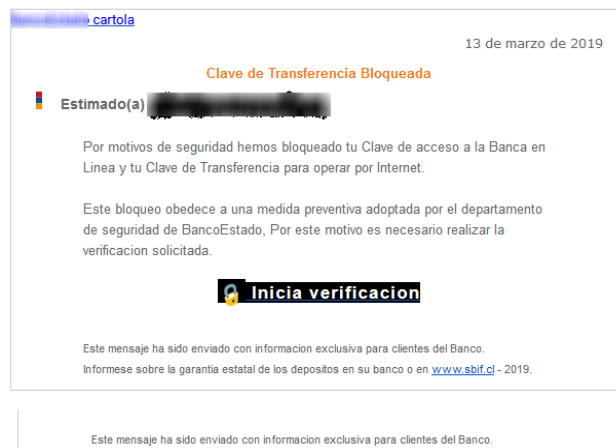


Figura 5: Ejemplo de correo de *phishing*. Fuente: WeLiveSecurity [7]

Puesto que está en riesgo la salud de los negocios, debido a las amenazas de los fraudes a través de *phishing*, es que se ha generado un interés mucho mayor en la ciberseguridad en las organizaciones. Educar y poner a prueba al personal mediante el lanzamiento de campañas de *phishing* es una de las formas más comunes para mitigar los riesgos de estas

prácticas, ya que en la mayoría de los casos, el eslabón más débil en un sistema de seguridad es una persona que no verifica el origen de un correo electrónico malicioso.

1.2 La Empresa y su desafío

El desafío, presentado en el PMM 2020, fue propuesto por una empresa especializada en ciberseguridad que opera a nivel internacional, de ahora en adelante “La Empresa” o la contraparte, la cual entrega servicios y soluciones, de acorde a su rubro, dentro de los que se pueden rescatar para el desarrollo de esta memoria:

- Formación: la Empresa proporciona, a organizaciones y su personal, conocimientos sobre la seguridad y ciberinteligencia, a través de capacitaciones y workshops.
- Ingeniería social: la Empresa proporciona servicios que incluyen campañas de *phishing* simuladas, con el fin de entrenar al personal de sus clientes y que se pueda medir el nivel de concientización en ciberseguridad.

La Empresa pretende proveer a las organizaciones un programa de concientización (*awareness*) en ciberseguridad, en el que se incluya las campañas de *phishing* (y otras variantes) simuladas y la formación a través de campañas educativas.

1.3 Problemas y oportunidades

En esta sección se analizan las problemáticas y oportunidades, con el fin de que posteriormente se proponga una solución que sirva como parte de un programa de concientización en la ciberseguridad.

A partir de la entrevista con la contraparte del desafío, y en relación a los servicios de ingeniería social y formación que entregan se puede decir que:

- Actualmente, lleva adelante las campañas de *phishing* simuladas por medio de un sistema interno, el cual se configura de manera manual utilizando los datos que reciba por parte de la Organización que haya contratado el servicio. Al no ser un sistema abierto o transparente, la Organización no está en conocimiento del desarrollo de las campañas hasta el final de ella cuando recibe un informe escrito con los resultados resumidos.
- Lo anterior, genera muchas veces que el Cliente pierda interés en los resultados, o que pierda confianza en lo que le están entregando como retroalimentación. Esto se traduce en que la Organización no logre la mejora continua a nivel de concientización en ciberseguridad.
- En cuanto a formación, no hay un canal estándar para la difusión de campañas o recomendaciones educativas.
- Se identifica una oportunidad para automatizar o mejorar la entrega de estos servicios de ingeniería social que provee La Empresa, de tal manera que se puedan centralizar algunos procesos como son las campañas educativas y entrenamiento por medio de campañas de *phishing*.

- Se identifica una oportunidad para mejorar la experiencia de las Organizaciones durante el lanzamiento de campañas, y a su vez del proceso mismo de concientización en ciberseguridad.

En la [Tabla 1](#), se resumen los actores identificados en este desafío y sus necesidades.

Tabla 1: Actores identificados. Fuente: Equipo Multidisciplinario

	Actores	
	La Empresa	Organizaciones
¿Quién(es) es(son)?	Una empresa especializada en ciberseguridad, proveedora de servicios relacionados al área.	Organizaciones especialmente del rubro bancario o financiero.
Necesidades	1. Facilitar la gestión del servicio de ingeniería social. 2. Disminuir el trabajo manual en la entrega de los servicios. 3. Centralizar los procesos de las campañas de awareness.	1. Comprobar si sus colaboradores/personal están preparados ante amenazas cibernéticas. 2. Educar en ciberseguridad a su organización.

1.4 Objetivos

1.4.1 Objetivo general

OG - Generar un sistema de autogestión de campañas de ingeniería social y despliegue de información sobre los resultados obtenidos en ellas, que permita a sus usuarios tomar acciones correctivas.

1.4.2 Objetivos específicos

OE1 - Comprender el proceso de concientización de la ciberseguridad dentro de la empresa y reconocer las soluciones actuales para resolver la problemática.

OE2 - Diseñar el sistema de autogestión de campañas de *phishing*, definiendo los requerimientos a satisfacer, y su arquitectura.

OE3 - Desarrollar una aplicación web para usuario Cliente que le permita gestionar una

o más campañas de *phishing*.

OE4 - Desarrollar una aplicación web para los administradores de la plataforma, que permita llevar de manera fácil la gestión del servicio de *phishing*.

En el [Anexo D](#), se muestra en detalle el plan de trabajo de acuerdo a los objetivos planteados.

CAPÍTULO 2: MARCO CONCEPTUAL

2.1 Estado del Arte: Soluciones existentes

Es importante conocer las soluciones existentes en el mercado que ayudan a concientizar usando servicios de ingeniería social. Dentro de las cuales se encuentran:

1. NIVEL4 - Phishing Live Monitor¹

Nivel 4 es una empresa de origen chileno que trabaja en el ámbito de la ciberseguridad, y que ofrece un amplio conjunto de servicios que incluyen soporte tecnológico externo, servicios administrados, herramientas de software, pruebas de penetración, auditoría de sistemas, análisis de vulnerabilidad y consultoría.

La herramienta Phishing Live Monitor que provee Nivel 4, permite visualizar la ejecución de una campaña de *phishing* en tiempo real, monitoreando el comportamiento de los usuarios, a través de diversas métricas, entre las cuales están: el número de correos enviados y por enviar; los usuarios que han leído y abierto el correo malicioso, cantidad de usuarios que han caído en el *phishing* y que han ingresado datos a los formularios, entre otras [8].

2. Oznet Cybersecurity - Concientización de Seguridad

Oznet Cybersecurity es una empresa chilena que ofrece servicios y soluciones de ciberseguridad ofensiva como, por ejemplo, hackeo ético, análisis de vulnerabilidades, red team, ingeniería social; y por otro lado ciberseguridad defensiva con servicios de detección de ataques en tiempo real, disponibilidad y rendimiento de redes de TI, monitoreo antifraude, *blue team*, programa de concientización de seguridad, inteligencia de amenazas, entre otros.

El servicio de concientización de seguridad ofrece pruebas de vulnerabilidad a través de *phishing*. Como destacan, su servicio funciona por medio de estas etapas: diseño de campaña, envío de prueba, carga de base de datos, envío de campaña, y una aplicación para revisar métricas [9].

3. KnowBe4 - Security Awareness Training

Knowbe4 es una empresa estadounidense que entrega servicios de entrenamiento de concientización en seguridad TI y simulaciones *phishing*.

Su principal producto es el Security Awareness Training Program, que consta de tres módulos importantes: Entrenamiento, que incluye contenido educativo;

¹ <https://www.phishingtest.cl/>

Phishing que incluye creación de campañas; y Reportería que provee métricas de la efectividad del programa [10].

4. Rhino Security Labs - Email Phishing Assessment

Rhino Security Labs es una empresa ubicada en Seattle, Estados Unidos, dedicada a la evaluación de seguridad y pruebas de penetración, con enfoque en *pentesting* en la nube (AWS, GCP, Azure), *pentesting* de redes, *pentesting* de aplicaciones web y *phishing*.

Dentro de sus servicios ofrece campañas de ingeniería social aplicando pruebas de *phishing* de correo electrónico tradicionales, interacciones de *vishing* o evaluaciones en el sitio e intentos de acceso a edificio físico, a través de ingenieros sociales entrenados [11].

2.1.1 Evaluación de las soluciones existentes

Del estudio de soluciones existentes se puede decir que:

- Tanto la plataforma ‘NIVEL4 - Phishing Live Monitor’ como el servicio que ofrece Oznet Cybersecurity se restringe a solo ser un dashboard, por lo que es muy limitado en cuanto a la autogestión y planificación de campañas. Las métricas que provee son las estándar para analizar el comportamiento del público objetivo.
- La plataforma KnowBe4 es una herramienta ampliamente utilizada por lo que es una buena referencia para la solución a desarrollar. Dado que es programa Norteamericano tiene sus limitaciones, por lo que sus templates o plantillas de *phishing* están orientadas a otro tipo de público objetivo.
- A nivel internacional hay un gran número de empresas que ofrecen servicios de entrenamiento y concientización de ciberseguridad, no así a nivel local, donde las opciones y funcionalidades que proveen se reducen.

2.2 Herramientas de trabajo

A continuación, se detallan conceptos y tecnologías que sirven para comprender la solución que se propone en el capítulo 3. En primer lugar, se definen los *frameworks* a utilizar para el desarrollo web (*backend* y *frontend*). En segundo lugar, se describe *Gophish* como el motor de campañas de *phishing* a utilizar. En tercer lugar, se describen los servicios cloud utilizados para la arquitectura de la aplicación. Finalmente, se describe Postman para las pruebas de API.

2.2.1 Frontend

Para el desarrollo *frontend*, es decir, la capa de presentación de las aplicaciones web, existen diversas opciones, sin embargo, en la actualidad es común y recomendable utilizar un *framework Javascript* ya que proveen: mantenibilidad, separa la aplicación en componentes reusables; separación de intereses, se preocupan solo de tomar información y mostrarla de forma intuitiva y eficiente; rapidez, proveen de código *boilerplate* o repetitivo sin tener que preocuparse de aquello; colaboración, permiten a desarrolladores mantener la aplicación debido a que tiene patrones de diseño similares; comunidad, son muy utilizados y populares entre los desarrolladores [12]. Dentro de las opciones a *frameworks* están:

- React.js²: es una biblioteca Javascript de código abierto para crear interfaces de usuario. Su objetivo es facilitar el desarrollo de aplicaciones SPA. Es mantenido por Facebook y la comunidad de software libre.
- Vue.js³: es un framework de JavaScript de código abierto y creado por Evan You. Permite la creación de interfaces de usuario y aplicaciones SPA.
- Angular⁴: es un framework para aplicaciones web desarrollado en TypeScript, de código abierto, mantenido por Google, que se utiliza para crear y mantener aplicaciones web SPA.

Comparativa

Los tres anteriores frameworks están dentro de los más populares en 2020 según la encuesta de Desarrolladores realizada por Stackoverflow [13].

En la [Tabla 2](#), confeccionada por Voutilainen [14] y adaptada con los criterios más relevantes, se califica entre 1 y 3 según la importancia del factor en la elección del *framework*. Cada factor se describe a continuación:

Tabla 2: Evaluación de *frameworks* de *frontend*. Fuente: Adaptado desde Voutilainen [14]

Factor evaluado	React	Angular	Vue
Components	2	2	2
Startup Performance and buildup times	2	3	2
Scripting and rendering	2	3	3
Platform support	2	2	2
External Libraries and User Interfaces	3	2	2

² <https://es.reactjs.org/>

³ <https://vuejs.org/>

⁴ <https://angular.io/>

Documentation and Community Support	2	2	3
Learning Curve and Developer Experience	2	1	3
Popularity and Future	2	3	2
Total	17	18	19

1. *Components*: Los "Componentes" son los objetos en los cuales se agrupan gran parte de las herramientas definidas del framework. Se evalúa facilidad de uso, las funcionalidades y la sintaxis de los componentes.
2. *Startup performance and build times*: Este punto habla del rendimiento de iniciado y tiempos de carga.
3. *Scripting and rendering*: En este punto se hace hincapié en la creación y manejo de scripts, y como se ven afectados estos aspectos según distintas operaciones DOM a una página de prueba que muestra registros y que el usuario puede crear, editar o borrar, entre otras.
4. *Platform support*: Se evalúa el soporte a los navegadores web por parte de los frameworks.
5. *External libraries and user interface components*: En el contexto de las herramientas basadas en Javascript, se pueden incluir bibliotecas externas para agregar funcionalidades a la plataforma, algunas son *ad-hoc* para los frameworks en específico. Se mide el estado de desarrollo de herramientas externas y la envergadura de las funciones de cada *framework*.
6. *Documentation and community support*: el autor evalúa la facilidad de acceso a la información en la documentación, su rápido y fácil entendimiento y la actividad de la comunidad que soporta bugs y preguntas.
7. *Learning curve and developer experience*: Se toma en cuenta distintas percepciones medidas por encuestas respecto de qué tan "pesada" es la curva de aprendizaje de cada framework, y cómo fue el proceso de aprender dicha tecnología.
8. *Popularity and future*: Se mide mediante encuestas, la presencia de los frameworks en el estado del arte, la industria y sus proyecciones a futuro.

