UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA EN TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN CIBER ATAQUES DE INGENIERÍA SOCIAL PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN, DE LA UNIVERSIDAD TÉCNICA DE AMBATO.

Trabajo de Integración Curricular Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniera en Tecnologías de la Información

ÁREA: Seguridad de la Información

LÍNEA DE INVESTIGACIÓN: Tecnología de la Información y Sistemas de Control

AUTOR: Shirley Dennise Flores López

TUTOR: Ing. David Omar Guevara Aulestia, Mg.

Ambato – Ecuador

marzo – 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Integración Curricular con el tema: ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN CIBER ATAQUES DE INGENIERÍA SOCIAL PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN, DE LA UNIVERSIDAD TÉCNICA DE AMBATO, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Shirley Dennise Flores López, estudiante de la Carrera de Tecnologías de la Información de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 de las segundas reformas al Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado en la Universidad Técnica de Ambato y el numeral 7.4 del respectivo instructivo del reglamento.

Ambato, marzo 2023

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Omar Guevara Aulestia, Mg.
TUTOR

AUTORÍA

El presente trabajo de Integración Curricular titulado: ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN CIBER ATAQUES DE INGENIERÍA SOCIAL PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN, DE LA UNIVERSIDAD TÉCNICA DE AMBATO, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2023

Shirley Dennise Flores López

C.C. 1805246376

AUTORA

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Integración Curricular como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Integración Curricular en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, marzo 2023

Shirley Dennise Flores López

C.C. 1805246376

AUTORA

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Integración Curricular presentado por la señorita Shirley Dennise Flores López, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN CIBER ATAQUES DE INGENIERÍA SOCIAL PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN, DE LA UNIVERSIDAD TÉCNICA DE AMBATO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 de las segundas reformas al Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado en la Universidad Técnica de Ambato y al numeral 7.6 del respectivo instructivo del reglamento. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, marzo 2023

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
FELIX OSCAR FERNANDEZ PENA

Ing. Félix Oscar Fernández Peña
PROFESOR CALIFICADOR

Firmado electrónicamente por:
CARLOS ISRAEL NUNEZ MIRANDA

Ing. Carlos Israel Núñez Miranda
PROFESOR CALIFICADOR

DEDICATORIA

El presente proyecto es dedicado a mi madre, Patricia López, que es la persona más importante en mi vida, gracias por confiar en mi desde el primer momento que empezó este gran sueño, lleno de retos, obstáculos pero con la fe de que todo es posible, ya que es mi ejemplo, mi motor para salir Adelante y me demostró que con amor, sacrificio esfuerzo y dedicación se cumplen las metas y así termino una etapa maravillosa en mi vida.

A mis hermanos Estefanía y Juan Sebastían que siempre estuvieron motivandome para continuar con lo que había empezado.

A mis abuelitos, Manuel y Blanca que siempre me brindaron su apoyo incondicional y estuvieron pendientes de mi progreso en mi carrera universitaria.

A mi Tía Rocío López, que me animó en cada semestre y estaba al pendiente de mis estudios, gracias por cada llamada de aliento, que me impulsaron a ser mejor cada día.

Shirley Dennise Flores López

AGRADECIMIENTO

Agradezco a Dios, por las grandes oportunidades que me ha dado en la vida, gracias por brindarme la sabiduría y fortaleza para afrontar las adversidades, por guiarme e iluminarme siempre, por haber puesto en mi camino a personas que han sido mi soporte y compañía durante todo este tiempo, y por darme la oportunidad de crecer profesionalmente.

A mi madre en especial no tengo palabras para expresar mi gratitud por todo el amor y apoyo que me brindó durante toda mi etapa estudiantil.

A mis hermanos por estar siempre conmigo y me han brindado su ayuda cuando más lo he necesitado.

A mis abuelitos que siempre han estado apoyándome en cada momento y a toda mi familia que de una u otra manera estuvieron siempre dispuestos a ayudar.

A mis amigos y compañeros, gracias por todos los momentos compartidos a lo largo de esta hermosa carrera universitaria.

Gracias a todas las personas que confiaron en mí y fueron parte de todo este proceso universitario, me ayudaron a crecer tanto personalmente como profesionalmente mil gracias por todo su apoyo.

Shirley Dennise Flores López

Índice General

Índice de tablas y gráficos

Tablas

Gráficos

RESUMEN EJECUTIVO

La Ingeniería Social es un conjunto de técnicas, que permiten obtener información confidencial a través de la manipulación de personas. De manera práctica es una habilidad que ciertas personas hacen uso para obtener información, acceso a sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido.

Para el desarrollo del presente proyecto se ha utilizado la plataforma DigitalOcean para el servicio virtualizado en la nube, el framework Gophish que se utilizó para la creación, planificación y ejecución de simulación de ataques, mediante la técnica de Phishing y la Herramienta Hunter.io para el descubrimiento y recolección de correos electrónicos.

Es importante evaluar la seguridad de los sistemas informáticos que manejan información de la institución, sin embargo, el componente humano que manipula esta, puede llegar a ser una fuente de revelación de la misma, siendo útil para un atacante. Por consiguiente, es de vital importancia conocer el nivel de concientización sobre ciberseguridad que tienen los estudiantes y docentes.

El objetivo principal de estas pruebas es fortalecer la Seguridad de la Información en la institución, reforzando la conciencia de seguridad de los estudiantes y docentes de la Facultad de Ciencias Humanas y de la Educación, preparándolos para enfrentar diferentes escenarios de riesgos que podrían presentarse frente a un ataque real.

Palabras clave: Ingeniería social, digitalOcean, gophish, ataque, seguridad, concientización.

ABSTRACT

Social Engineering is a set of techniques that allow obtaining confidential information through the manipulation of people. In a practical way, it is an ability that certain people make use of to obtain information, access to information systems that allow them to carry out some act that harms or exposes the person or organization involved.

For the development of this project, the DigitalOcean platform was used for the virtualized cloud service, the Gophish framework was used for the creation, planning and execution of attack simulation, using the Phishing technique and the Hunter.io tool for the discovery and collection of emails.

It is important to evaluate the security of computer systems that handle information of the institution, however, the human component that manipulates this, can become a source of disclosure of the same, being useful for an attacker. Therefore, it is of vital importance to know the level of cybersecurity awareness of students and teachers.

The main objective of these tests is to strengthen Information Security in the institution, reinforcing the security awareness of students and teachers of the Faculty of Human Sciences and Education, preparing them to face different risk scenarios that could occur in the event of a real attack.

Keywords: Social engineering, digitalocean, gophish, attack, security, awareness.

CAPÍTULO I.-
MARCO TEÓRICO

1.1. Tema de Investigación

ANÁLISIS DE VULNERABILIDADES EN EL USO DE LAS REDES SOCIALES EN CIBER ATAQUES DE INGENIERÍA SOCIAL PARA FORTALECER LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS HUMANAS Y DE LA EDUCACIÓN, DE LA UNIVERSIDAD TÉCNICA DE AMBATO.

1.1.1. Planteamiento del Problema

Actualmente, las Redes Sociales (RRSS) se han convertido en el principal medio de comunicación de los seres humanos; como avanza la tecnología, se incrementa significativamente los diferentes tipos de ataques informáticos existentes en la actualidad, en el cual, las empresas, instituciones públicas o privadas, deben ir adaptándose a los cambios e innovaciones para mantener seguro el activo más valioso que es la información [1].

El amplio uso de las Redes Sociales afecta a los usuarios en los problemas de seguridad y privacidad, provenientes de la información, que se consigue fácilmente a través de publicaciones que comparten en estos medios, convirtiéndolas en uno de los principales vectores de ataque, por parte de los Ciberdelincuentes. A la par del crecimiento de los riesgos por el uso inadecuado de las Redes Sociales, aumenta también el crecimiento de los hackers, spammers, desarrolladores de virus y ladrones de datos e identidades, que se dedican al rastreo del tráfico de información que circula a través de las Redes Sociales [2].

Los principios de seguridad de la información: confidencialidad, integridad y disponibilidad, tienen como principal objetivo proteger la información de la entidad, en la actualidad existen diversos mecanismos de protección a nivel de software y hardware los cuales precautelan la seguridad de la información frente a ciberataques, sin embargo, en la actualidad varios ciberataques tienen como vector principal de ataque a la Ingeniería Social [3].

La Ingeniería Social es un problema, que se ha incrementado con el tiempo y con la tecnología, teniendo como objetivo a los usuarios y a los sistemas informáticos, ya que es el eslabón más débil en seguridad [4].

Los empresarios y líderes mundiales consideraron a los ataques cibernéticos como uno de los principales riesgos a los que se enfrentan en la actualidad, siendo la ciberseguridad su mayor reto [5].

Investigadores de la empresa de Antivirus ESET analizaron las detecciones de ataques de Ingeniería Social del pasado año e identificaron un importante crecimiento de este tipo de amenazas con respecto a 2019. En 2020, se duplicaron las detecciones de ataques de Ingeniería Social en Latinoamérica con Perú, Brasil y México como los países que se registraron la mayor cantidad de detecciones de ataques [6].

De acuerdo con un informe de la empresa de seguridad Kaspersky elaborado en agosto de 2021, los ataques cibernéticos en Latinoamérica aumentaron en un 24% en los primeros meses del año pasado, donde el Ecuador es uno de los países más vulnerados por los ciberdelincuentes, solo detrás de Brasil con el 13,3% de usuarios perjudicados. Así mismo, el portal de Cyber Economía "Cyber Magazine" estimó que para el 2025, las pérdidas causadas por el cibercrimen podrían costar 10,5 billones de dólares a la economía del mundo [7].

En base a lo establecido en el informe de Kaspersky en Ecuador, el término "CIBERSEGURIDAD" no es muy conocido por las diferentes sociedades, ya que no existe una estricta cultura de concientización y del uso adecuado de los medios digitales de comunicación en el ámbito educativo, laboral y social.

Hoy en día, se cuenta con varias herramientas de apoyo, para realizar diferentes acciones de Ingeniería Social y la manera de obtener información, esto facilita el trabajo y simplifica el conocimiento para cometer algún delito que puede llegar a tener consecuencias fatales para la mayor parte de las organizaciones [8].

Cada vez, la información es más vulnerable, ya que obtenerla no depende de algún malware malicioso, que sea el causante de la pérdida o fuga de la misma, en los ambientes informáticos, empresariales, educativos y personales, sino el uso y la ejecución de las diferentes técnicas, métodos, o medios dentro de la Ingeniería Social [9].

Las RRSS, brindan la oportunidad de comunicarse en tiempo real, interactuar, y permiten el intercambio de información entre personas, y/o empresas. Se conoce que

un usuario de Internet, posee al menos una red social activa. A partir de esto, los usuarios se ven expuestos a un conjunto de amenazas, que pueden atentar contra su información personal, algún tipo de extorsión o incluso su propia integridad.

En el uso diario de las RRSS en la ciudad de Ambato, en la facultad de Ciencias Humanas y de la Educación, los estudiantes exponen datos personales, que pueden ser ventajosos para el atacante, y ser sujeto de robo de identidad [10]. La Ingeniería Social es uno de los ataques más relevantes con la utilización de métodos psicológicos para el robo de la información de la víctima, en la cual, el ciberdelincuente realiza numerosas acciones fraudulentas, que perjudican al usuario final [11].

1.2. Antecedentes Investigativos

Revisando la investigación bibliográfica en algunas Universidades del Ecuador y artículos internacionales se han encontrado trabajos que servirán de apoyo en el trabajo de investigación.

(J. Urrutia franco y G. Hernández Flores), en el proyecto de investigación titulado "Ingeniería Social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil" en su análisis determino que los usuarios son susceptibles a ataques informáticos por el uso indebido de Ingeniería Social, conforme evoluciona la tecnología, las empresas públicas o privadas y personas deben ir adaptándose a los cambios e innovaciones

(R. Rocohano Ramos y L. Silva Ordoñez), en el proyecto de investigación titulado "Detección de Vulnerabilidades en el Comportamiento de las Personas para Evitar que sean Víctimas de Ataques de Ingeniería Social." indican que uno de los ataques más efectivos en la ciberseguridad, es el de Ingeniería Social, en que el atacante engaña a un usuario final, con la finalidad de perjudicarlo.

(J. Villacís Freire), en el artículo titulado "Social engineering attacks: a systematic mapping study" explora las tendencias en la seguridad tecnológica contra los ataques de Ingeniería Social, e identifica direcciones potenciales para futuras investigaciones.

(W. Chérrez y D. Pesantez), en el artículo titulado "Ciberseguridad en las Redes Sociales: una revisión teórica" expone que las Redes Sociales, constituyen una de las formas más novedosas de comunicación a nivel mundial. Su utilización es exponencial y paradójicamente a las innumerables ventajas que tiene, se evidencia un alto grado de

vulnerabilidad, debido entre otros aspectos a los constantes ataques y amenazas de las cuales son objeto.

(L. Gil Lluís), en el artículo titulado "Estudio de los ataques y su defensa en la Ingeniería Social" indica que, en el mundo de los ataques informáticos, la Ingeniería Social, irrumpe como una de las técnicas de mayor uso, dada su efectividad y el resultado que obtiene el atacante. Aprovechándose de que en el mundo tecnológico no todos los usuarios tienen conocimientos para no exponerse a dichos ataques.

1.3. Fundamentación Teórica

TIC's.- Las Tecnologías de Información y Comunicación (TICs) son el conjunto de herramientas relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de la información. Un aliado del emprendimiento, tanto en nuevos conceptos como en lo tradicional [17].

Seguridad de la Información.- Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos [18].

Ingeniería Social.- Es la combinación de técnicas basadas en el ser humano o en tecnología, las cuales son utilizadas por atacantes maliciosos para explotar al eslabón más débil de una organización, con el fin de obtener información confidencial o realizar acciones para comprometer la seguridad de la información [19].

Comunicación Digital.- Es el intercambio de información y conocimiento haciendo uso de las herramientas digitales disponibles, puestas a nuestra disposición por la investigación y desarrollo tecnológico [20].

Redes Sociales.- Son plataformas digitales formadas por comunidades de individuos con intereses, actividades o relaciones en común (como amistad, parentesco, trabajo). Las Redes Sociales permiten el contacto entre personas y funcionan como un medio para comunicarse e intercambiar información [21].

Usuarios.- Un usuario es aquel individuo que utiliza de manera habitual un producto, o servicio. Es un concepto muy utilizado en el sector informático y digital [22].

Vulnerabilidad.- es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad [23].

Riesgo.- Es una probabilidad de que una amenaza informática se convierta en un evento real que resulte en una pérdida para la empresa [24].

Activo de Información. - Son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades [25].

Ciberseguridad. - Es el conjunto de procedimientos y herramientas que se implementan para proteger los sistemas importantes y la información confidencial de los ataques digitales [26].

Ciberataque. - Es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas [27].

Osint. - (Open Source Intelligence)**,** traducido como Inteligencia de Fuentes Abiertas**,** hace referencia al conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en conocimiento útil [41]**.**

Humint. – es la inteligencia elaborada en base a la información obtenida y facilitada por fuentes humanas. Es decir, son personas las que obtienen información de personas [42].

Gophish. - es una plataforma gratuita y de código abierto diseñada especialmente para facilitar la formación de terceras personas en cuanto a seguridad [43].

Phishing. - Es un ataque informático de ingeniería social que usa medios de comunicación digitales, como el correo electrónico, para engañar y estafar a las personas. A través de técnicas de manipulación emocional genera confianza en las personas para poder robar su información y dinero [44].

Metodología Ágil. - es un conjunto de técnicas aplicadas en ciclos de trabajo cortos, con el objetivo de que el proceso de entrega de un proyecto sea más eficiente [45].

Kanban. - es un sistema visual para gestionar el trabajo a medida que avanza en un proceso. Kanban visualiza tanto el proceso (el flujo de trabajo) como el trabajo real que pasa por ese proceso [46].

WIP. - es la cantidad de tareas en las que un equipo está trabajando actualmente. Delimita la capacidad de los flujos de trabajo de sus equipos en cualquier momento [47].

Hunter.io. - es un portal web que permite buscar los emails de personas que trabajan en una empresa con solo introducir su página web [48].

1.4. Objetivos

1.4.1. Objetivo General

Fortalecer la Seguridad de la Información en el uso de las Redes Sociales en ciber ataques de Ingeniería Social en la Facultad de Ciencias Humanas y de la Educación, de la Universidad Técnica de Ambato.

1.4.2. Objetivos Específicos

1. Definir un plan de ataque de Ingeniería Social que permita cuantificar el nivel de seguridad del uso de las redes sociales en la Facultad de Ciencias Humanas y de la Educación.
2. Identificar las distintas brechas de seguridad relacionados con las Redes Sociales que pueden ser atacadas por medio de la Ingeniería Social.
3. Elaborar una estrategia de capacitación de los usuarios de las redes sociales en la Facultad de Ciencias Humanas y de la Educación.
4. Evaluar los resultados de la aplicación de la estrategia propuesta.

CAPÍTULO II.-
METODOLOGÍA

2.1. Materiales

Para el desarrollo del presente proyecto se utilizó dos encuestas con formulario para estudiantes y docentes de la Facultad de Ciencias Humanas y de la Educación, con la finalidad de recolectar información y determinar el nivel de conocimiento que tienen los estudiantes y docentes acerca del uso seguro de las redes sociales y conceptos de ciberseguridad.

2.2. Métodos

2.2.1. Modalidad de la Investigación

Los tipos de investigación que se aplicará en el estudio serán los siguientes:

2.2.1.1. Investigación de Campo

Se recopilará la información en la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato, dentro de la Ciudad de Ambato.

2.2.1.2. Bibliográfica

La investigación será Bibliográfica debido a que se tomará como apoyo a nuestra investigación el uso de libros, artículos científicos y fuentes existentes ya que serán de gran utilidad para respaldar científicamente las variables de esta indagación.

2.2.1.3. Nivel o tipo de investigación

Investigación Descriptiva

La investigación será Descriptiva porque se realizará un análisis de vulnerabilidades para determinar el nivel de riesgo en base a la usabilidad de las Redes Sociales, bajo la modalidad de Ingeniería Social.

Investigación Correlacional

La investigación será correlacional ya que el análisis se observa cuando existe mayor uso de Redes Sociales y exposición de datos, la Ingeniería Social permitiría la extracción de esta información.

Investigación Explicativa

La investigación es Explicativa porque se va a poder sustentar la importancia que tiene la seguridad de la información y la aplicación de la Ingeniería Social, a los usuarios por medio de Redes Sociales.

2.2.2. Población y Muestra

2.2.2.1. Población

Para la presente investigación, la Población está conformada por los docentes y estudiantes de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato.

2.2.2.2. Muestra

Para la presente investigación, se usará la técnica de muestreo probabilístico, para seleccionar de manera aleatoria, una muestra del total de la población seleccionada.

Población Docentes

Tabla 1. Población Docentes

Población Docentes	Número	Porcentaje
Pedagogía Carrera de Idiomas Nacionales y Extranjeros.	14	15.56%
Carrera de Educación Básica.	19	21.11%
Carrera de Educación Inicial.	18	20%
Pedagogía de Cultura Física y el Deporte.	20	22.22%

Carrera de Turismo y Hotelería.	19	21.11%
Total:	90	100%

Elaborado por: Shirley Flores

En virtud de que la población de docentes a ser investigadas no supera los cien elementos, se trabajará con la totalidad del universo sin que sea necesario obtener la muestra representativa.

