Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ciencias y Sistemas

DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA

Christian Enrique Ramos Alvarez
Asesorado por Ing. Marco Tulio Aldana Prillwitz

Guatemala, febrero de 2024

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

CHRISTIAN ENRIQUE RAMOS ALVAREZ
ASESORADO POR ING. MARCO TULIO ALDANA PRILLWITZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, FEBRERO DE 2024

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. José Francisco Gómez Rivera (a.i.)
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton De León Bran
VOCAL IV	Ing. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Ing. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. José Francisco Gómez Rivera (a.i.)
EXAMINADORA	Inga. Floriza Felipa Ávila Pesquera de Medinilla
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
EXAMINADOR	Ing. Carlos Alfredo Azurdia Morales
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la Ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería de Ciencias y Sistemas, con fecha 02 de noviembre de 2022.

Christian Enrique Ramos Alvarez

Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencia y Sistemas

Guatemala 30 de agosto de 2023

Ingeniero Oscar Argueta Hernández
Director de la Unidad de Ejercicio Profesional Supervisado -EPS-
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Ingeniero Argueta

Reciba usted un saludo muy cordialmente, deseándole éxitos en sus labores diarias. Por este medio me permito informarle que he revisado el informe final con el tema denominado **"DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA"**, el cual se encuentra elaborado a cargo del estudiante **Christian Enrique Ramos Alvarez** de la carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, quien se identifica con número de DPI **2815756570101** y registro académico **201504444**, hago constar que el informe final está finalizado y lo doy por aprobado para que pueda continuar con el proceso de revisión.

Agradeciendo la atención a la presente. Sin otro particular me suscribo.

Atentamente,

Marco Tulio Aldana Prillwitz
Master in Bussiness Intelligence
and Data Analytics
Colegio de Humanidades 30747

Msc. Marco Tulio Aldana Prillwitz
Asesor de EPS
Escuela de Ingeniería en Ciencias y Sistemas
Universidad de San Carlos de Guatemala

Universidad de San Carlos de Guatemala

Facultad de Ingeniería
Unidad de EPS

Guatemala, 13 de septiembre de 2023.
REF.EPS.DOC.373.09.2023.

Ing. Oscar Argueta Hernández
Director Unidad de EPS
Facultad de Ingeniería
Presente

Estimado Ingeniero Argueta Hernández:

Por este medio atentamente le informo que como Supervisora de la Práctica del Ejercicio Profesional Supervisado, (E.P.S) del estudiante universitario de la Carrera de Ingeniería en Ciencias y Sistemas, **Christian Enrique Ramos Alvarez, Registro Académico 201504444 y CUI 2815 75657 0101** procedí a revisar el informe final, cuyo título es **DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA.**

En tal virtud, **LO DOY POR APROBADO**, solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Universidad de San Carlos de Guatemala
COORDINADOR(A) EPS
ÁREA TECNOLOGÍA Y CIENCIAS
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

Inga. Floriza Felipa Ávila Pesquera de Medinilla
Supervisora de EPS
Área de Ingeniería en Ciencias y Sistemas

FFAPdM/RA

Universidad de San Carlos de Guatemala

Facultad de Ingeniería
Unidad de EPS

Guatemala, 14 de septiembre de 2023.
REF.EPS.D.299.09.2023.

Ing. Carlos Gustavo Alonzo
Director Escuela de Ingeniería Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ingeniero Alonzo:

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA,** que fue desarrollado por el estudiante universitario **Christian Enrique Ramos Alvarez, Registro Académico 201504444 y CUI 2815 75657 0101** quien fue debidamente asesorado por el Lic. Marco Tulio Aldana Prillwitz y supervisado por la Inga. Floriza Felipa Ávila Pesquera de Medinilla.

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación del mismo por parte del Asesor y la Supervisora de EPS, en mi calidad de Director apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,
"Id y Enseñad a Todos"

Universidad de San Carlos de Guatemala
DIRECCIÓN
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

Ing. Oscar Argueta Hernández
Director Unidad de EPS

/ra

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 19 de septiembre de 2023

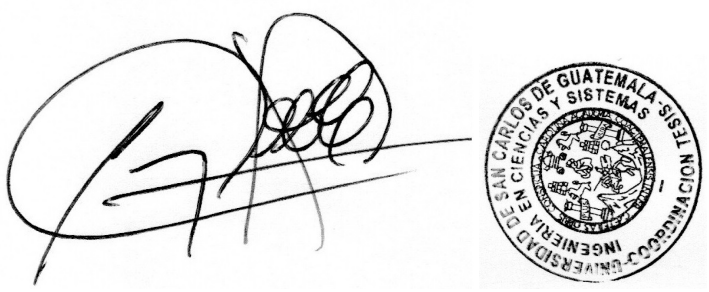
Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS del estudiante **CHRISTIAN ENRIQUE RAMOS ALVAREZ** carné **201504444** y CUI **2815 75657 0101,** titulado: **"DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA,"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,



Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

LNG.DIRECTOR.013.EICCSS.2024

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador de área y la aprobación del área de lingüística del trabajo de graduación titulado: **DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA**, presentado por: **Christian Enrique Ramos Álvarez** , procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería.

"ID Y ENSEÑAD A TODOS"

Ing. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

MSc. Ing. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, febrero de 2024

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.056.2024

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **DESARROLLO DE UN SISTEMA PARA EL DIAGNÓSTICO Y CAPACITACIÓN A USUARIOS EN TEMAS RELACIONADOS A SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA,** presentado por: **Christian Enrique Ramos Álvarez,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO a.i.
Facultad de Ingeniería

Ing. José Francisco Gómez Rivera

Decano a.i.

Guatemala, febrero de 2024

JFGR/gaoc

ACTO QUE DEDICO A:

Dios	Por darme la vida, guiándome en cada etapa de la carrera para poder culminar mis estudios.
Mi madre	Celina Alvarez, por su incondicional apoyo y motivación constante para seguir adelante.
Mi padre	Carlos Ramos, por apoyarme a culminar esta etapa y guiarme a ser un mejor profesional.
Mis hermanos	Carlos, Andrea, Javier y Maria José Ramos, por su cariño y apoyo.
Mi abuela	Carmelina Xitamul, por motivarme a siempre seguir adelante y apoyarme en todo momento.
Mi abuelo	José Alvarez, por ser una fuente de inspiración para ser una mejor persona y profesional, (q. e. p. d.).

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la casa de estudio que me formó profesionalmente y me permitió lograr mis metas.
Pueblo de Guatemala	Por permitirme tener las herramientas necesarias para ser un profesional, gracias a los impuestos que se pagan.
Mis amigos	Por su apoyo en momentos difíciles, en cada etapa de la carrera, por los buenos recuerdos y las grandes anécdotas vividas.
Mi asesor de EPS	Por su tiempo, apoyo y guía en todo el proceso de la realización del EPS.
Mi familia	Por estar a mi lado siempre, aconsejándome y sabiendo guiarme en las decisiones importantes.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES V
LISTA DE SÍMBOLOS VII
GLOSARIO IX
RESUMEN XI
OBJETIVOS XIII
INTRODUCCIÓN XV

1. FASE DE INVESTIGACIÓN 1
1.1. Antecedentes de la empresa 1
1.1.1. Reseña histórica 1
1.1.2. Misión 2
1.1.3. Visión 2
1.1.4. Servicios que realiza 2
1.2. Descripción de las necesidades 2
1.2.1. Necesidades identificadas 3
1.3. Diagnóstico FODA del proyecto 4
1.3.1. Análisis interno 4
1.3.1.1. Fortalezas 5
1.3.1.2. Debilidades 5
1.3.2. Análisis externo 6
1.3.2.1. Oportunidades 6
1.3.2.2. Amenazas 6

2. FASE TÉCNICO PROFESIONAL 9
2.1. Descripción del proyecto 9

2.2. Investigación preliminar para la solución del proyecto 10
2.3. Presentación de la solución al proyecto 11
2.3.1. Casos de uso del sistema 11
2.3.2. Roles del sistema 30
2.3.2.1. Administrador 30
2.3.2.2. Usuario 31
2.3.3. Descripción de módulos 31
2.3.3.1. Módulo de inicio de sesión 32
2.3.3.2. Módulo de dashboard 32
2.3.3.3. Módulo de creación de campañas 33
2.3.3.4. Módulo de creación de reportes 36
2.3.3.5. Módulo de usuarios 38
2.3.3.6. Módulo de grupos 39
2.3.3.7. Módulo de administración de ataque 40
2.3.3.8. Módulo de administración de entrenamiento 42
2.3.3.9. Módulo de administración de evaluación 43
2.3.3.10. Módulo de administración de usuario remitente 45
2.3.3.11. Módulo de curso de entrenamiento 47
2.3.4. Justificación de plataformas y herramientas 48
2.3.5. Especificaciones técnicas 49
2.3.6. Arquitectura del software 50
2.3.7. Diagrama entidad relación del sistema 51
2.4. Costos del proyecto 53
2.5. Beneficios del proyecto 54

3. FASE ENSEÑANZA-APRENDIZAJE 57
3.1. Capacitación propuesta 57

3.1.1. Capacitación a usuarios finales por videollamada 57
3.2. Material elaborado 57
3.2.1. Manual de usuario 58
3.2.2. Manual técnico 58

CONCLUSIONES 59
RECOMENDACIONES 61
REFERENCIAS 63
APÉNDICE 65

ÍNDICE DE ILUSTRACIONES

FIGURAS

Figura 1. Caso de uso: CU-001 11
Figura 2. Caso de uso: CU-002 13
Figura 3. Caso de uso: CU-003 15
Figura 4. Caso de uso: CU-004 17
Figura 5. Caso de uso: CU-005 19
Figura 6. Caso de uso: CU-006 21
Figura 7. Caso de uso: CU-007 23
Figura 8. Caso de uso: CU-008 25
Figura 9. Caso de uso: CU-009 27
Figura 10. Caso de uso: CU-010 28
Figura 11. Diagrama de la arquitectura del proyecto 50
Figura 12. Diagrama de base de datos 52

TABLAS

Tabla 1. Descripción del valor del proyecto en el mercado 53

LISTA DE SÍMBOLOS

Símbolo	Significado
GB	GgaByte
KB	KiloByte
MB	MegaByte
Q	Quetzal

GLOSARIO

Ataque cibernético Es la acción de robar, alterar o manipular la información de una persona por un medio electrónico.

Backend Parte del proyecto que no se puede ver, donde se lleva el control de todo lo que se realiza en la página web.

Contenedores Recipiente que virtualiza un sistema operativo que permite desplegar una aplicación.

Credenciales Son los datos de un usuario para ser identificado en un sistema de inicio de sesión, comúnmente se utiliza para referirse al nombre y la contraseña del usuario.

Despliegue Forma de indicar que un proceso está activo y puede ser utilizado.

Frontend Parte del proyecto que sí es visible para el usuario, es decir, es todo lo que se puede visualizar en una página web.

Hackeo Término utilizado para referirse a que personas desconocidas robaron información por algún medio electrónico.

INACIF	Instituto Nacional de Ciencias Forenses de Guatemala.
Phishing	Técnica comúnmente utilizada en el envío de correos electrónicos para redirigir a la víctima a una pantalla donde se le pueda robar su información.
Seguridad informática	Más conocida como ciberseguridad, la cual está enfocada en la protección de la infraestructura computacional.
Sistema operativo	Conjunto de programas y recursos que administra los recursos de hardware de una computadora.
SSO	Es el inicio de sesión único, el cual permite realizar múltiples inicios de sesión en diferentes aplicaciones con las credenciales registradas.
Virtualizar	Utiliza los recursos de software para crear un sistema operativo virtual y poder trabajar sobre este entorno.

RESUMEN

Se realizó una aplicación que amplía los conocimientos de los empleados del INACIF, por medio de una aplicación que permite al empleado aprender y analizar mejor las posibles vulnerabilidades que puedan tener al momento de estar en internet, ya que la seguridad de la información es todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de la institución, para que de esta forma se puedan asegurar que esa información no salga del sistema de la empresa y caigan en las manos equivocadas que puedan afectar directamente los servicios de la institución. Para esto se realizarán 3 diferentes niveles que permitirán al trabajador de INACIF poder ir creciendo en los conocimientos que tenga y de conocer más a fondo los tipos de ataques.

Así mismo, se realizó una aplicación capaz de contemplar diferentes módulos donde tendrán niveles (básico, intermedio y avanzado), que le permite al usuario que inicie a aprender los conocimientos básicos (en nivel básico), que lo ayuden a no ser tan inexperto en el tema de la seguridad de la información, para las personas que ya tiene conocimientos previos poder aprender aún más y desarrollarse de mejor manera. Este ámbito ayudará tanto a su desarrollo personal como al desarrollo dentro de la institución, permitiendo tener mejores empleados, con menos probabilidades de ser vulnerables a hackeos o pérdidas de información, y poder confiar de mejor manera en la información que administra la unidad de informática.

OBJETIVOS

General

Desarrollar un sistema de información que permita determinar las necesidades de capacitación y reforzar los conocimientos en temas relacionados a la seguridad de la información para todos los trabajadores del Instituto Nacional de Ciencias Forenses de Guatemala.

Específicos

1. Facilitar un mecanismo que permita lanzar un ataque controlado para determinar las capacidades de formación en usuarios finales.

2. Crear plantillas con niveles básico, intermedio y avanzado, para poder medir la eficiencia de usuarios.

3. Realizar evaluaciones a los empleados de INACIF, de los contenidos aprendidos para verificar las destrezas obtenidas.

INTRODUCCIÓN

En este trabajo de EPS, se realizó un proyecto que ayuda a concientizar sobre las altas vulnerabilidades que tiene un usuario al navegar en internet, porque si no se tiene el conocimiento correcto de los diferentes tipos de ataques cibernéticos que hay, se tiende a ser un usuario fácil de hackear o de permitir accesos no deseados, no solo en el equipo personal sino de vulnerar la seguridad de la empresa donde se está trabajando.

Estas personas que realizan los ataques su principal enfoque es robar información o pedir dinero para recuperar algún contenido de valor que hayan robado, que por lo general lo que pretenden es robar las bases de datos con toda la información importante que tenga la empresa o institución.

Este proyecto se realizó recopilando información de diferentes tipos de ataques cibernéticos actuales y de esta forma poder realizar ataques similares a los trabajadores de la institución.

También se pretende recopilar hechos históricos que hayan sucedido sobre formas de realizar ataques cibernéticos por medio de correo electrónico, esto para tener más información de formas de evaluar a los trabajadores de la institución.

Este proyecto de EPS cuenta con una gran variedad de contenido interactivo para el usuario, para que cada persona pueda aprender de forma práctica y sea agradable el interactuar con el sistema, así mismo, se tienen

diferentes evaluaciones para cada tipo de contenido, esto con la finalidad de ir comprobando que se esté aprendiendo correctamente cada tema impartido.

Se busca concientizar no solo a los trabajadores de la institución de INACIF, si no se pretende tener un alcance a nivel nacional, donde toda aquella persona que desee aprender un poco más y educarse en el tema de la seguridad de la información pueda hacerlo, teniendo una herramienta de uso gratuito que facilite estos conocimientos.

Se implementó la realización ataques simulados dentro de la institución de INACIF. Dichos ataques se realizan por medio de correo electrónico, esto para poder tener más alerta de un posible ataque a los trabajadores de INACIF y tengan los conocimientos previos para evitarlo y saber que hacer al momento de encontrarse con un correo que pueda poner en riesgo la integridad de la información que se tenga en la institución.