Si bien tanto Angular como Vue tienen buenas calificaciones, para el desarrollo de esta memoria lo que contribuye a que se use determinado *framework* es su curva de aprendizaje, dado el tiempo para llevar adelante el proyecto, además de la documentación y comunidad que esta posea. Por lo que Vue.js es una buena alternativa para generar el prototipo web.

2.2.2 Backend

Para el *backend*, o sea, la capa de lógica de negocios de nuestra plataforma, ocurre exactamente lo mismo que con el *frontend*. Debemos elegir el *framework* que mejor se adapte a nuestras necesidades para lograr los objetivos.

Dentro de las herramientas más utilizadas para *backend* se encuentran:

- Django⁵: es un framework de desarrollo web *open-source*, escrito en lenguaje Python, que utiliza el patrón de diseño Modelo Vista Controlador (MVC).
- Laravel⁶: es un framework *open-source* creado en 2011 para desarrollar aplicaciones y servicios web con lenguaje PHP.
- Ruby On Rails⁷: es un framework de aplicaciones web *open-source* escrito en lenguaje Ruby, que sigue el patrón Modelo Vista Controlador (MVC).
- Spring⁸: es un framework para el desarrollo de aplicaciones y contenedor de inversión de control, *open-source* para la plataforma Java.

Comparativa

Los cuatro frameworks anteriores son buenas opciones para comenzar el proyecto, sin embargo se analiza en la literatura para tomar una mejor decisión.

En la [Tabla 3](#), se resumen los criterios que se consideran más relevantes para la elección del *framework*.

Los criterios fueron extraídos de Kaluza et al [15], se califica con 0 (si no cumple), 0.5 (si cumple parcialmente), 1 (si cumple). La explicación de cada uno está descrito posteriormente.

Tabla 3: Evaluación de *frameworks* de *backend*. Fuente: Adaptado de Kaluza et al. [15]

Criterion	Laravel	Ruby On Rails	Django	Spring
Basic criteria				
Code generator	1	1	1	1
Project Health	1	1	1	1
Developer's perception	1	1	1	1

⁵ <https://www.djangoproject.com/>

⁶ <https://laravel.com/>

⁷ <https://rubyonrails.org/>

⁸ <https://spring.io/>

Developer's availability	0.5	0.5	0.5	1
Testing	1	1	1	1
Validation	1	1	1	1
Licensing	1	1	1	1
The possibility of integration with third-party solutions	1	1	1	1
Plugins/add-ons	1	1	1	0
Additional criteria				
Customized for large applications	0	0	1	1
High scalability	0	0	1	1
Adapted to beginners	1	1	1	0
Good for businesses applications development	0	0	1	1
Rapid prototype development	1	0	1	0
Star Rating on GitHub	1	0.5	0.5	0.5
The number of Stack Overflow tags	0.5	1	0.5	0.5
Total	12	11	14.5	12

1. *Code generator*: Se evalúa si el framework tiene la facultad de generar código inteligente para construir vistas, controladores, rutas, entre otros.

2. *Project Health*: Se evalúa si el *framework* posee buenas fuentes de información, documentación de alta calidad y gran número de referencias en Stack Overflow.
3. *Developers perception*: Se evalúa la satisfacción de los desarrolladores con el *framework*.
4. *Developers availability*: Se evalúa de acuerdo al número de desarrolladores que han listado el *framework* en su perfil de LinkedIn.
5. *Testing*: Se evalúa si el soporte de pruebas está embebido en el *framework*
6. *Validation*: Se evalúa si el *framework* soporta validación de datos.
7. *Licensing*: Se evalúa si el *framework* no limita a la aplicación a desarrollar.
8. *The possibility of integration with third-party solutions*: Se evalúa si el *framework* es capaz de integrar una o más partes de la aplicación con soluciones de terceros.
9. *Plugins/add-ons*: Se evalúa si el *framework* está disponible para configurar *plugins* o extensiones.
10. *Customized for large applications*: Se evalúa si el *framework* se adapta a aplicaciones grandes.
11. *High scalability*: Se evalúa si el *framework* es altamente escalable.
12. *Adapted to beginners*: Se evalúa si el *framework* es recomendado para principiantes.
13. *Good for businesses applications development*: Se evalúa si el *framework* es recomendado para aplicaciones empresariales.
14. *Rapid prototype development*: Se evalúa si el *framework* es bueno para prototipar de manera rápida el desarrollo.
15. *Star Rating on GitHub*: Se evalúa de acuerdo a la calificación del *framework* en GitHub.
16. *The number of StackOverflow tags*: Se evalúa de acuerdo al número de etiquetas en StackOverflow.

De acuerdo a la evaluación y considerando en la comparativa anterior que alcanza buena calificación global y en criterios como *Project Health*, *Rapid Prototyping*, *Good for Business applications development*, *High Scalability*, *Adapted for beginners*, es que se decide por utilizar Django como el *framework* para Backend.

Finalmente, se puede destacar que todos estos *frameworks* modernos analizados poseen distintas formas para mitigar posibles ataques de seguridad. Por ejemplo, Django se preocupa de la inyección de código SQL incorporando una serie de funcionalidades para abstraer las consultas SQL. Además, provee de funcionalidades para manejar la autenticación de usuarios y permisos de la aplicación [16]

2.2.3 Gophish

Gophish⁹ es un entorno de trabajo, escrito en Go, de código abierto y lanzado en 2016, que permite la simulación de ataques de *phishing*. La plataforma tiene las siguientes funcionalidades:

⁹ <https://getgophish.com/>

1. Usuarios y Grupos: permite la gestión del público objetivo a través de grupos.
2. Plantillas de Correo: permite la creación de plantillas de correo para el *phishing*.
3. *Landing Pages*: permite la creación de las páginas web que son parte del *phishing*.
4. *Sending Profile*: permite configurar el servidor de correo que permite el envío masivo.
5. Lanzamiento de campañas: permite la creación de campañas de *phishing*.
6. Resultados: permite acceder a resultados en tiempo real de las campañas.

Además, provee de un cliente escrito en Python que permite interactuar con la API REST de Gophish, de tal forma de automatizar y usarlo como 'motor' de las campañas de *phishing*

2.2.4 AWS

AWS¹⁰ es una colección de servicios *cloud* ofrecidos por Amazon, el cual se lanzó en 2006. Brinda servicios en forma de bloques, estos bloques se pueden utilizar para crear e implementar cualquier tipo de aplicación en la nube.

Estos servicios o componentes básicos están diseñados para funcionar entre sí y dan como resultado aplicaciones sofisticadas y altamente escalables. Dentro de los servicios se encuentran: de cómputo, almacenamiento, base de datos, migración, red y distribución de contenidos, herramientas de gestión, seguridad y mensajería [17].

- Amazon RDS: es un servicio web que facilita la configuración, el funcionamiento y el escalamiento de una base de datos relacional en AWS Cloud. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional estándar y se ocupa de las tareas de administración de bases de datos comunes [18]
- Amazon S3: Amazon Simple Storage Service es un servicio de almacenamiento de objetos. Posee una interfaz de servicios web simple que sirve para almacenar y recuperar cualquier cantidad de datos, en cualquier momento y desde cualquier parte de la web. [19]

2.2.5 Postman

Postman¹¹ es una herramienta que permite crear peticiones sobre APIs para probar o monitorear su funcionamiento.

¹⁰ <https://aws.amazon.com/es/>

¹¹ <https://www.postman.com/>

Postman ofrece un conjunto de utilidades para poder gestionar las APIs de una forma más sencilla, entre las que se encuentran: agrupar peticiones en colecciones, entorno colaborativo, establecer variables de entorno, entre otros [20]

CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

3.1 Descripción de la solución

La solución propuesta consiste en una plataforma web que permita a organizaciones autogestionar campañas de *phishing*.

Con esta solución una organización podría comenzar un período de envío masivos de *phishing* a su personal con el fin de ponerlos a prueba, conocer cómo se comportan y a partir de los resultados poder tomar acciones que refuercen las debilidades en ámbitos de ciberseguridad.

3.1 Usuarios del sistema

En la [Tabla 4](#) se muestra el detalle para los dos usuarios identificados, La Empresa, y el Usuario Cliente. En primer lugar, se describe por qué para ese usuario la solución le beneficiaría. Por último, se describen las fases generales o las actividades que realizaría el usuario con la plataforma.

Tabla 4: Perfiles de Usuario. Fuente: Elaboración Propia

	Usuarios	
	Usuario La Empresa	Usuario Organización Cliente
¿Por qué utilizaría la solución?	1. Fácil administración de cuentas del cliente. 2. Centraliza los procesos de campañas de awareness. 3. Ahorraría tiempo y esfuerzo durante la entrega de los servicios.	1. Porque permite educar y poner a prueba a sus colaboradores, de tal manera de evitar fraudes o ataques informáticos a futuro que pongan en riesgo su negocio.
Fases Generales (cuáles son sus funciones en la plataforma)	1. Alimentar la plataforma con templates de phishing y contenido educativo. 2. Enrolamiento de nuevos clientes. 3. Inspección de actividad de sus clientes. 4. Inspeccionar resultados de campañas.	1. Ingresar datos de colaboradores y de la organización. 2. Lanzar Campañas de Phishing. 3. Visualizar resultados de campañas. 4. Revisar sugerencias de acciones educativas.

Como se ha mencionado, se han identificado 2 usuarios principales. Sin embargo, como se especifica en la [Figura 6](#), el Usuario Cliente se puede descomponer en 3 usuarios dependiendo de los permisos que tendrán en la plataforma y que en la sección 3.2 queda detallado de acuerdo a los requisitos del sistema.

Estos 3 usuarios que descomponen a la Organización Cliente son el Owner (dueño de la cuenta), Admin (administrador de las campañas de *phishing*) y Viewer (puede ver resultados de campañas de *phishing*).

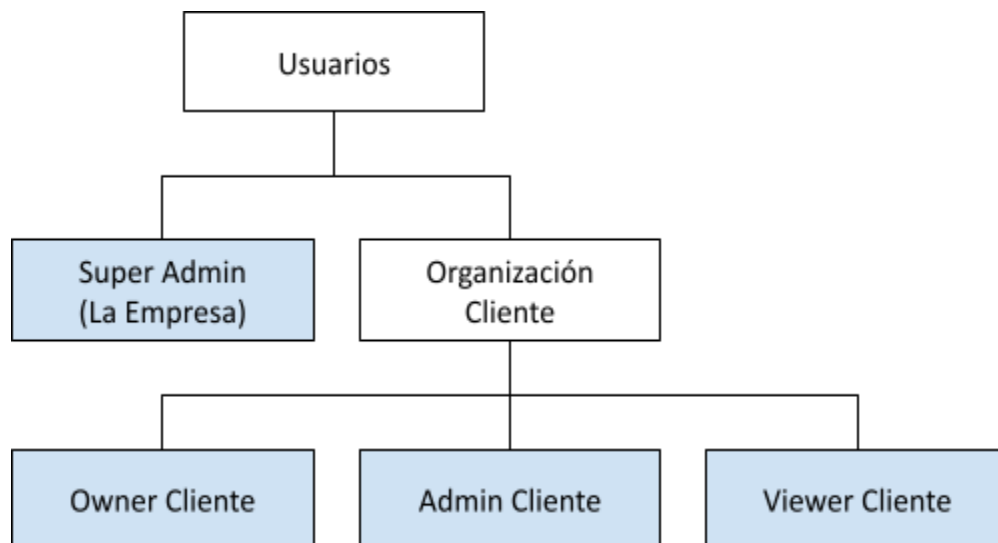


Figura 6: Desglose de usuarios de la plataforma. Fuente: Elaboración Propia

3.2 Requisitos del sistema

A continuación se detallan los requisitos funcionales y no funcionales de la solución, categorizados en distintos módulos de acuerdo a características similares. Se usó como técnica para recopilar estos requisitos la entrevista con la contraparte. Posteriormente se transcribieron los requisitos funcionales en forma de historia de usuario, como una forma de facilitar la lectura entre las partes.

3.2.1 Lanzamiento de campañas

[RF0] Creación de material de campañas de phishing.

- Historia de Usuario: **Como Super Admin, quiero** crear plantillas de correo y *landing page* **para** que las organizaciones lleven adelante campañas con dicho material.

[RF1] Lanzamiento de campañas de *phishing*.

- Historia de Usuario: **Como** Owner Cliente/Admin Cliente, **quiero** lanzar campañas de *phishing* **para** conocer el comportamiento del personal de mi organización y tomar acciones correctivas.

[RF1.1] Información básica de las campañas

- Historia de Usuario: **Como** Owner Cliente/Admin Cliente, **quiero** asignar un nombre de campaña **para** identificarla de mejor manera.

[RF1.2] Público objetivo de las campañas

- Historia de Usuario: **Como** Owner Cliente/Admin Cliente, **quiero** ingresar datos del público objetivo de las campañas **para** establecer los grupos a los cuáles estarán dirigidas las simulaciones.