Muestra de Estudiante

Tabla 2. Muestra de Estudiantes

Población Estudiantes	Número	Porcentaje
Pedagogía Carrera de Idiomas Nacionales y Extranjeros.	354	21.16%
Carrera de Educación Básica.	371	22.18%
Carrera de Educación Inicial.	324	19.37%
Pedagogía de Cultura Física y el Deporte.	374	22.35%
Carrera de Turismo y Hotelería.	250	14.94%
Total:	**1673**	**100%**

Elaborado por: Shirley Flores

Cálculo de Muestra

Tamaño de la muestra N = 1673

Confianza Z = 0,95 -> 1,96

Error de muestreo e = 0,05

Desviación estándar s = 0,5

$$\boldsymbol{n = \frac{(1673)(0,5)^2(1,96)^2}{(1673-1)(0,05)^2 + (0,5)^2\,(1,96)^2}}$$

$$n = 313\ estudiantes$$

2.2.3. Recolección de la Información

Para el desarrollo de la presente investigación se empleó la técnica de la encuesta (Anexo A.1), misma que se aplicó a los estudiantes, y docentes de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato que ha permitido la extracción necesaria de información.

2.2.3.1. Resultados de las Encuestas aplicadas

Las encuestas fueron aplicadas a 304 estudiantes y 90 docentes de la Facultad de Ciencias Humanas y de la Educación de la Universidad Técnica de Ambato siendo un total de 394 encuestados, en donde se obtuvo los siguientes resultados:

1. Pregunta 1: ¿Señale el género al que pertenece?

Tabla 3. Género de encuestados

Género	Cantidad	Porcentaje
Femenino	249	63%
Masculino	145	37%
Total	394	100%

Elaborado por: Shirley Flores

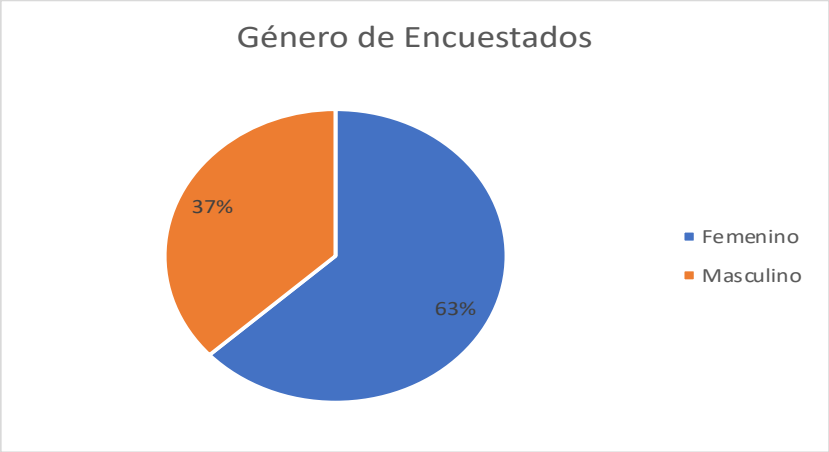


Gráfico 1. Género de encuestados

Elaborado por: Shirley Flores

Análisis

En la encuesta realizada sobre el tema a desarrollarse 394 de los encuestados de la Facultad de Ciencias Humanas y de la Educación, 249 son femeninas representando el 63%, y las 145 personas restantes son masculinos representando el 37%.

Interpretación de resultados

Se determina que la mayor cantidad de estudiantes y docentes son mujeres dentro de la facultad de Ciencias Humanas y de la Educación.

2. Pregunta 2: ¿En qué rango de edad se encuentra?

Tabla 4. Rango de edades

Edad	Cantidad	Porcentaje
14-18 años	35	9%
19-24 años	192	49%
25-34 años	89	23%
35-44 años	29	7%
45-55 años	42	11%
Más de 55 años	7	2%
Total	394	100%

Elaborado por: Shirley Flores

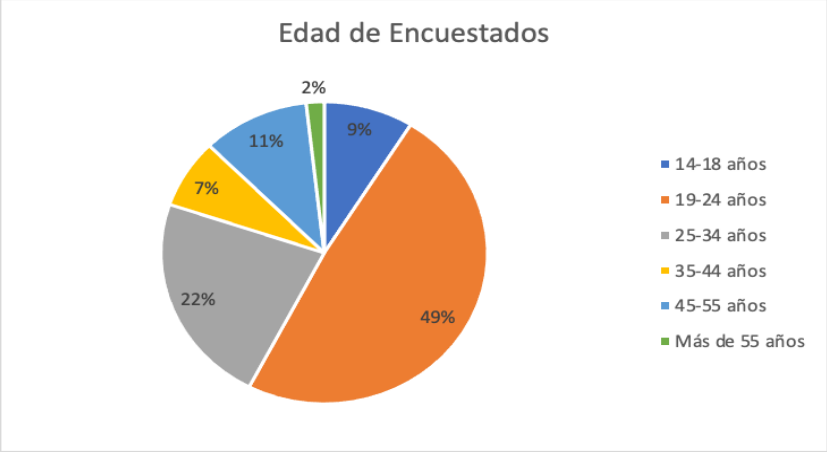


Gráfico 2. Rango de edades
Elaborado por: Shirley Flores

Análisis

De los 394 encuestados, 35 pertenecen al grupo de 14 a 18 años de edad representando el 9%, 192 encuestados se encuentran en el grupo 19 a 24 años de edad representando el 49%, los 89 encuestados se encuentran en el grupo de 25 a 34 años de edad representando el 23%. Los 29 encuestados se encuentran en el grupo de 35 a 44 años siendo esto el 7%, los 42 encuestados son el 11% del grupo de 45 a 55 años y los 7 encuestados siendo el 2% perteneciente al grupo más de 55 años.

Interpretación de resultados

El 49% representan a estudiantes de entre los 19 y 24 años de edad, estos pueden ser considerados como estudiantes que se encuentran en formación profesional.

3. Pregunta 3: ¿Con qué fin utiliza las redes sociales?

Tabla 5. Uso de redes sociales

Finalidad del Uso de Redes Sociales	Cantidad	Porcentaje
Entretenimiento	95	24%
Educativo	57	14%
Informativo	45	11%
Trabajo	31	8%
Todas las anteriores	154	39%
Otras	12	3%
Total	394	100%

Elaborado por: Shirley Flores

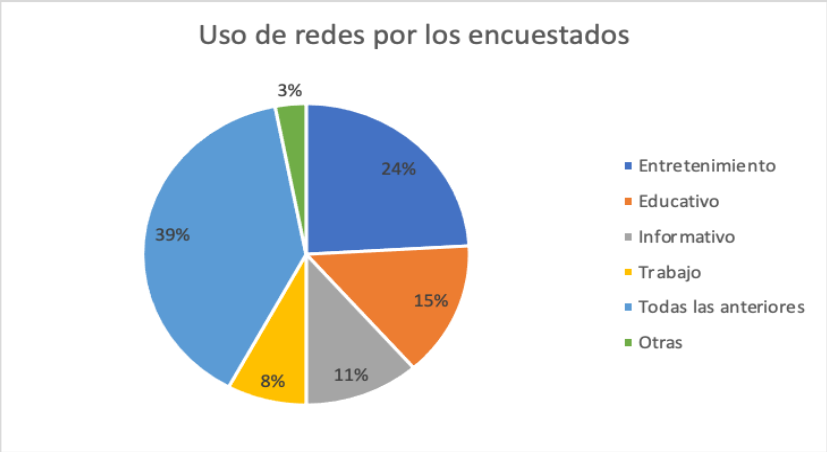


Gráfico 3. Uso de redes sociales
Elaborado por: Shirley Flores

Análisis

Cuando se utiliza una red social es para compartir información, por lo que, de los 394 encuestados, 95 encuestados que representa el 24% mismos que utilizan como entretenimiento, 57 encuestados lo utilizan para educación siendo el 14%, 45 lo utilizan como informativo siendo el 11%. Los 31 encuestados que representa el 8% utiliza para trabajo; los 154 encuestados que representa el 39% utiliza en todos los ámbitos mencionados anteriormente y el 3% restante siendo 12 encuestados utiliza para otros fines.

Interpretación de resultados

Generalmente, los encuestados y público en general utilizan las redes sociales como medios de ocio, para fines profesionales y de comercio esto también para el conocimiento de la situación de su localidad.

4. Pregunta 4: ¿Cuántos caracteres utiliza en las contraseñas para registrarse en la cuenta de las redes sociales?

Tabla 6. Uso de caracteres en las contraseñas

Num. Caracteres en Contraseña	Cantidad	Porcentaje
5 - 8	184	47%
9 - 12	163	41%
13 - 16	47	12%
Total	394	100%

Elaborado por: Shirley Flores

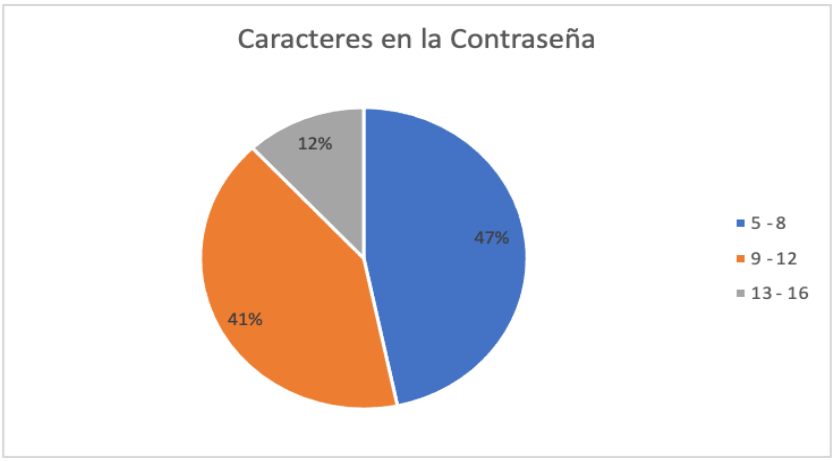


Gráfico 4. Uso de caracteres en las contraseñas
Elaborado por: Shirley Flores

Análisis

De los 394 encuestados siendo el 100%, el 47% representado por 184 personas, usan de 5 a 8 caracteres en sus contraseñas, el 41% representado por 163 personas establecen de 9 a 12 caracteres en sus contraseñas y el 12% restante representado por 47 personas utilizan de 13 a 16 caracteres en sus contraseñas.

Interpretación de resultados

Se puede suponer que los usuarios encuestados el 47% mantiene una contraseña considerada como seguridad baja, no obstante, pueden ser contraseñas de fácil recordatorio, nombres, frase o palabras comunes. El 12% posiblemente tenga un ligero conocimiento en materia de seguridad.

5. Pregunta 5: ¿Qué nivel de conocimiento tiene respecto a las amenazas y los riesgos informáticos que están presentes en las redes sociales?

Tabla 7. Conocimiento de las amenázas informáticas

Conocimiento de Amenazas	Cantidad	Porcentaje
Alto	91	23%
Medio	179	45%
Bajo	124	31%
Total	394	100%

Elaborado por: Shirley Flores

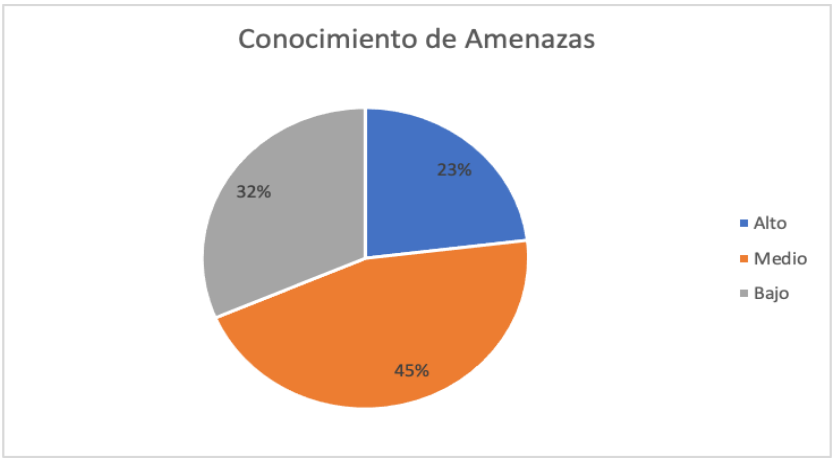


Gráfico 5. Conocimiento de las amenázas informáticas
Elaborado por: Shirley Flores

Análisis

De 394 encuestados, 91 representado por el 23% tienen alto conocimiento de las amenazas y los riesgos informáticos, 179 encuestados mantienen un conocimiento medio sobre las amenazas y los riesgos informático siendo el 45%, y los 124 encuestados restantes representado por el 31% tiene conocimientos bajos sobre amenazas y riesgos informáticos.

Interpretación de resultados

Se puede mencionar que los 91 encuestados posiblemente mantengan una noción de las amenazas de ciberseguridad, lo cual permitiría reducir el impacto de robo de información, a diferencia de los 179 encuestados, que tienen un conocimiento medio sobre amenazas de ciberseguridad. Y, por último 124 encuestados que se debe mantener una capacitación exhaustiva para mejorar el entendimiento sobre amenazas de ciberseguridad.

6. Pregunta 6: ¿Utiliza contraseñas diferentes para sus cuentas electrónicas como redes sociales, email, aula virtual?

Tabla 8. Contraseñas diferentes

Contraseñas diferentes	Cantidad	Porcentaje
Si	239	61%
No	155	39%
Total	394	100%

Elaborado por: Shirley Flores

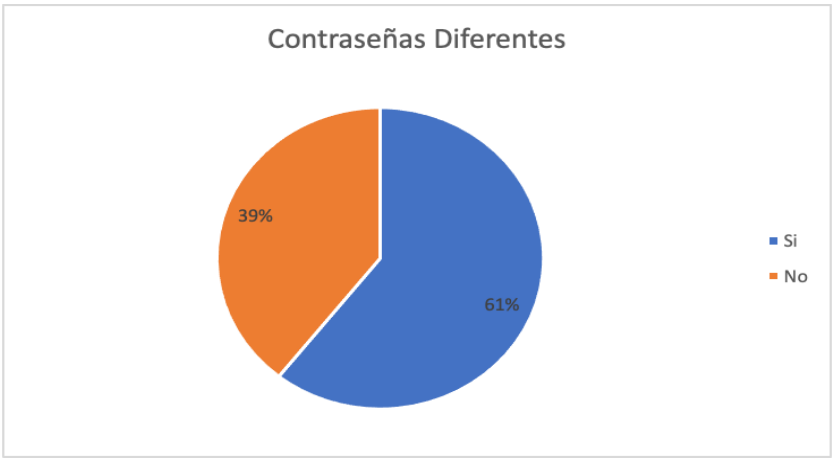


Gráfico 6. Contraseñas diferentes
Elaborado por: Shirley Flores

Análisis

De los 394 encuestados, 239 estudiantes siendo el 61% tienen diferentes contraseñas en sus redes sociales, y las 155 personas restantes siendo el 39% mantiene la misma contraseña para diferentes redes sociales.

Interpretación de resultados

Se puede especular que un bajo porcentaje siendo el 39% mantienen la misma contraseña, por temas de recordatorio y fácil manejo de claves.

7. **Pregunta 7: Asigna un valor, donde 0 es nada frecuente y 5 es muy frecuente, ¿Qué tanto utiliza las siguientes redes sociales? Facebook, Twitter, Instagram WhatsApp, LinkedIn, Tic Tok, Snapchat, Telegram.**

Tabla 9. Uso de redes sociales

Utilización de Redes Sociales	0	1	2	3	4	5
Facebook	7,87%	12,18%	12,69%	23,35%	23,35%	20,56%
Twitter	48,22%	15,99%	12,69%	7,11%	7,87%	8,12%
Instagram	13,71%	12,44%	14,21%	16,50%	15,99%	27,16%
WhatsApp	0,51%	0,51%	3,05%	6,60%	16,50%	72,84%
LinkedIn	53,81%	10,91%	6,35%	7,61%	4,31%	17,01%
Tic Tok	25,13%	10,41%	10,41%	17,51%	14,97%	21,57%
Snapchapt	46,95%	18,27%	11,17%	9,64%	4,06%	9,90%
Telegram	43,15%	20,56%	11,17%	11,42%	4,31%	9,39%

Elaborado por: Shirley Flores

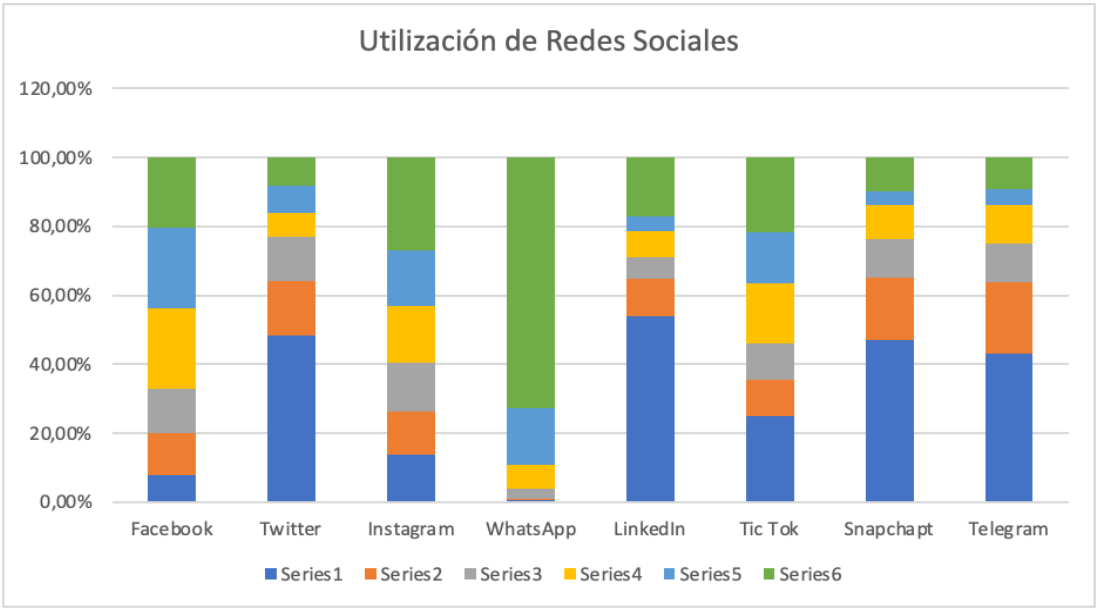


Gráfico 7. Uso de redes sociales
Elaborado por: Shirley Flores

Análisis

En la escala de Likert se mantienen 8 redes sociales que son utilizadas frecuentemente, de una escala de 0 siendo la red social menos usada hasta 5 siendo la red más usada, por lo que, Facebook para el 7,87% de encuestados nunca utiliza esta red, el 12,18% rara vez utiliza esta red, el 12,69% ocasionalmente utiliza esta red, 23,35% frecuentemente utiliza esta red y el 23,35% casi siempre utilizan esta red, y el 20,56%

de encuestados siempre ocupan Facebook. Para el caso de Twitter el 48,22% de encuestados nunca utiliza esta red, el 15,99% rara vez utiliza esta red, el 19,69% ocasionalmente utiliza esta red, 7,11% frecuentemente utiliza esta red y el 7,87% casi siempre utilizan esta red, y el 8,12% de encuestados siempre ocupan Twitter. Para Instagram el 13,71% de encuestados nunca utiliza esta red, el 12,44% rara vez utiliza esta red, el 14,21% ocasionalmente utiliza esta red, 16,50% frecuentemente utiliza esta red y el 15,99% casi siempre utilizan esta red, y el 27,16% de encuestados siempre ocupan Instagram. WhatsApp el 0,51% de encuestados nunca utiliza esta red, el 0,51% rara vez utiliza esta red, el 3,05% ocacionalmente utiliza esta red, 6,60% frecuentemente utiliza esta red y el 16,50% casi siempre utilizan esta red, y el 72,84% de encuestados siempre ocupan WhatsApp, siendo una de las redes sociales más utilizadas. Para LinkedIn una red social para profesionales el 53,81% de encuestados nunca utiliza esta red, el 10,91% rara vez utiliza esta red, el 6,35% ocasionalmente utiliza esta red, 7,61% frecuentemente utiliza esta red y el 4,31% casi siempre utilizan esta red, y el 17,01% de encuestados siempre ocupan LinkedIn que ayuda a darse a conocer dentro del mercado laboral. Tic Tok el 25,13% de encuestados nunca utiliza esta red, el 10,41% rara vez utiliza esta red, el 10,41% ocasionalmente utiliza esta red, 17,51% frecuentemente utiliza esta red y el 14,97% casi siempre utilizan esta red, y el 21,57% de encuestados siempre ocupan Tic Tok como entretenimiento. Snapchat el 46,95% de encuestados nunca utiliza esta red, el 18,27% rara vez utiliza esta red, el 11,17% ocasionalmente utiliza esta red, 9,64% frecuentemente utiliza esta red y el 4,06% casi siempre utilizan esta red, y el 9,90% de encuestados siempre ocupan Snapchat. Y finalmente se menciona a Telegram, el 43,15% de encuestados nunca utiliza esta red, el 20,56% rara vez utiliza esta red, el 11,17% ocasionalmente utiliza esta red, 11,42% frecuentemente utiliza esta red y el 4,31% casi siempre utilizan esta red, y el 9,39% de estudiantes siempre ocupan Telegram.