Para este trabajo de EPS se tuvo la colaboración de los ingenieros asesores, de la institución de INACIF, el ingeniero de la escuela de ingeniería y las asesoras de ingeniería que dieron un seguimiento constante de los diferentes puntos alcanzados en este trabajo, por lo que se les agradece su constante apoyo, colaboración y seguimiento en este trabajo, ya que son las personas que lograron aportar lo necesario y lograron ampliar el alcance de este proyecto para que sea posible realizarlo.

1. FASE DE INVESTIGACIÓN

1.1. Antecedentes de la empresa

Creación del Instituto Nacional de Ciencias Forenses de Guatemala (2006):

> El Instituto Nacional de Ciencias Forenses de Guatemala -INACIF- es creado con el Decreto 32-2006 del Congreso de la República de Guatemala publicado en el Diario de Centroamérica el 18 de septiembre de 2006, como resultado de la necesidad de contar con medios de prueba válidos y fehacientes en los procesos judiciales. Cuenta con la cooperación de expertos y peritos en ciencias forenses que aplican los avances tecnológicos, metodológicos y científicos de la medicina legal y criminalística, como elementos esenciales en la investigación criminal y de cualquier otra naturaleza. (párr. 1)

1.1.1. Reseña histórica

INACIF inicia sus funciones el día 19 de julio de 2007, y nace como institución auxiliar de la administración de justicia, con autonomía funcional, personalidad jurídica, patrimonio propio y con toda la responsabilidad en materia de peritajes técnico-científicos.

1.1.2. Misión

“Somos la Institución responsable de brindar servicios de investigación científica forense fundamentada en la ciencia y el arte, emitiendo dictámenes periciales útiles al sistema de justicia, mediante estudios medicolegales y análisis técnico-científicos, apegados a la objetividad y transparencia” (Instituto Nacional de Ciencias Forenses de Guatemala, 2006, párr. 1).

1.1.3. Visión

“Ser una Institución reconocida y altamente valorada a nivel nacional e internacional, por su liderazgo en las ciencias forenses, los aportes a la investigación científica, la calidad en la gestión institucional y el respeto a la dignidad humana” (Instituto Nacional de Ciencias Forenses de Guatemala, 2006, párr. 2).

1.1.4. Servicios que realiza

El INACIF es una institución del Gobierno de Guatemala que unifica y fortalece los servicios periciales forenses en Guatemala, teniendo como finalidad principal la prestación de servicios de investigación científica emitiendo dictámenes técnicos científicos.

1.2. Descripción de las necesidades

Implementar una aplicación que permita tener en constante capacitación a los trabajadores en INACIF sobre ataques de *phishing*, teniendo una aplicación que permita al usuario aprender y analizar mejor las posibles vulnerabilidades que se puedan tener.

Esta aplicación tendrá diferentes modalidades para el constante aprendizaje, permitiendo realizar ataques de *phishing* por medio de correo electrónico, contando con 3 diferentes niveles para mejorar la eficiencia que se tenga en la misma. Se contará con contenido multimedia que será el encargado de ampliar los conocimientos de los usuarios que deseen visualizar dicha información.

1.2.1. Necesidades identificadas

A continuación, se describen las necesidades identificadas, que fueron utilizadas para reforzar la idea de implementar la aplicación que permitirá tener en constante capacitación a los colaboradores del Instituto de Ciencias Forenses ante los ataques de *phishing*:

- Login al sistema usando el SSO de la institución de INACIF para autenticarse como usuario válido.

- Sincronización de todos los trabajadores de INACIF en el sistema, para poder realizar el envío de las simulaciones de ataques de *phishing*.

- Creación de una interfaz que permita visualizar de forma clara e interactiva con el usuario el contenido multimedia y las evaluaciones.

- Registro de plantillas de ataques de *phishing*, para tener mayor facilidad al momento de enviar una campaña en el sistema.

- Registro de credenciales de los perfiles de origen de donde se realizan los envíos de correos electrónicos.

- Registro de contenido para agregar o modificar el contenido multimedia que actualmente cuenta la aplicación.

- Registro de evaluaciones para tener un mejor control de cada evaluación realizada.

- Creación de campañas que permitan el envío de las simulaciones de ataques de *phishing* a los diferentes trabajadores registrados.

- Creación de reportes que permita visualizar el alcance que se logró tener con las campañas de *phishing* previamente enviadas, el cual contará con reportes en formato XLS y PDF.

1.3. Diagnóstico FODA del proyecto

Para poder visualizar de forma clara la situación en la cual se implementó el proyecto, se realizó un análisis interno y externo sobre el proyecto y el INACIF y de esta forma tener un panorama más amplio de las fortalezas, debilidades, oportunidades y amenazas que se tendrían.

1.3.1. Análisis interno

El análisis interno comprende todas las fuerzas que intervienen dentro del proyecto con implicaciones específicas para la eficacia del mismo.

A continuación, se describen los factores internos encontrados en la elaboración del proyecto.

1.3.1.1. Fortalezas

Las fortalezas corresponden a los puntos fuertes, particularidades internas del proyecto que facilitarán y ayudarán para el cumplimiento de los objetivos planteados, las fortalezas del proyecto son:

- Mejora de los conocimientos que tienen los trabajadores en INACIF
- Tener trabajadores alerta frente a un ataque de *phishing* real
- Capacitación a los usuarios en temas sobre seguridad de la información
- Determinar las necesidades de capacitación y reforzar los conocimientos en temas relacionados a seguridad de la información.

1.3.1.2. Debilidades

Corresponden a los puntos débiles o debilidades, las características internas del proyecto que puedan crear barreras para el cumplimiento de objetivos.

Las debilidades del proyecto son:

- No abarcar todas las vulnerabilidades que pueda tener un usuario en internet.
- Lentitud en el envío de correos electrónicos.

1.3.2. Análisis externo

El propósito del análisis externo es crear una lista finita de oportunidades que beneficiarán al proyecto, además identificar las amenazas que deberán ser eludidas.

A continuación, se describen las oportunidades externas encontradas en la elaboración del proyecto.

1.3.2.1. Oportunidades

Son consideradas como oportunidades aquellas situaciones que se presentan en el entorno del proyecto y que pueden ayudar a la consecución de los objetivos expuestos.

Las oportunidades del proyecto son:

- Mejora en las habilidades y destrezas al momento de recibir un ataque de *phishing* real.
- Ampliar los conocimientos en el ámbito de la seguridad de la información.
- Mejora de las políticas actuales sobre el manejo del correo electrónico.

1.3.2.2. Amenazas

Se comprende por amenazas aquellas situaciones identificadas en el entorno del proyecto y que pueden perjudicar negativamente a la consecución de los objetivos planteados para el mismo.

Las amenazas del proyecto son:

- No poder profundizar a detalle todos los ataques que se tienen en el ámbito de la seguridad de la información y no capacitar correctamente a los trabajadores de INACIF.

- Fallas en la conexión a internet por parte del proveedor del servicio.

2. FASE TÉCNICO PROFESIONAL

2.1. Descripción del proyecto

El proyecto consiste en implementar una aplicación web que permite enviar simulaciones de ataques de *phishing* a los diferentes colaboradores de la institución de INACIF, esta aplicación permite administrar diferentes etapas de las campañas de *phishing*, cómo:

- Visualizar el progreso de cada colaborador
- Generar reportes de las campañas realizadas
- Agregar nuevos usuarios
- Creación de ataques
- Creación de entrenamientos
- Creación de evaluaciones
- Agregar los perfiles que envían las campañas

Así mismo, se tendrá implementada otra aplicación que estará enfocada en poder brindarle al colaborador una serie de entrenamientos y evaluaciones que le puedan servir para adquirir mejores destrezas y estar preparado frente a un ataque de *phishing* real que pueda poner en riesgo la información y seguridad de la institución.

Los módulos principales de la aplicación son los siguientes:

- Inicio de sesión
- Dashboard

- Creación de campañas
- Reportes
- Administración de usuarios
- Creación de ataques
- Creación de entrenamientos
- Creación de evaluaciones
- Administración de correos de perfiles de origen
- Módulo de entrenamiento

2.2. Investigación preliminar para la solución del proyecto

En la institución de INACIF se tuvo un precedente de ataque de *phishing* donde se vio vulnerada su seguridad y se tuvo una pérdida grande de información en sus bases de datos, por esto se pensó en la implementación de este proyecto, para su realización se investigaron diferentes herramientas para poder tomar ideas y formar una propuesta de proyecto más clara con base a la necesidad que como institución requieren (Global, 2022).

Así mismo, se realizó una investigación de los principales ataques cibernéticos en la actualidad, para la creación de los ataques que se enviarán en las campañas, la creación de entrenamientos y la creación de las diferentes evaluaciones que se tendrán en la aplicación.

Con base a lo antes expuesto, INACIF requiere de una aplicación que pueda solventar esta problemática que como institución desea mejorar, que es tener colaboradores más conscientes en la seguridad informática de la empresa y estén más alertas frente a un ataque de *phishing* real que pueda poner en riesgo nuevamente la información de la institución (Hacknoid, 2019).

2.3. Presentación de la solución al proyecto

A continuación, se define como está compuesto el proyecto y las funcionalidades que tiene el mismo.

2.3.1. Casos de uso del sistema

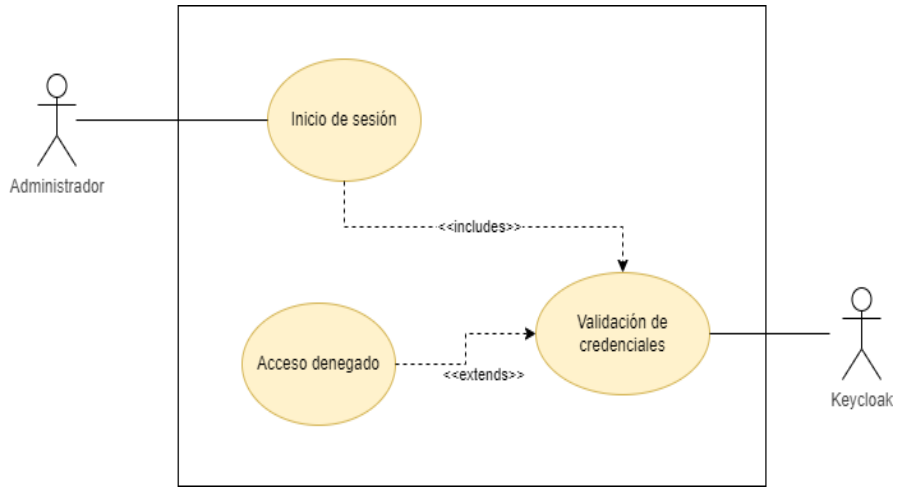
En este apartado, se describen los casos de uso del sistema a través de tablas para mejor comprensión, es decir, el flujo que tienen las funcionalidades principales en el sistema a implementar en la institución.

Figura 1.

Caso de uso: CU-001

Nombre	Inicio de sesión
Actores	Usuario Administrador Keycloak
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador quiera iniciar sesión.
Precondición	El usuario debe estar registrado en el sistema de Keycloak de la institución.

Continuación de la figura 1.

Diagrama de caso de uso


Flujo básico	
Paso	Acción
1.	El usuario ingresa a la vista de inicio de sesión
2.	El usuario ingresa sus credenciales
3.	El usuario solicita acceso al sistema (FA)
4.	Se muestra la pantalla principal de la aplicación
5.	Fin

Flujo alterno	
Paso	Acción
1.	Keycloak valida que el usuario sea correcto
2.	Keycloak valida que la contraseña sea correcta
3.	Keycloak regresa un mensaje de validación de permisos
4.	Fin

Continuación de la figura 1.

Requerimientos no funcionales
Iniciar sesión en el sistema debe responder al usuario en menos de 5 segundos. Validar correctamente las credenciales de los usuarios que estén registrados en Keycloak.

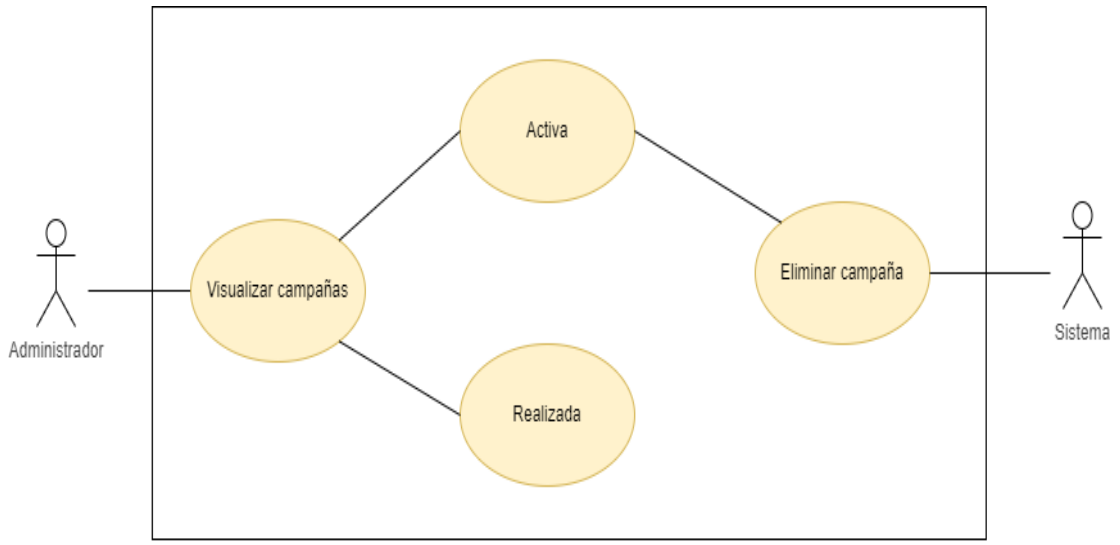
Nota. Descripción del inicio de sesión en el sistema. Elaboración propia, realizado con Draw.io.

Figura 2.

Caso de uso: CU-002

Nombre	Módulo de dashboard
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador requiera visualizar una campaña en el módulo de dashboard.
Precondición	Que el usuario esté logueado en el sistema y se tenga enviada una campaña.

Continuación de la figura 2.

Diagrama de caso de uso


Flujo básico	
Paso	Acción
1.	El usuario ingresa a la vista de dashboard
2.	El usuario visualiza las tablas de campañas activas y realizadas
3.	El usuario hace *click* en la opción de eliminar (FA)
4.	Fin

Flujo alterno	
Paso	Acción
1.	El sistema valida que la campaña aún esté activa
2.	El sistema muestra eliminación de campaña activa
3.	Se actualiza la tabla de campañas activas
3.	Fin

Continuación de la figura 2.

Requerimientos no funcionales
Cargar las campañas activas y realizadas del sistema debe responder al usuario en menos de 5 segundos. El sistema debe hacer eliminaciones lógicas únicamente de campañas que aún no se envían.