[RF1.3] Elección de la temática de las campañas

- Historia de Usuario: **Como** Owner Cliente/Admin Cliente, **quiero** elegir dentro de un catálogo la plantilla de correo y landing page **para** definir la temática de la campaña.

[RNF1] El ID de seguimiento a cada usuario no debe ser predecible. Esto quiere decir, que cada objetivo debe tener un ID resultante de una función *hash* criptográfica en la URL del *phishing*, que hace seguimiento de quienes son parte del ejercicio.

3.2.2 Visualización de resultados

[RF2] Visualización en tiempo real

- Historia de Usuario: **Como** Super Admin/Owner Cliente/Admin Cliente/Viewer Cliente, **quiero** acceder y visualizar resultados actualizados en tiempo real de las campañas activas de *phishing* **para** conocer el comportamiento del personal y poder tomar acciones correctivas a tiempo.

[RF3] Contraste de resultados

- Historia de Usuario: **Como** Super Admin/Owner Cliente/Admin Cliente/Viewer Cliente, **quiero** comparar los resultados de una campaña con otras **para** conocer la evolución en el tiempo del personal.

[RF4] Descarga de resultados

- Historia de Usuario: **Como** Super Admin/Owner Cliente/Admin Cliente/Viewer Cliente, **quiero** descargar los resultados de una campaña en formato CSV **para** tener la opción de analizar los datos de otra manera.

[RF5] Filtro de resultados

- Historia de Usuario: **Como** Super Admin/Owner Cliente/Admin Cliente/Viewer Cliente, **quiero** poder filtrar los resultados de las campañas **para** tener criterios más refinados cuando se analice la información.
- Tipos de filtro identificados, por: Nombre, Correo electrónico, Estado de interacción de los colaboradores (por ejemplo: envío de correo, apertura de correo, *click* en el enlace, ingreso de datos), Tiempo (Hora específica de las pruebas y el detalle de avance de estas), Segmentos de la organización y Reincidentes.

[RNF2] Los resultados de las pruebas deben ser mostrados de forma gráfica.

3.2.3 Gestión de usuarios

[RF6] Gestión de organizaciones

- Historia de Usuario: **Como** Super Admin, **quiero** poder crear cuentas de Owner, Admins y Viewers de otras organizaciones **para** tener control sobre las cuentas que usan la plataforma y servicio entregado.

[RF7] Creación de cuentas

- Historia de Usuario: **Como** Owner Cliente/Admin Cliente, **quiero** poder crear cuentas de Admin Cliente y Viewer Cliente para mi organización **para** invitar y dar acceso con privilegios a colaboradores estratégicos.
- Historia de Usuario: **Como** Viewer Cliente, **quiero** poder crear cuentas de Viewer Cliente en mi organización **para** entregar la posibilidad de que otra persona pueda ver resultados de campañas.

[RF8] Perfil de Organización

- Historia de Usuario: **Como** Owner Cliente, **quiero** poder cambiar datos de mi organización y actualizar información de contacto **para** que, cuando se requiera, la comunicación con La Empresa no se pierda.

[RF9] Transferencia de credenciales

- Historia de Usuario: **Como** Owner Cliente, **quiero** transferir mis credenciales **para** ceder el control y acceso al servicio a otro usuario.

[RNF3] La creación de cuentas Admin Cliente o Viewer Cliente debe generar invitaciones por correo electrónico.

3.2.4 Registro de actividad

[RF10] Registro de actividad

- Historia de Usuario: **Como Super Admin, quiero** acceder a un registro de actividad **para** estar al tanto de toda acción que se realice en la plataforma.

3.2.5 Lanzamiento de campañas personalizadas

[RF11] Solicitud de campaña personalizada

- Historia de Usuario: **Como Owner Cliente/Admin Cliente, quiero** generar una solicitud de plantilla de correo y landing page personalizados **para** lanzar una campaña ajustada a las necesidades de la organización
- Historia de Usuario: **Como Super Admin, quiero** responder a las solicitudes de campañas personalizadas **para** para que las organizaciones puedan continuar con el proceso de lanzamiento.

[RNF4] El sistema debe responder a dominios personalizados.

3.2.6 Sugerencias educativas

[RF12] Gestión de contenido educativo

- Historia de Usuario: **Como Super Admin, quiero** poder leer, agregar y editar contenido de campañas educativas **para** mantener informadas a las organizaciones.

[RF13] Acceso a contenido de mi organización

- Historia de Usuario: **Como Owner Cliente/Admin Cliente, quiero** leer los contenidos de las campañas educativas **para** educar en cuanto a ciberseguridad al personal de la organización.
- Historia de Usuario: **Como Owner Cliente/Admin Cliente, quiero** recibir recomendaciones luego de una campaña de *phishing* **para** focalizar los esfuerzos al tomar acciones remediales.

3.2.7 Integración vishing, smishing, phishing por Whatsapp

[RNF5] El sistema debe integrar servicios externos para el lanzamiento de campañas de *smishing*, *vishing* y *phishing* por *Whatsapp*.

3.2.8 Autenticación de dos pasos

[RNF6] El sistema debe permitir la autenticación de dos pasos. Esto, para agregar una capa más de seguridad a la aplicación al momento de loguearse.

3.2.9 Resumen de requisitos

En la [Tabla 5](#), se muestra un resumen de los requisitos considerados en la etapa de diseño de la solución. A su lado, se establece si dicho requisito se desarrollará como parte del prototipo funcional o PMV dado el alcance establecido en la presente memoria.

Tabla 5: Tabla resumen de requisitos por usuario. Fuente: Elaboración propia

Requisito	Prototipo Funcional (Alcance)	Usuario			
		La Empresa	Organización Cliente		
		Super Admin	Owner	Admin	Viewer
[RF0] Creación de material de campañas de phishing.	✓	✓	×	×	×
[RF1] Lanzamiento de campañas de phishing.	✓	×	✓	✓	×
[RF2] Visualización en tiempo real	✓	✓	✓	✓	✓
[RF3] Contraste de resultados.	×	✓	✓	✓	✓
[RF4] Descarga de resultados	×	✓	✓	✓	✓
[RF5] Filtro de resultados	×	✓	✓	✓	✓
[RF6] Gestión de organizaciones	✓	×	×	×	×
[RF7] Creación de cuentas	✓ ¹²	×	✓	✓	✓
[RF8] Perfil de Organización	✓	×	✓	×	×
[RF9] Transferencia de credenciales	×	×	✓	×	×

¹² El desarrollo de este requisito para el prototipo funcional implica la creación de las cuentas con las respectivas credenciales sin considerar el envío de invitación por correo electrónico.

[RF10]	Registro de actividad	x	✓	x	x	x
[RF11]	Solicitud de campaña personalizada	x	✓ ¹³	✓	✓	x
[RF12]	Gestión de contenido educativo	x	✓	x	x	x
[RF13]	Acceso a contenido educativo de mi organización	x	x	✓	✓	✓

3.3 Arquitectura del sistema

La [Figura 7](#) muestra un diagrama de la arquitectura del sistema que se desarrolló para este proyecto de memoria.

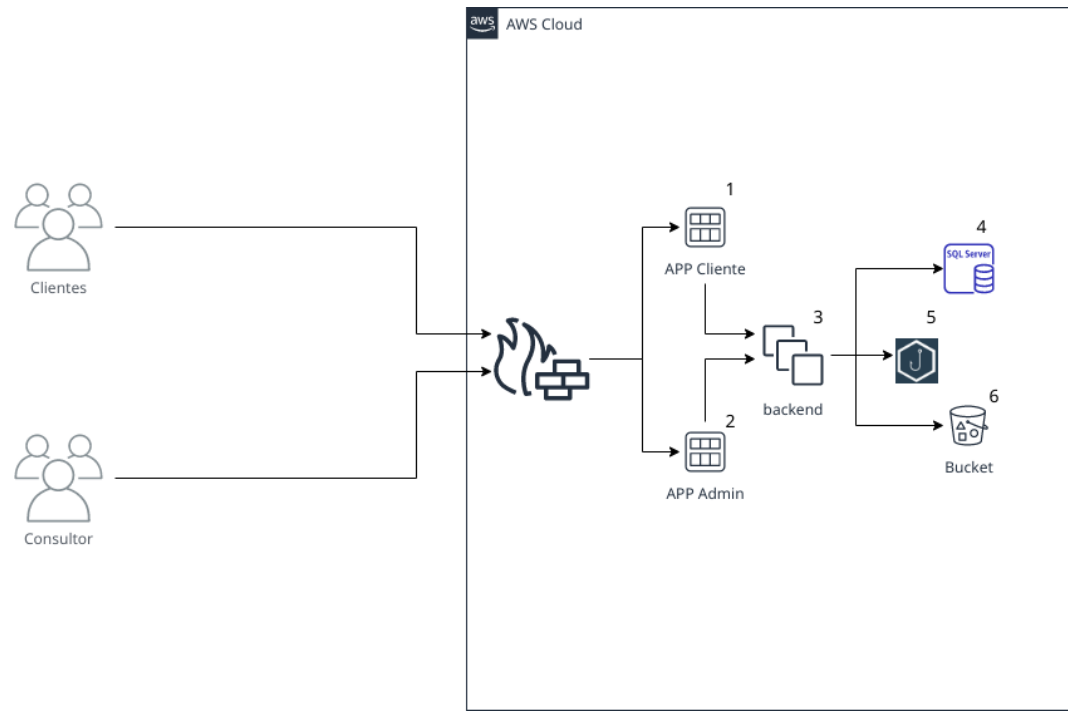


Figura 7: Diagrama de arquitectura. Fuente: Elaboración Equipo Multidisciplinario.

¹³ Para el usuario Super Admin implica responder a la solicitud de campaña personalizada.

3.3.1 Descripción de componentes y tecnologías

A continuación se describe en detalle cada uno de los componentes de la arquitectura del sistema expuesto en la [Figura 7](#).

1. **App Cliente:** aplicación desarrollada con el *framework* Vue.js que es la interfaz usuaria de cara al Usuario Cliente en donde se realizan y se gestionan las campañas de *phishing*.
2. **App Super Admin:** aplicación desarrollada con el *framework* Vue.js que es la interfaz usuaria de cara al administrador (La Empresa) donde se realiza la gestión de usuarios y administración general de la plataforma.
3. **Backend:** aplicación Django que realiza la lógica de negocios de todo el sistema, a modo de API REST.
4. **Amazon RDS:** servicio AWS, que funciona como base de datos relacional asociada al *backend*.
5. **Gophish:** instancia del motor de *phishing*. A través de la API REST que provee es posible crear grupos objetivos, crear *landing pages*, crear plantillas de correo, configurar SMTP, lanzar campañas, ver resultados, entre otros.
6. **Amazon S3:** servicio AWS, el cual funciona a modo de repositorio de archivos estáticos, como imágenes o contenido multimedia.

3.3.2 División del trabajo

Si bien todo el equipo multidisciplinario trabajó en la definición de la problemática y el diseño de la solución, una vez desarrollada la arquitectura del sistema se definieron los roles para la implementación del prototipo o PMV, los cuales son:

- José Catalán: estudiante de Ingeniería Civil Telemática, desarrollo del *backend* (Componente 3) e interacción con sus componentes.
- Matías Ramírez: estudiante de Ingeniería Civil Informática, desarrollo del *frontend* de la aplicación Cliente (Componente 1)
- Esteban Jara: estudiante de Ingeniería Civil Telemática, desarrollo del *frontend* de la aplicación Super Admin (Componente 2)

3.5 Diseño de interfaces usuarias

Las aplicaciones web necesitan de un proceso de diseño antes de comenzar a programar. Además, es importante poder reconocer y validar con los usuarios que las interfaces cumplan con sus necesidades.

En primer lugar, se inició reconociendo las principales vistas o interfaces usuarias mediante el diseño de un diagrama funcional que mostrara, mediante un flujo, las principales funciones de cada usuario en su aplicación (ver [Anexo A](#) y [Anexo B](#)).

En segundo lugar, se llevó a cabo un proceso de *sketching* que permitiera, de manera ágil, dibujar bosquejos de cada una de las vistas descritas en el diagrama funcional, para lo cual se utilizó la herramienta colaborativa *InVision*¹⁴. Como se ve en la [Figura 8](#), esto permitió que a través de sesiones cortas, se pudiera recibir el feedback de los usuarios del sistema e ir recogiendo nuevos aspectos, los cuales se agregaban en notas adhesivas.