Interpretación de resultados

En la actualidad la red social más utilizada es el WhatsApp, siendo una herramienta de comunicación para todos los usuarios, para el envío de datos, información y comunicación directa, a pesar de ello, es una app que puede ser vulnerable para los usuarios mismos.

8. Pregunta 8: ¿Con que frecuencia publica información en sus redes sociales?

Tabla 10. Frecuencia de publicaciones

Frecuencia de publicación	Cantidad	Porcentaje
Todos los días	69	18%
2 veces por semana	39	10%
1 vez a la semana	61	15%
Al menos una vez cada 15 días	181	46%
Solo los fines de semana	44	11%
Total	394	100%

Elaborado por: Shirley Flores

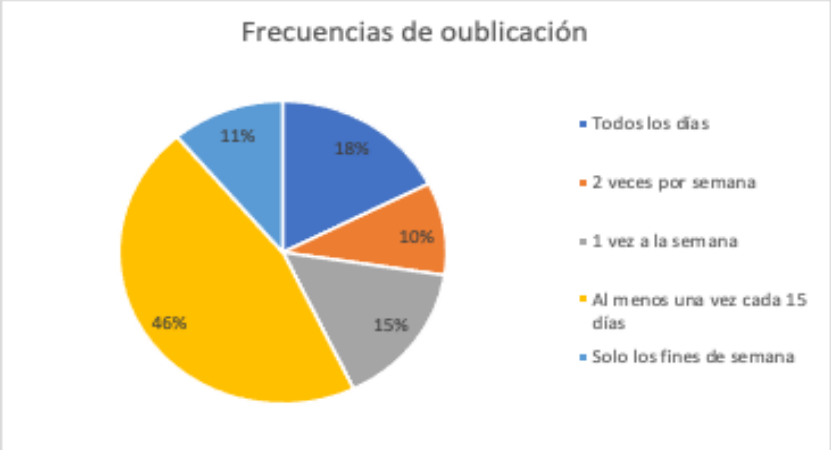


Gráfico 8. Frecuencia de publicaciones
Elaborado por: Shirley Flores

Análisis

De 394 encuestados, el 18% representado por 69 personas publican información todos los días, el 10% siendo 39 personas publican 2 veces por semana, el 15% siendo 61 personas 1 vez a la semana, el 46% siendo 181 personas publican información al menos una vez cada quince días y el 11% restante siendo 44 personas publican solo los fines de semana.

Interpretación de resultados

Se puede mencionar que la publicación de información, ha permitido a los ciberdelincuentes suplantar identidad, sabiendo de que los usuarios ignoran estas prácticas tecnológicas.

9. Pregunta 9: ¿Qué tipo de Contenidos, publica con mayor frecuencia en redes sociales?

Tabla 11. Tipo de publicación

Tipos de Publicaciones	Porcentaje
Solo Textos	11,42%
Texto con Imagen o Fotografía	39,85%
Solo Imágenes o Fotografías	24,62%
Videos	21,07%
Videos con Texto	22,59%
Audios	1,52%
Historias	51,27%
No publico nada	9,90%

Elaborado por: Shirley Flores

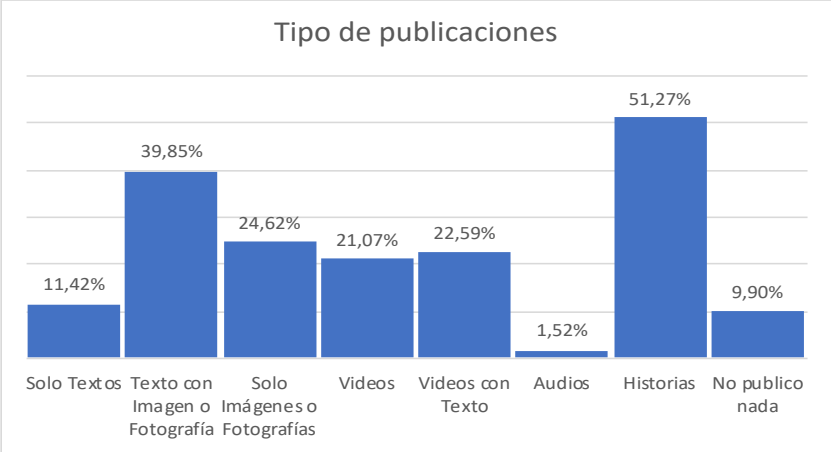


Gráfico 9. Tipo de publicación
Elaborado por: Shirley Flores

Análisis

Los estudiantes encuestados han establecido lo que les gusta publicar, el 11,42% menciona que publica solo textos, el 39,85% texto con imagen o fotografía, el 24,62% solo imágenes o fotografías, el 21,07% publica videos, 22,59% videos con texto, el 1,52% publica audios, el 51,27% publica historias y el 9,90% no publica nada.

Interpretación de resultados

Se puede mencionar que los estudiantes normalmente publica sus actividades diarias atreves de historias, estas pueden ser publicadas en WhatsApp, Facebook e Instagram. Se puede suponer que el 25% siempre publica imagen con anecdotas.

10. Pregunta 10: ¿Conoce acerca de lo qué es la Ingeniería Social?

Tabla 12. Conocimiento de ingeniería social

Conocimiento de Ingeniería Social	Cantidad	Porcentaje
Si	107	27%
No	287	73%
Total	394	100%

Elaborado por: Shirley Flores

Gráfico 10. Conocimiento de ingeniería social
Elaborado por: Shirley Flores

Análisis

De los 394 encuestados, 107 personas representado el 27% si conocen lo que es la ingeniería social, y el 73% restante siendo 287 personas no conocen sobre lo que significa ingeniería social.

Interpretación de resultados

Se menciona que el porcentaje más alto el 88% pueden ser personas que en su diario vivir presentan ataques de ingeniería social sin conocer sus efectos y las consecuencias que provoca de dicha técnica.

11. Pregunta 11: ¿Cuál de estos ciberataques conoce, y que los podría explicar a otras personas?

Tabla 13. Ciberataques

Conocimiento de Ciberataques	Porcentaje
Ransomware	7,87%
Phishing	28,93%
Ataques por denegación de servicios (DDoS)	9,64%
Troyanos	26,40%
Ninguna	52,54%

Elaborado por: Shirley Flores

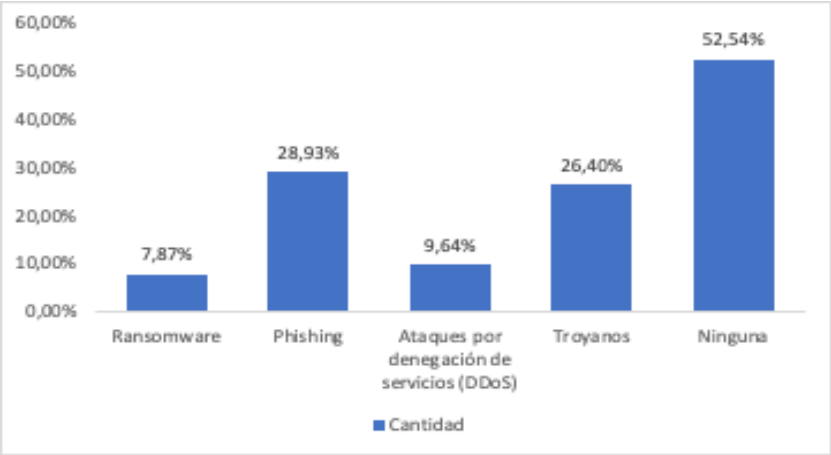


Gráfico 11. Ciberataques
Elaborado por: Shirley Flores

Análisis

Los estudiantes encuestados han establecido que, el 7,87% conoce lo que es un ransomware, el 28,93% conoce lo que es el phishing, el 9,64% conoce de ataques por denegación de servicios (DDoS), el 26,40% conoce de troyanos, el 52,54% no conoce ningún ciberataque.

Interpretación de resultados

Se puede mencionar que el 50% de estudiantes desconoce sobre los ataques realizados en la infraestructura de la red, el otro 50% tal vez por publicaciones realizadas por diferentes medios de comunicación acerca del robo de información en las diferentes entidades ecuatorianas, han permitido desarrollar cierto criterio sobre la ciberseguridad.

12. Pregunta 12: ¿Qué tipo de fraudes electrónicos le genera mayor temor?

Tabla 14. Fraudes electrónicos

Fraudes Electrónicos	Cantidad	Porcentaje
Que me roben dinero de mis cuentas bancarias	124	31%
Suplantación de identidad	136	35%
Que secuestren mi WhatsApp	85	22%
Estafas en sitios web ilegítimos	49	12%
Total	394	100%

Elaborado por: Shirley Flores

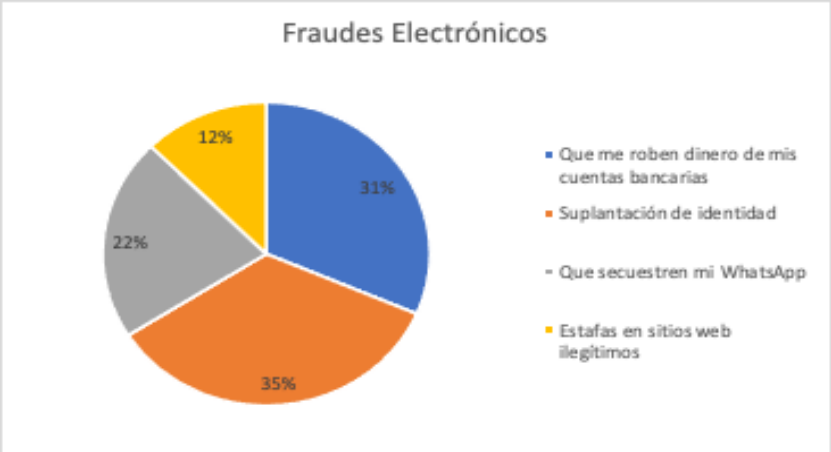


Gráfico 12. Fraudes electrónicos
Elaborado por: Shirley Flores

Análisis

De 394 encuestados, 124 personas que representa el 31% presentan el temor de sustracción de efectivo de las cuentas bancarias, 136 personas que representa el 35% presenta temor a la suplantación de identidad, 85 personas que representa el 22% presentan temor en el secuestro de WhatsApp y los 49 encuestados restantes que representa el 12% presentan el temor de ser estafados en sitios web ilegítimos.

Interpretación de resultados

Uno de las técnicas más utilizadas por los ciberdelincuentes es la suplantación de identidad, esto se puede verificar con entidades financieras donde su personal hasta los gerentes presenta suplantación para la entrega de servicios financieros.

13. Pregunta 13: ¿Alguna vez han vulnerado la seguridad de sus cuentas electrónicas (Redes Sociales, email, banco virtual, etc.)?

Tabla 15. Vulneración en cuentas

Vulnerabilidad Expuesta	Cantidad	Porcentaje
Si	107	27%
No	287	73%
Total	394	100%

Elaborado por: Shirley Flores

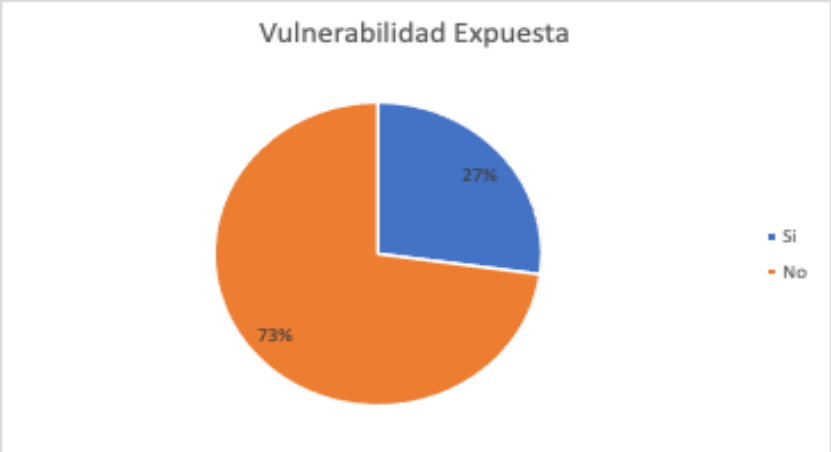


Gráfico 13. Vulneración en cuentas
Elaborado por: Shirley Flores

Análisis

De los 394 encuestados, 107 personas representados por el 27% alguna vez si han sido vulneradas sus cuentas electrónicas, ya sea Redes Sociales, email, banco virtual etc., y el 73% restante no han sido víctimas de ninguna vulnerabilidad expuesta por el exterior.

Interpretación de resultados

A pesar de un bajo conocimiento en seguridad de la información, no se han presentado ataques a la seguridad de sus cuentas. Sin embargo, los encuestados que han presentado afectación en sus cuentas han sido vulnerados por la falta de conocimiento.

14. Pregunta 14: ¿Le gustaría formar parte de las capacitaciones de seguridad de la información?

Tabla 16. Participación en capacitación

Capacitación de Ciberseguridad	Cantidad	Porcentaje
Si	301	76%
No	93	24%
Total	394	100%

Elaborado por: Shirley Flores

Gráfico 14. Participación en capacitación
Elaborado por: Shirley Flores

Análisis

De los 394 encuestados, 301 personas que representa el 76% tienen presente que es necesario conocer sobre la ciberseguridad y seguridad de la información para mejorar sus prácticas en el uso de herramientas informáticas y redes sociales, y el 24% restante no tiene interés alguno.

Interpretación de resultados

Existe un alto interés por parte de los encuestados entre estudiantes y docentes, que desean conocer información acerca de seguridad de la información, ciberseguridad y como protegerse de ataques informáticos que ponen en riesgo su información. Al ser un tema netamente técnico ayuda al usuario a mejorar en este ámbito que en teoría es nuevo para las diferentes áreas no relacionadas a tecnologías de la información.

2.2.3.2. Coeficiente Alfa de Cronbach

Fórmula Estadística

$$\alpha = \frac{k}{k-1} * \left(1 - \frac{\sum S_i^2}{S_T^2}\right)$$

En donde:

K: El número de ítems
Si^2: Sumatoria de Varianzas de los Ítems
ST^2: Varianza de la suma de los Ítems
α: Coeficiente de Alfa de Cronbach

Se realizó el cálculo del coeficiente del Alfa de Cronbach, validando el instrumento utilizado en la recolección de datos, dando como resultado la siguiente tabla.

Tabla 17. Coeficiente Alfa de Cronbach

K:	14
Si^2:	13,82
ST^2:	14,11
α:	**0,99**

Elaborado por: Shirley Flores

Entre más cerca de 1 está α, más alto es el grado de confiabilidad, eso quiere decir que el nivel de confiabilidad es elevado y no hay error en la medición.

2.2.4. Procesamiento y Análisis de Datos

De acuerdo con las encuestas realizadas, a los estudiantes, y a los docentes de la Facultad de Ciencias Humanas y de la Educación se demostró que:

- Los encuestados entre hombres y mujeres no tienen una cultura de ciberseguridad, ya que tienen desconocimiento en términos relacionados con tecnología de la información.
- Los estudiantes tienen un alto interés de aprender sobre ciberseguridad y participar en las capacitaciones de seguridad de la información, ya que es fundamental que exista una concientización adecuada, debido a que es el activo

más valioso que tiene la organización, por lo tanto, es un riesgo latente de sufrir pérdidas y fuga de información.

- Los estudiantes tienen temor a ser víctimas de algún tipo de ataque, lo cual demuestra que el usuario es vulnerable, para ser objeto de estudio de Ingeniería Social.
- Una de las Redes Sociales más utilizadas, dentro del ámbito educativo, es el WhatsApp, ya que es el medio de comunicación diario de los estudiantes, lo cual al estar presente en el mismo se corre los riesgos de afrontar una Ingeniería Social.
- Muy pocas personas entienden el término de Ingeniería Social y es importante que conozcan que es, en que consiste, y como puede estar alerta a posibles casos que se den tanto en el ámbito educativo, como el profesional, ya que los estudiantes encuestados se encuentran cursando los diferentes niveles de carrera y en un futuro se encontrarán en diferentes puestos de trabajo, el cual serán un blanco fácil para ser vulnerados y obtener información confidencial.

Los resultados obtenidos de las encuestas realizada a los estudiantes y docentes de la facultad de Ciencias Humanas y de la Educación, permite establecer planes de concientización como es la capacitación para el mejor entendimiento sobre la ciberseguridad que conlleva la Ingeniería Social.

CAPÍTULO III.-
RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

3.1.1. Análisis Comparativo entre plataformas de servicio virtualizado en la nube

Tabla 18. Análisis Comparativo entre DigitalOcean y Google Cloud

Herramientas / Características	DigitalOcean	Google Cloud
Compañía matriz	Independiente	Google
Modelo de precios	Precio con todos los servicios incluido.	Precio por Servicio
SLA	99,99%	99,99%
Ubicaciones de los centros de datos	8 ubicaciones en todo el mundo repartidas en los EE. UU., Europa e India.	25 regiones de todo el mundo repartidas en los EE. UU., Europa, América del Sur, India, Australia y Asia Pacífico.
Facilidad de uso	Muy fácil	Fácil
Enfoque	Centrado en el desarrollador	Centrado en la empresa
Precio	Menos costoso	Más costoso
Facturación	Por hora	Por segundo
Créditos	$200 para nuevos usuarios	$300 para nuevos usuarios
Características	Menos completo	Completo
Seguridad	Muy buena	Muy buena
Orientado para	Aplicaciones de gran ancho de banda. El costo por GB transferido es de $0.01/GB.	Aplicaciones empresariales más sofisticadas.

Elaborado por: Shirley Flores

Para el presente proyecto se eligió la Plataforma DigitalOcean, ya que es una excelente opción para servidores en la nube. Esta solución facilita el lanzamiento y la ampliación a medida que el proyecto crece ya que es un software escalable. La escalabilidad se debe a que los servicios de DigitalOcean están basados en la nube, esto le convierte en una opción superior ante opciones tradicionales.

3.1.2. Características

3.1.2.1. CPU Virtual dedicado

Para la creación del servidor se consideró trabajar con la opción Standard, ya que es óptimo para llevar a cabo la ejecución del ataque.