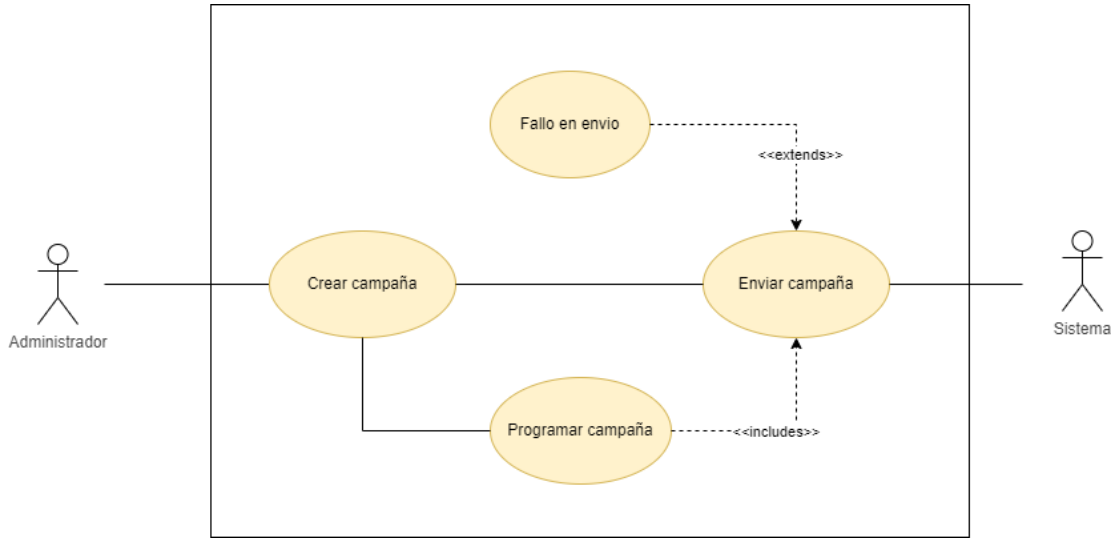
Nota. Descripción de los tipos de campañas que se pueden visualizar en el sistema. Elaboración propia, realizado con Draw.io.

Figura 3.

Caso de uso: CU-003

Nombre	Creación de campañas
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador quiera enviar una campaña.
Precondición	Que el usuario esté logueado en el sistema y debe de existir al menos un ataque de *phishing* previamente creado.

Continuación de la figura 3.

Diagrama de caso de uso


Flujo básico	
Paso	Acción
1.	El usuario ingresa a la vista de campañas
2.	El usuario crea una nueva campaña
3.	El usuario puede programar la fecha y hora del envío de la campaña
4.	El usuario envía la campaña (FA)
5.	Fin

Flujo alterno	
Paso	Acción
1.	El sistema valida que la campaña sea correcta
2.	El sistema envía la campaña
3.	Fin

Continuación de la figura 3.

Requerimientos no funcionales
El registro de la nueva campaña creada debe responder al usuario en menos de 5 segundos. Enviar correctamente la campaña a los usuarios definidos en la fecha y hora establecida.

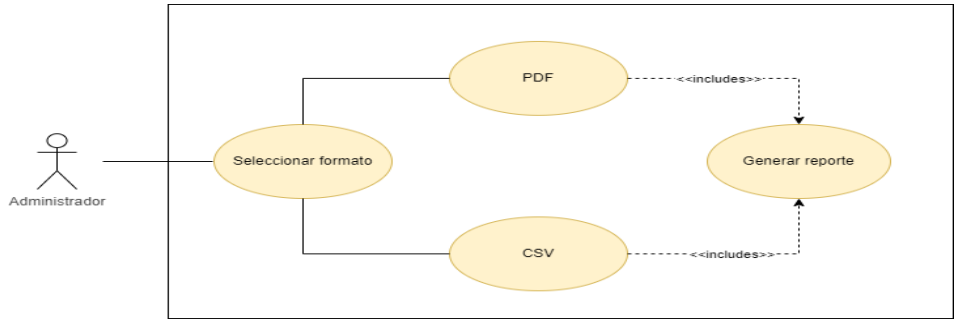
Nota. Descripción de las fases para la creación de una campaña. Elaboración propia, realizado con Draw.io.

Figura 4.

Caso de uso: CU-004

Nombre	Creación de reportes
Actores	Usuario Administrador
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador requiera realizar un reporte.
Precondición	Que el usuario esté logueado en el sistema y se tenga enviada una campaña de phishing.

Continuación de la figura 4.

Diagrama de caso de uso	
	
Flujo básico	
Paso	Acción
1.	El usuario ingresa a la vista de reportes
2.	El usuario selecciona el tipo de reporte a realizar
3.	El usuario genera el reporte seleccionado (FA)
4.	Se descarga el reporte seleccionado
5.	Fin
Flujo alterno	
Paso	Acción
1.	Se obtiene la información de la campaña
2.	Se construye el reporte de la campaña indicada
3.	Se descarga el reporte generado
4.	Fin
Requerimientos no funcionales	
Generar correctamente el reporte de la campaña indicada con el progreso actual de los usuarios asignados.	

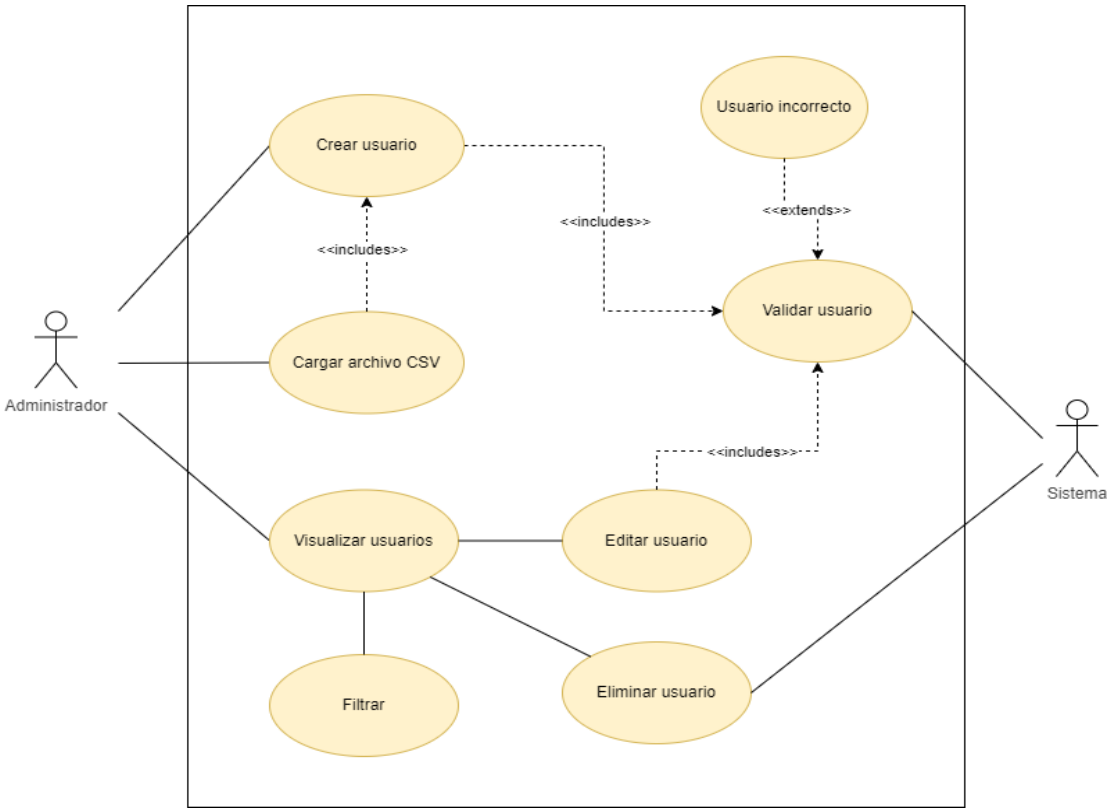
Nota. Descripción de las fases para la creación de un reporte. Elaboración propia, realizado con Draw.io.

Figura 5.

Caso de uso: CU-005

Nombre	Módulo de usuarios
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador requiera crear, editar, eliminar o visualizar un usuario.
Precondición	Que el usuario esté logueado en el sistema.

Diagrama de caso de uso



Continuación de la figura 5.

Flujo básico	
Paso	Acción
1.	El usuario administrador ingresa a la vista de usuarios
2.	El usuario administrador puede crear un nuevo usuario (FA)
3.	El usuario administrador puede realizar una carga masiva de muchos usuarios al sistema
4.	El usuario administrador puede visualizar los diferentes usuarios creados
5.	El usuario administrador puede eliminar un usuario
6.	El usuario administrador puede editar la información de un usuario previamente creado
7.	El usuario administrador puede filtrar los usuarios por su nombre
8.	Fin
Flujo alterno	
Paso	Acción
1.	El sistema obtiene la información del nuevo usuario
2.	El sistema valida que sea un usuario correcto
3.	El sistema guarda el nuevo usuario
4.	El sistema regresa un mensaje de validación de usuario
5.	Fin
Requerimientos no funcionales	
Crear un nuevo usuario en el sistema debe de responder al usuario administrador en menos de 5 segundos.	

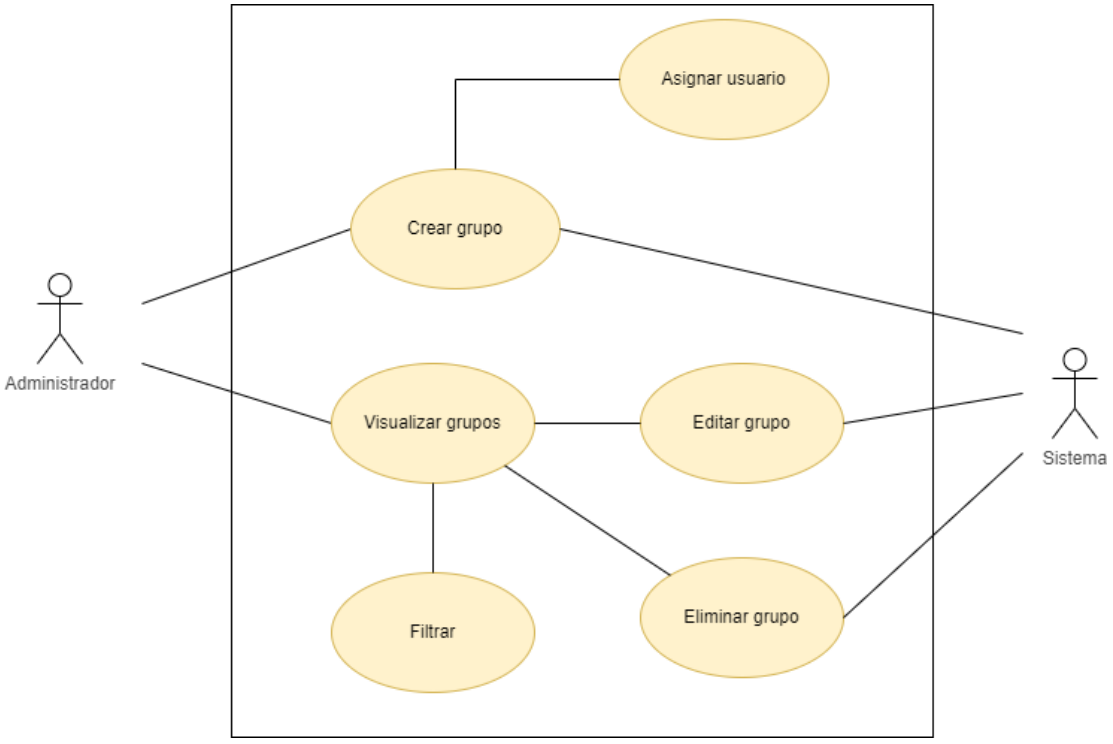
Nota. Descripción de las fases para ingresar un nuevo usuario. Elaboración propia, realizado con Draw.io.

Figura 6.

Caso de uso: CU-006

Nombre	Módulo de grupos
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador requiera crear, editar, eliminar o visualizar un grupo.
Precondición	Que el usuario esté logueado en el sistema.

Diagrama de caso de uso



Continuación de la figura 6.

Flujo básico	
Paso	Acción
1.	El usuario administrador ingresa a la vista de grupos
2.	El usuario administrador puede crear un nuevo grupo (FA)
3.	El usuario administrador puede visualizar los diferentes grupos creados
4.	El usuario administrador puede eliminar un grupo
5.	El usuario administrador puede editar la información de un grupo previamente creado
6.	El usuario administrador puede filtrar los grupos por su nombre
7.	Fin
Flujo alterno	
Paso	Acción
1.	El usuario administrador define el nombre del nuevo grupo
2.	El usuario administrador selecciona los usuarios que se asignan en el grupo
3.	El usuario administrador guarda los cambios realizados
4.	Fin
Requerimientos no funcionales	
Crear un nuevo grupo en el sistema debe de responder al usuario administrador en menos de 5 segundos.	

Nota. Descripción de las fases para ingresar un nuevo grupo. Elaboración propia, realizado con Draw.io.

Figura 7.

Caso de uso: CU-007

Nombre	Creación de plantilla para campaña
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador requiera crear, editar, eliminar o visualizar una plantilla para el envío de campañas.
Precondición	Que el usuario esté logueado en el sistema.
Diagrama de caso de uso	

Continuación de la figura 7.

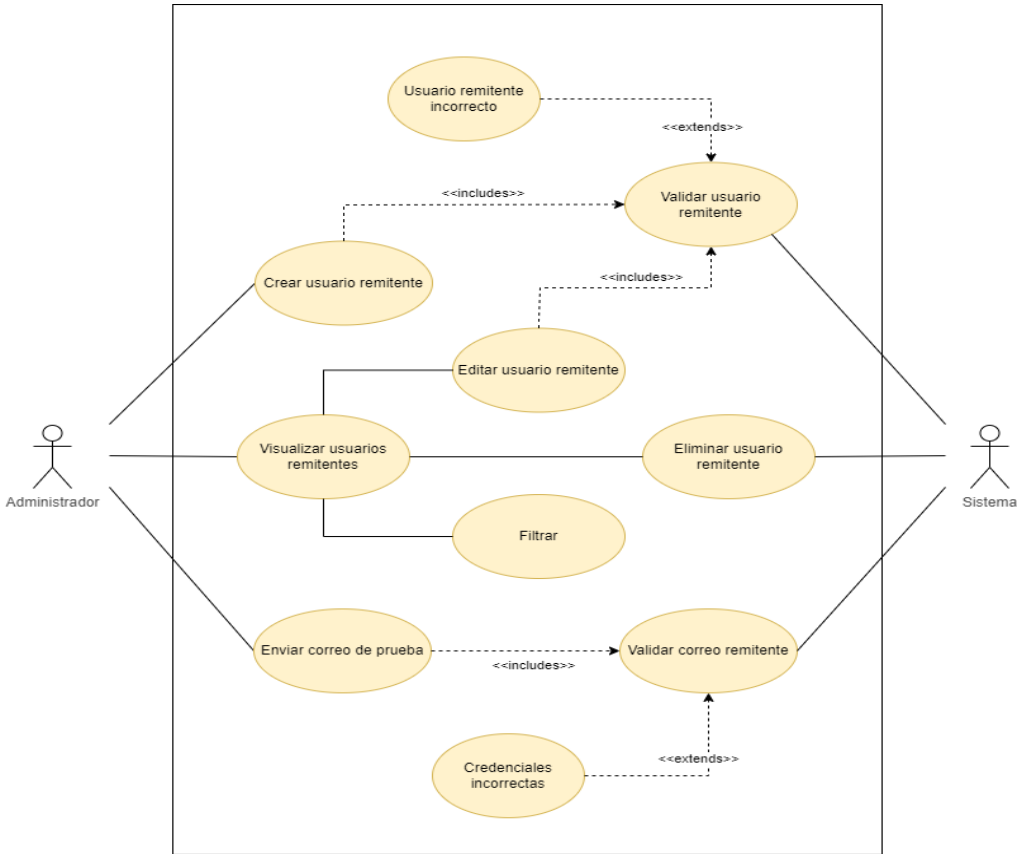
Flujo básico	
Paso	Acción
1.	El usuario administrador ingresa a la vista de plantillas
2.	El usuario administrador puede crear una nueva plantilla (FA)
3.	El usuario administrador puede editar la información de una plantilla previamente creada
4.	El usuario administrador puede visualizar las diferentes plantillas existentes en el sistema
5.	El usuario administrador puede eliminar una plantilla
6.	El usuario administrador puede filtrar las plantillas por su nombre
7.	Fin
Flujo alterno	
Paso	Acción
1.	El usuario administrador ingresa los atributos de la plantilla
2.	El sistema valida que la plantilla sea correcta
3.	El sistema guarda la nueva plantilla
4.	El sistema regresa un mensaje de validación de plantilla
5.	Fin
Requerimientos no funcionales	
Crear una nueva plantilla en el sistema debe de responder al usuario administrador en menos de 5 segundos.	