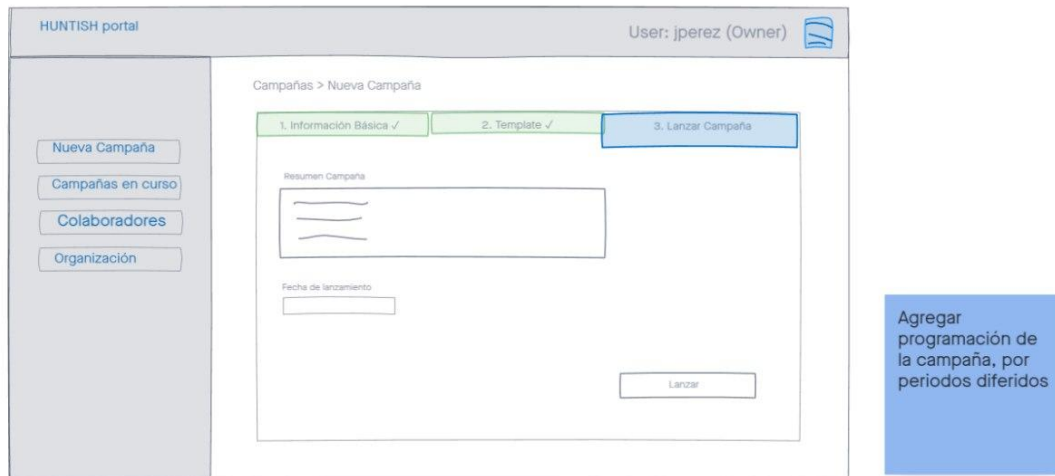


Figura 8: *Sketching* y retroalimentación de parte de La Empresa. Fuente: Equipo Multidisciplinario.

En tercer lugar, el output del *sketching* generó el input para el proceso de creación de *mockups* mediante la plataforma *Adobe XD*¹⁵. Los *mockups* intentan mostrar el diseño avanzado o final de una aplicación, además son artefactos que permiten la interacción con los clientes y *stakeholders*. En la [Figura 9](#), se muestra un *mockup* de la plataforma, específicamente la vista de campañas de un cliente, en donde se aprecia además los resultados de una campaña seleccionada.

¹⁴ <https://www.invisionapp.com/>

¹⁵ <https://www.adobe.com/la/products/xd.html>



Figura 9: Mockup plataforma en Adobe XD. Vista de campañas. Fuente: Equipo Multidisciplinario.

En los siguientes links se pueden encontrar los mockups finales de la aplicación [Cliente](#) y [Super Admin](#).

CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN

4.1 Prototipo funcional

4.1.1 Contexto general del prototipo

Para llevar adelante la etapa del prototipo funcional, y dado el periodo disponible para desarrollarlo (alrededor de 1 mes), se establecieron aquellos requerimientos mínimos que debía satisfacer, considerando que el núcleo o las funcionalidades más importantes de la plataforma son el lanzamiento de una campaña de *phishing* y la posterior visualización de resultados (ver [Tabla 5](#)). Así, el prototipo funcional considera lo siguiente:

1. App Super Admin La Empresa:
 - Login: El Super Admin puede loguearse con sus credenciales en el sistema. Como precondition, la cuenta de La Empresa debe estar creada.
 - Creación de organizaciones y Owner respectivo: El Super Admin puede crear una organización cliente, y como resultado, disponer del Owner asociado. A su vez, es posible crear otros usuarios dependientes de esta organización, asignándoles el rol de Admin o Viewer.
2. App Cliente:
 - Login: Un cliente (Owner/Admin) puede loguearse usando las credenciales creadas por La Empresa.
 - Creación de grupos objetivos: Un cliente puede crear un grupo de objetivos, a partir de un archivo CSV.
 - Creación y lanzamiento de una campaña de *phishing*: Un cliente puede lanzar una campaña, ingresando el nombre de esta, eligiendo los grupos destinatarios, la configuración SMTP (por defecto) y el material asociado como *landing page* y plantilla de correo.
 - Visualización de resultados: Un cliente puede ver los resultados instantáneos que genere la campaña que ha sido creada.

4.1.2 Cumplimiento de requisitos

Para verificar el prototipo funcional, se comprueba que se cumplan con los requisitos anteriormente establecidos en el alcance de la memoria. Para cada requisito se hicieron pruebas en la aplicación del Usuario Cliente, por medio de la cuenta Owner que posee todos los privilegios de ese usuario, a excepción del RF0 y del RF6 (requisito relativo a La Empresa).

1. **[RF0]** Creación de material de campañas de phishing.

Para cumplir este requisito se probó realizando una petición POST a la base de datos mediante la herramienta POSTMAN, la cual permitió cargar el material

correspondiente a *landing pages* y plantillas de correo. Dicho material luego queda disponible en el lanzamiento de campañas. En la [Figura 10](#) se aprecia la estructura de envío del material a cargar.

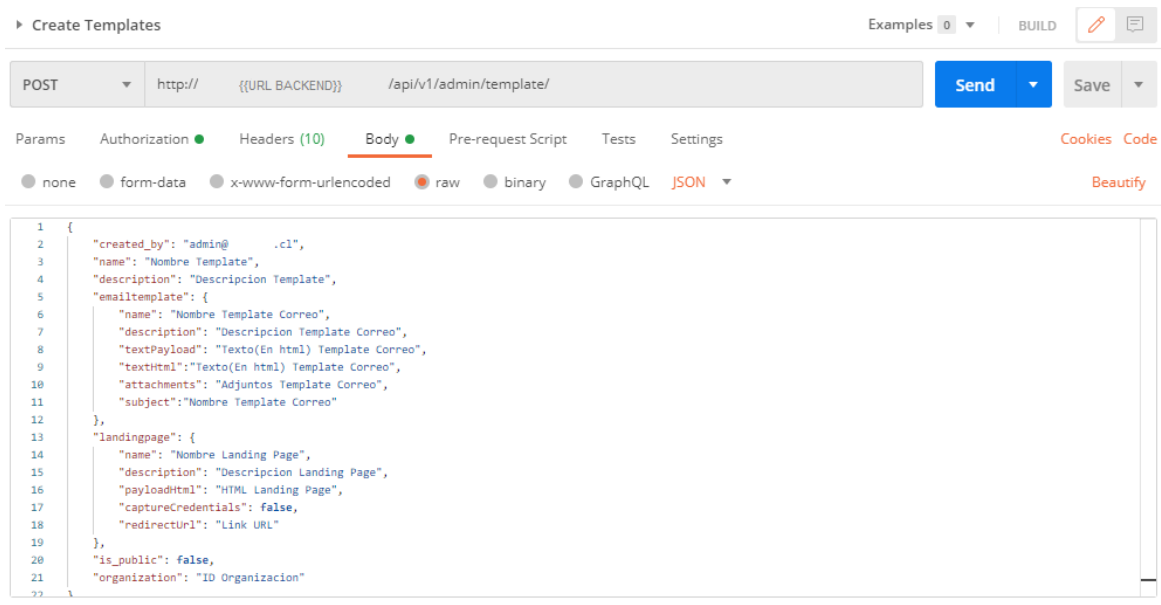
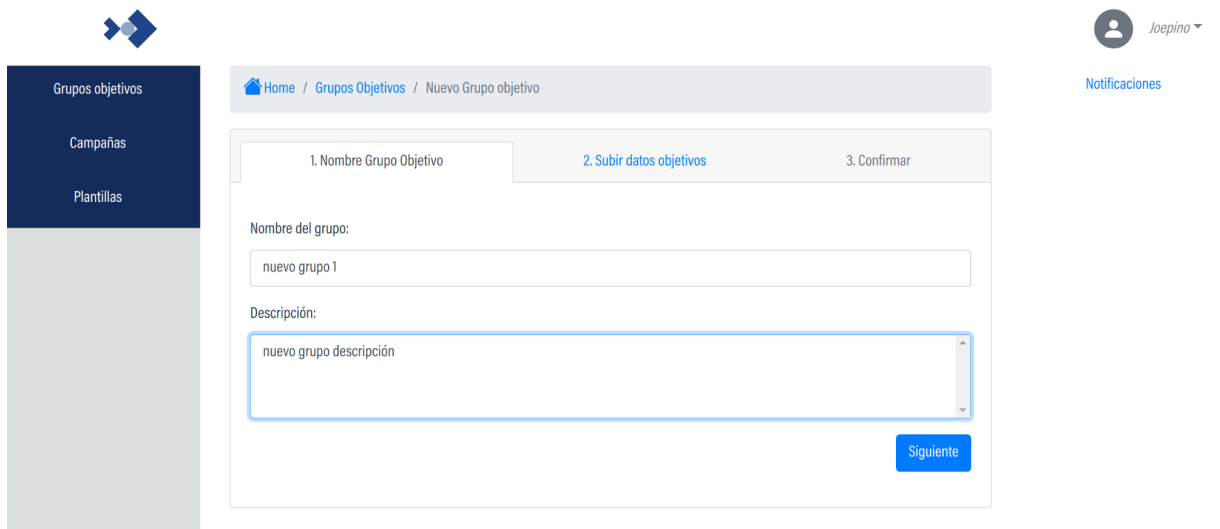


Figura 10: Estructura de carga de material de *phishing* por medio de POSTMAN. Fuente: Equipo Multidisciplinario.

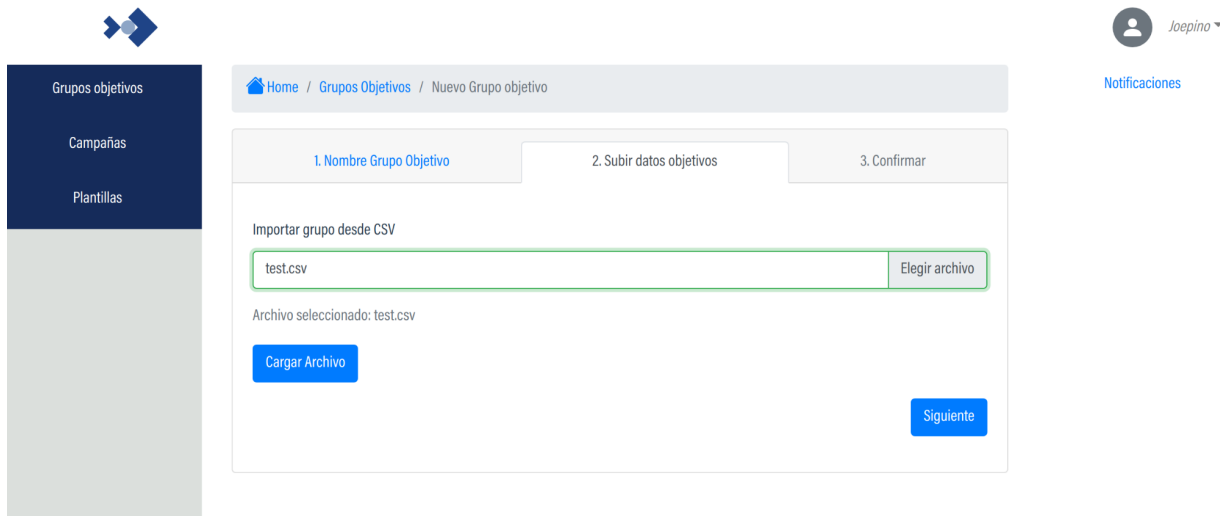
2. [RF1] Lanzamiento de campañas de phishing.

Para cumplir este requisito, en primer lugar se necesita la creación de los grupos objetivos, por medio de un formulario presente en la plataforma. En la [Figura 11](#), [Figura 12](#) y [Figura 13](#) se aprecia el flujo del formulario.



The screenshot shows a web application interface for creating a new objective group. On the left is a dark blue sidebar with a logo and three menu items: 'Grupos objetivos', 'Campañas', and 'Plantillas'. The top right shows a user profile icon labeled 'Joepino' and a 'Notificaciones' link. The main content area has a breadcrumb trail: 'Home / Grupos Objetivos / Nuevo Grupo objetivo'. Below this is a tabbed interface with three tabs: '1. Nombre Grupo Objetivo' (selected), '2. Subir datos objetivos', and '3. Confirmar'. The first tab contains a form with two fields: 'Nombre del grupo:' with a text input containing 'nuevo grupo 1', and 'Descripción:' with a text area containing 'nuevo grupo descripción'. A blue 'Siguiente' button is at the bottom right of the form.

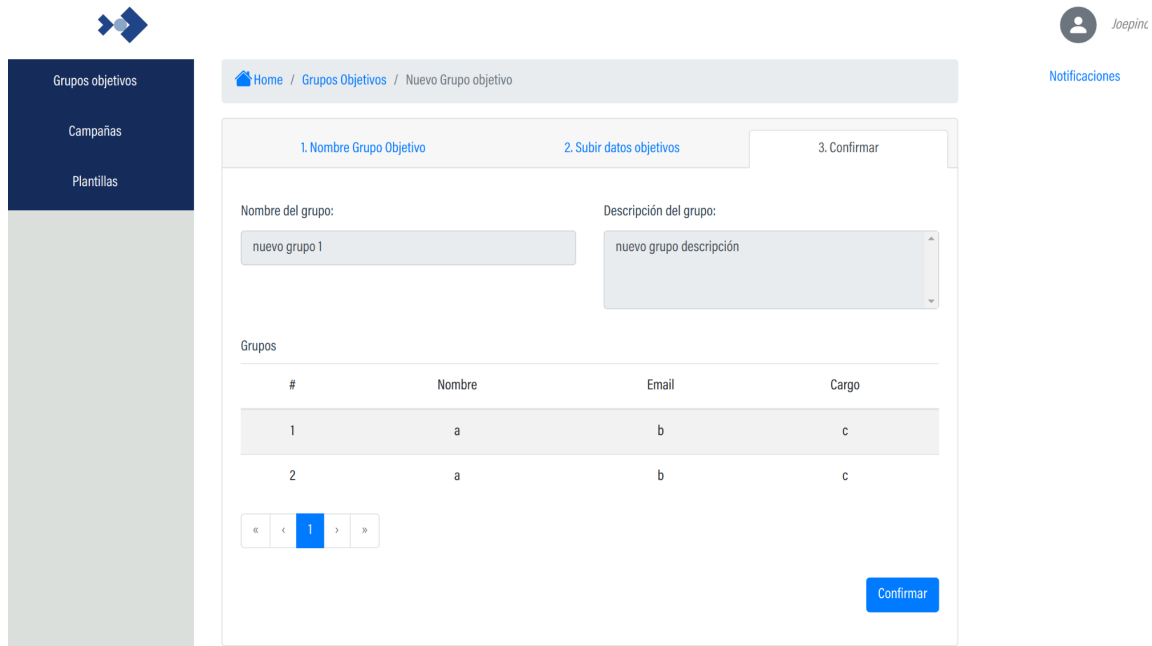
Figura 11: Formulario de grupo objetivo. Nombre grupo objetivo. Fuente: Equipo Multidisciplinario.