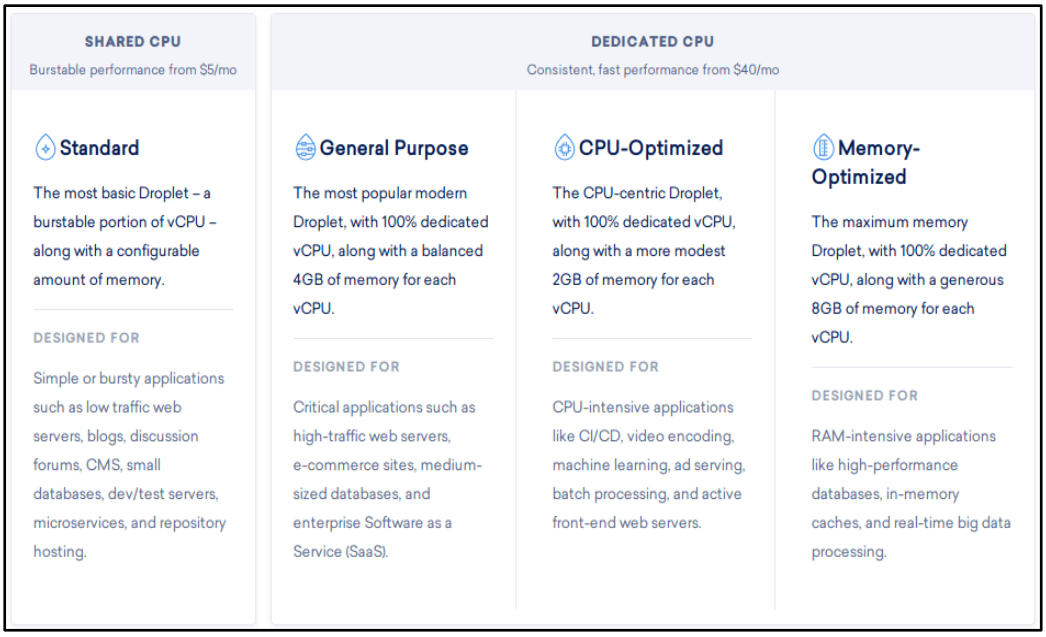


Gráfico 15. CPU Virtual Dedicado
Fuente: [30]

3.1.2.2. Determinación de GNU/Linux

La herramienta DigitalOcean ofrece algunas distribuciones, por lo cual se elaboró una tabla comparativa de las distros más utilizadas, se consideró 4 de ellas considerando el objetivo del presente proyecto, se muestra a continuación la siguiente tabla:

Tabla 19. Análisis Comparativo de los Sistemas Operacionales basados en Linux

Características / Distribución	Definición	Arquitectura	Tipo	Usos	Seguridad
CENTOS	CentOS se basa básicamente en el marco de Linux y una distribución de Linux para implementar una plataforma informática gratuita, compatible con la comunidad que sea compatible con la fuente ascendente correspondiente, Red Hat Linux.	La arquitectura de CentOS se basa principalmente en el código fuente de Red Hat para implementar el diseño central similar a Red Hat Enterprise Linux y está disponible de forma gratuita, (X86-64).	Gratuita	Servidores	En el caso de CentOS, se basa en el marco de Linux y, por lo tanto, está muy protegido y pasa por 3 capas de parches de seguridad. También es menos propenso a las amenazas de seguridad web.
UBUNTU	Ubuntu es básicamente una distribución de código abierto y Linux que se basa en Debian. Es uno de los sistemas operativos más populares para la nube.	Los paquetes de Ubuntu se crean principalmente en el formato Debian y este paquete en realidad dibuja el marco arquitectónico básico de Ubuntu de acuerdo con la mejora continua en el mismo (X86-64, Power PC, Sparc64).	Gratuita Comercial	Est. trabajo Escritorios Producción	En el caso de Ubuntu, los parches de seguridad también funcionan bien, pero a veces debido a las actualizaciones frecuentes, es más propenso a las amenazas web. Además, a veces es necesario degradarlo a versiones inferiores debido a la presencia de actualizaciones recientes con errores.

FEDORA	El sistema operativo Fedora es un sistema operativo estable mantenido gracias a una comunidad de ingenieros, diseñadores gráficos y usuarios que se encargan de informar fallos y de probar nuevas tecnologías. Este sistema busca incluir software libre de código abierto.	Fedora posee arquitectura de gestión de activos digitales (Digital Asset Management, DAM), sobre la cual se pueden construir muchos tipos de biblioteca digital, repositorios (archivos) institucionales, archivos digitales, y sistemas de bibliotecas digitales (X86-64, Power PC).	Gratuita	Multiuso Vanguardia	SELinux ("Security-Enhanced Linux") se destaca entre las características de seguridad de Fedora, pues implementa una gran variedad de políticas de seguridad, incluyendo control de acceso obligatorio (MAC "Mandatory Access Control"), a través de los módulos de Seguridad que están en el núcleo Linux del sistema.
KALI- LINUX	Kali Linux es una distribución de Linux basada en Debian, específicamente diseñada para temas de seguridad muy variados, diseñada principalmente para la auditoría y seguridad informática en general. Es la distro de penetración y hacking más popular.	Kali se distribuye en imágenes ISO compiladas para diferentes arquitecturas (32/64 bits y ARM).	Gratuita	-Análisis -Pruebas de Penetración -Hacking - Recolección datos.	Kali Linux se encuentra entre las distribuciones de seguridad de Linux más usadas, ya que es una de las mejores, tanto para uso personal como profesional, proporcionando a los usuarios paquetes de herramientas como Foremost, Wireshark, Maltigo as-Aircrack-ng, Kismet, etc.

Elaborado por: Shirley Flores

Después de comparar las distintas distros de Linux en una variedad de factores, se puede concluir que para el levantamiento de servidores según el tipo de necesidad de este proyecto se va a trabajar con Ubuntu con una versión LTS ya que mediante una investigación bibliográfica, este sistema operativo es el más común y usado para el levantamiento de servidores con este fin, existen guías de usuario más entendibles para el usuario, y tiene una mejor compatibilidad con la herramienta a utilizar para la ejecución de la simulación del ataque. Es una versión LTS, ya que tendrá soporte y será actualizada durante más tiempo que una versión normal. Ubuntu nos facilitará el montaje de la plataforma y es la más viable por su facilidad de uso y por el poco consumo de recursos.

3.1.2.3. Óptimo coste-beneficio

Cloud Spectador, una empresa independiente de evaluación comparativa, descubrió que DigitalOcean ofrecía el mejor rendimiento de CPU por dólar en comparación con AWS y Google. Gracias a los precios sencillos, es fácil predecir su factura mensual. [30].

La relación de coste-beneficio de Digital Ocean es muy buena en comparación con otras empresas de hosting.

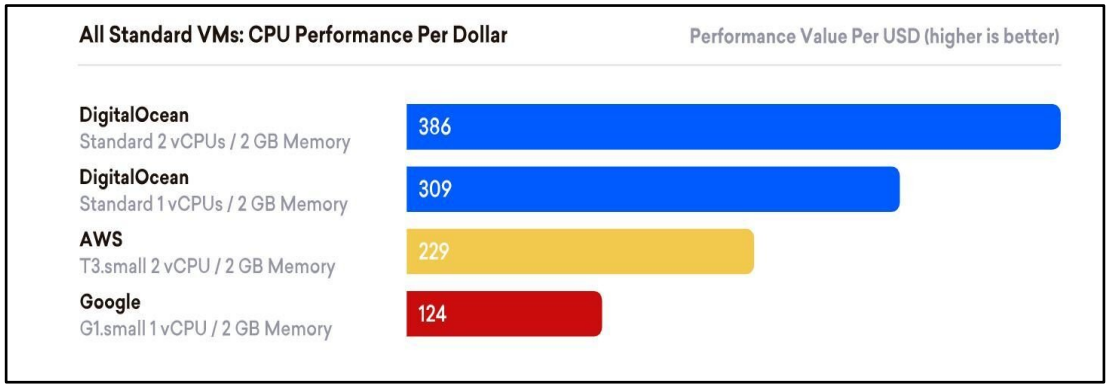


Gráfico 16. Comparación Coste-Beneficio con otros Hostings
Fuente: [30]

3.1.2.4. Herramientas

Digital Ocean ofrece Herramientas como firewall, backup, análisis de métricas y gestión de equipos. Algunas de estas recién destaque en la página que presenta los Droplets [28].

DigitalOcean Monitoring es un servicio opcional gratuito que recopila métricas sobre la utilización de recursos a nivel de gota. Proporciona gráficos Droplet adicionales y admite políticas de alerta de métricas configurables con notificaciones de Slack por correo electrónico integradas para ayudarlo a realizar un seguimiento del estado operativo de su infraestructura [31].

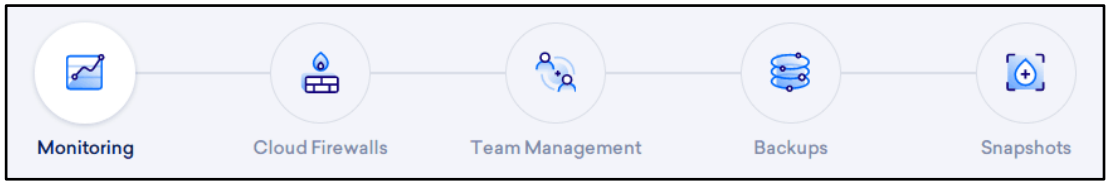


Gráfico 17. Herramientas de Digital Ocean
Fuente: [28]

3.1.2.5. Escalabilidad

Este es uno de los principales beneficios ofrecidos por Digital Ocean. Por lo tanto, al optar por esta herramienta de hosting cloud, no es necesario contratar con un servicio robusto y complejo, sino que se puede empezar con recursos simples a medida de las necesidades del proyecto.

3.1.3. Determinación de Herramienta de Simulación de Ataques de Phishing – Gophish

Para el presente proyecto se determinó el uso de Gophish, una herramienta OpenSource, para el establecimiento y creación de todo el circuito del que está compuesto una campaña de Phishing. Esta permite definir los objetivos, lanzar una campaña, realizar un análisis y seguimiento de los resultados de los que hayan tenido éxito y las que no, teniendo una idea más clara de hacia dónde enfocar una posible formación.

Gophish es un framework de seguridad que tiene todas las funcionalidades necesarias para implementar una campaña de phishing, por lo cual dentro del entorno OpenSource es uno de los más usados y recomendados.

Esta es una herramienta indispensable en cualquier equipo de ciberseguridad, es de gran utilidad para las organizaciones, ya que se puede medir el impacto del phishing y sirve para preparar a los usuarios, poniendo a prueba el conocimiento en la

identificación de correos maliciosos y suplantaciones, mediante simulaciones de ataque de Phishing, para saber cómo actuar frente a un ataque real.

3.1.3.1. Características

Las principales características de esta herramienta son: [37].

- Cuenta con un gran número de plantillas por defecto, idénticas pixel a pixel
- Permite configurar campañas de Phishing automáticas
- Multiplataforma, disponible para Windows, Linux y Mac
- Totalmente gratuito y de código abierto.

3.1.3.2. Menú de Gophish

Tablero (Dashboard)

En esta sección se muestra un panel con estadísticas generales, en donde se visualiza el progreso de la ejecución, información de la cantidad de correos enviados, correos abiertos, correos a los que han interactuado con el enlace, y los usuarios que enviaron datos. También guarda una recopilación de todas las campañas, configuraciones realizadas y la cantidad de grupos de usuarios creados, para el cumplimiento del objetivo propuesto, así como se visualiza en el Gráfico 18.

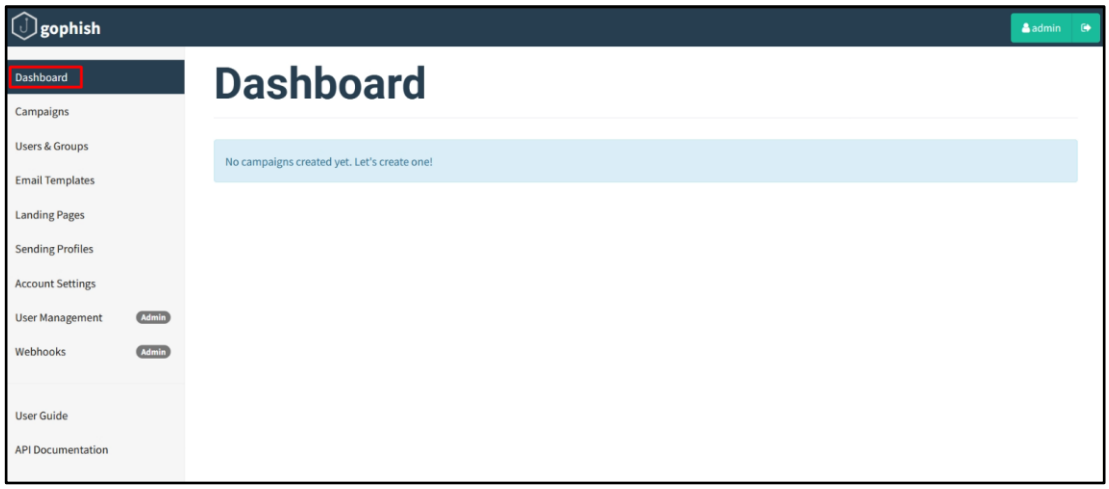


Gráfico 18. Dashboard
Elaborado por: Shirley Flores

Campañas (Campaigns)

En esta sección, se crea una campaña en el cual, solicitan algunos datos para su configuración los cuales son los siguientes:

- Nombre de la Campaña.
- Plantilla Creada previamente para el envío de la campaña.
- Pagina fraudulenta creada previamente para redirigir a los usuarios.
- URL del servidor en donde se encuentra el framework Gophish instalado. Es la URL Base de la Landing Page.
- Se puede programar la campaña para que se despliegue según la configuración establecida, se puede indicar la fecha y hora finales del envío y se ejecuta durante el periodo de tiempo establecido.
- Se añade el perfil de envío del servidor de correo que se utiliza en la campaña.
- Se selecciona el grupo victima al que se quiere destinar la campaña.

Una vez creada la campaña, se puede acceder a su estado, estadísticas, duplicarla o eliminarla. Se pueden crear múltiples campañas, enfocadas a distinta población lo cual facilita segmentar la información de los resultados obtenidos. El menú de Campañas se lo visualiza en el gráfico 19.

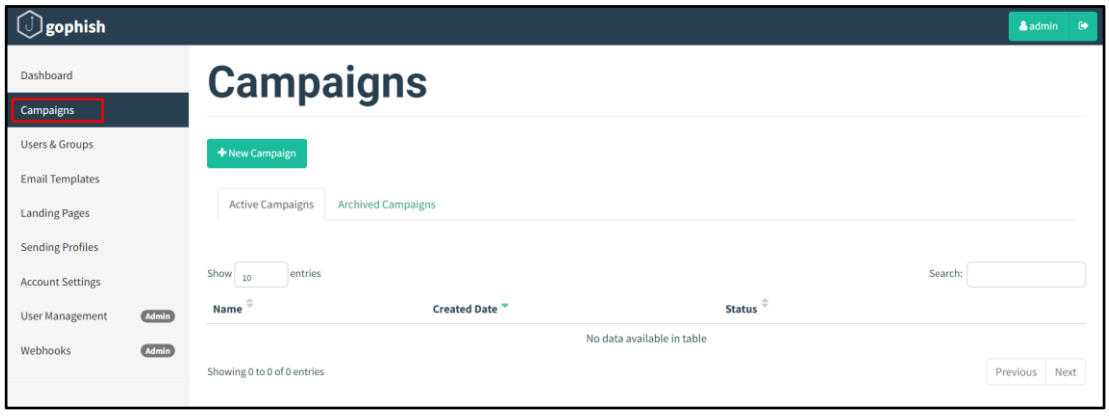


Gráfico 19. Campaigns
Elaborado por: Shirley Flores

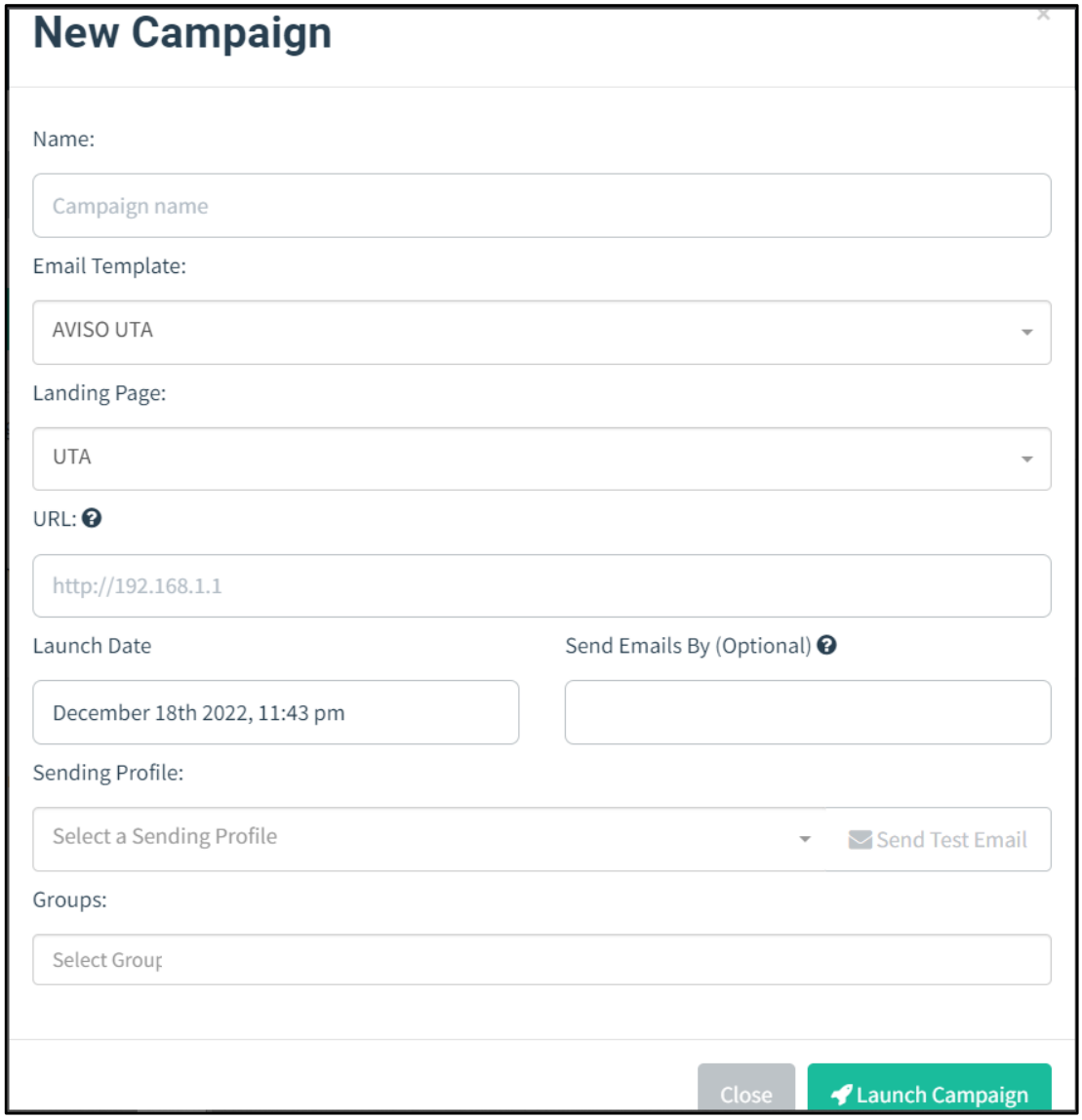


Gráfico 20. New Campaign
Elaborado por: Shirley Flores

Usuarios y Grupos (Users & Groups)

En esta sección se registra el grupo de víctimas que serán el objeto del ataque simulado, se pueden agregar los grupos que sean necesarios y para el registro se lo puede hacer manual o masivamente. El formato que se debe cumplir es el nombre, apellido, correo electrónico y cargo que desempeña, siendo el correo electrónico un campo obligatorio ya que sin él no se continuara con el proceso de creación de usuarios o grupos. Se puede importar los datos en bloque, mediante la carga de un archivo exclusivamente en formato .CSV con la siguiente sintaxis, como se muestra en el Gráfico 21.

```
First Name,Last Name,Email,Position
```

Gráfico 21. Sintaxis CSV
Elaborado por: Shirley Flores

El menú para la creación de Usuarios y Grupos se visualiza en el Gráfico 22.