Nota. Descripción de las fases para ingresar una nueva plantilla de phishing. Elaboración propia, realizado con Draw.io.

Figura 8.

Caso de uso: CU-008

Nombre	Módulo de usuario remitente
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario administrador requiera crear, editar, eliminar o visualizar un usuario remitente.
Precondición	Que el usuario esté logueado en el sistema.
Diagrama de caso de uso	



Continuación de la figura 8.

Flujo básico	
Paso	Acción
1.	El usuario administrador ingresa a la vista de perfiles de origen
2.	El usuario administrador puede crear un usuario remitente (FA)
3.	El usuario administrador puede editar la información de un usuario remitente previamente creado
4.	El usuario administrador puede visualizar los diferentes usuarios remitentes existentes en el sistema
5.	El usuario administrador puede eliminar un usuario remitente
6.	El usuario administrador puede filtrar los usuarios remitentes por su nombre
7.	Fin
Flujo alterno	
Paso	Acción
1.	El usuario administrador ingresa las credenciales del usuario remitente
2.	El sistema valida que las credenciales ingresadas sean correctas
3.	El sistema guarda el nuevo usuario remitente
4.	El sistema regresa un mensaje de validación de usuario remitente
5.	Fin
Requerimientos no funcionales	
Validar que las credenciales del nuevo usuario remitente sean correctas para el envío de correos electrónicos.	

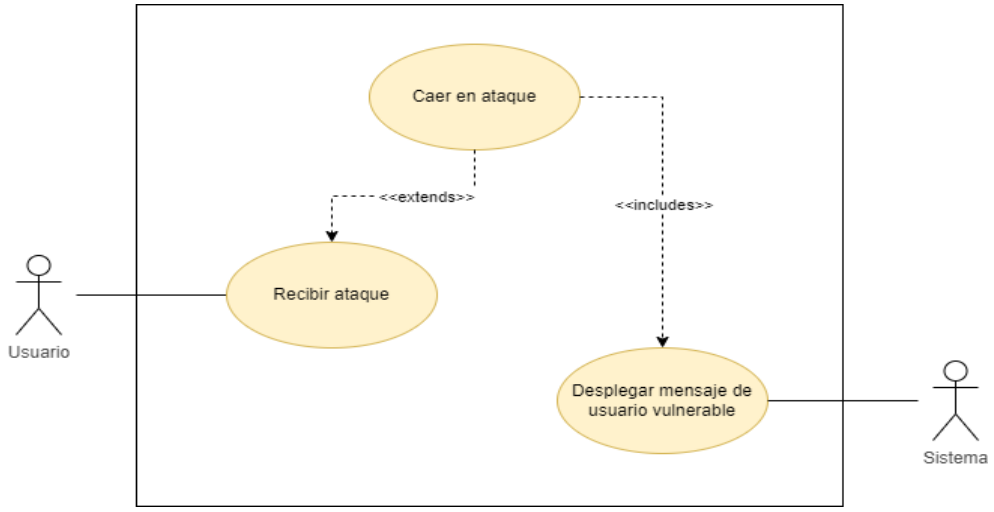
Nota. Descripción de las fases para ingresar un nuevo usuario remitente de correos electrónicos. Elaboración propia, realizado con Draw.io.

Figura 9.

Caso de uso: CU-009

Nombre	Recepción de campaña de phishing
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario reciba un correo electrónico con un ataque de phishing.
Precondición	Que se le asigne al usuario en una campaña enviada

Diagrama de caso de uso



Flujo básico

Paso	Acción
1.	El usuario recibe el ataque de phishing
2.	El usuario puede caer en el ataque de phishing
3.	Se redirigirá al usuario a la pantalla de usuario vulnerable (FA)
4.	Fin

Continuación de la figura 9.

Flujo alterno	
Paso	Acción
1.	El sistema obtiene el usuario que cayó en el ataque de phishing
2.	El sistema almacena la información del usuario y la acción de haber caído en el ataque de phishing
3.	El sistema regresa el nombre del usuario para mostrarse en la pantalla de usuario vulnerable
4.	Fin
Requerimientos no funcionales	
Tener un correcto control de la ruta de ataques de phishing para poder tener un correcto control de los usuarios vulnerables. Mostrar la pantalla de usuario vulnerable debe de responder al usuario en menos de 5 segundos.	

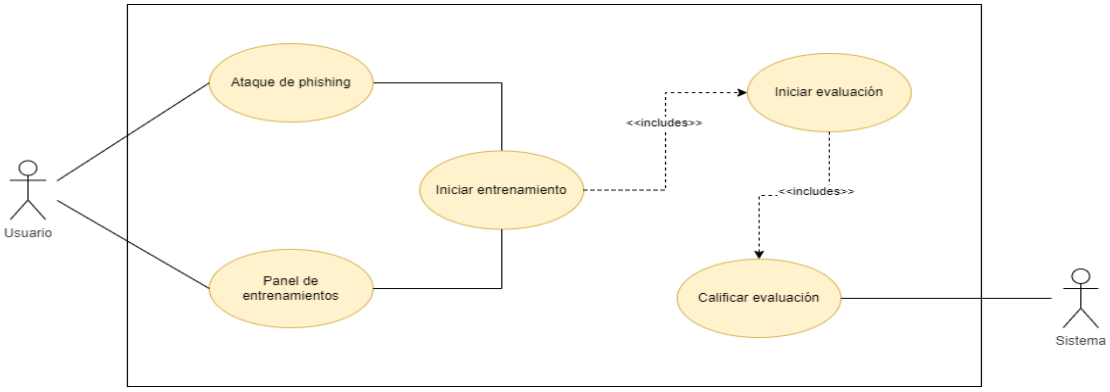
Nota. Descripción de las fases al recibir un ataque de phishing. Elaboración propia, realizado con Draw.io.

Figura 100.

Caso de uso: CU-010

Nombre	Módulo de curso de entrenamiento
Actores	Usuario Administrador Sistema
Descripción	El sistema deberá comportarse como se describe en el siguiente caso de uso cuando el usuario requiera realizar un entrenamiento.

Continuación de la figura 10.

Diagrama de caso de uso


Flujo básico	
Paso	Acción
1.	El usuario puede recibir un ataque de phishing que tenga un entrenamiento asignado
2.	El usuario puede ingresar al panel de entrenamientos
3.	El usuario puede iniciar el entrenamiento
4.	El usuario inicia la evaluación asignada al entrenamiento en curso
5.	El usuario envía la evaluación realizada a calificar (FA)
6.	Fin

Flujo alterno	
Paso	Acción
1.	El sistema obtiene las respuestas realizadas por el usuario
2.	El sistema valida las respuestas correctas
3.	El sistema almacena la nota obtenida del usuario
4.	El sistema regresa la nota obtenida del usuario
5.	Fin

Continuación de la figura 10.

Requerimientos no funcionales
Validar las respuestas correctas en la evaluación y regresar la nota obtenida del usuario. Realizar la evaluación asignada del entrenamiento debe de responder al usuario en menos de 5 segundos.

Nota. Descripción de las fases para realizar un entrenamiento en el sistema. Elaboración propia, realizado con Draw.io.

2.3.2. Roles del sistema

Una vez, presentados el uso de casos del sistema se procede a describir los roles y permisos que tendrán los diferentes usuarios en el sistema, en otras palabras, el papel del administrador y usuario.

2.3.2.1. Administrador

El encargado de poder administrar y gestionar el sistema de envío de campaña, a su vez podrá crear las diferentes plantillas que se usarán para el envío de las campañas de phishing.

- Accesos
    - Todos los módulos del sistema de gestión de campañas

2.3.2.2. Usuario

El usuario podrá realizar los diferentes entrenamientos y evaluaciones que se encuentran en el sistema de entrenamientos, el mismo tendrá accesos a todos los módulos del sistema de entrenamiento.

- Accesos
    - Todos los módulos del sistema de entrenamiento

2.3.3. Descripción de módulos

Ahora bien, los módulos a utilizar en el proyecto son:

- Módulo de inicio de sesión
- Módulo de dashboard
- Módulo de creación de campañas
- Módulo de creación de reportes
- Módulo de usuarios
- Módulo de grupos
- Módulo de administración de ataque
- Módulo de administración de entrenamiento
- Módulo de administración de evaluación
- Módulo de administración de usuario remitente
- Módulo de curso de entrenamiento

Estos módulos se describen a continuación.

2.3.3.1. Módulo de inicio de sesión

En este módulo los usuarios administradores podrán acceder al sistema de gestión de campañas, los usuarios que quieran acceder al sistema deben estar previamente registrados en la herramienta de KeyCloak, posteriormente podrán acceder al sistema ingresando sus credenciales.

Si el usuario que intenta iniciar sesión no cuenta con los permisos necesarios para tener acceso, el sistema le mostrará un mensaje al usuario indicando que no cuenta con los permisos necesarios para acceder al sistema, por lo que deberá estar registrado previamente en KeyCloak.

Las credenciales necesarias para iniciar sesión son las siguientes:

- Nombre de usuario: este será el nombre que permita al sistema identificar al usuario que esté por iniciar sesión.

- Contraseña: esta será un atributo único que permita validar la autenticación del usuario.

2.3.3.2. Módulo de dashboard

En este módulo el usuario administrador podrá visualizar las campañas activas y realizadas que se hayan generado previamente. En este módulo el usuario administrador podrá inhabilitar el envío de las campañas activas que estén pendientes de ser enviadas.

Los 2 tipos de campañas existentes son los siguientes:

- Campañas activas: son todas aquellas campañas que tienen programado su envío posterior al momento en que se estén visualizando dichas campañas.

- Campañas realizadas: son todas aquellas campañas que ya fueron enviadas; pudiendo visualizar las interacciones que tuvo cada usuario en la campaña asignada.

2.3.3.3. Módulo de creación de campañas

En este módulo el administrador podrá crear una nueva campaña por medio de una serie de pasos que permitirá personalizar la campaña a realizar, esto acorde al tipo de ataque que se quiera cubrir en ese momento, teniendo los siguientes pasos para la creación de campañas:

- Paso 1: en este paso el usuario deberá indicar el nombre de la campaña a realizar y deberá seleccionar de 1 a 5 ataques de *phishing* previamente creados. En este paso se pueden realizar búsquedas por nombre del ataque o filtrar los ataques por categoría o por nivel, con la finalidad de realizar una búsqueda más rápida y fácil según los criterios que el usuario administrador esté tomando para la creación de la campaña.

- Paso 2: en este paso el usuario deberá indicar si desea asignar un entrenamiento a la campaña a realizar, si lo requerido es no asignar ningún entrenamiento se podrá indicar que no se le asignará ningún entrenamiento a la campaña, si lo requerido es asignar un entrenamiento se podrá seleccionar 1 entrenamiento.

- Paso 3: en este paso el usuario podrá editar los diferentes ataques

seleccionados en el paso 1, pudiendo editar: el usuario remitente, el asunto y el mensaje del ataque. Si los cambios realizados en el ataque no fueran requeridos, se cuenta con una funcionalidad que permite regresar los cambios iniciales del ataque editado sin la necesidad de salirse del paso 3.

- Paso 4: en este paso el usuario deberá seleccionar todos los usuarios que recibirán la campaña a realizar, teniendo las siguientes secciones:

    - Usuarios: en esta sección se podrá visualizar un listado con todos los usuarios registrados en el sistema, pudiendo agregar desde uno a todos los usuarios a la vez, así mismo, se podrá realizar una búsqueda por nombre de usuario y facilitar un usuario previamente creado.

    - Grupos: en esta sección se podrá visualizar un listado con todos los grupos de usuarios registrados en el sistema; donde en cada grupo se tienen agregados diferentes usuarios, según los criterios que el usuario administrador haya tenido. En esta sección se puede agregar desde uno a todos los grupos a la vez, teniendo como consideración que los usuarios repetidos se agregaran solo una vez, así mismo, se podrá realizar una búsqueda por nombre de grupo y facilitar encontrar un grupo previamente creado.

    - Random: en esta sección se podrá agregar una cantidad de usuarios de forma aleatoria según sea lo requerido; al indicar la cantidad de usuarios el sistema mostrará un listado de usuarios aleatorio según la cantidad mencionada, teniendo diferentes funcionalidades al momento de obtener el listado de usuarios

random:

- Agregar: si se tuvieran usuarios previamente agregados en alguna de las secciones de usuario o grupo, con esta opción se agregan al listado de usuarios que se tiene actualmente; si no existieran usuarios previamente agregados, los usuarios random serían los únicos usuarios agregados.

- Reemplazar: si se tuvieran usuarios previamente agregados en alguna de las secciones de usuario o grupo, con esta opción se reemplaza el listado de usuarios que se tiene actualmente y se tendría únicamente el nuevo listado de usuarios random; si no existieran usuarios previamente agregados, los usuarios random serían los únicos usuarios agregados.

- Eliminar: con esta opción se podrá quitar los usuarios seleccionados del listado de usuarios random.

- Paso 5: en este paso el usuario podrá programar la fecha de envío de la campaña y podrá agregarle una imagen para representar de mejor manera la campaña, así mismo, el usuario podrá visualizar un resumen de los atributos más importantes de la campaña a realizar. En este paso se podrá indicar la forma en que se enviaran los ataques, es decir, si el usuario seleccionó más de 1 ataque, podrá indicar la forma en que estos ataques seleccionados serán enviados a los diferentes usuarios asignados a la campaña, teniendo los siguientes tipos:

  - Random: en este tipo se enviarán de forma aleatoria los diferentes

ataques seleccionados del paso 1.

- Secuencial: en este tipo se enviará de forma ordenada según el orden de selección de los ataques del paso 1.

- Seleccionado: en este tipo se enviará únicamente el ataque que se tenga seleccionado en esta vista.

2.3.3.4. Módulo de creación de reportes

En este módulo el usuario administrador podrá visualizar las campañas realizadas que se hayan generado previamente; teniendo como principal diferencia al módulo de dashboard que en este módulo está plenamente enfocado a la gestión y generación de reportes según las interacciones obtenidas de los usuarios en las campañas.