This screenshot shows the same web application interface, but with the second tab, '2. Subir datos objetivos', selected. The 'Importar grupo desde CSV' section is active. It features a text input field with 'test.csv', a 'Elegir archivo' button to the right, and a 'Cargar Archivo' button below the input. Below the input field, it displays 'Archivo seleccionado: test.csv'. A blue 'Siguiente' button is located at the bottom right of the form area.

Figura 12: Formulario de grupos objetivos. Carga de archivos. Fuente: Equipo Multidisciplinario.

Para la carga de los objetivos, como se mencionaba anteriormente, debe hacerse por medio de un archivo CSV, con la siguiente estructura: *name* (nombre), *email* (correo) y *position* (cargo), cada uno separado por punto y coma (",").



Home / Grupos Objetivos / Nuevo Grupo objetivo

1. Nombre Grupo Objetivo 2. Subir datos objetivos 3. Confirmar

Nombre del grupo: nuevo grupo 1

Descripción del grupo: nuevo grupo descripción

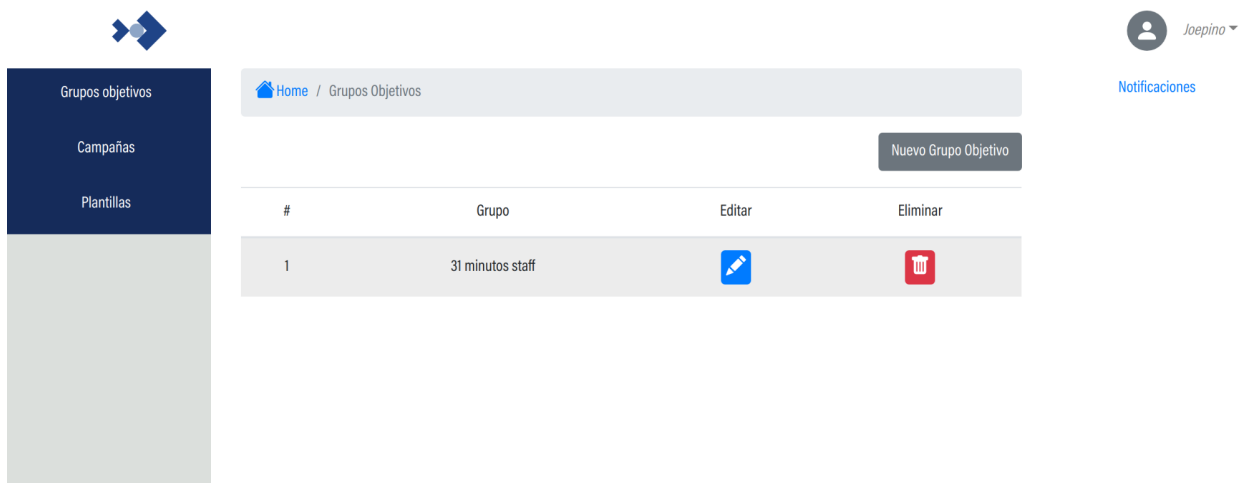
Grupos

#	Nombre	Email	Cargo
1	a	b	c
2	a	b	c

Confirmar

Figura 13: Formulario de grupos objetivos. Confirmar envío de datos. Fuente: Equipo Multidisciplinario.

Luego de enviar el formulario, el grupo queda guardado y listo para usarse en el lanzamiento de campañas. En la [Figura 14](#) se muestra el listado de grupos objetivos cargados a la plataforma.



Home / Grupos Objetivos

Nuevo Grupo Objetivo

#	Grupo	Editar	Eliminar
1	31 minutos staff		

Figura 14: Listado de grupos objetivos en la plataforma Cliente. Fuente: Equipo Multidisciplinario.

[RF1.1] - [RF1.2] Información y Público objetivo de las campañas

Para cumplir con estos requisitos, y una vez creado el o los grupos objetivos, se continúa con el formulario para crear una Nueva Campaña.

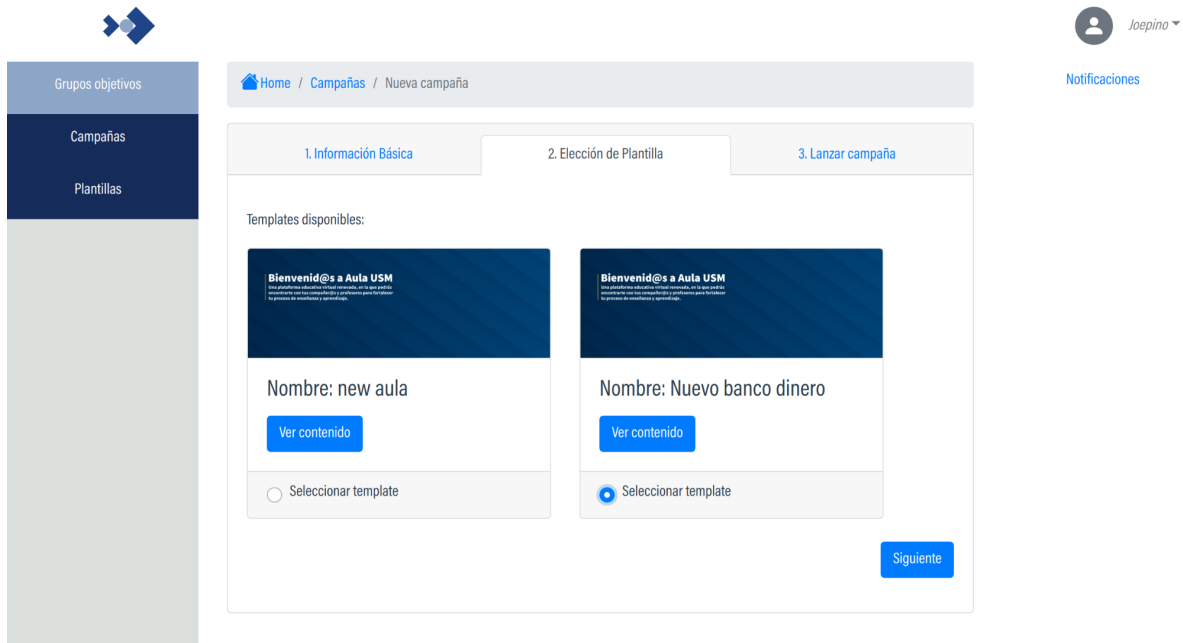
En primer lugar, se especifica el nombre de la campaña, los grupos objetivos, y la configuración SMTP definida por defecto (ver [Figura 15](#)).

Figura 15: Formulario de nueva campaña. Información Básica. Fuente: Equipo Multidisciplinario.

[RF1.2] Elección de la temática de las campañas

Luego, se continúa eligiendo la temática del *phishing* (ver [Figura 16](#)). El material aquí disponible se cargó como se especificó en el RF0.

En el [Anexo C](#) se puede encontrar el *landing page* usado para realizar la validación de la solución.



Home / Campañas / Nueva campaña

1. Información Básica 2. Elección de Plantilla 3. Lanzar campaña

Templates disponibles:

Bienvenid@s a Aula USM

Nombre: new aula

Ver contenido

☐ Seleccionar template

Bienvenid@s a Aula USM

Nombre: Nuevo banco dinero

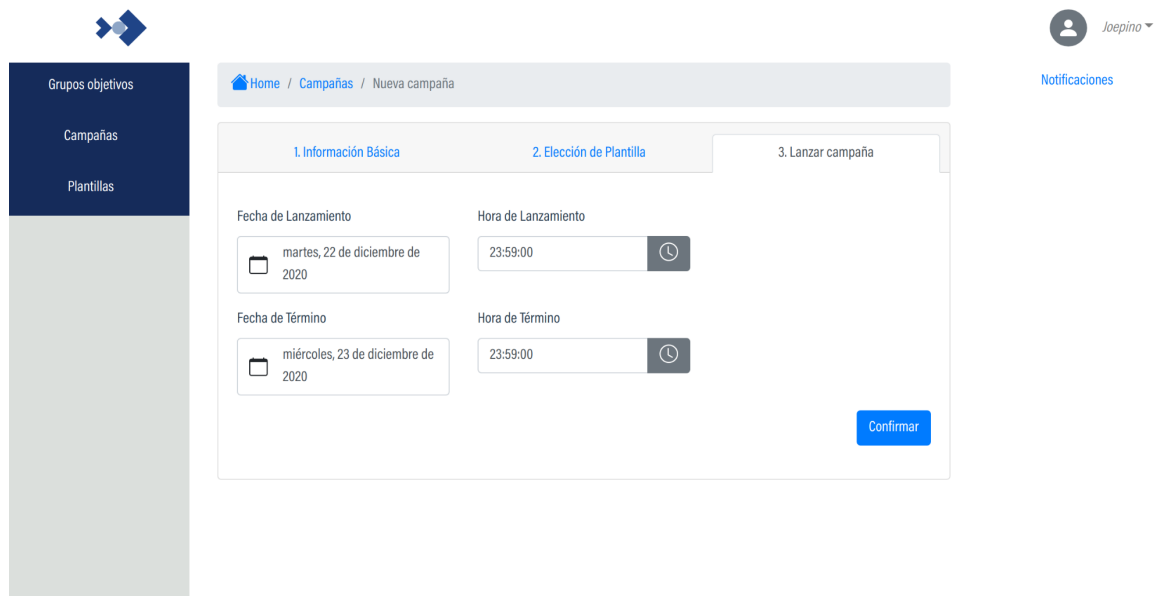
Ver contenido

☒ Seleccionar template

Siguiente

Figura 16: Formulario de nueva campaña. Elección de temática de *phishing*. Fuente: Equipo Multidisciplinario.

Una vez realizado lo anterior se procede a calendarizar la campaña (ver [Figura 17](#)) y hacer el respectivo lanzamiento de la campaña, que continúa con el envío masivo de *phishing* y posterior generación de resultados.



Home / Campañas / Nueva campaña

1. Información Básica 2. Elección de Plantilla 3. Lanzar campaña

Fecha de Lanzamiento: martes, 22 de diciembre de 2020

Hora de Lanzamiento: 23:59:00

Fecha de Término: miércoles, 23 de diciembre de 2020

Hora de Término: 23:59:00

Confirmar

Figura 17: Formulario de nueva campaña. Calendarización de campaña. Fuente: Equipo Multidisciplinario.

3. [RF2] Visualización en tiempo real

Para cumplir este requisito, se accede a la vista de Campañas, accesible desde el menú lateral. Desde ahí es posible ver todas las campañas activas (ver [Figura 18](#)) y acceder a los resultados de cada una (ver [Figura 19](#)).

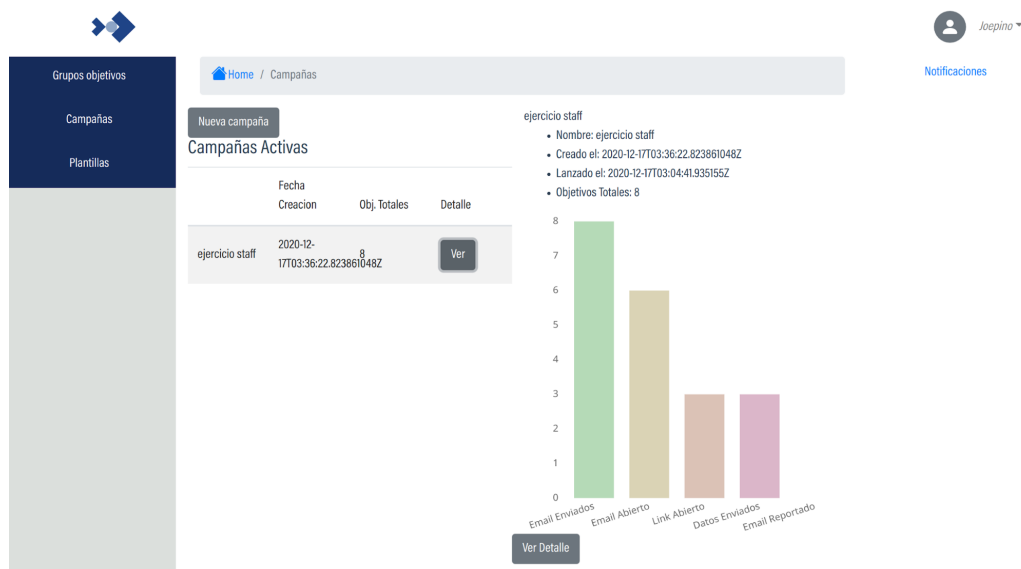


Figura 18: Listado de campañas activas. Campaña Seleccionada. Fuente: Equipo Multidisciplinario.