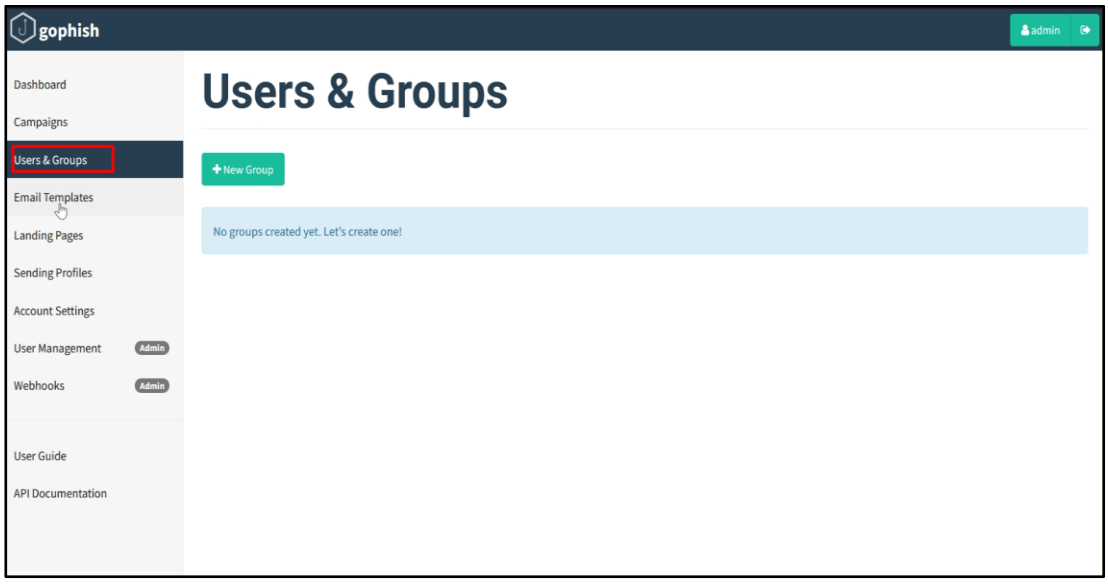


Gráfico 22. Grupos y Usuarios
Elaborado por: Shirley Flores

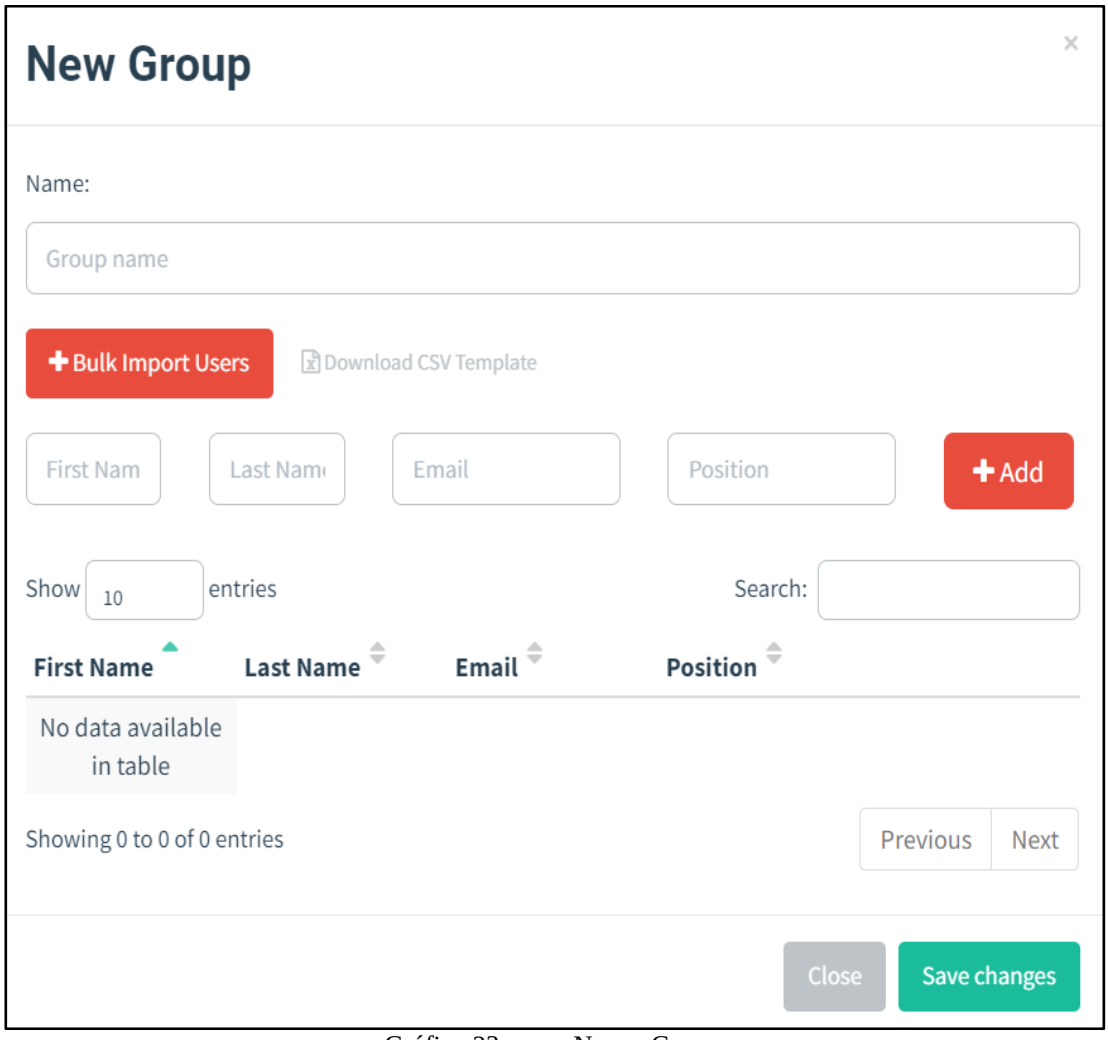


Gráfico 23. Nuevo Grupo
Elaborado por: Shirley Flores

Plantillas de correo electrónico (Email Templates)

En esta sección, se puede crear un correo electrónico personalizado, el cual será enviado a las víctimas, el cual contiene un enlace que redirecciona a la página creada con el formulario para la obtención de información. En el Gráfico 24 se visualiza el menú para la creación y en el Gráfico 25 se puede observar el módulo para configurar la nueva plantilla.

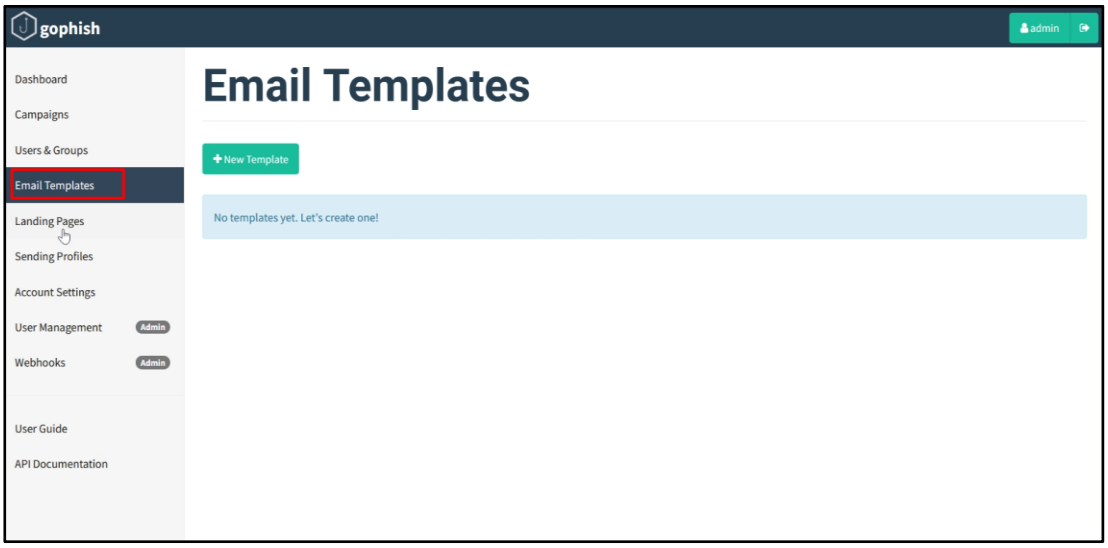


Gráfico 24. Plantilla Email
Elaborado por: Shirley Flores

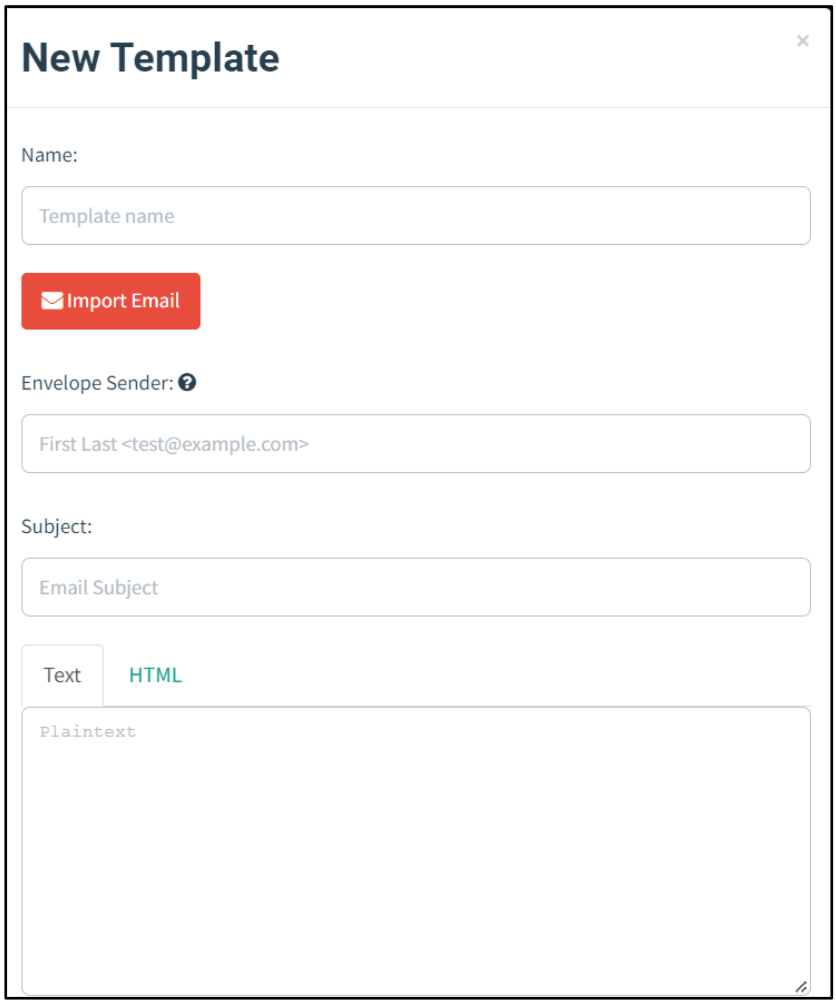


Gráfico 25. Nueva Plantilla
Elaborado por: Shirley Flores

Páginas de Destino (Landing Pages)

En esta sección, se configura la página de destino con la cual la victima va a interactuar, aquí se crea la página mediante código HTML o a su vez existe una opción de importar páginas. El diseño de la página web debe ser similar al de la página original, para obtener mejores resultados. También se puede configurar si se requiere la obtención de información, mediante la captura de los datos enviados por las víctimas.

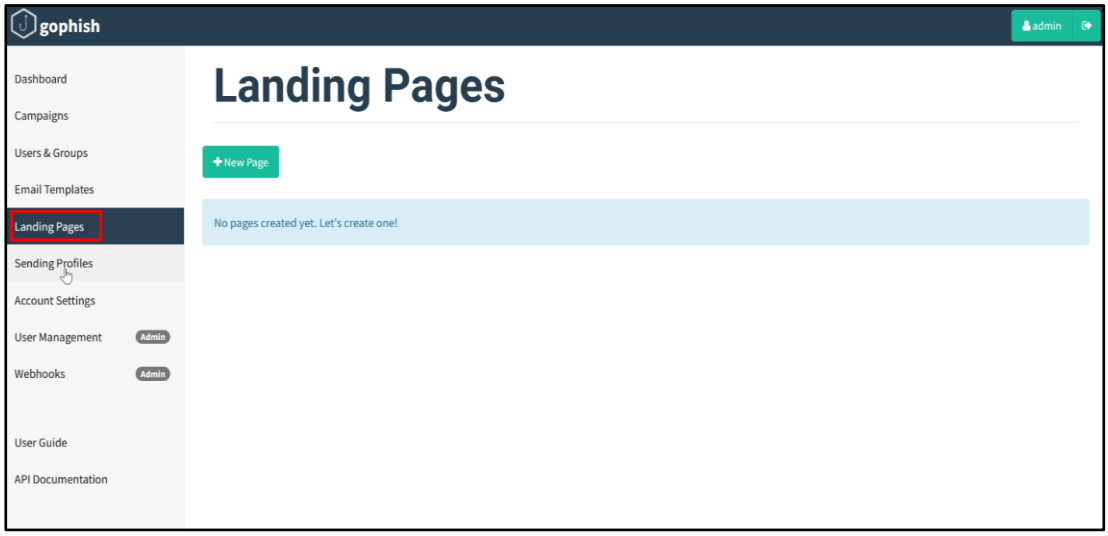


Gráfico 26. Páginas de destino
Elaborado por: Shirley Flores

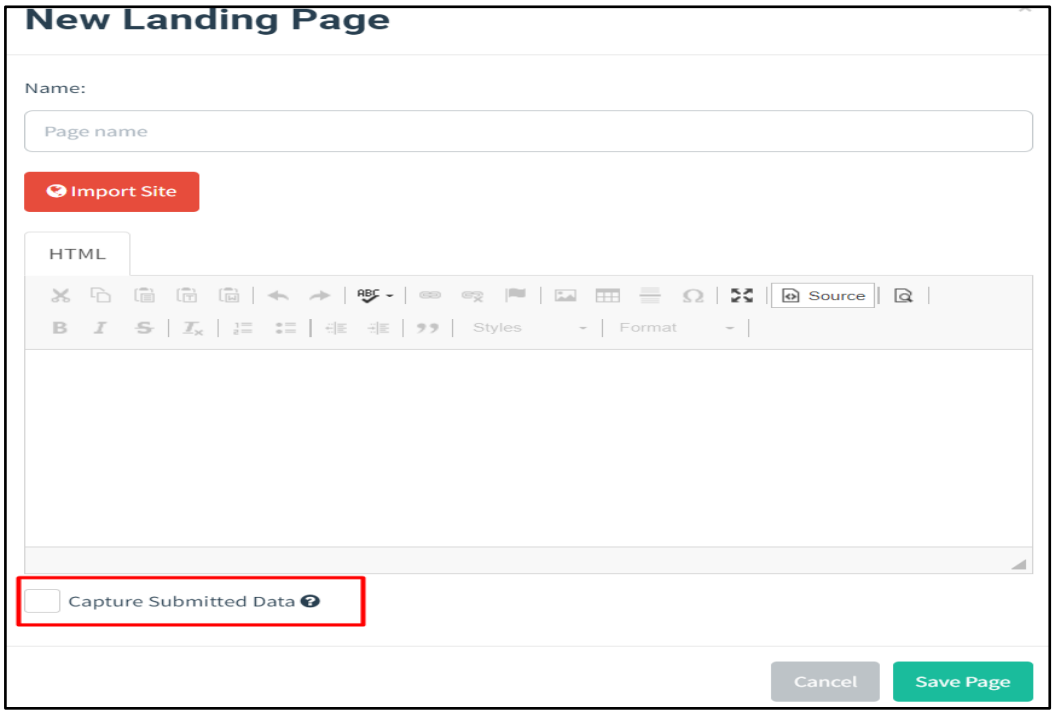


Gráfico 27. Nueva Página de destino
Elaborado por: Shirley Flores

Envío de perfiles (Sending Profiles)

En esta sección se realiza la configuración del envío de perfiles, en el cual se podrá anclar el correo electrónico con el cual se va a enviar el ataque, se pueden crear distintos perfiles según la necesidad del proyecto. Esta opción permite configurar a quien se quiere suplantar en la ejecución.

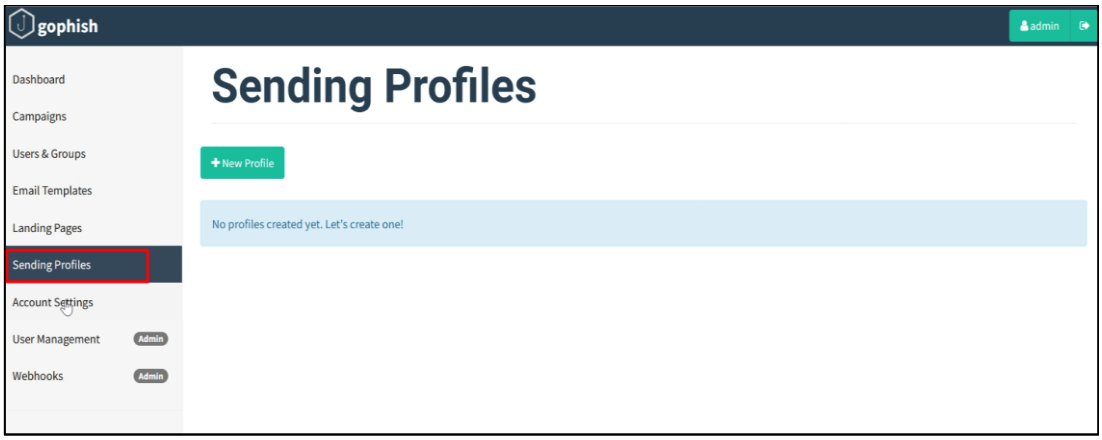


Gráfico 28. Envío de perfiles
Elaborado por: Shirley Flores

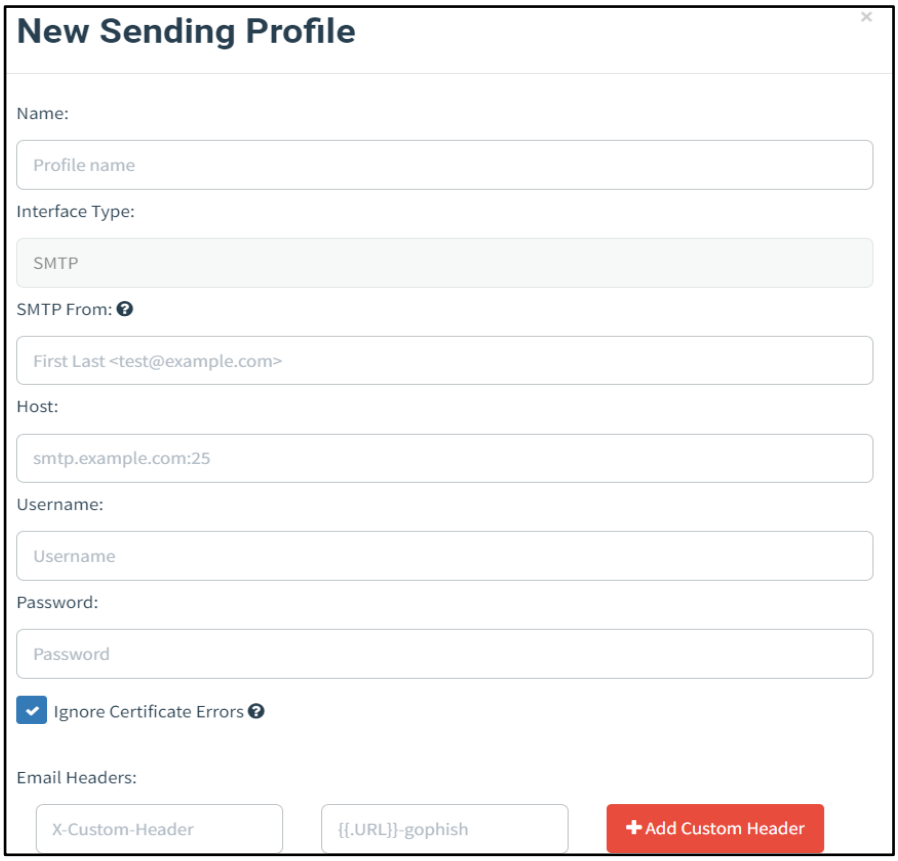


Gráfico 29. Nuevo Envío de Perfil
Elaborado por: Shirley Flores

Configuraciones de la cuenta (Account Settings)

En la sección de configuración se puede cambiar las credenciales de usuario y configurar opciones en los reportes, la interfaz o la cuenta.