Los 2 tipos de reportes que servirán para llevar un mayor control de las campañas y darles un mejor seguimiento a los usuarios, en estos reportes se podrá visualizar la interacción de cada usuario con la campaña que se le asignó, teniendo los siguientes formatos:

- Formato PDF
- Formato XLS

En los reportes generados se contará con la información necesaria para poder darle un correcto seguimiento a los usuarios, estos campos serán:

- Nombre de campaña: este atributo es el nombre asignado a la campaña generada.

- Tipo de campaña: este atributo es el tipo que se indicó en el paso 5 de la creación de campañas.

- Fecha: esta es la fecha y hora de cuando se envió la campaña.

- Nombre: este atributo es el nombre del usuario al cual se le envió la campaña.

- Ataque: este atributo es el nombre del ataque que fue enviado.

- From: este atributo es el correo de origen del cual se envió la campaña.

- Correo enviado: este atributo indica si el correo ya fue enviado al usuario destino.

- Click en enlace: este atributo indica si el usuario destino hizo click en el ataque de phishing recibido.

- Entrenamiento: este atributo indica si el usuario destino finalizó el entrenamiento asignado a esta campaña.

- Cantidad de intentos: este atributo indica la cantidad de intentos que hizo el usuario destino en la evaluación del entrenamiento.

- Nota final obtenida: este atributo indica la nota final que obtuvo el usuario.

Para facilitar la búsqueda de las campañas realizadas se cuenta con 2 tipos de filtros, los cuales facilitan encontrar las campañas realizadas según los criterios de búsqueda, estos son:

- Filtrado 1: en este tipo se podrá filtrar las campañas por; nombre, fecha de envío y el tipo de envío.

- Filtrado 2: en este tipo se podrá filtrar por usuario, es decir, colocando un nombre de usuario se realizará una búsqueda en todas las campañas y se mostrarán todas las campañas donde el usuario esté asignado.

2.3.3.5. Módulo de usuarios

En este módulo el usuario administrador podrá visualizar los diferentes usuarios que se tengan cargados en el sistema, los atributos mostrados por cada usuario son: nip, nombre, correo, sexo y fecha de nacimiento.

Se cuenta con 2 diferentes formas de cargar usuarios, esto para facilitar ingresar usuarios según la necesidad que se tenga en el momento, estas formas son:

- Agregar usuario: en esta forma se le abrirá una ventana al usuario administrador donde podrá agregar los atributos necesarios para cargar el nuevo usuario. Los atributos necesarios para agregar un nuevo usuario son; nip, nombre, correo, sexo y fecha de nacimiento.

- Carga masiva: en esta forma se podrán cargar múltiples usuarios simultáneamente, esta carga se podrá realizar subiendo un archivo xls con los atributos necesarios de los nuevos usuarios. Los atributos necesarios para cargar un nuevo usuario son; nip, nombre, correo, sexo y fecha de nacimiento.

Se contará con funcionalidades que ayudarán a tener un mejor control de los usuarios cargados en el sistema, estas son:

- Filtrado: el sistema permitirá al usuario administrador filtrar por el nip, nombre, y correo electrónico.

- Editar: el usuario administrador podrá editar la información del usuario previamente cargado y poder tener actualizada la información de cada usuario que se tenga en el sistema.

- Eliminar: el usuario administrador podrá eliminar algún usuario en dado caso no sea requerido para el envío de campañas.

2.3.3.6. Módulo de grupos

En este módulo el usuario administrador podrá visualizar los diferentes grupos y los usuarios asignados a cada grupo que se tengan en el sistema, los atributos mostrados por cada grupo son; nombre y usuarios.

Se contará con funcionalidades que ayudarán a tener una mejor administración de los grupos en el sistema, las cuales son:

- Crear grupo: al momento de crear un nuevo grupo se abrirá una ventana al usuario administrador donde podrá ingresar el nombre del nuevo grupo y agregar los usuarios que sean requeridos. El atributo necesario para la creación de un nuevo grupo es únicamente el nombre del grupo.

- Filtrado: el sistema permitirá al usuario administrador filtrar por el atributo del nombre de grupo.

- Editar: el usuario administrador podrá editar el nombre del grupo y podrá agregar o quitar los usuarios que se tengan asignados en el grupo.

- Eliminar: el usuario administrador podrá eliminar un grupo en dado caso no sea requerido en el sistema.

2.3.3.7. Módulo de administración de ataque

En este módulo el usuario administrador podrá visualizar las diferentes plantillas de ataques que se tengan en el sistema, los atributos mostrados por cada ataque son:

- Imagen
- Nombre
- Nivel
- Categoría
- Fecha de creado

Se contará con funcionalidades que ayudarán a tener una mejor administración de los ataques en el sistema, las cuales son:

- Crear ataque: al momento de crear un nuevo ataque se abrirá una ventana al usuario administrador donde podrá ingresar los atributos necesarios de un ataque, estos son:

    - Imagen: el usuario administrador podrá subir una imagen que servirá para representar de una forma visual el ataque creado.

    - Nombre: este atributo servirá para identificar al ataque.

- Categoría: este atributo ayudará a tener organizado de mejor manera los ataques creados.

- Rating: este atributo indica una ponderación cuantitativa de la eficiencia que tiene el ataque.

- Nivel: este atributo indica el nivel que tiene el ataque, contando con 3 niveles, los cuales son: básico, intermedio y avanzado.

- From: este atributo indica la sugerencia de usuario remitente para el envío de ese ataque.

- Asunto: este atributo indica la sugerencia de asunto para el envío de este ataque.

- Mensaje: este será el cuerpo del mensaje que se enviará al usuario destino, teniendo una barra de múltiples funciones donde el usuario administrador podrá editar y personalizar de mejor manera cada nuevo ataque.

- Filtrado: el sistema permitirá al usuario administrador filtrar por los siguientes atributos; nombre, nivel y categoría.

- Editar: el usuario administrador podrá editar todos los atributos de un ataque previamente creado.

- Eliminar: el usuario administrador podrá eliminar un ataque en dado caso ya no sea requerido en el sistema.

2.3.3.8. Módulo de administración de entrenamiento

En este módulo el usuario administrador podrá visualizar las diferentes plantillas de entrenamiento que se tengan en el sistema, los atributos mostrados por cada entrenamiento son: imagen, nombre, evaluación, pantallas y fecha creado.

Se contará con funcionalidades que ayudarán a tener una mejor administración de los entrenamientos en el sistema, estas son:

- Crear entrenamiento: al momento de crear un nuevo entrenamiento se abrirá una ventana al usuario administrador donde podrá ingresar los atributos necesarios de un entrenamiento, estos son:
    - Imagen: el usuario administrador podrá subir una imagen que servirá para representar de una forma visual cada entrenamiento.
    - Nombre: este atributo servirá para identificar al entrenamiento.
    - Evaluación: en este atributo se deberá asignar una evaluación, la cual debe estar previamente creada en el módulo de evaluación.
    - Rating: este atributo indica una ponderación cuantitativa de la calidad del entrenamiento.
    - Descripción: en este atributo se colocará una pequeña descripción que ayudará al usuario final a entender de qué trata este entrenamiento.

- Nueva pantalla: en este atributo se podrá ingresar una url del video que se agregará al entrenamiento creado.

- Listado de pantallas: el usuario administrador tendrá una tabla donde podrá visualizar cada nueva pantalla que fuera agregada al entrenamiento, en esta tabla el usuario administrador podrá indicar el orden en que se mostrará cada url en el entrenamiento y podrá eliminar alguna url si ya no fuera necesaria.

- Filtrado: el sistema permitirá al usuario administrador filtrar por los siguientes atributos: nombre y evaluación.

- Editar: el usuario administrador podrá editar todos los atributos de un entrenamiento previamente creado.

- Eliminar: el usuario administrador podrá eliminar un entrenamiento en dado caso ya no sea requerido en el sistema.

2.3.3.9. Módulo de administración de evaluación

En este módulo el usuario administrador podrá visualizar las diferentes plantillas de evaluación que se tengan en el sistema, los atributos mostrados por cada evaluación son: nombre, preguntas y fecha creado.

Se contará con funcionalidades que ayudarán a tener una mejor administración de las evaluaciones en el sistema, estas son:

- Crear evaluación: al momento de crear una nueva evaluación se abrirá una ventana al usuario administrador donde podrá ingresar los atributos

necesarios de una evaluación, estos son:

- Nombre: este atributo servirá para identificar la evaluación.

- Ingreso de nueva sección: para ingresar una nueva sección se debe de cumplir con los requerimientos establecidos, los cuales son: 1 pregunta, 1 respuesta y 3 opciones.

  - Atributo pregunta: en este atributo se permite seleccionar una pregunta previamente creada o bien ingresar una nueva pregunta.

  - Atributo respuesta: en este atributo se permite seleccionar una respuesta previamente creada o bien ingresar una nueva respuesta.

  - Opción: en este atributo se permite seleccionar una opción previamente creada o bien ingresar una nueva opción. Teniendo una funcionalidad que ayudará al usuario administrador a generar 3 opciones de forma automática, esto con la finalidad de agilizar la creación de una nueva sección.

- Listado: el usuario administrador tendrá una tabla donde podrá visualizar cada sección ingresada en la evaluación, en esta tabla el usuario administrador podrá editar alguna sección existente o bien eliminarla.

- Filtrado: el sistema permitirá al usuario administrador filtrar las

evaluaciones por el nombre.

- Editar: el usuario administrador podrá editar todos los atributos de una evaluación previamente creada.

- Eliminar: el usuario administrador podrá eliminar una evaluación en dado caso ya no sea requerida en el sistema.

2.3.3.10. Módulo de administración de usuario remitente

En este módulo el usuario administrador podrá visualizar los diferentes usuarios remitentes que se tengan en el sistema, los atributos mostrados por cada usuario remitente son:

- Nombre
- Username
- Correo
- Host
- Puesto

Se contará con funcionalidades que ayudarán a tener una mejor administración de los usuarios remitentes en el sistema, las cuales son:

- Agregar usuario: al momento de crear un nuevo usuario remitente se abrirá una ventana al usuario administrador donde podrá ingresar los atributos necesarios de un usuario remitente, estos son:

    - Nombre: este atributo servirá para identificar el usuario remitente

dentro del sistema.

- Username: este atributo será el que visualizará el usuario destino al momento de recibir un correo electrónico.

- Correo: este atributo será el correo electrónico que se utilizará para el envío de mensajes.

- Password: este atributo servirá para autenticar al usuario destino y validar que se tenga la autorización de enviar correos electrónicos desde esa cuenta.

- Host: este atributo servirá para identificar el proveedor de correos electrónicos del usuario remitente y facilitar el envío de mensajes.

- Puerto: este atributo indica la puerta de acceso con la que tiene permitido el proveedor el envío de correos electrónicos.

- Funcionalidad test: esta funcionalidad sirve para enviar un mensaje por correo electrónico al usuario que se indique, con la única finalidad de validar la autorización correcta del nuevo usuario destino.

- Filtrado: el sistema permitirá al usuario administrador filtrar los usuarios destino por; nombre, username y correo.

- Editar: el usuario administrador podrá editar todos los atributos de un usuario remitente previamente creado.

- Eliminar: el usuario administrador podrá eliminar un usuario remitente en dado caso ya no sea requerida en el sistema.

2.3.3.11. Módulo de curso de entrenamiento

En este módulo los usuarios podrán realizar diferentes cursos de entrenamiento que se tengan creados, estos cursos están enfocados a poder mejorar los conocimientos de los trabajadores de INACIF y fortalecer los temas que como institución desean mejorar, Legro (2023) indica que existe una gran variedad de ataques informáticos que su único objetivo es robar la información de la persona o empresa que se encuentra conectada a internet.

Se cuenta con una vista que indica que el usuario es vulnerable, es una vista donde el usuario que recibe una simulación de ataque de *phishing* y cae en el ataque, se le redireccionará a esta vista de usuario vulnerable, para poder indicarle que cayó en la campaña de *phishing* enviada, si en la campaña se asignó un entrenamiento, el usuario podrá continuar y realizar el entrenamiento que se asignó, de lo contrario será el final del flujo de la campaña enviada.

Se tiene una sección donde el usuario puede ir navegando en las diferentes pantallas con las que cuente el entrenamiento seleccionado, en cada pantalla se contará con un video donde podrá aprender diferentes temas relacionados al curso en proceso, contando con las opciones para avanzar o retroceder según sea lo requerido por el usuario.

Se cuenta con una sección de evaluación, la cual, se podrá realizar una vez se haya completado todo el entrenamiento de la sección anterior, al estar en la evaluación el usuario podrá realizarla o bien si considera necesario podrá regresar al entrenamiento para reforzar algún tema de la lección, una vez

completada la evaluación, el usuario podrá darle finalizar y el sistema le mostrará la nota obtenida.

Se tiene una sección donde se puede visualizar de una forma intuitiva y agradable al usuario todos los entrenamientos que se tengan creados y el usuario podrá realizarlos si son de su interés, cada entrenamiento estará representado con su imagen, nombre y descripción para que el usuario pueda tener una idea más clara antes de iniciarlo, al momento de seleccionar un entrenamiento se dirigirá a la sección de entrenamiento y seguirá todo el flujo que se detalla previamente.

2.3.4. Justificación de plataformas y herramientas

La justificación de plataformas y herramientas corresponde a la descripción de las diferentes tecnologías que se utilizarán para la elaboración del proyecto, estas son:

- Angular: este es un framework sumamente robusto el cual está basado en componentes, el cual ayuda a tener un mejor orden y distribución de funcionalidades en las vistas, así mismo, este framework es de los más utilizados a nivel mundial ya que es altamente escalable, además se acopla muy bien a la forma de trabajo que tienen en la institución de INACIF, por lo que se utilizó este framework para realizar el desarrollo de las vistas de todo el proyecto. Esta es una tecnología con la que como institución han trabajado y tienen un mayor grado de conocimiento, lo que representa una facilidad al momento de darle mantenimiento al proyecto.

- Apache Tomcat: se utilizó esta tecnología ya que permite desplegar un servidor de aplicaciones web fácilmente, así mismo, es un entorno que

permite tener un alto nivel de tráfico de información y brindar alta disponibilidad, lo cual es sumamente importante para tener una correcta gestión del servidor en el proyecto. Esta tecnología permite a la institución de INACIF realizar un mantenimiento más fácil y poder darle un mejor seguimiento si se quisieran implementar nuevas funcionalidades en el proyecto.

- SQL Server: como motor de base de datos se utilizó SQL Server en su versión 2014, este es un gestor de base de datos relacional, el cual permite realizar consultas rápidas y eficientes que ayudan a optimizar el proceso de las consultas; en la institución de INACIF cuentan con este servidor de base de datos, el cual facilitó la implementación en el proyecto y representó una reducción de costos del proyecto para la institución.

- Docker: se utilizó esta herramienta ya que permite encapsular el proyecto y desplegar la aplicación en diferentes entornos sin la necesidad de preocuparse por dependencias o paquetes para el funcionamiento de este. Para poder encapsular el proyecto, tanto para el frontend como para el backend se optó por utilizar esta tecnología, se eligió ya que es una herramienta de uso libre y permite desplegar cada parte del proyecto de una manera eficiente y rápida.

2.3.5. Especificaciones técnicas

A continuación, se describen las especificaciones técnicas de las tecnologías utilizadas.