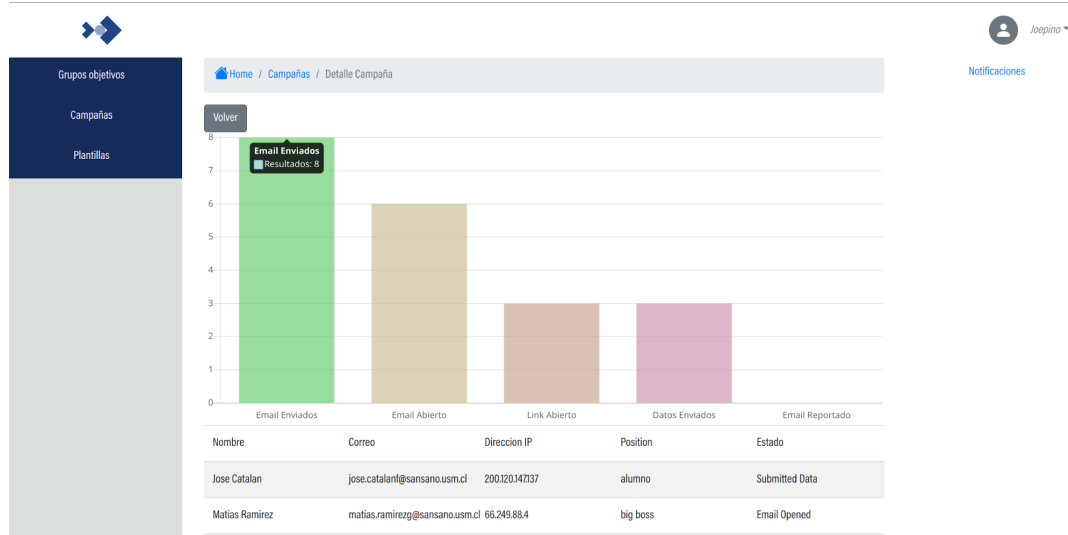


Figura 19: Resultados de campaña específica. Fuente: Equipo Multidisciplinario.

4. [RF6] Gestión de organizaciones

Para cumplir este requisito, se accede a la vista de Organizaciones, accesible desde el menú lateral en la aplicación del Super Admin (La Empresa). Desde ahí es posible acceder a un formulario para agregar una organización (ver [Figura 20](#)). El proceso genera una cuenta de Owner que permite usar la aplicación Cliente.

Grupos objetivos

Campañas

Plantillas

Solicitudes

Organizaciones

Registro de Actividad

Home / Organizaciones / Nueva Organización

Notificaciones

Nombre de la Organización:

Ingresar Nombre de fantasía de la organización

Giro de la Organización:

Ingresar giro real de la organización

Correo Owner:

Ingrese el correo del representante de la organización

Ciudad Empresa:

Ingrese la ciudad organización

Volver Reset Submit

Figura 20: Formulario de Nueva Organización. Fuente: Equipo Multidisciplinario.

La organización se crea, y es posible acceder a sus datos y cuentas asociadas desde el mismo menú Organizaciones (ver [Figura 21](#)).

Grupos objetivos

Campañas

Plantillas

Solicitudes

Organizaciones

Registro de Actividad

Home / Organizaciones

Notificaciones

Nueva Organización

Nombre Organización	Correo Owner	Fecha Creación	Action
memoria 1	memoria@gmail.com	2020-12-17T03:07:53.084Z	Ver
31 minutos	elsenormanguera@31minutos.cl	2020-12-17T03:33:53.319Z	Ver
Banco Estado	bancoestado@correo.cl	2020-12-21T21:37:37.775Z	Ver

Figura 21: Listado de Organizaciones. Fuente: Equipo Multidisciplinario.

5. [RF6] Creación de cuentas

Para cumplir este requisito, se accede a la vista de Organizaciones, accesible desde el menú lateral en la aplicación del Super Admin (La Empresa). Desde ahí es posible acceder a un formulario para agregar cuentas a una organización específica (ver [Figura 22](#)). El proceso genera una cuenta de Admin o Viewer que permite usar la aplicación Cliente con los privilegios correspondientes.

Grupos objetivos

Campañas

Plantillas

Solicitudes

Organizaciones

Registro de Actividad

Home / Organizaciones / Agregar Usuario

Notificaciones

Usuario:

Ingresar Nombre de Usuario

Correo:

Ingresar Correo

Password:

Ingresar Password

Repita Password:

Repetir Password

Seleccione Rol:

Please select an option

Volver Reset Submit

Figura 22: Formulario de Nueva Cuenta Organización (Admin o Viewer). Fuente: Equipo Multidisciplinario.

Grupos objetivos

Campañas

Plantillas

Solicitudes

Organizaciones

Registro de Actividad

Home / Organizaciones

Notificaciones

Nueva Organización

Nombre Organización	Correo Owner	Fecha Creación	Action
memoria 1	memoria@gmail.com	2020-12-17T03:07:53.084Z	Ver
31 minutos	elsenormanguera@31minutos.cl	2020-12-17T03:33:53.319Z	Ver
Banco Estado	bancoestado@correo.cl	2020-12-21T21:37:37.775Z	Ver

31 minutos

ID	Usuario	Correo	Rol
4	31 minutos	elsenormanguera@31minutos.cl	owner
5	Joepino	joepino@31minutos.cl	admin

Agregar Usuario

Figura 23: Cuentas asociadas a una organización específica. Fuente: Equipo Multidisciplinario.

6. [RF6] Perfil de Organización

Para cumplir este requisito, se accede al Perfil de Empresa/Organización, accesible desde la barra de navegación (esquina superior derecha). Desde ahí es posible acceder a un formulario para Actualizar Datos de la empresa. Para el caso del prototipo o PMV, esto solo significó editar los datos de contacto con el Owner (representante de la organización)

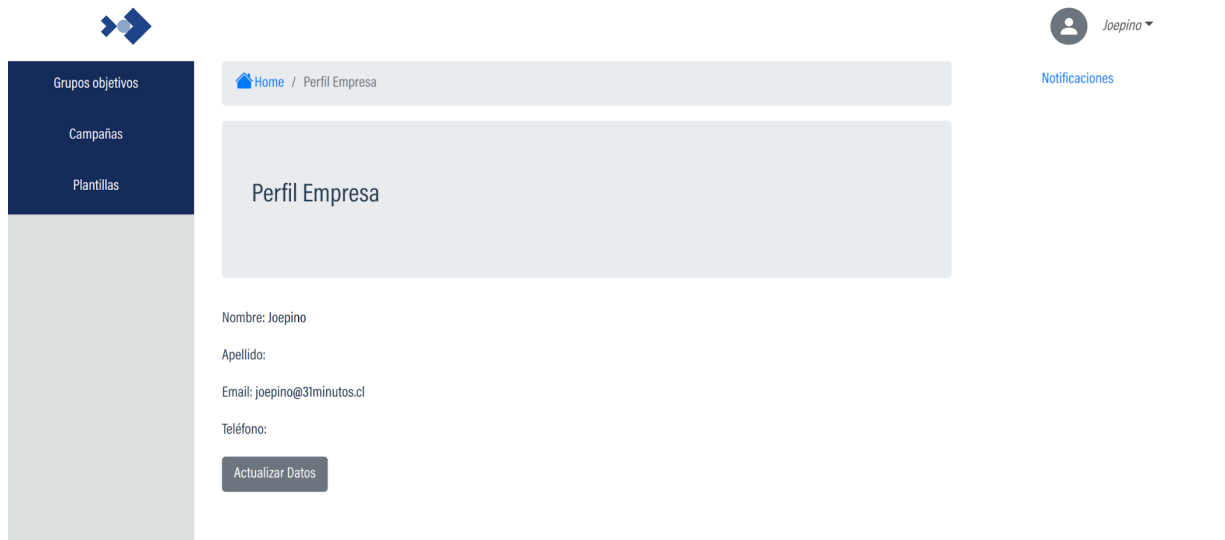


Figura 24: Perfil de organización (Owner). Fuente: Equipo Multidisciplinario.

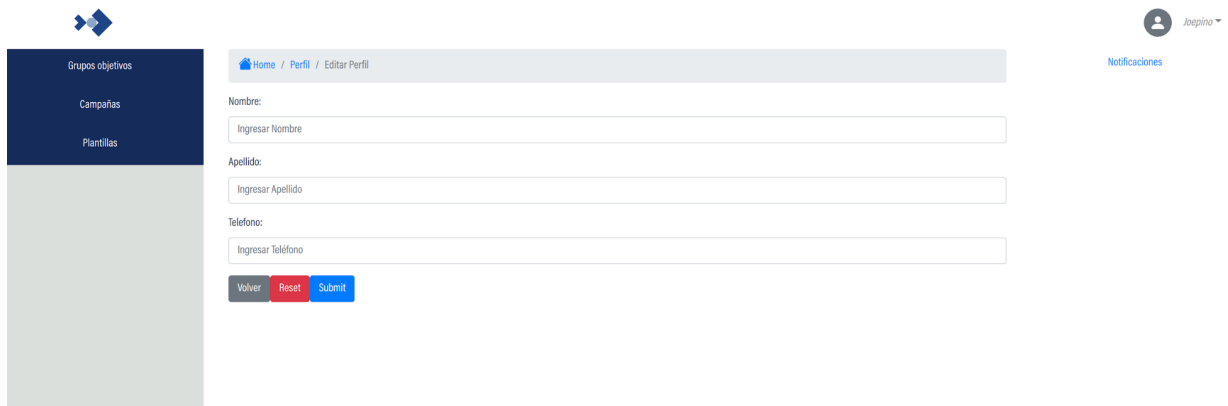


Figura 25: Actualizar Perfil de organización (Owner). Fuente: Equipo Multidisciplinario.

Se adjunta [link](#) con el prototipo en funcionamiento.

CAPÍTULO 5: CONCLUSIONES

5.1 Conclusiones generales

El *phishing* es una amenaza cibernética que viene hace muchos años generando problemas a niveles empresariales. La poca educación y preparación en este sentido hace que sea un foco para realizar estas prácticas.

A futuro se prevé que haya un alza en los ataques de *phishing*, considerando los avances en las tecnologías y los cambios que han hecho los atacantes en sus metodologías. Es importante para las organizaciones estar al tanto de los riesgos que esto implica y que existe la necesidad de invertir en ciberseguridad.

En esta memoria, se presentó una solución que va en apoyo a una empresa especializada en ciberseguridad, pero también que puede ser de gran valor para las organizaciones que quieren educar y concientizar en cuanto a ciberseguridad a las personas que son parte de ella.

La campaña lanzada en la validación de la solución fue exitosa, involucró a un grupo de 8 personas, de las cuales 6 abrieron el email, 3 abrieron el link presente en el correo, y 3 ingresaron credenciales (como se aprecia en la [Figura 19](#)). Los resultados se actualizaban 10 segundos luego de que ocurriera algún tipo de evento, lo que permite actuar rápidamente ante situaciones críticas.

5.2 Cumplimiento de objetivos

Con respecto al objetivo general:

Se logró diseñar y posteriormente desarrollar un prototipo que pudiera autogestionar campañas de *phishing* con todo lo que esto implica, como la gestión de grupos objetivos, la elección de la temática (correo y *landing page*), entre otros. A su vez, el hecho de poder generar resultados en tiempo real entrega la posibilidad, a quienes usen la plataforma, de poder tomar acciones correctivas a tiempo.

Con respecto a los objetivos específicos:

1. En primer lugar, se logró comprender el proceso de concientización de la ciberseguridad, identificando los actores involucrados, en este caso La Empresa que otorga los servicios de ingeniería social y las organizaciones que están en búsqueda de mejorar el nivel de concientización en seguridad. Además, se logró identificar los problemas y oportunidades que permitieron dar el puntapié a este proyecto de memoria. Finalmente, se realizó un estudio de las soluciones existentes que guardan relación con la concientización de la ciberseguridad y el entrenamiento a través de campañas de *phishing*, se pudo concluir sobre las

ventajas y desventajas de cada uno de ellos para después desarrollar la solución con conocimiento de esto.

2. En segundo lugar, se logró el diseño de una plataforma web identificando los requisitos tomados con la contraparte (La Empresa) y los usuarios de ella. Se definió una arquitectura con sus principales componentes, satisfaciendo requisitos de ambiente y cuidando la seguridad de la infraestructura.
3. En tercer lugar, se logró desarrollar una aplicación para los usuarios relacionados a la Organización Cliente, tomando en cuenta las funcionalidades principales relacionadas al lanzamiento de una campaña de *phishing*.
4. Finalmente, se logró desarrollar una aplicación para los administradores de la plataforma (La Empresa), que cumple con los requisitos relacionados a la gestión del servicio de *phishing*.