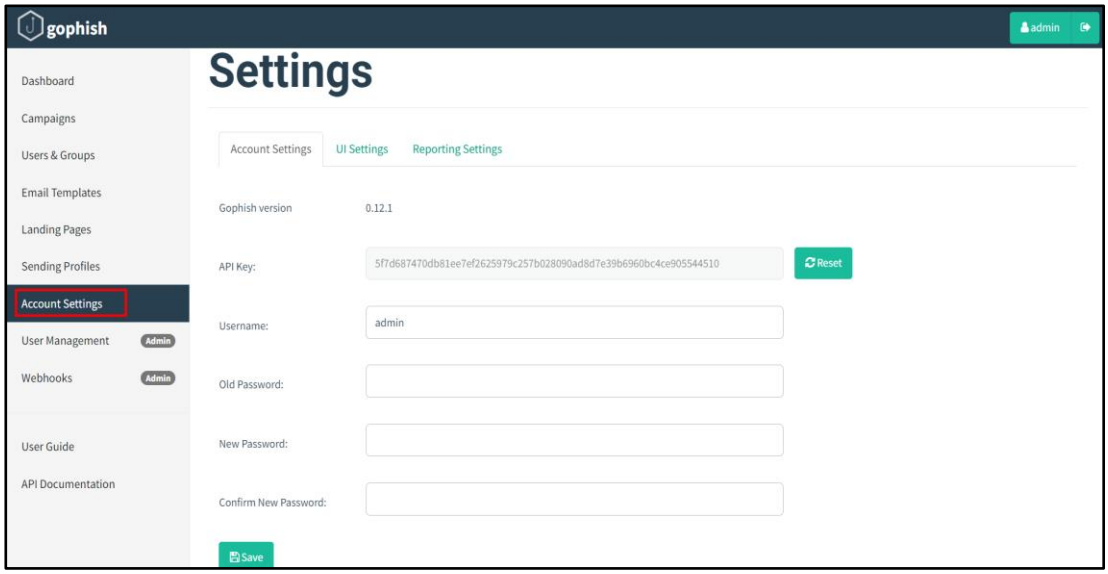


Gráfico 30. Configuración
Elaborado por: Shirley Flores

Gestión de usuarios (User Management)

Esta opción permite gestionar distintos usuarios que podrán acceder a la plataforma y a la interfaz de administración. Por defecto existirá el usuario administrador, pero se podrá agregar más usuarios, según las necesidades del proyecto.

Webhooks

En esta sección permite la creación de Webhooks, en el caso de que se quiera recibir notificaciones HTTP de los resultados de las campañas en un endpoint de la elección que se desee, se podrá hacerlo con esta opción. Será necesario poseer los permisos de administrador.

Guía del usuario (User Guide)

En esta sección, se puede encontrar información del framework, lo cual sirve como una guía en el manejo y ejecución de la simulación del ataque.

Documentación API (API Documentation)

En esta sección se puede obtener información de cómo está desarrollada la Api de GoPhish. Para el presente trabajo no será necesario consultarla.

3.1.4. Determinación de dominios de correo electrónico a utilizar para la ejecución del Ataque.

Tabla 20. Características de correo

Correos Electrónicos / Características	GMAIL	OUTLOOK
Propietario	**Google**	**Microsoft**
Espacio	15 GB. El límite de almacenamiento se comparte entre Google Drive, Gmail y Google Photos. Si has alcanzado el límite, se puede comprar almacenamiento extra. Tu cuenta de Google también tiene almacenamiento en la nube de Google Drive.	Mientras que el límite actual no es claro, parece que se puede comenzar con 5 GB de almacenamiento y este se incrementa a medida que pasa el tiempo. Tu cuenta Microsoft también cuenta con almacenamiento en la nube de OneDrive.
Capacidad de Búsqueda	Busca cualquier combinación de los siguientes elementos usando la búsqueda avanzada: • Etiqueta, pestaña o categoría • De (Remitente) • Para (destinatario) • Asunto	Outlook.com tiene una búsqueda más sencilla. La opción de búsqueda de correo o de contactos te permite buscar cualquier combinación de: Todas las carpetas, bandeja de entrada o borradores

	• Palabras clave • cuerpo del texto • archivos adjuntos • Charlar • Tamaño del mensaje • Fecha	• De (Remitente) • Opciones de fecha incluida, Todas, Esta semana, Semana pasada, Este mes o cualquier rango.
Seguridad	Incluye dos formas de verificación, y detección de correo no deseada. Se puede activar un icono de verificación para los correos de remitentes verificados a través de Google Labs.	Incluye dos formas de verificación. Usa iconos de remitentes seguros. Correo no deseado sospechoso aparece con barras de seguridad rojas o amarillas en la parte superior del mensaje.
Organización de la bandeja de entrada	La organización por defecto de Gmail se basa en etiquetas y hasta cinco pestañas. Asigna colores a las etiquetas y usa estrellas y otros símbolos para hacer relevantes los mensajes importantes. Además, puede convertir su bandeja de entrada a la bandeja de entrada clásica o una bandeja de entrada con prioridades.	La organización por defecto de Outlook está basada en categorías, carpetas y subcarpetas. Hace relevante los mensajes importantes o los sujetos en la parte superior de la carpeta.
Mensajería instantánea	Gmail usa la función de chat para mensajería instantánea, que se puede encontrar en la parte	Outlook usa Skype para mensajería instantánea. Skype se encuentra en la parte superior derecha de

	inferior izquierda de la bandeja de entrada.	tu bandeja de entrada.
Detección de Phishing	Gmail contiene potentes funciones para proteger contra el spam, el phishing y el software malicioso antes de que lleguen a la bandeja de entrada. Gmail bloquea más del 99,9 % del spam, los intentos de phishing y el software malicioso que llega a tu bandeja de entrada. [34].	En Outlook se puede reportar un posible phishing a Microsoft fácilmente. Para ello basta con seguir una serie de pasos. Lo primero es acceder a nuestra cuenta y entrar en el correo que se quiere denunciar. Hay que mencionar que depende de la versión nueva o antigua, ya que en la nueva versión el proceso es más largo [36].

Elaborado por: Shirley Flores

En base al análisis comparativo de los dominios de correo electrónico realizado en la **Tabla 20**, se seleccionó el dominio Outlook para la ejecución de ataque de phishing, ya que en las características el nivel de seguridad de los correos tiene mayor protección Gmail y las pruebas de Ingeniería Social desde Google son mucho más rápido detectadas y baneadas.

3.1.5. Metodología Kanban

Para el presente trabajo de investigación, se eligió la metodología ágil Kanban ya que esta se basa en el desarrollo incremental, dividiendo el trabajo en tareas y utiliza técnicas visuales para ver el estado en el que se encuentran las mismas. Su objetivo es organizar, gestionar y controlar el proyecto de manera global, la forma en la que se van completando las tareas. Permite limitar la acumulación de actividades pendientes, aumentando la eficiencia y calidad del flujo de trabajo. La metodología Kanban dispone de 5 propiedades principales que deben estar presentes para que el proyecto sea desarrollado desde el inicio hasta su finalización de una manera productiva e interactiva.

Para la implementación de la Metodología Kanban, se utilizó una herramienta de gestión de proyectos, denominada Trello el cual es un software que permite gestionar el flujo de trabajo propuesto, priorizando y supervisando tareas.

a) Visualizar el Flujo de Trabajo

Se realizó una planificación inicial de las actividades a realizar para la ejecución y el cumplimiento de cada uno de los objetivos establecidos en el presente proyecto.

Para visualizar el flujo de trabajo, se creó un tablero Kanban, en el cual se especificó cada una de las tareas.

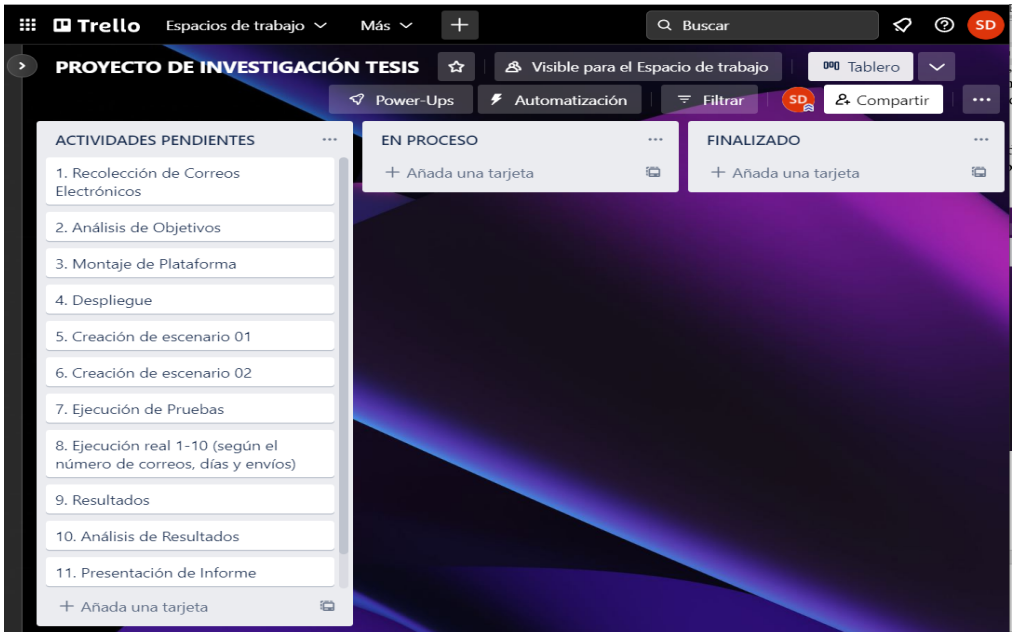


Gráfico 31. Flujo de trabajo
Elaborado por: Shirley Flores

En el Gráfico 31, muestra las actividades definidas para el desarrollo y ejecución del presente proyecto. Cada tarea está representada por una tarjeta en la cual se puede agregar información adicional para dar un adecuado seguimiento y se puede determinar la priorización de cada una mediante etiquetas.

b) Limitar el Work-In-Progress (WIP)

Establecer los límites de trabajo en proceso tienen una buena aceptación en los flujos de trabajo, ya que acelera la finalización de las tareas y reduce el tiempo de espera en cada una de las fases.

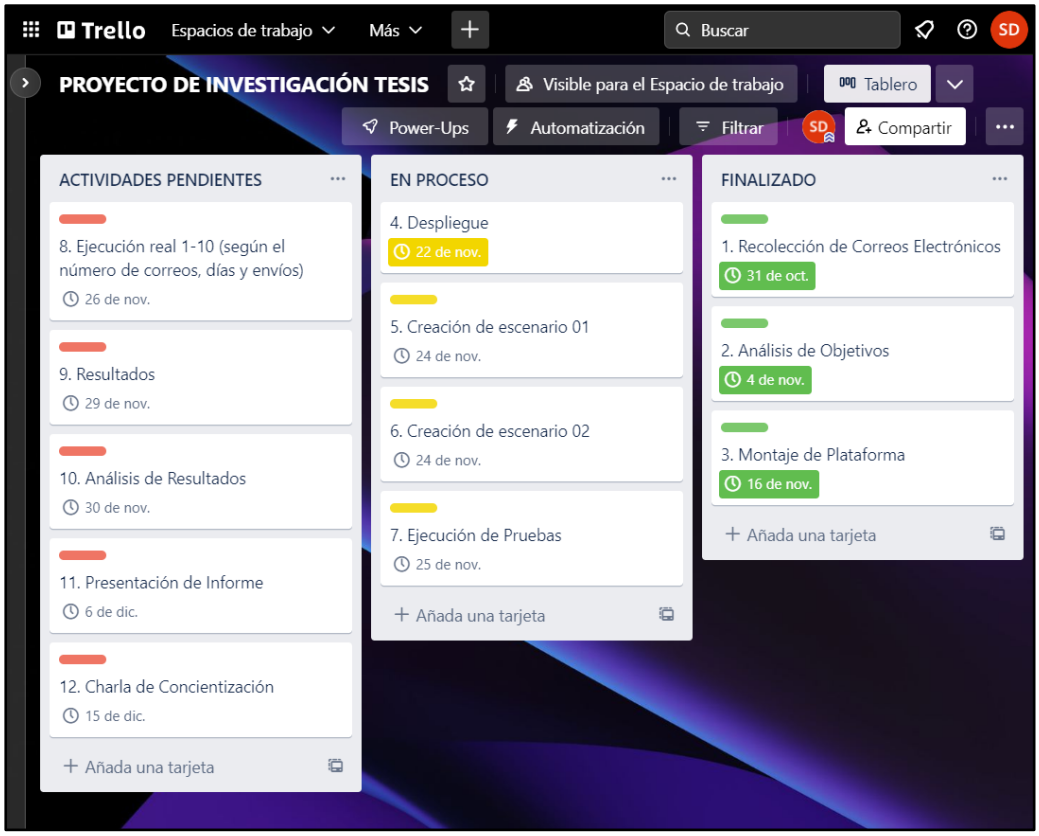


Gráfico 32. Tablero Kanban Priorizado por Etiquetas

Elaborado por: Shirley Flores

En el Gráfico 32, se puede observar que se limitó el número de tareas que se pueden realizar en cada fase, para tener un mejor control y evitar la acumulación de trabajo sin terminar. Las actividades se encuentran distribuidas en “Actividades Pendientes”, “En proceso”, y “Finalizado”, según se vaya cumpliendo las tareas, se cambiará la priorización en cada una de las etapas. Se ha asignado un color de etiqueta, según la

priorización de la actividad, así se tendrá un mejor control en el seguimiento de cada una de las fases establecidas.

c) Medir el Flujo

El formato visual del tablero de Kanban, muestra fácilmente la manera en el que un elemento se mueve a través de un proceso, y se observa como las tareas pasan de una etapa a otra. En el análisis del flujo se puede determinar la fluidez del proceso, y si existen actividades que contribuyen o no a su productividad.

Para medir el flujo de trabajo, se añadió en cada una de las tarjetas el tiempo o plazo de entrega, más conocida como una de las métricas de la metodología Kanban denominada "lead time", que es el tiempo que se demora en completar una actividad, la cual permitirá realizar un control para la entrega del proyecto.

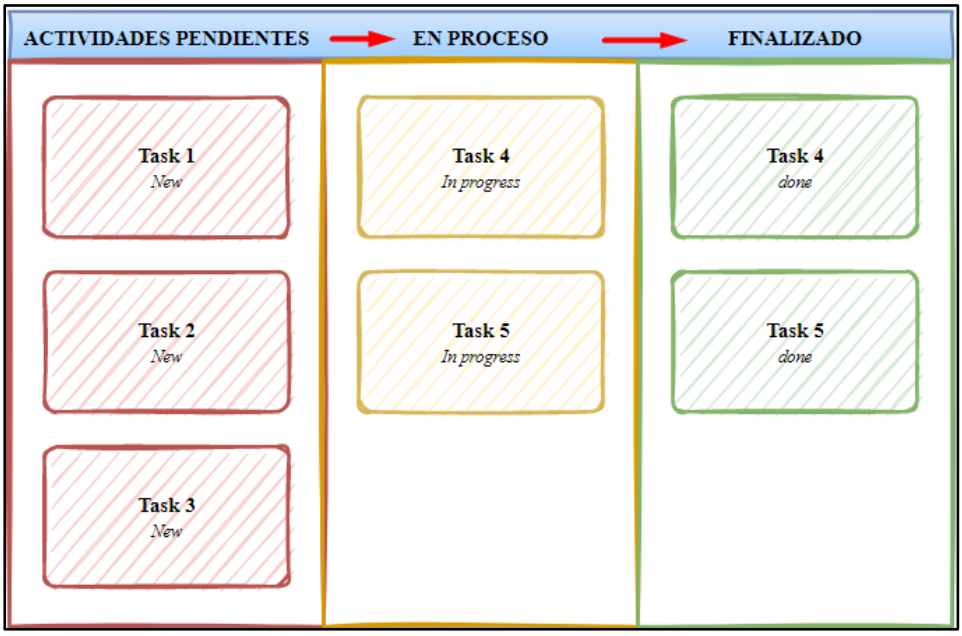


Gráfico 33. Flujo de trabajo

Elaborado por: Shirley Flores

d) Explicitar las Políticas de los procesos

Las políticas ayudan a cumplir con el proceso establecido, ya que es una guía para la toma de decisiones y contribuye para avanzar con el proceso de la mejor manera posible. Se ha implementado políticas explicitas en base a las necesidades y expectativas para el cumplimiento de los objetivos, las cuales nos indica la manera como se va a cumplir con el flujo de trabajo.

e) Usar Modelos para evaluar Oportunidades de Mejora

Trello es una herramienta digital de gestión de proyectos, que optimiza el proceso manual del control de actividades. En cada fase se determina una nueva oportunidad de mejora, se puede agregar tareas con automatización, aumentando la eficiencia del proceso y eliminando tareas no necesarias, el cual ayudará a mantener un flujo de trabajo fluido desde el inicio hasta la culminación del proyecto.

3.1.6. Plan de Ataque de Ingeniería Social

Para definir el plan de ataque, se basa en el uso de la técnica de Phishing a través del correo electrónico, la cual se caracteriza por intentar adquirir información confidencial. Como parte de la metodología empleada y de las pruebas de ingeniería social se definió la ejecución de las siguientes etapas como parte de la investigación:

1. Descubrimiento y Recolección de correos electrónicos.
2. Análisis de objetivos.
3. Montaje de Plataforma.
4. Despliegue.
5. Creación de Escenario 01.
6. Creación de Escenario 02.
7. Creación de la Página de Destino.
8. Ejecución de Pruebas.
9. Ejecución Real 1-10 (según el número de correos, días y envíos).
10. Ejecución de Ataque de Phishing con simulación de Página Facebook.
11. Resultados.

3.2. Desarrollo de la Propuesta

3.2.1. Descubrimiento y Recolección de Correos

Para el descubrimiento de los correos se ha utilizado la técnica de la inteligencia de fuentes abiertas (OSINT) ya que se ha utilizado la herramienta Hunter.io, como se visualiza en el Gráfico 34, en el cual se tendrá acceso a las direcciones de correo electrónico que tengan relación con la universidad, mediante el dominio web

uta.edu.ec y ahí encontrar el patrón del correo electrónico con el cual se va a poder identificar como está estructurado e ir descubriendo cada uno de los correos de los estudiantes a aplicar Ingeniería Social, atacando al eslabón más débil para acceder a nueva información.

Gráfico 34. Descubrimiento y recolección de correos

Elaborado por: Shirley Flores

3.2.2. Análisis de Objetivos

Para determinar y cumplir con el objetivo estudiantes se solicitó un documento en el cual, se pueda visualizar la nómina de estudiantes legalmente matriculados en el presente periodo de las distintas carreras de la Facultad de Ciencias Humanas y de la Educación, únicamente con los nombres y apellidos y el número de identificación correspondiente. De igual manera para el objetivo docentes se solicitó la nómina de los docentes que se encuentren laborando a nómina o a contrato en dicha facultad, con los mismos requerimientos. En este proceso se aplicó el método de obtención de la información, Inteligencia de Fuentes Humanas (HUMINT).