- Sistema operativo: windows 11

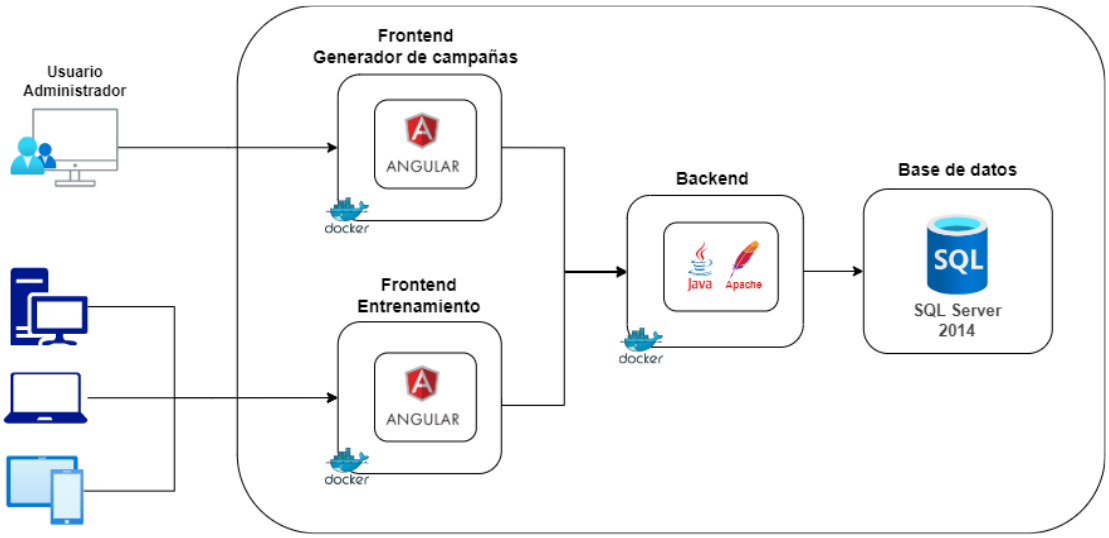
- Frontend: angular v14.0.4, Node v14.17.5, Npm: v7.21.1
- Backend: java con Apache Tomcat
- Base de datos: SQL Server 2014
- Contenedor: docker

2.3.6. Arquitectura del software

En este apartado, se muestra el diagrama completo de la arquitectura del proyecto. Teniendo dos aplicaciones de frontend diferentes, pero que comparten un mismo backend, ya que uno es el encargado de administrar todo lo relacionado al envío de campañas, mientras que el otro está enfocado únicamente a gestionar los entrenamientos y evaluaciones.

Figura 111.

Diagrama de la arquitectura del proyecto



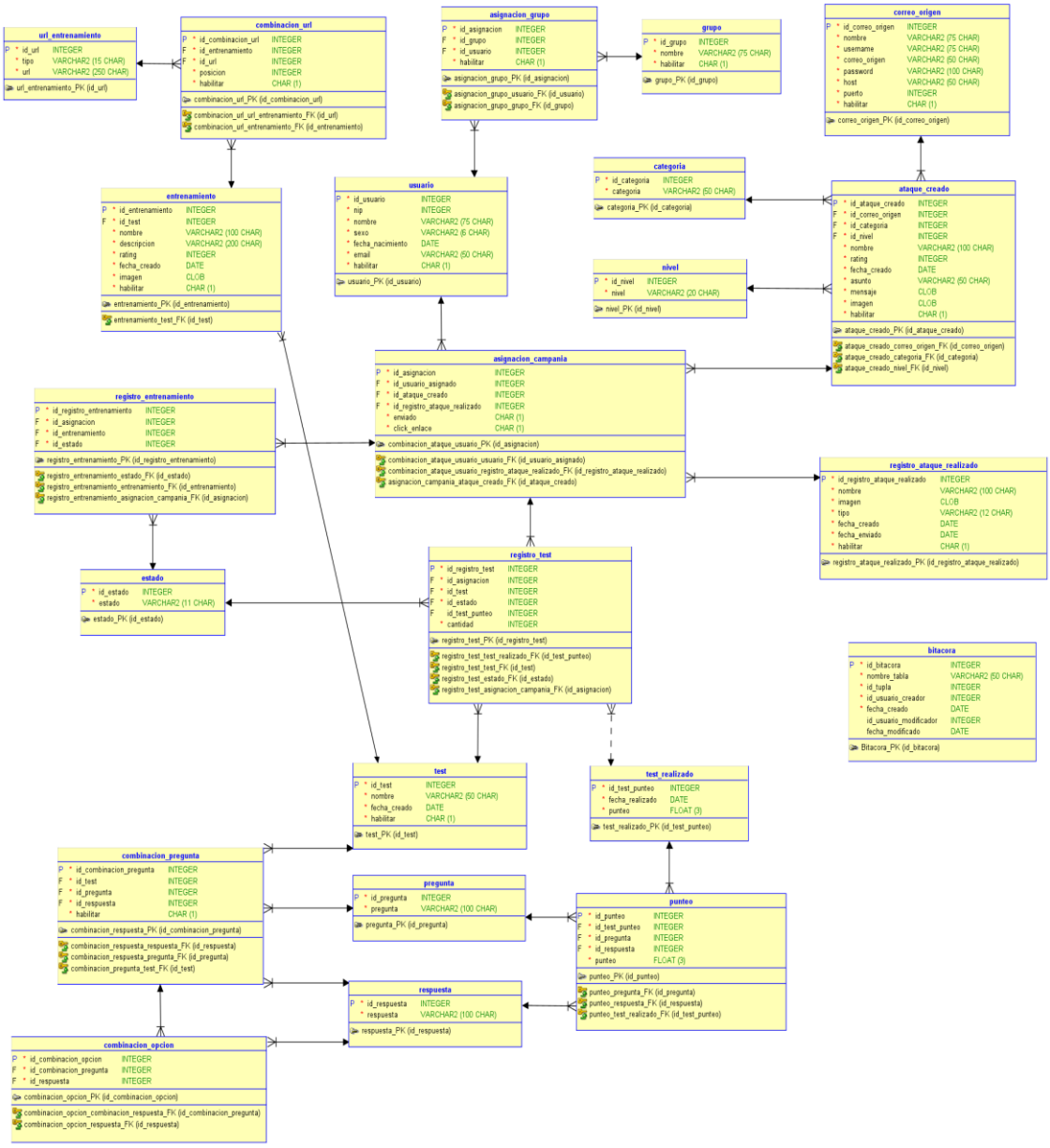
Nota. Visualización del diagrama de la arquitectura del proyecto. Elaboración propia, realizado con draw.io.

2.3.7. Diagrama entidad relación del sistema

A continuación, se muestran las tablas del modelo relacional de bases de datos utilizado para el desarrollo del proyecto.

Figura 112.

Diagrama de base de datos



Nota. Visualización del diagrama de base de datos del proyecto. Elaboración propia, realizado con Data Modeler.

2.4. Costos del proyecto

En este apartado se describen los costos del proyecto, los cuales pueden visualizarse a través de la siguiente tabla que especifica los costos equivalentes en el mercado actual.

Tabla 1.

Descripción del valor del proyecto en el mercado

Recurso	Cantidad	Costo unitario	Subtotal
Analista	1 Analista 8 horas/semana 6 meses	Q 5,000.00 /mes	Q 30,000.00
Desarrollador	1 desarrollador frontend 1 desarrollador backend 4 horas/día 6 meses	Q 10,000.00 c/desarrollador /mes	Q 120,000.00
DBA	1 DBA 2 horas/semana 6 meses	Q 2,500.00 /mes	Q 15,000.00
Project Manager	1 Project Manager 2 hora/semana 6 meses	Q 5,000.00 /mes	Q 30,000.00
Asesores de institución	2 asesores 1hora/semana 6 meses	Q 1,000.00 c/asesor /mes	Q 12,000.00
Asesores de Escuela en Ciencias en Sistemas	1 asesor 1hora/semana 6 meses	Q 1,000.00 /mes	Q 6,000.00
Servicio de Internet	6 meses	Q 299.00	Q 1,794.00
Energía eléctrica	6 meses	Q 250.00	Q 1,500.00
Mobiliario y equipo	1 laptop 1 mouse 1 silla 1 escritorio 1 impresora 1 UPS	Q 13,500.00 Q 445.00 Q 1,800.00 Q 1,500.00 Q 1,130.00 Q 500.00	Q 18,875.00

Continuación de la tabla 1.

Recurso	Cantidad	Costo unitario	Subtotal
Material de oficina	Resma de hojas, lapiceros, folder, tinta, entre otros	Q 1,250.00	Q 1,250.00
Servicios en la nube	1 Ambiente de pruebas en la nube 1 Servidor en la nube	Q 325.00 /mes Q 799.00 /mes	Q 6,744.00
		Total	Q 243,163.00

Nota. El presupuesto fue elaborado con los recursos necesarios para el desarrollo de este sistema, el cual cubre un tiempo de 6 meses. Elaboración propia, realizado con Word 365.

2.5. Beneficios del proyecto

La implementación de este proyecto logra mejorar las necesidades que tienen actualmente como institución, las cuales se pretenden mejorar al tener en constante capacitación de ataques de *phishing* a los diferentes trabajadores de la institución.

Se tiene una aplicación escalable que permite tener la facilidad de ir creando diferentes ataques cibernéticos constantemente y tener actualizados a todos los trabajadores de la institución con los diferentes conocimientos que puedan adquirir en el sistema de entrenamiento.

Se cuenta con buena estabilidad del sistema, ya que, al estar desplegado en el ambiente de desarrollo de la institución, este contará con buen espacio en la nube y los recursos suficientes del servidor para poder tener una aplicación rápida y que pueda ser completamente funcional para el usuario administrador y los usuarios que estén en el sistema de entrenamiento.

Por último, se cuenta con un ecosistema que podrá mejorar la cultura del área cibernética a toda la población de Guatemala, ya que el sistema de entrenamiento estará desplegado en la página oficial de la institución, lo cual facilita que cualquier persona pueda hacer uso de este sistema y pueda aprender constantemente sobre estos temas.

3. FASE ENSEÑANZA-APRENDIZAJE

En esta fase se brindan las herramientas necesarias para que el usuario final de la institución de INACIF pueda conocer ampliamente el proyecto y pueda tener los conocimientos necesarios para un uso correcto.

3.1. Capacitación propuesta

En este apartado se describe la capacitación a usuarios finales por videollamada, realizada al personal técnico de la institución, para que tengan el conocimiento de las funcionalidades del proyecto.

3.1.1. Capacitación a usuarios finales por videollamada

Se tuvo una videollamada con los usuarios finales, personal técnico y usuarios interesados en el sistema, esto para poderles mostrar el flujo del proyecto y las funcionalidades con las que se cuentan. Se realizó una demostración en donde se mostró cómo utilizar el sistema de creación de campañas y el sistema de entrenamiento.

3.2. Material elaborado

A continuación, se describen los manuales realizados para que los usuarios finales de la institución de INACIF puedan tener los conocimientos necesarios y darle el uso correcto al sistema.

3.2.1. Manual de usuario

Este es el documento que permite orientar de mejor manera al usuario final, este manual es el encargado de indicar las funcionalidades que se pueden realizar en cada módulo y cómo utilizarlo de mejor manera.

Este manual está separado por módulos y cada uno indica el flujo a seguir en el sistema.

3.2.2. Manual técnico

Este es el documento que explica de una forma técnica la estructura que tiene el proyecto y como poder realizar nuevas implementaciones o mejoras, según sea lo requerido por la institución. Cuenta con una detallada explicación paso a paso de cómo poder migrar el sistema a un servidor diferente en dado caso sea lo requerido por la institución.

CONCLUSIONES

1. Se desarrolló un sistema que permite el envío de correos electrónicos para realizar ataques de *phishing* controlados y tener en constante capacitación a los trabajadores de la institución. Teniendo un sistema que permite medir las interacciones que tiene el usuario que recibe cada ataque de *phishing* y poder conocer qué usuarios son más vulnerables de recibir un ataque de *phishing* real.

2. Se creó un sistema que permite crear plantillas y medir su eficiencia con los niveles de básico, intermedio y avanzado. Teniendo otros atributos que ayudan a una medición más precisa, como lo es el atributo de rating, el cual brinda una ponderación cuantitativa que ayuda a conocer mejor la eficiencia de cada plantilla.

3. Se realizó el sistema de entrenamiento que permite visualizar los diferentes entrenamientos en el sistema y evaluar los conocimientos aprendidos de cada usuario, cada evaluación realizada por los trabajadores de la institución es registrada en el sistema para poder darle un mejor seguimiento a cada trabajador.

RECOMENDACIONES

1. Gestionar los seguimientos a los usuarios más vulnerables en la institución, para contar con personal altamente capaz de reconocer un ataque de phishing real y saber cómo actuar en esa situación.

2. Elaborar plantillas sobre temas actualizados que permitan evaluar mejor a todos los trabajadores de la institución y mejorar constantemente los conocimientos previamente adquiridos.

3. Crear múltiples entrenamientos que permitan abarcar la gran cantidad de tipos de ciberataques que existen en el mundo y poder fortalecer los conocimientos sobre seguridad de la información en la institución.