5.3 Trabajo futuro

Este proyecto implica muchos desafíos futuros, ya que si bien el prototipo funcional obtenido abarca las funcionalidades más importantes, a su vez hay gran parte del diseño que no se pudo desarrollar por el alcance de esta memoria, como lo son:

- La integración del *phishing* por llamada telefónica (*vishing*), el *phishing* por SMS y el *phishing* por medio de Whatsapp. Según ENISA [21], los atacantes están evolucionando en la forma de hacer *phishing*, por lo que poner a prueba con las nuevas tendencias le daría gran valor a la plataforma.
- El contenido educativo. Podría ser implementado en la plataforma, de tal manera que las organizaciones puedan acceder a este, a medida que La Empresa lo vaya facilitando. Esto permitiría que la plataforma no solo se centre en el entrenamiento vía simulaciones, sino que sea un sistema completo que incluya formación y educación.

Además, hay funciones que sería interesante agregar a esta plataforma, como son:

- Análisis del comportamiento histórico del personal de una organización a través de las campañas. Esto permitiría tener una visión global y progreso de las organizaciones en cuanto a seguridad.
- La implementación de un sistema de notificaciones para los usuarios que pueda informar sobre actividad en la plataforma y nuevo material disponible (templates).
- Un *chat* que haga que la comunicación entre La Empresa y las organizaciones sea más efectiva y rápida, ya sea para la solicitud de personalización de campañas como también para soporte.

Por último, agregar que el desarrollo del prototipo, si bien siguió estándares de seguridad, se hace necesario a futuro comprobar si existen vulnerabilidades a través de pruebas de penetración.

5.4 Trabajo multidisciplinario

Con respecto al trabajo multidisciplinario durante el PMM, se sacan conclusiones positivas. Si bien el proyecto tuvo una corta duración, se pudo lograr finalmente un resultado de gran calidad, gracias además del apoyo de La Empresa participante.

La experiencia con los alumnos de la carrera Ingeniería Civil Telemática fue realmente buena, cada uno aportó con su perfil técnico y se complementó de buena manera con las habilidades personales.

Añadir además, la gran labor de los profesores guías que acompañaron durante este proceso, y del ayudante Alejandro Carvallo, quien aportó mucho en el diseño de la plataforma, y de la ayudante Arlette Arancibia que aportó en el ámbito más comercial relacionado al análisis de la competencia.

Destacar además el gran valor que dejó cada uno de los módulos online que se llevaron a cabo, lo que permitió visualizar el desafío desde una perspectiva diferente.

REFERENCIAS BIBLIOGRÁFICAS

- [1] ENISA, “ENISA Threat Landscape - The year in review”, oct. 2020.
- [2] Eset, “Tendencias en ciberseguridad para el 2021”, 2020.
- [3] T. N. Jagatic, N. A. Johnson, M. Jakobsson, y F. Menczer, “Social phishing”, *Commun. ACM*, vol. 50, n° 10, pp. 94–100, 2007.
- [4] CSIRT-Chile, “Informe anual de gestión 2020”, ene. 2021.
- [5] A. Aleroud y L. Zhou, “Phishing Environments, Techniques, and Countermeasures: A Survey”, *Comput. Secur.*, vol. 68, 2017, doi: 10.1016/j.cose.2017.04.006.
- [6] B. B. Gupta, N. Arachchilage, y K. Psannis, “Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions”, *Telecommunication Systems*, vol. 67, 2018, doi: 10.1007/s11235-017-0334-z.
- [7] L. Lubeck, “Alerta: phishing bancario apunta a clientes de Chile”, *WeLiveSecurity*, mar. 13, 2019.
<https://www.welivesecurity.com/la-es/2019/03/13/alerta-phishing-bancario-apunta-clientes-chile/> (accedido feb. 03, 2021).
- [8] “Phishing test: Simulación de ataques dirigido a organizaciones”, *NIVEL4*.
<https://blog.nivel4.com/nivel4/nivel4-phishing-test> (accedido dic. 23, 2020).
- [9] “Concientización de Seguridad”, *Oznet Cibersecurity*.
<https://oznet.cl/ciberseguridad-defensiva/concientizacion-de-seguridad> (accedido dic. 24, 2020).
- [10] “Enterprise Security Awareness Training”, *KnowBe4*.
<https://www.knowbe4.com/products/enterprise-security-awareness-training/> (accedido feb. 03, 2021).
- [11] “Email Phishing Assessment”, *Rhino Security Labs*.
<https://rhinosecuritylabs.com/assessment-services/social-engineering/email-phishing-assessment/> (accedido feb. 03, 2021).
- [12] M. Pekarsky, “Does your web app need a front-end framework?”, *StackOverflow Blog*.
<https://stackoverflow.blog/2020/02/03/is-it-time-for-a-front-end-framework/> (accedido ene. 26, 2021).
- [13] “Stack Overflow Developer Survey 2020”, *Stack Overflow*.
<https://insights.stackoverflow.com/survey/2020#technology-web-frameworks-all-respondents-2> (accedido January 26, 2021).
- [14] J. Voutilainen, “Evaluation of Front-end JavaScript Frameworks for Master Data Management Application Development”, Bachelor of Engineering, Metropolia University of Applied Sciences, 2017.
- [15] M. Kaluža, M. Kalanj, y B. Vukelić, “A comparison of back-end frameworks for web application development”, *Zbornik Veleučilišta u Rijeci*, vol. 7, pp. 317–332, 2019.
- [16] J. Boyer, “How Secure Are Popular Web Frameworks? Here Is a Comparison”, *Veracode*, jul. 17, 2018.
<https://www.veracode.com/blog/secure-development/how-secure-are-popular-web-frameworks-here-comparison> (accedido ene. 27, 2021).
- [17] H. Sharma, “What is AWS ? – An Introduction to AWS”, *Edureka*, jul. 16, 2020.
<https://www.edureka.co/blog/what-is-aws/> (accedido feb. 03, 2021).
- [18] “¿Qué es Amazon Relational Database Service (Amazon RDS)?”, *AWS*.
https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/Welcome.html (accedido

feb. 03, 2021).

[19] “¿Qué es Amazon S3?”, AWS.

https://docs.aws.amazon.com/es_es/AmazonS3/latest/dev/Welcome.html (accedido feb. 03, 2021).

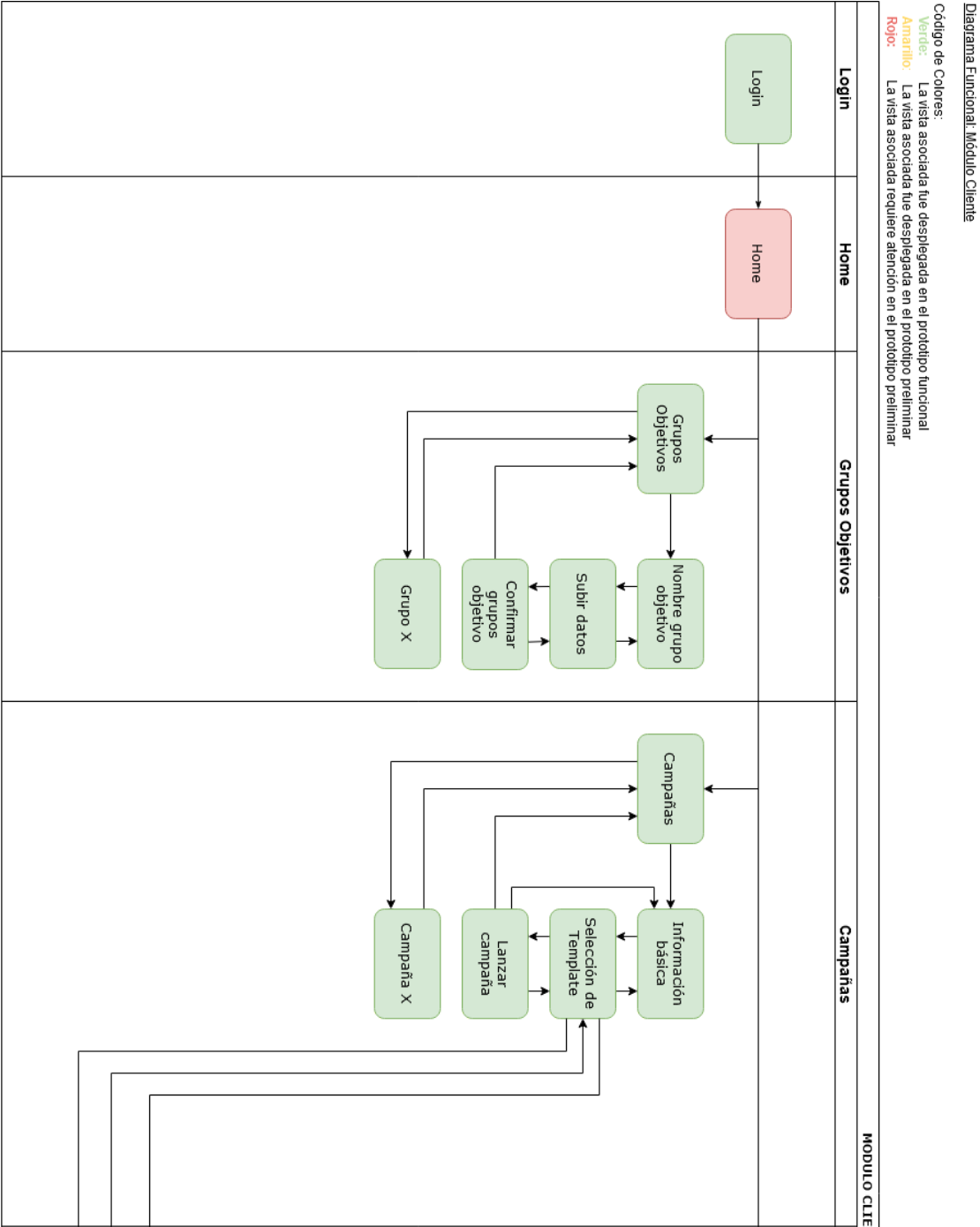
[20] V. Cuervo, “¿Qué es Postman?”, *Arquitecto IT*, feb. 14, 2019.

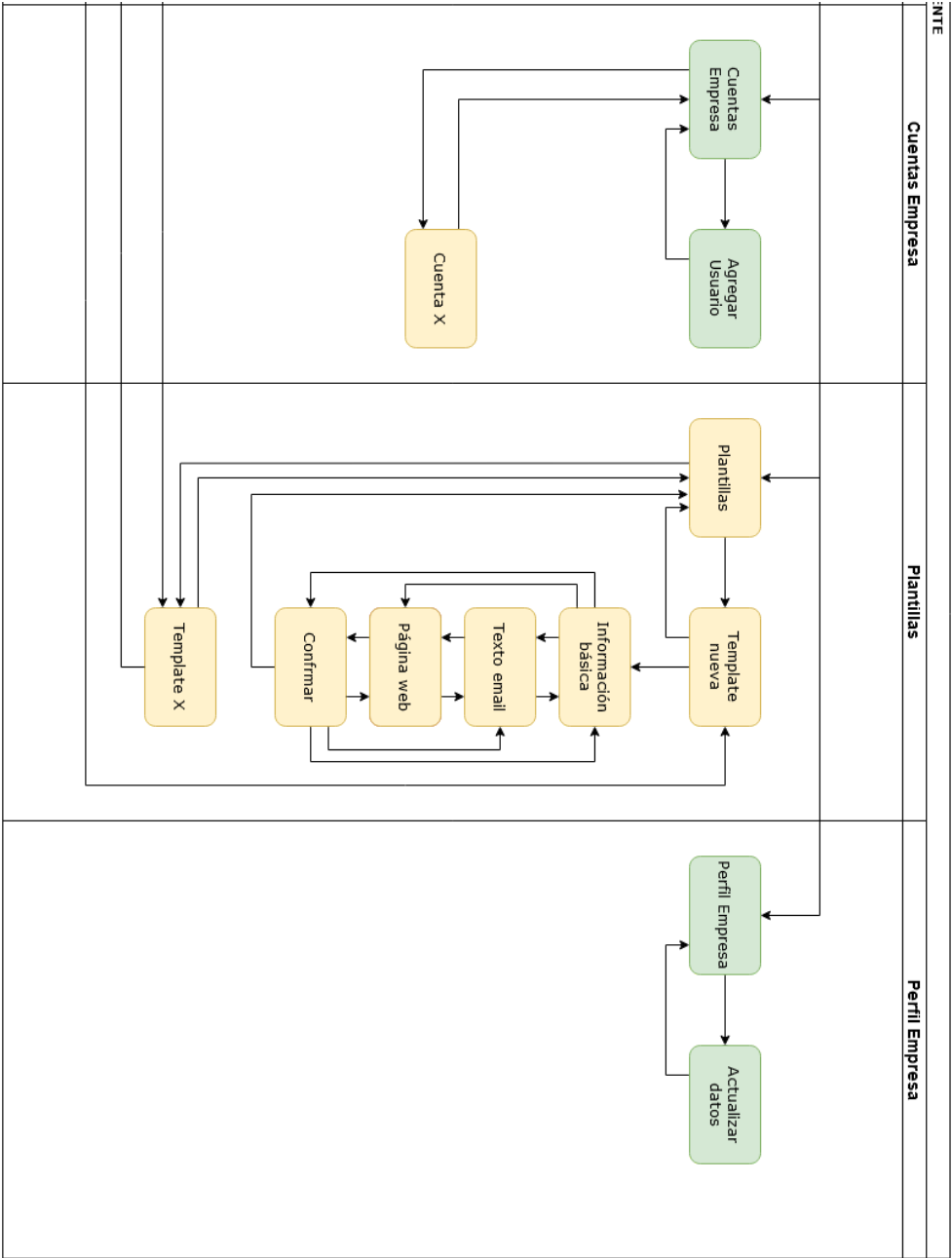
<http://www.arquitectoit.com/postman/que-es-postman/> (accedido feb. 03, 2021).