3.2.3. Montaje de la Plataforma

Para el desarrollo de la Ingeniería Social, ya establecida la información como lo son los correos y selección a las personas a realizar pruebas de ataque se debe establecer una plataforma que permita el levantamiento de los diferentes servicios para la ejecución del mencionado ataque. Tanto por cuanto, se estableció un servicio en la nube para el levantamiento de un servidor.

DigitalOcean ha sido considerada como un servicio en la nube que permite la creación de aplicaciones modernas para desarrolladores [38]. Esta solución mantiene ciertas ventajas que permite a los desarrolladores obtener código abierto, mismo que permite la modificación a sus servicios; la misión más importante que mantiene dicha empresa es la de poner al alcance este servicio a todo el mundo. Y, por otro lado, una de las ventajas que brinda dicha plataforma es regalar a sus usuarios un valor de USD 200.00, para montar cualquier servidor. La desventaja no tan relevante es que el servicio se encuentra en idioma inglés.

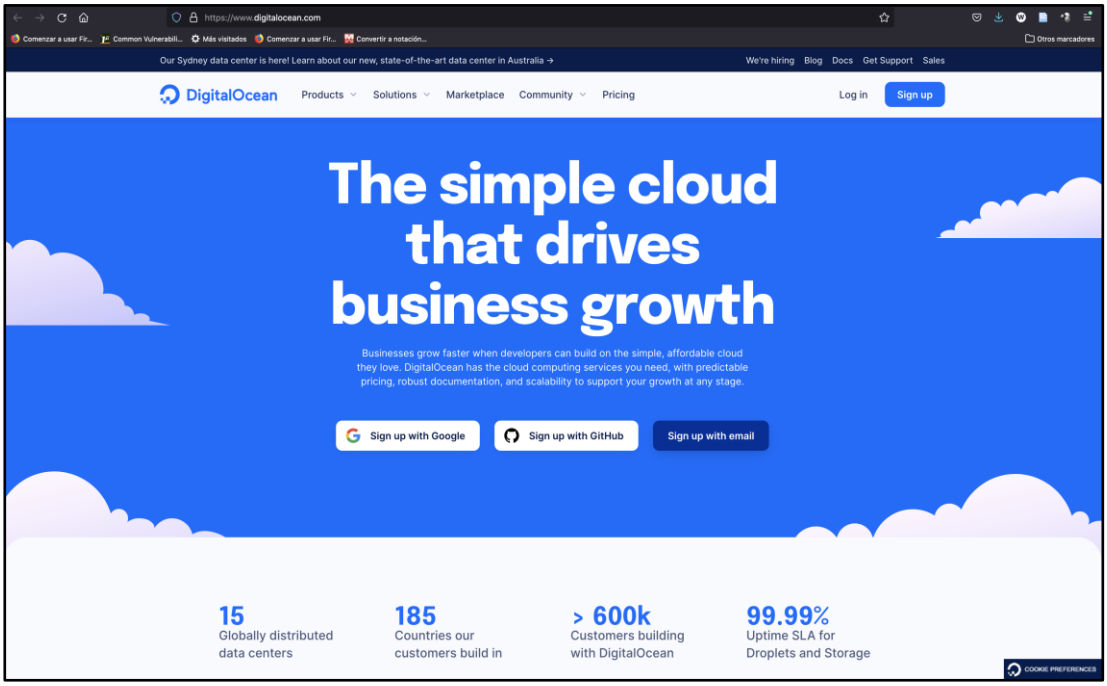


Gráfico 35. Página Oficial DigitalOcean

Fuente: [32]

3.2.3.1. Creación de cuenta

Para la utilización de este servicio se debe crear una cuenta en digitalocean.com, de la siguiente manera:

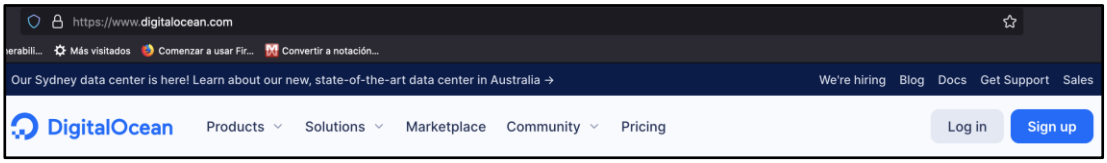


Gráfico 36. Menú DigitalOcean

Fuente: [32]

Para crear una cuenta se debe dar clic en el botón sign up (registrarse), mismo que muestra el siguiente formulario:

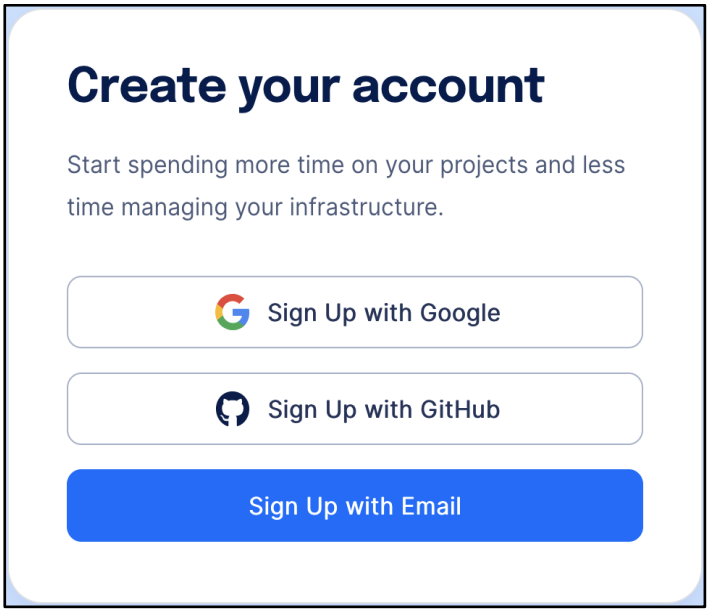


Gráfico 37. Iniciar Sesión

Fuente: [32]

DigitalOcean permite la creación de una cuenta a través de:

1. Registro con el uso de una Cuenta de Google.
2. Registro con el uso de una Cuenta de GitHub.
3. Registro con el uso de una Cuenta propia de DigitalOcean.

El registro se realizó con una cuenta propia de DigitalOcean, se crea una cuenta ingresando el nombre completo, correo electrónico de registro y la contraseña que cumpla con las características de contraseñas seguras.

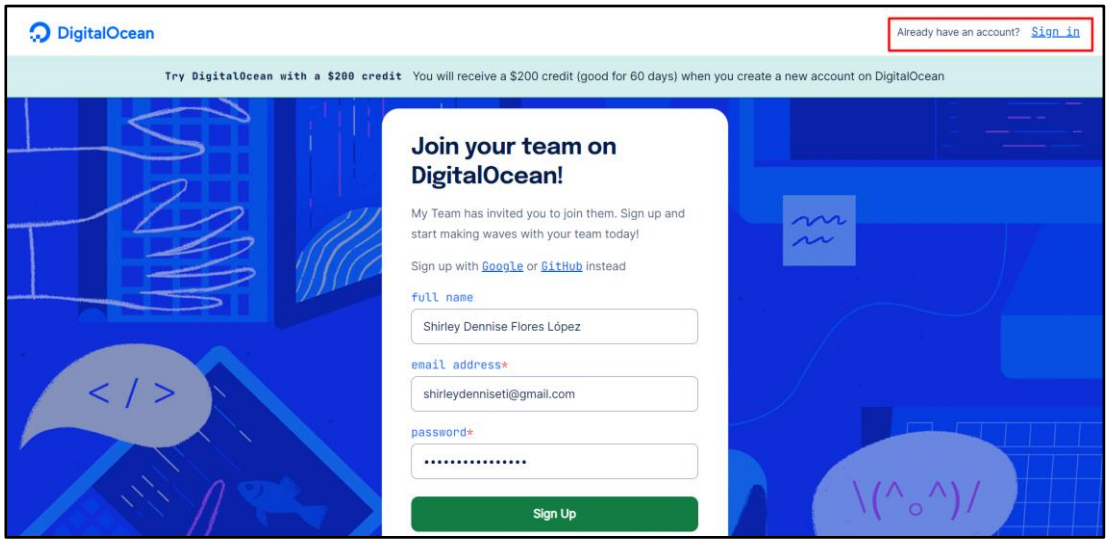


Gráfico 38. Formulario de registro
Fuente: [32]

Por la creación de la Cuenta, Digital Ocean ofrece un crédito de $200, para su uso por el tiempo de 60 días considerado de prueba, es una ventaja ya que se puede utilizar el cupo sin ningún inconveniente para la ejecución de pruebas correspondientes en el servidor.

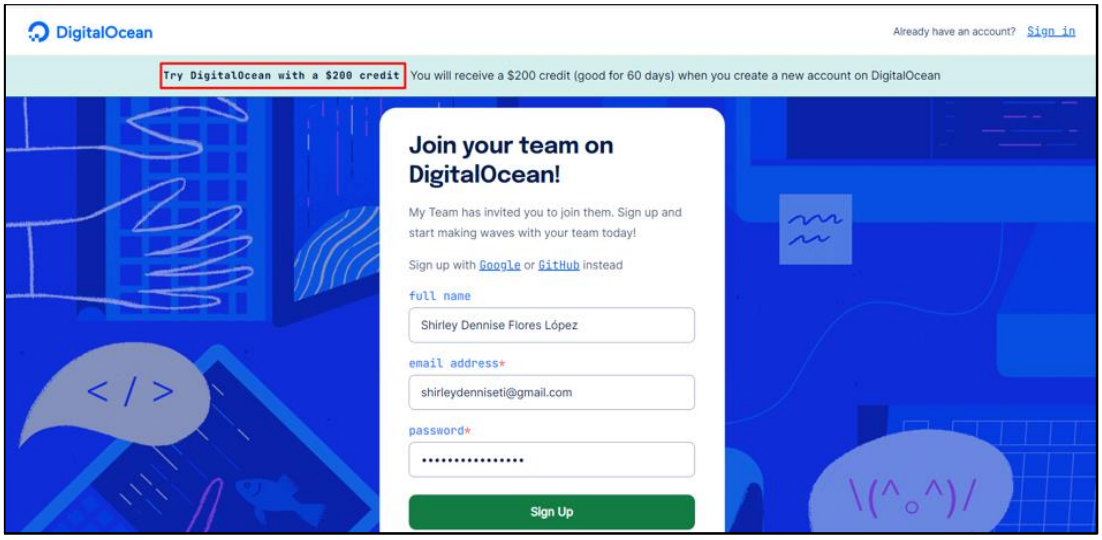


Gráfico 39. Datos cuenta
Fuente: [32]

Una vez que ya se encuentra creada la cuenta, se accede con las credenciales correspondientes a la plataforma.

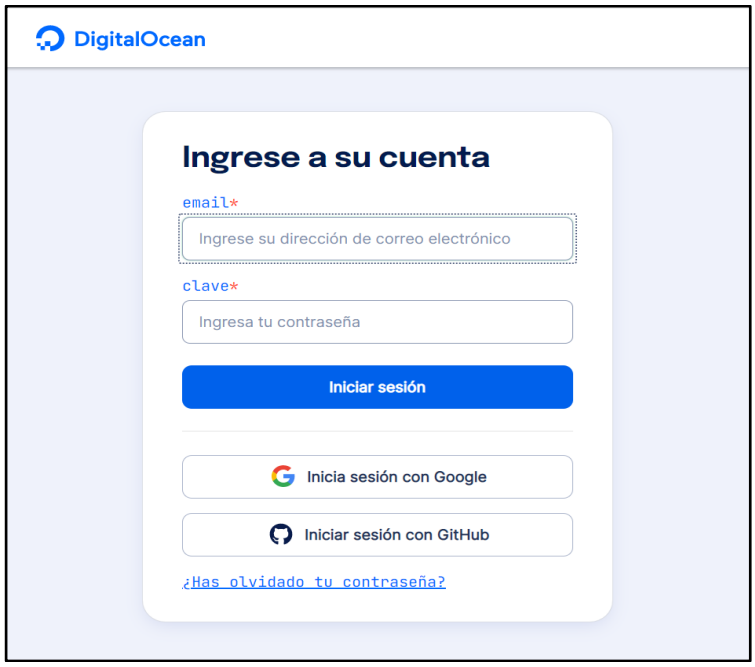


Gráfico 40. Iniciar Sesión
Fuente: [32]

3.2.3.2. Creación de instancia

Para crear una instancia, en el lado izquierdo de la pantalla se visualiza un título que dice “PROJECTS” proyectos, y dar clic en “New Project” como se muestra en la siguiente imagen:

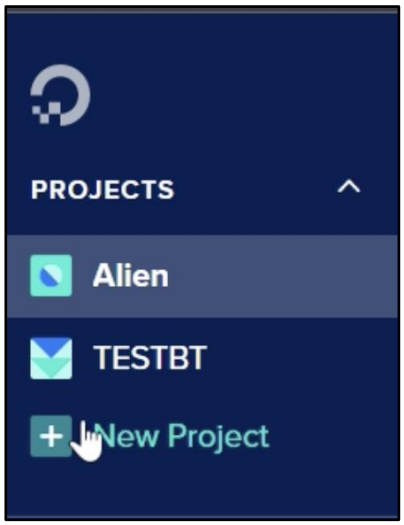


Gráfico 41. Proyectos
Fuente: [32]

Después, se muestra un formulario el cual, se debe establecer los siguientes parámetros del proyecto, como se muestra en el Gráfico 42:

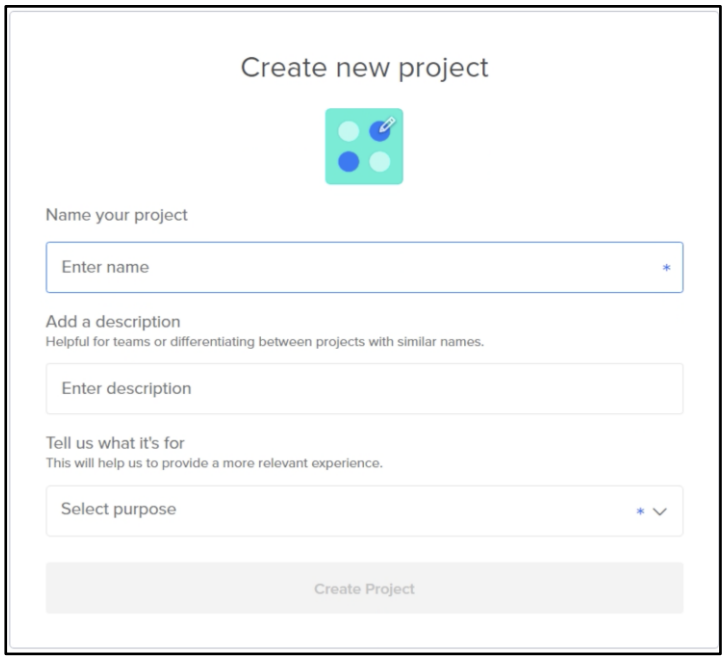


Gráfico 42. Crear nuevo proyecto
Fuente: [32]

- Name Project (Nombre del Proyecto): UTA
- Description (Descripción del Proyecto): Ingeniería Social
- Propose Project (Propósito del Proyecto): Class / Educational Propose

Una vez, ingresada la información solicitada, dar clic en “Create Project”, la instancia se crea y en ciertos casos solicita cargar configuración de otro servidor como se muestra en la siguiente imagen:

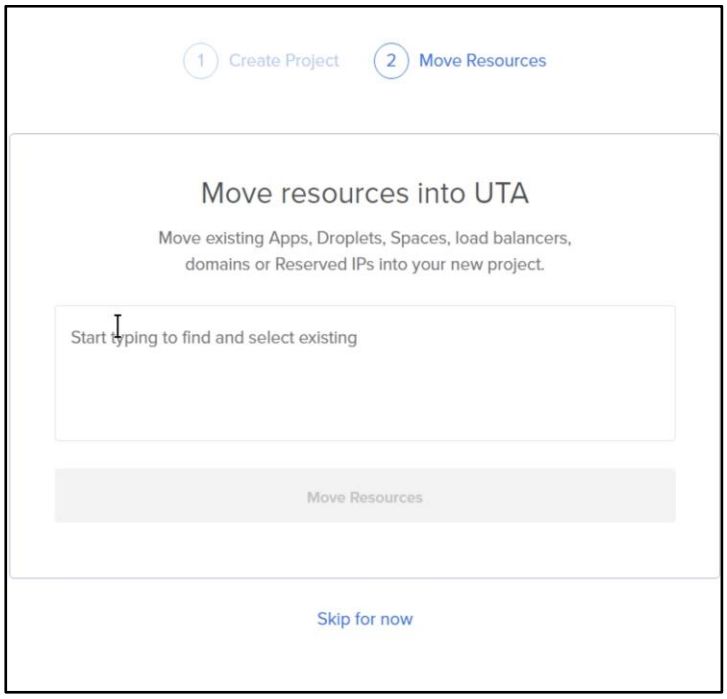


Gráfico 43. Mover requerimientos desde otro proyecto
Fuente: [32]

Al ser un proyecto nuevo, se puede omitir dicho paso por el momento.

En la siguiente imagen se puede visualizar la creación del proyecto, mismo que se encuentra con una configuración limpia o vacía.