REFERENCIAS

Global, R. (9 de marzo de 2022). *Herramientas de ciberseguridad para proteger tu empresa.* Infosecurity. https://www.infosecuritymexico.com/es/blog/herramientas-de-ciberseguridad-para-proteger-tu-empresa.html

Hacknoid. (2 de julio de 2019). *Importancia de la seguridad informática de las empresas.* HANCKNOID. https://www.hacknoid.com/hacknoid/importancia-de-la-seguridad-informatica-de-las-empresas

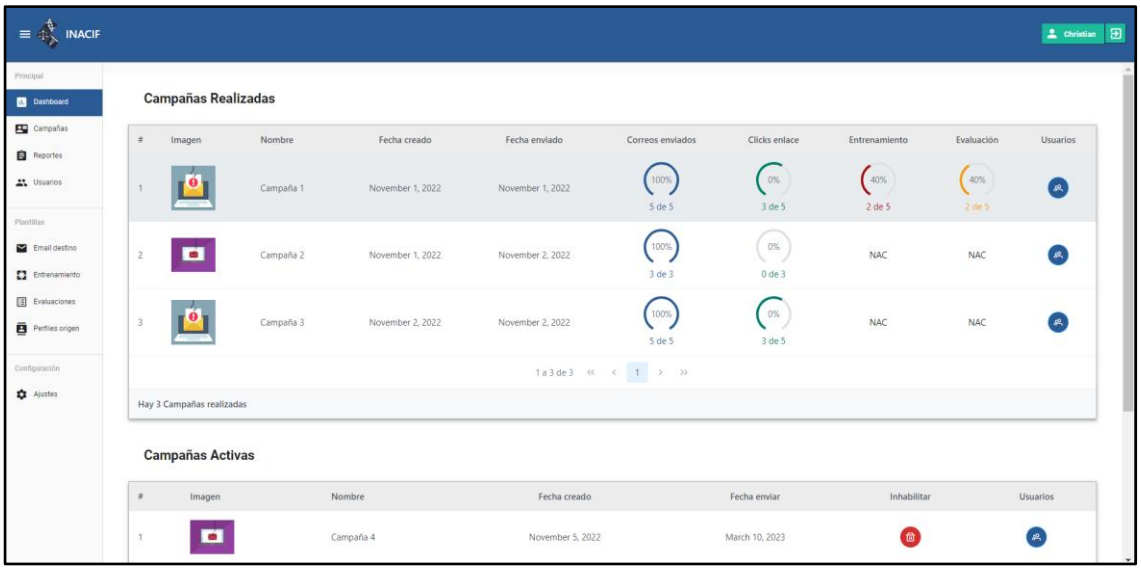
Instituto Nacional de Ciencias Forenses de Guatemala. (2018). *Misión y visión*. https://www.inacif.gob.gt/index.php/inacif/mision-vision

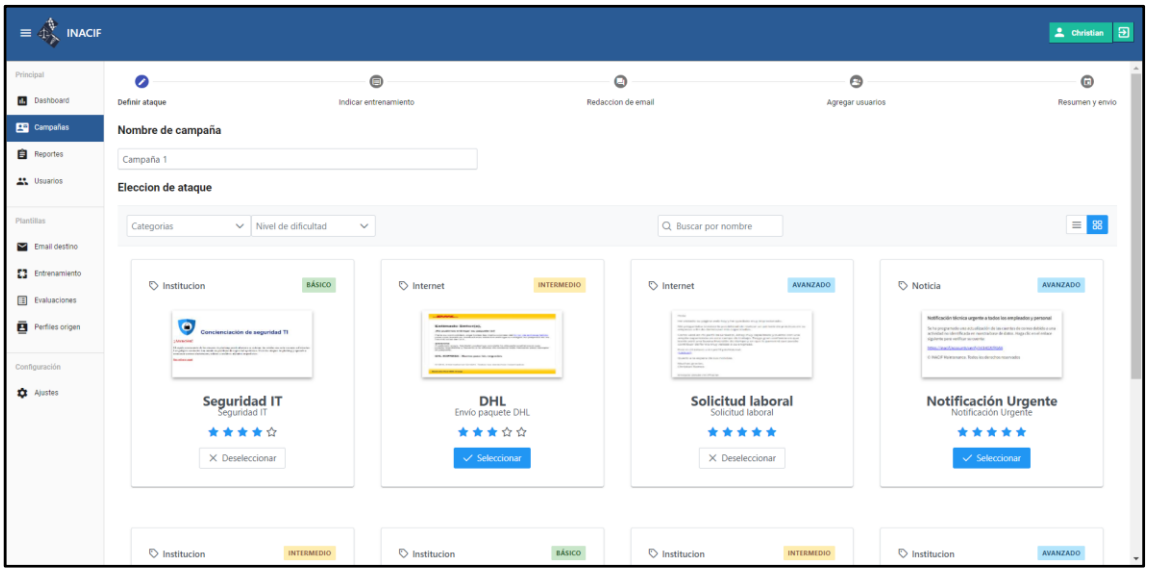
Legro, A. (2 de agosto de 2022) *Ataques informáticos: causas, tipos, consecuencias y prevenciones.* Win E Empresas. https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022

APÉNDICE

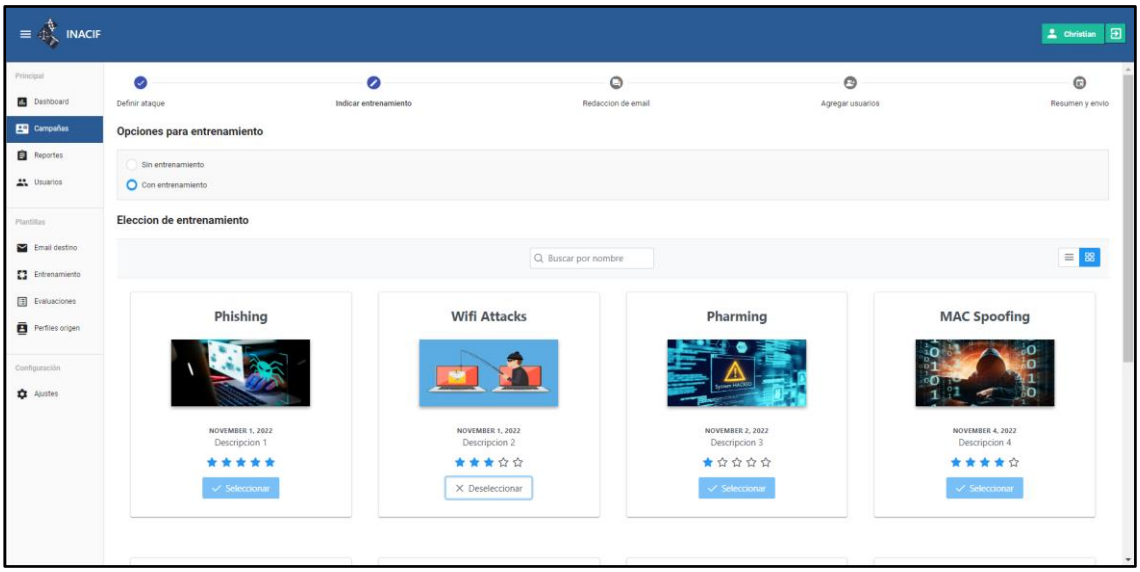
Apéndice 1.

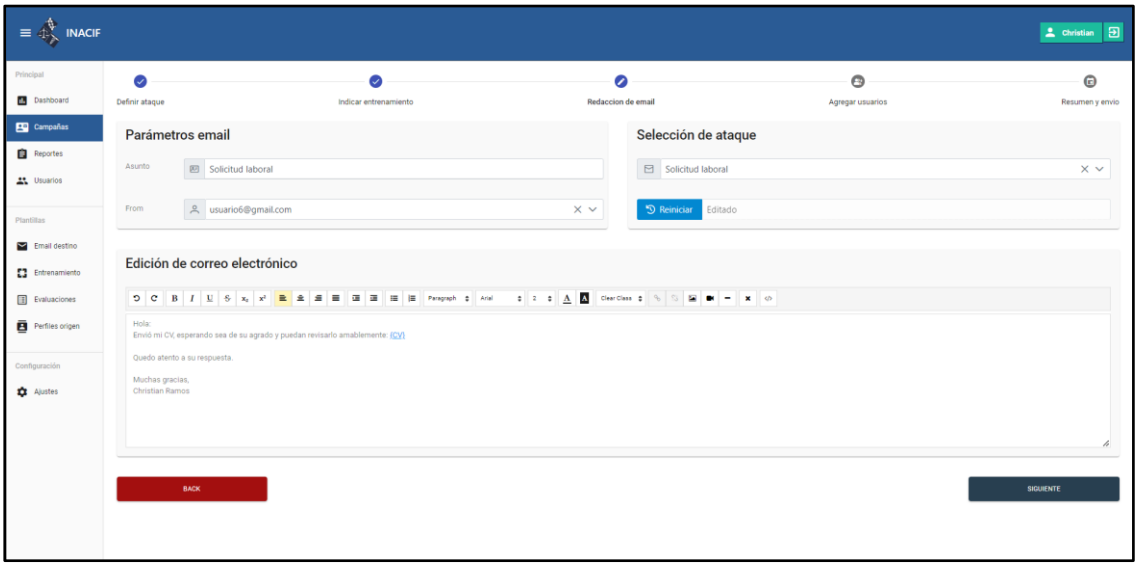
Capturas de pantalla del proyecto



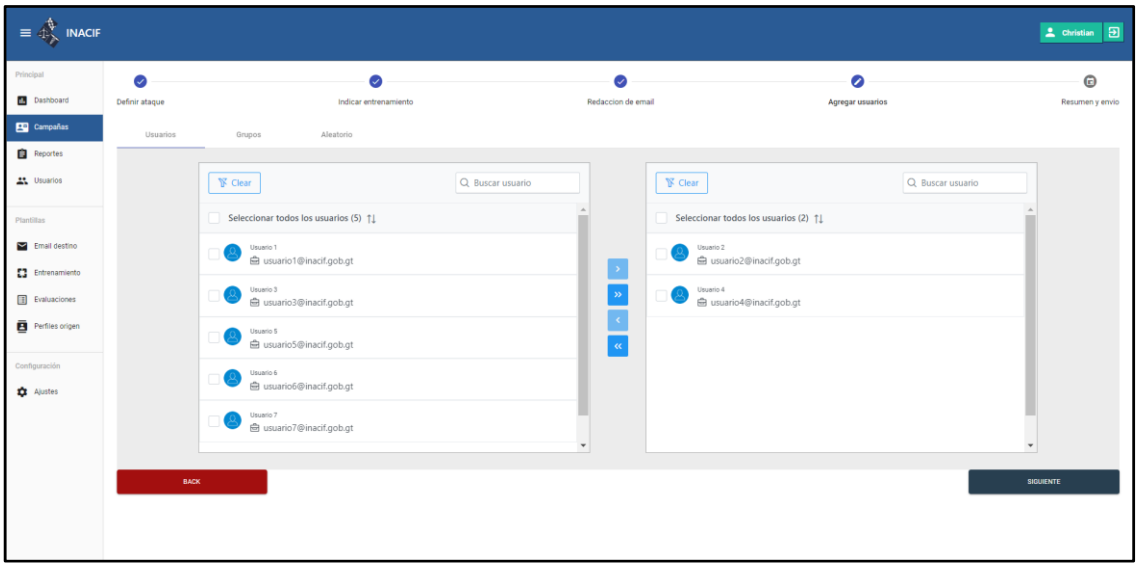


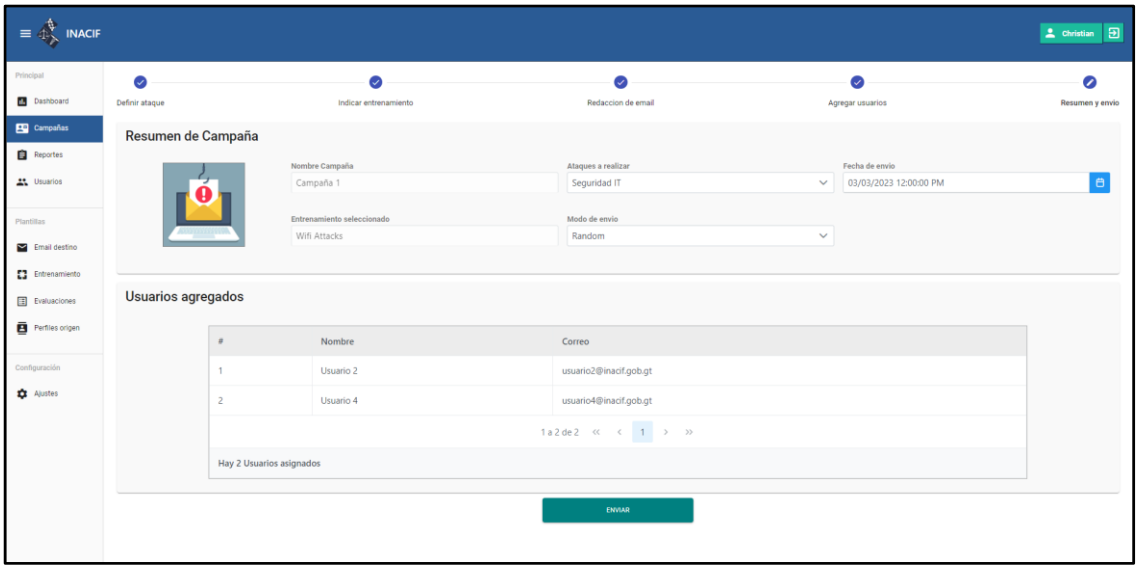
Continuación del apéndice 1.



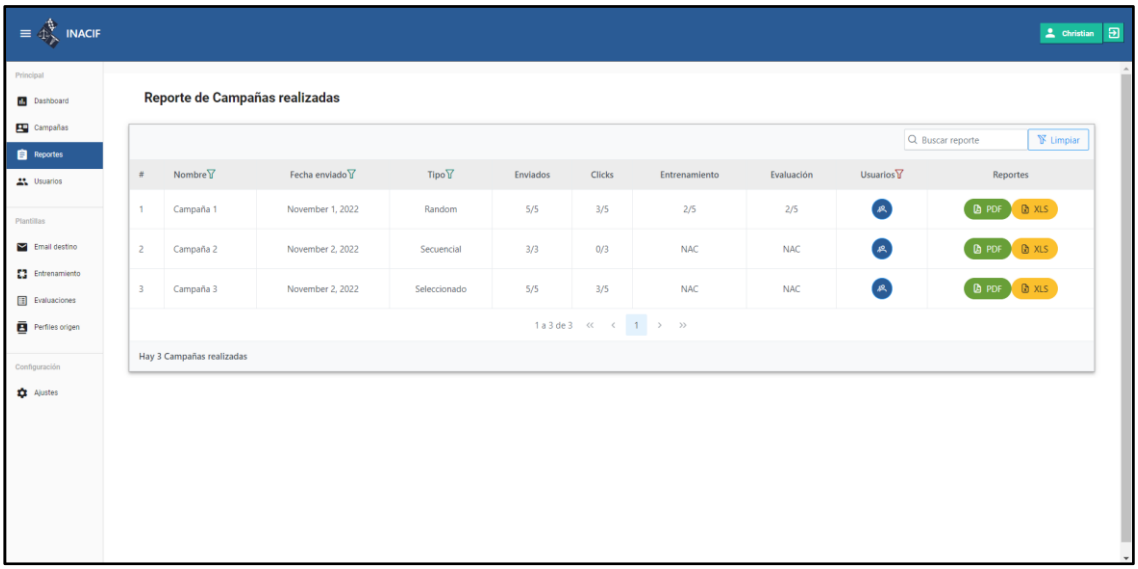


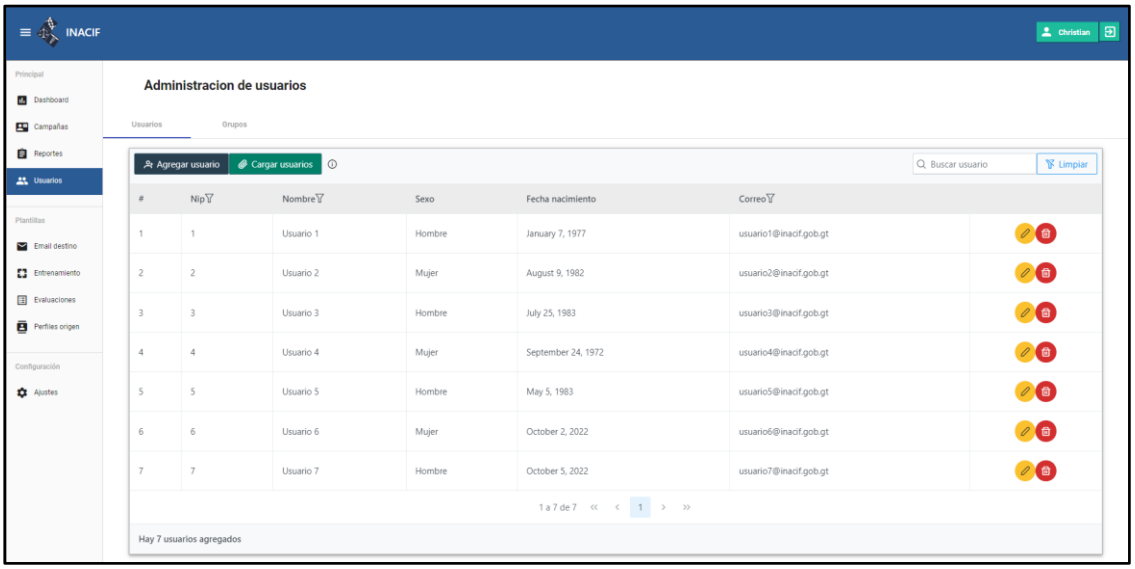
Continuación del apéndice 1.