[21] ENISA, “ENISA Threat Landscape 2020 - Phishing”, oct. 2020.

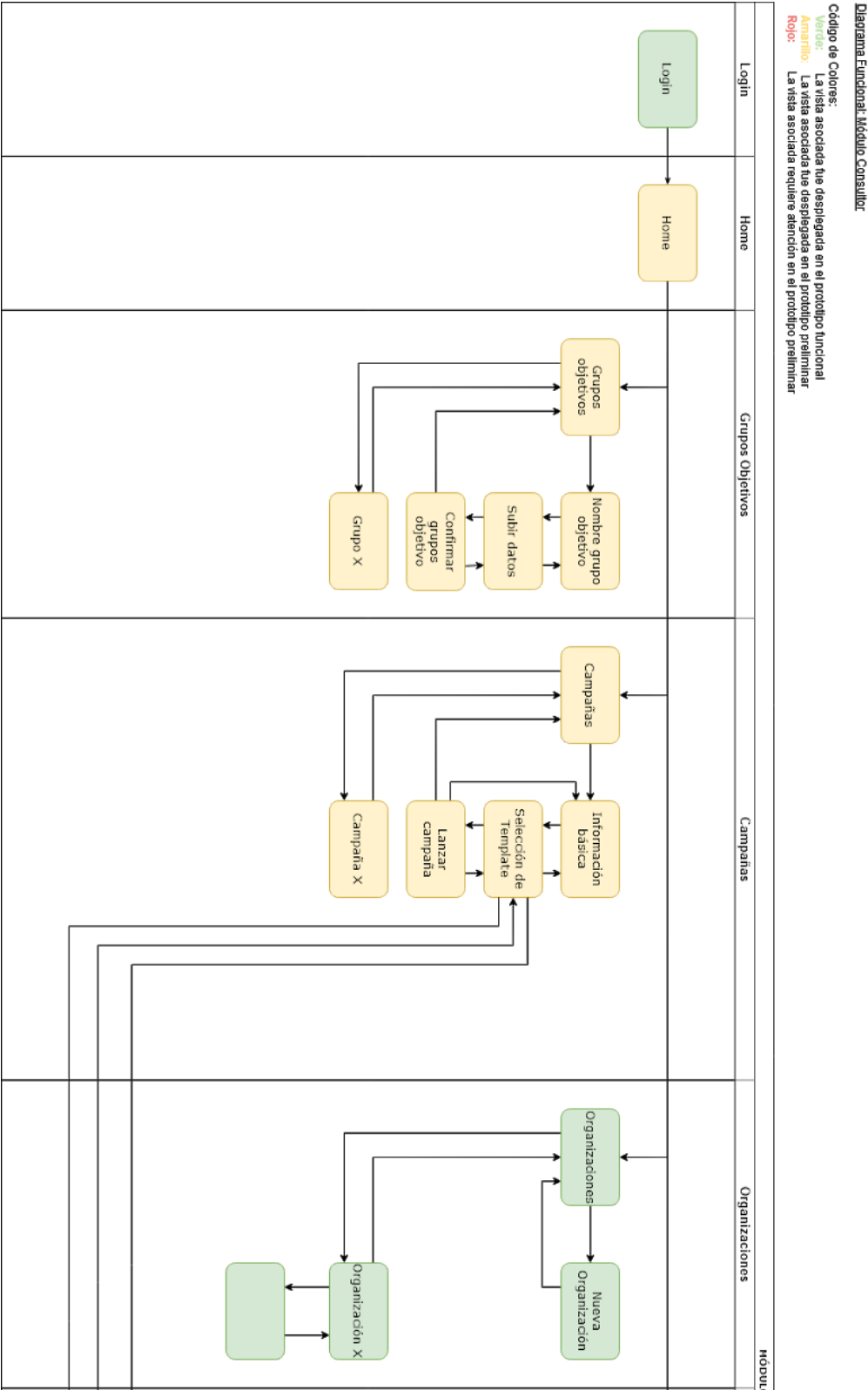
ANEXOS

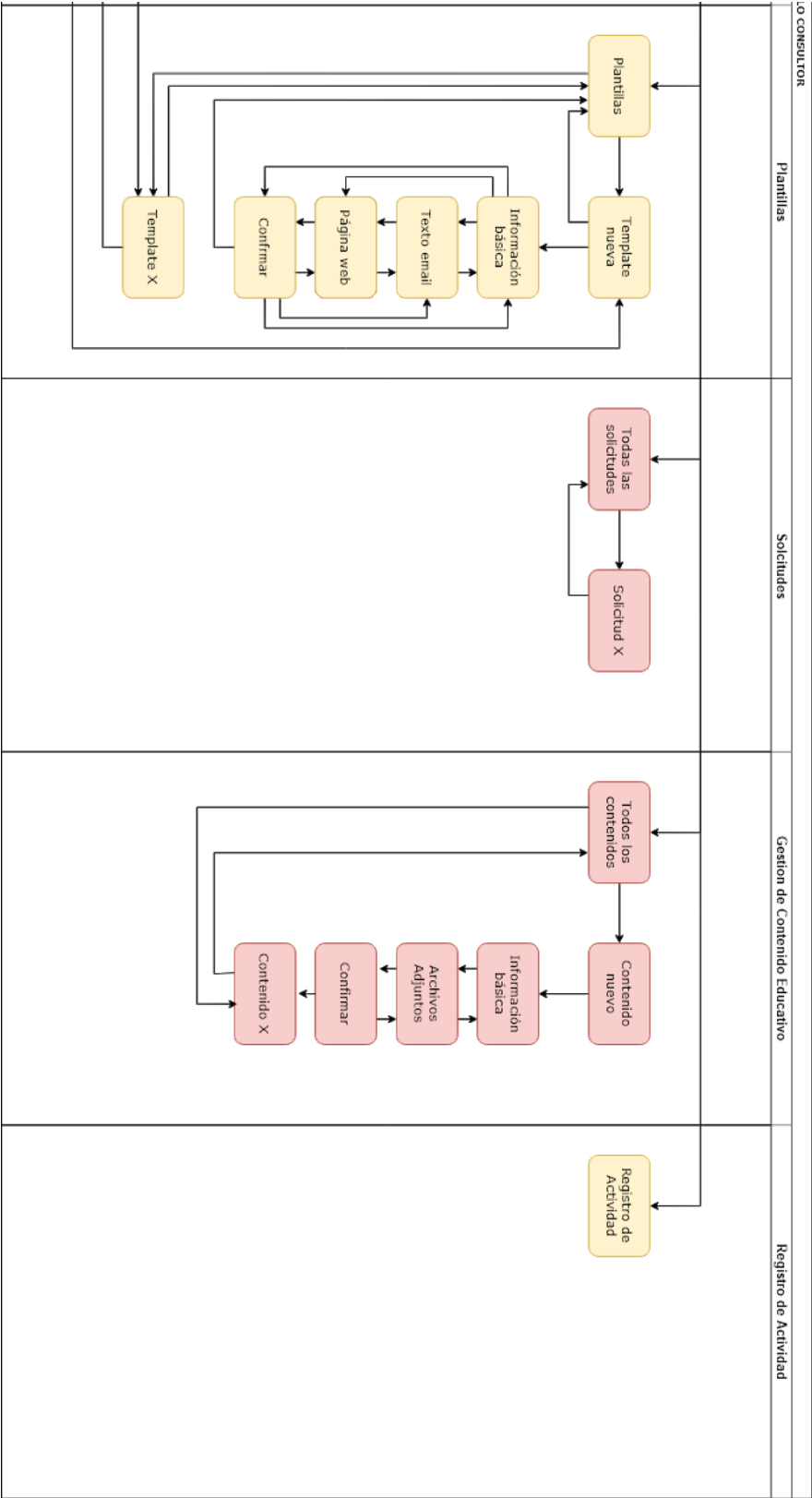
Anexo A. Diagrama Funcional, plataforma Cliente



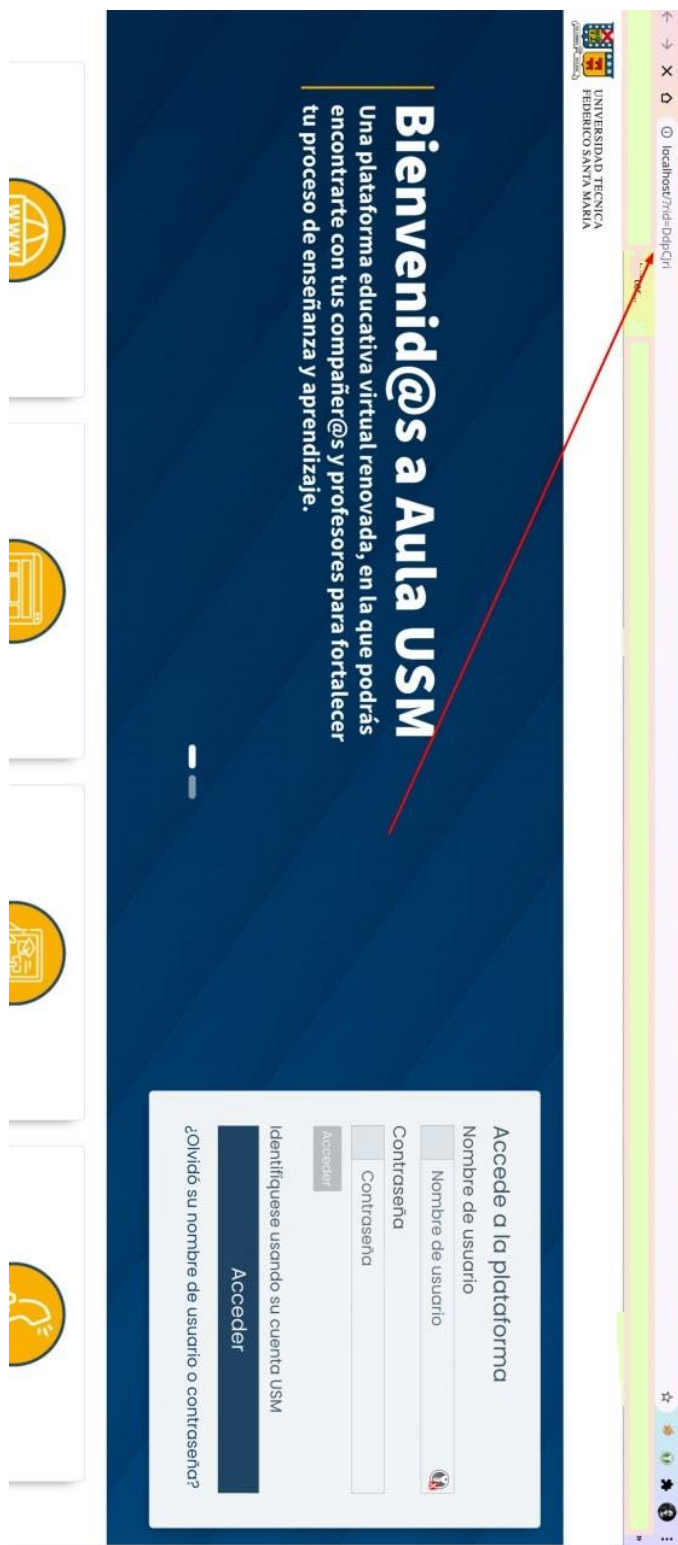


Anexo B. Diagrama Funcional, plataforma Super Admin/Consultor (La Empresa)





Anexo C. Landing page para la validación de la solución.



Anexo D. Plan de Trabajo. Carta Gantt

El proyecto de memoria se llevó a cabo con la siguiente planificación, considerando los objetivos específicos mencionados en el Capítulo 1.

	2020					
	Jul	Ago	Sep	Oct	Nov	Dic
OE1						
RP1						
M1.1						
M1.2						
OE2						
RP2						
M2.1						
OE3						
RP3						
M3.1						
OE4						
RP4						
M4.1						

Cabe destacar que los hitos de cada objetivo específico son:

M1.1 Conexión e interacción con la infraestructura de la empresa del desafío.

M1.2 Estado del arte o Análisis de Competencia

M2.1 Diseño Preliminar de la solución

M3.1 Prototipo funcional o PMV para usuario Cliente.

M4.1 Prototipo funcional o PMV para usuario Empresa.