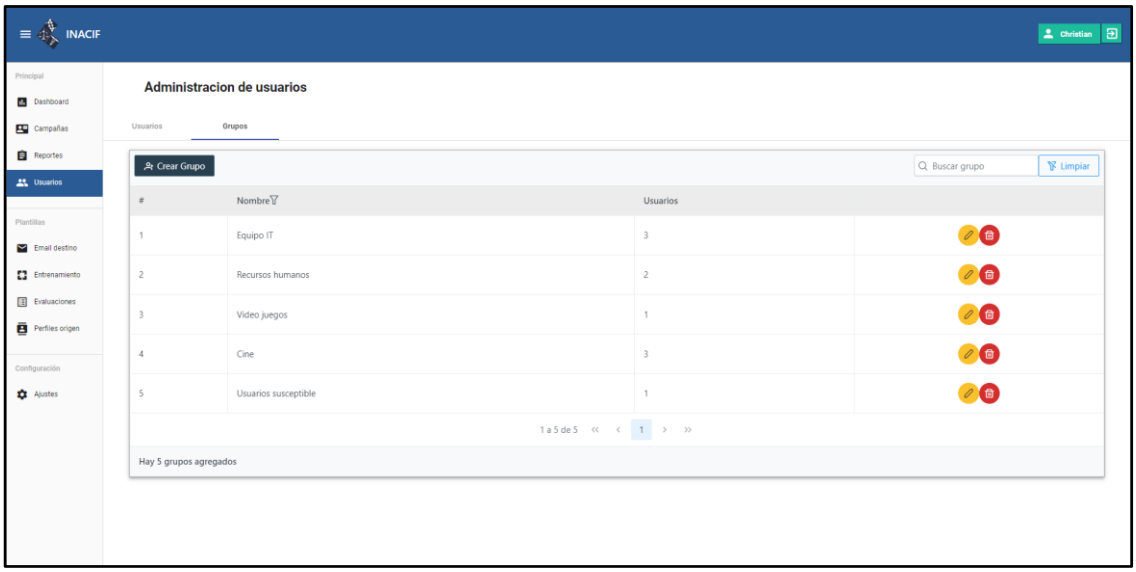


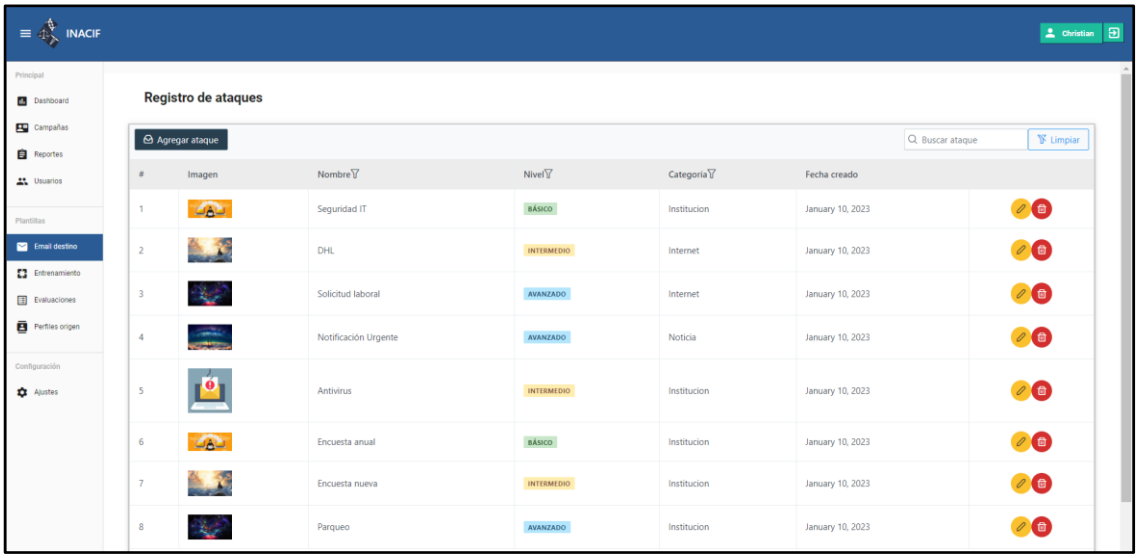
Continuación del apéndice 1.



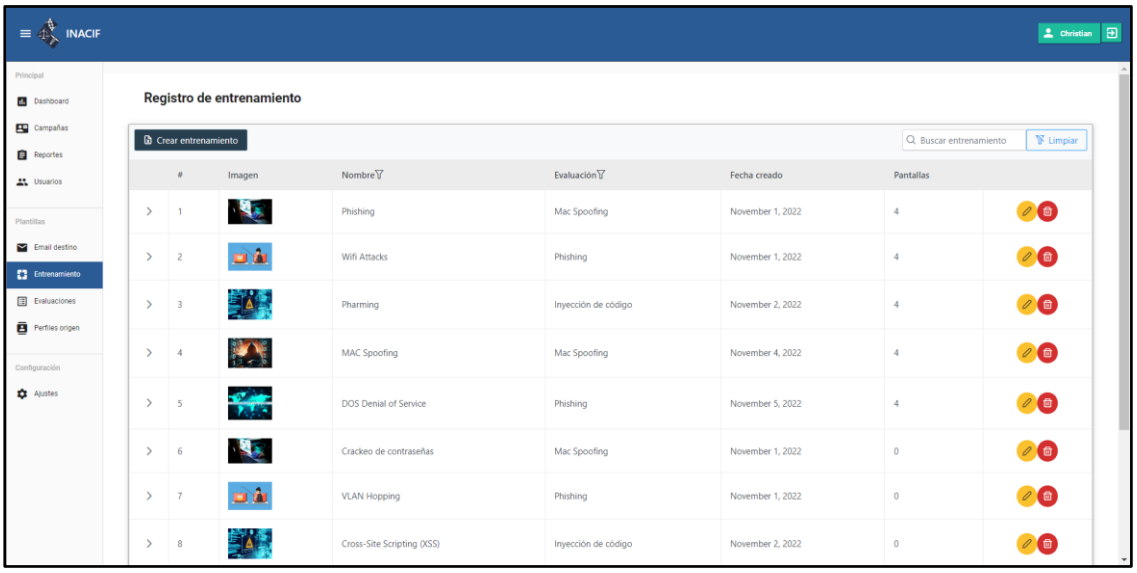


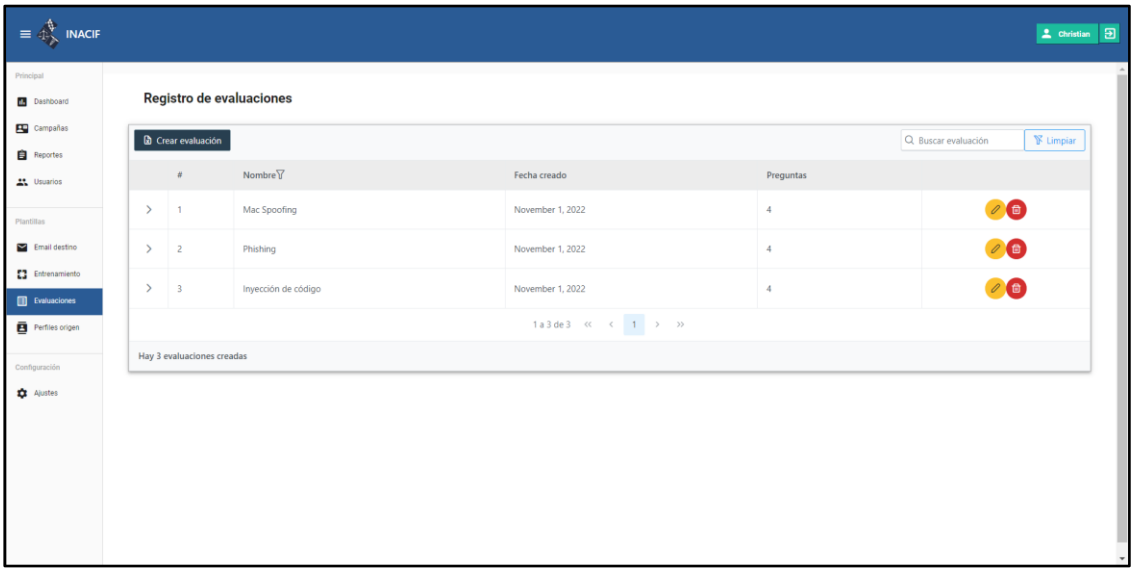
Continuación del apéndice 1.



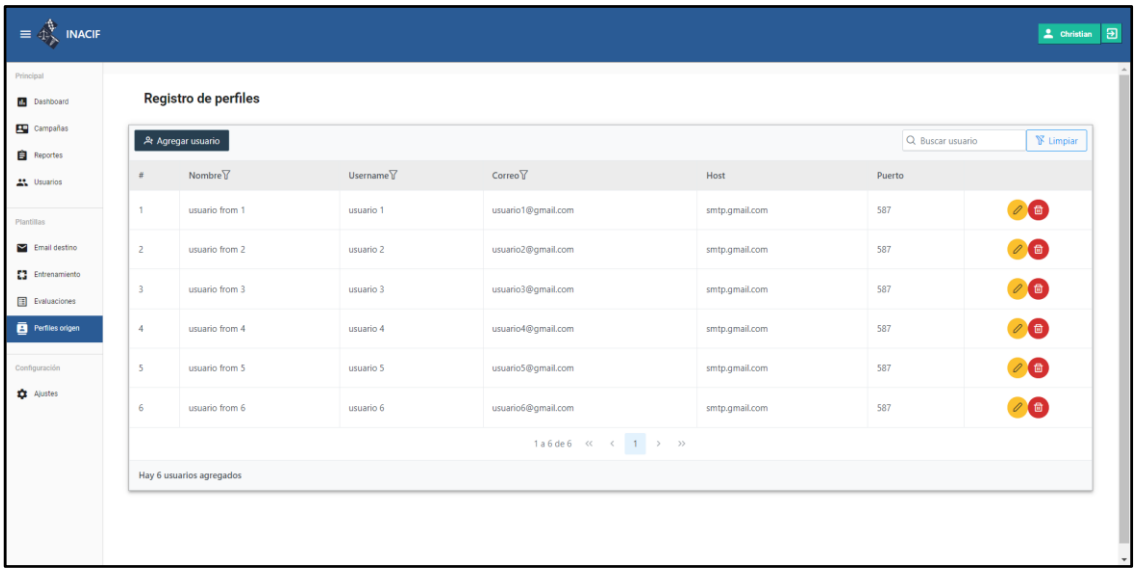


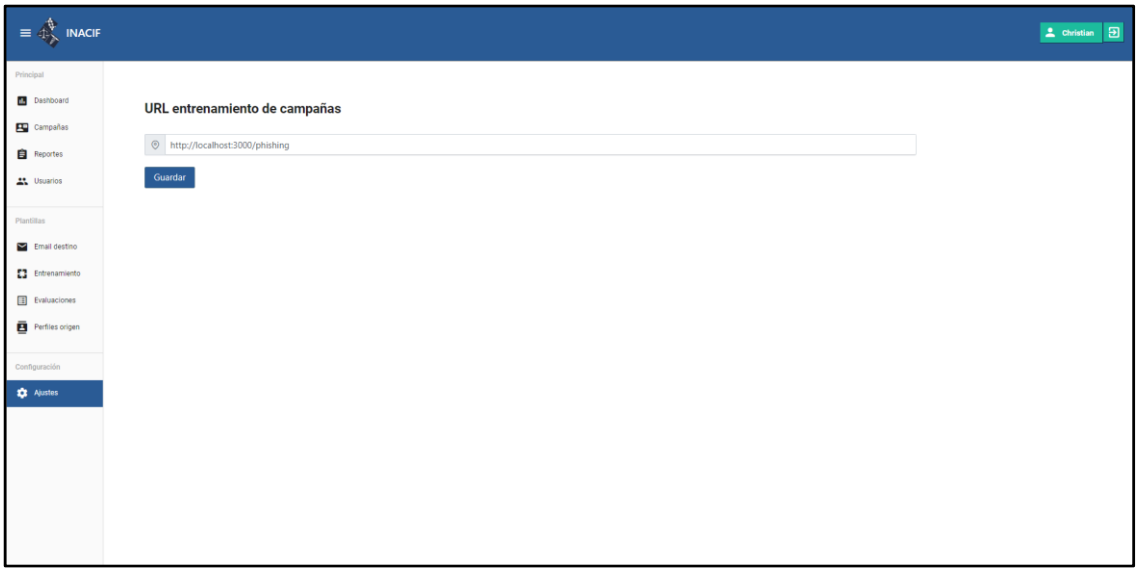
Continuación del apéndice 1.





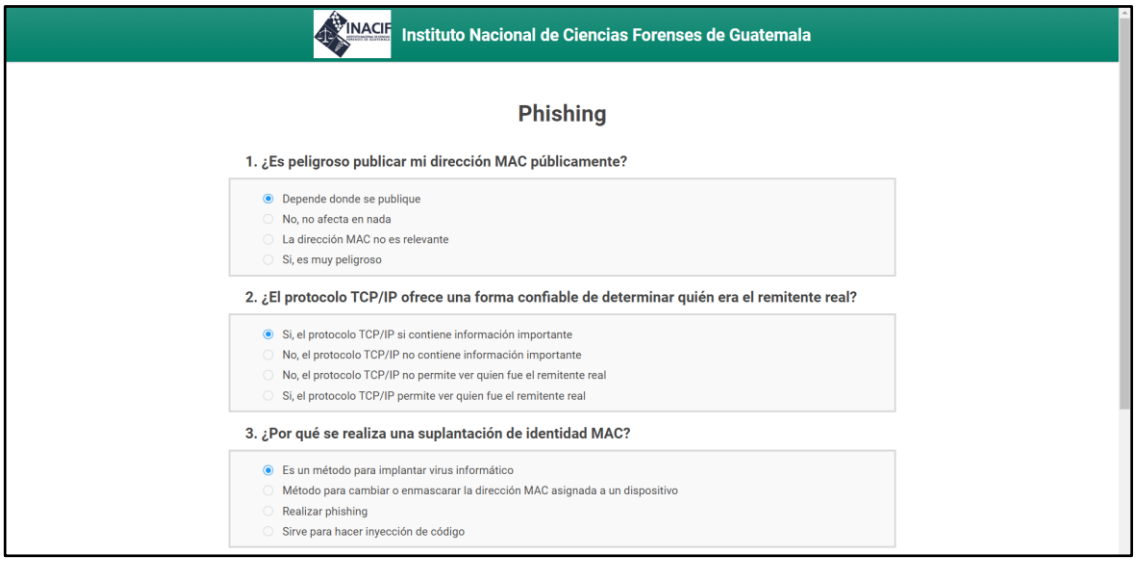
Continuación del apéndice 1.





Continuación del apéndice 1.

Continuación del apéndice 1.



Nota. Visualización de la propuesta del proyecto. Elaboración propia, realizado con draw.io.