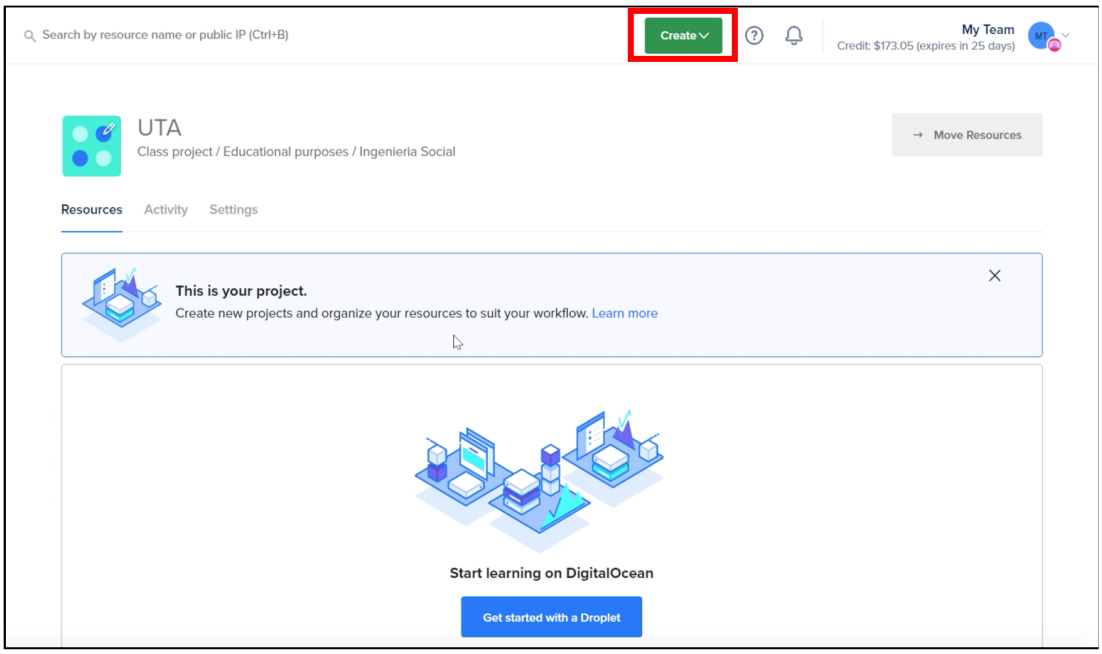


Gráfico 44. Proyecto creado
Fuente: [32]

En el Gráfico 44, se puede observar en el recuadro de color rojo, un menú desplegable que permite crear:

- Droplets Creación de servidores en la nube
- Kubernets
- Aplicativos
- Funciones
- Base de Datos
- Volúmenes
- Espacios
- Servidor de Dominio o DNS
- Cortafuegos en la Nube.
- IP´s reservadas
- Balance de Carga
- Alerta de Recursos

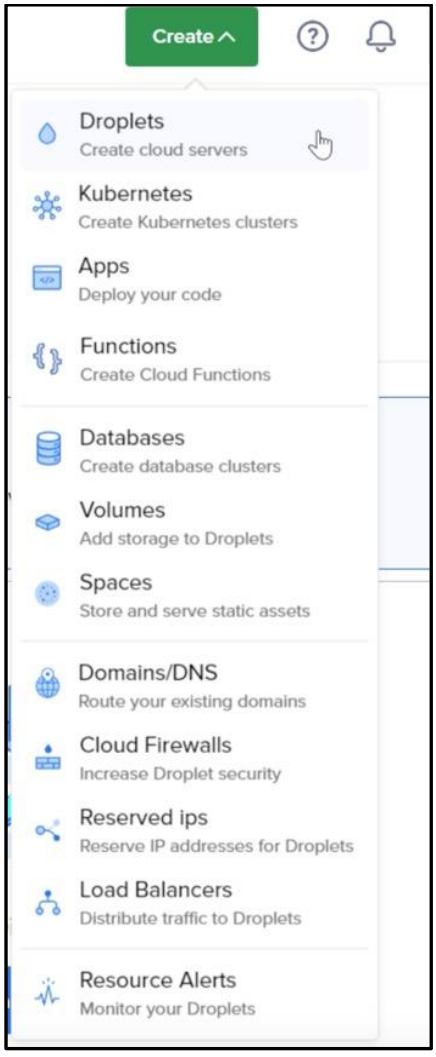


Gráfico 45. Menú de creación

Fuente: [32]

Para el desarrollo de la presente investigación se utilizará un laboratorio en la nube, y como lo denomina DigitalOcean es crear Droplets, para ello se define los siguientes requisitos para el servidor virtual:

3.2.3.3. Región del Data Center:

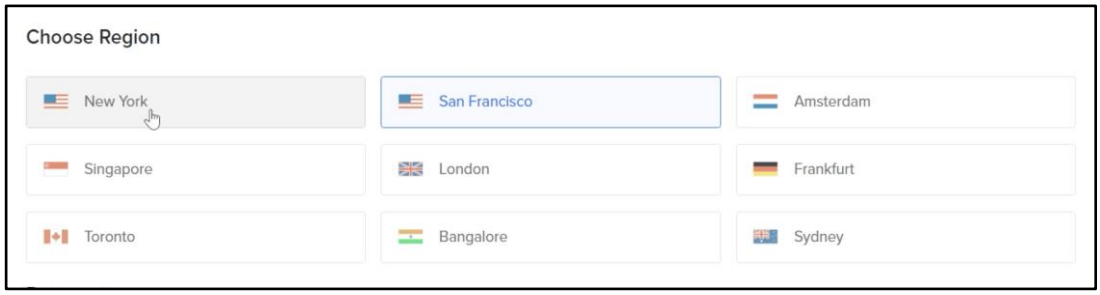


Gráfico 46. Creación de región del servidor
Fuente: [32]

3.2.3.4. DataCenter:

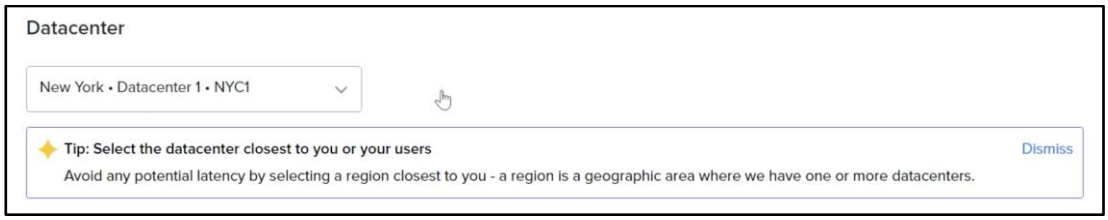


Gráfico 47. Centro de datos
Fuente: [32]

El datacenter automáticamente se actualiza a NY.

3.2.3.5. Sistema Operativo de arranque y versión:

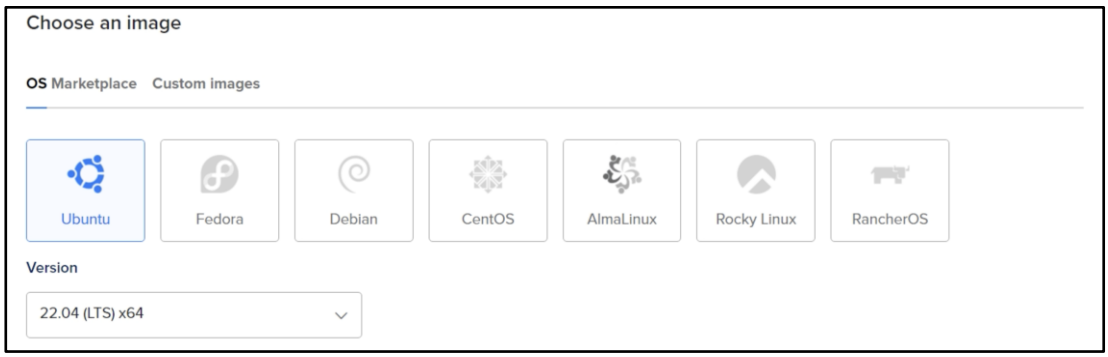


Gráfico 48. Selección del Sistema Operativo
Fuente: [32]

Para el proyecto se utiliza Ubuntu (consola), y la versión 22.04 (LTS) x64, se menciona que al mantener un LTS permite soporte en las actualizaciones del mismo, así como también, suelen ser versiones más estables que las normales.

3.2.3.6. Espacio CPU

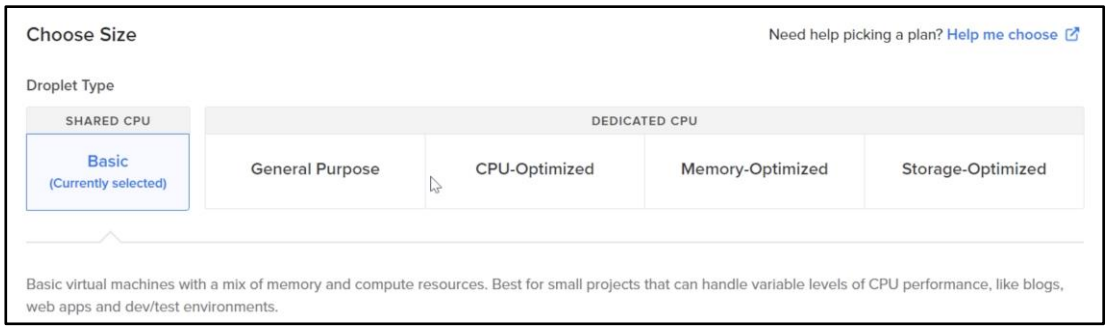


Gráfico 49. Espacio CPU
Fuente: [32]

Al considerase un laboratorio de pruebas, la opción básica del performance del equipo es el adecuado, cabe recalcar, que si fuera una empresa que realiza asesoramiento de seguridad de la información a través del hacking ético se debería establecer requerimientos para un servidor en producción.

3.2.3.7. Costos del CPU

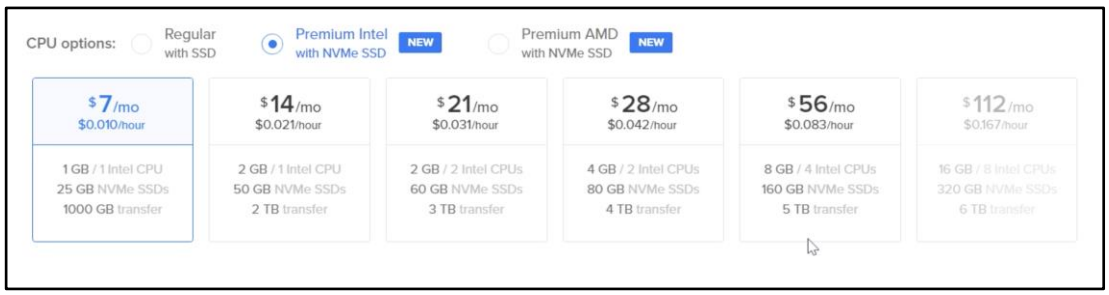


Gráfico 50. Costos del CPU
Fuente: [32]

El aplicativo funciona correctamente con:

- Procesador: 1 GB / 1 Intel CPU
- Almacenamiento: 25 GB NVMe SSDs
- Transferencia: 1 TB

3.2.3.8. Método de Autenticación

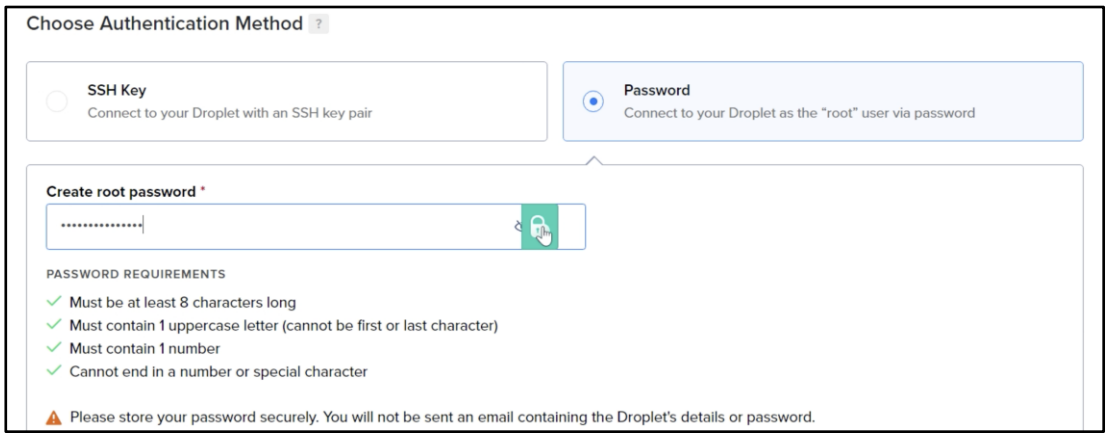


Gráfico 51. Método de autenticación
Fuente: [32]

Se utilizará a través de contraseña, mismo que debe cumplir con las características de seguridad, cumpliendo el estándar de contraseñas seguras.

3.2.3.9. Detalles Finales

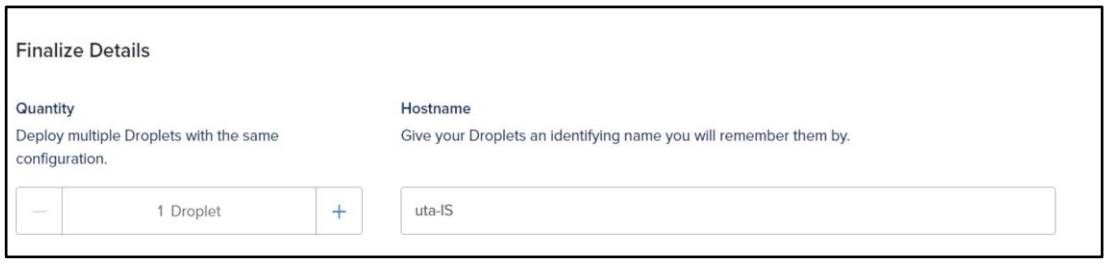


Gráfico 52. Detalles Finales
Fuente: [32]

Finalmente, se establece el número de servidores que se desea desplegar, sin embargo, este laboratorio utilizará una instancia. Por otra parte, se define el hostname mismo que lleva el nombre de "uta-IS"

Creación

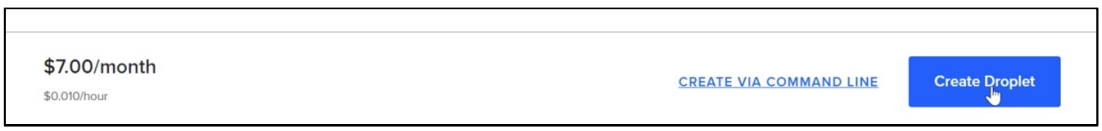


Gráfico 53. Creación del servidor
Elaborado por: Shirley Flores

Dar clic en crear instancia, proceso que se demora 30 segundos.

Gráfico 54. Tiempo de creación

Elaborado por: Shirley Flores

Una vez que la instancia se haya creado, se visualiza la región del servidor en donde fue montado el servidor, 1GB de RAM, 25 GB en Disco y la IP pública asignada al servidor.

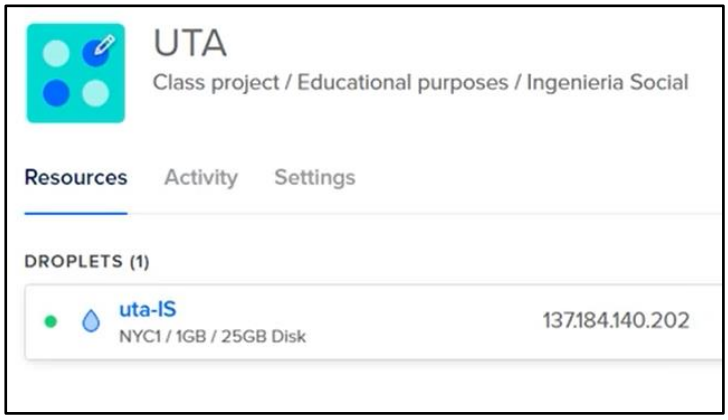


Gráfico 55. Proyecto creado

Elaborado por: Shirley Flores

Se verifica que el servidor se encuentre correctamente creado, mediante una conexión ssh con la herramienta MobaXterm, como se muestra en el Gráfico 56.

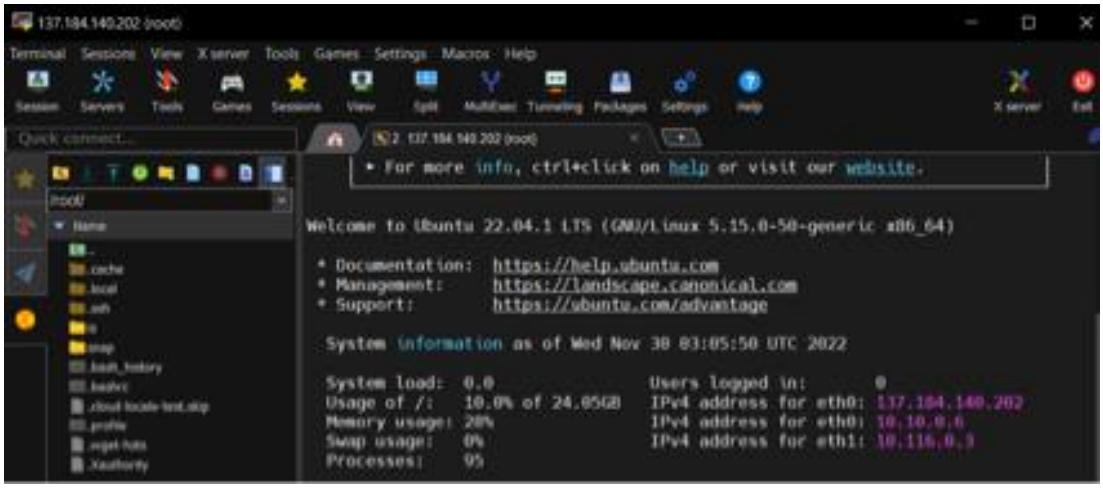


Gráfico 56. MobaXterm

Elaborado por: Shirley Flores

3.2.4. Despliegue

3.2.4.1. Instalación de Gophish

En esta fase de instalación, se accede a la página de descarga de Gophish en el siguiente enlace: https://getgophish.com/, y se da clic en la opción de Download.

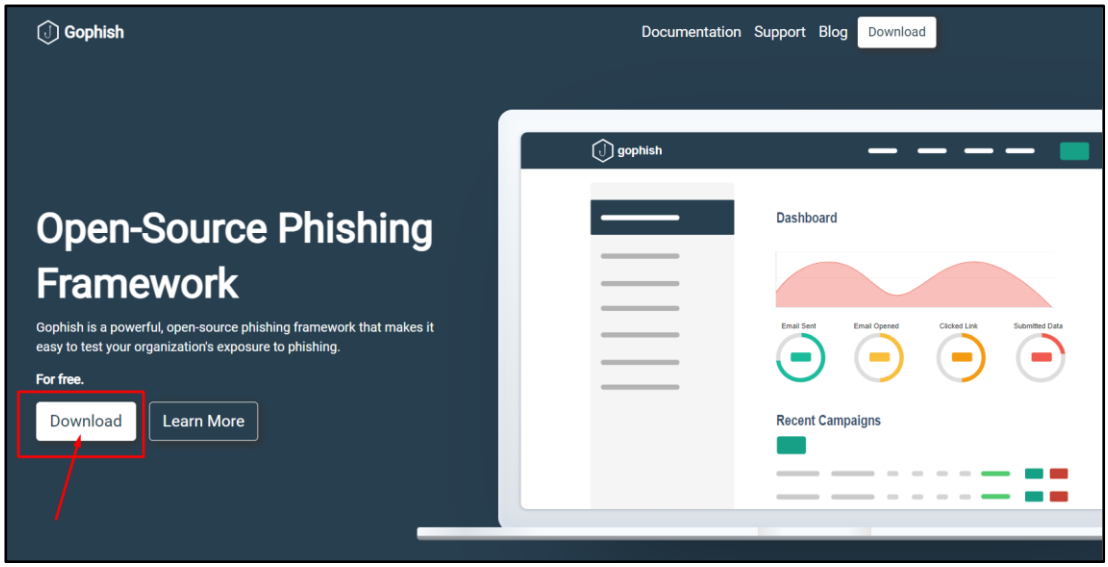


Gráfico 57. Descarga de Gophish

Elaborado por: Shirley Flores

La opción anterior, redireccionará a una página de GitHub, en la que se encuentran alojadas las opciones de descargas del framework con sus versiones, la cual se ha considerado la última versión para el presente proyecto.

Una vez ya identificadas las características que se necesita para la instalación, según la versión y el sistema operativo, se procede a copiar la dirección del enlace de descarga.

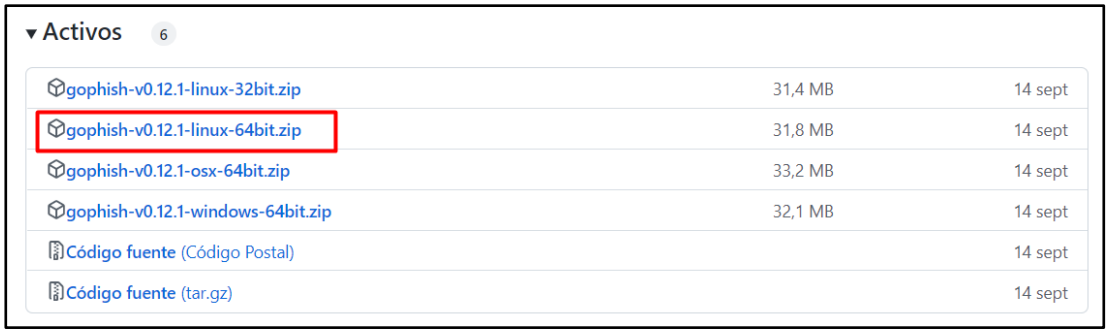


Gráfico 58. Imagen Gophish

Elaborado por: Shirley Flores

En la consola de MobaXterm, mediante la conexión ssh al servidor, se realiza las configuraciones correspondientes.

Se crea una carpeta denominada IS, y se aplica el comando wget, el cual sirve para realizar descargas de una página web determinada.

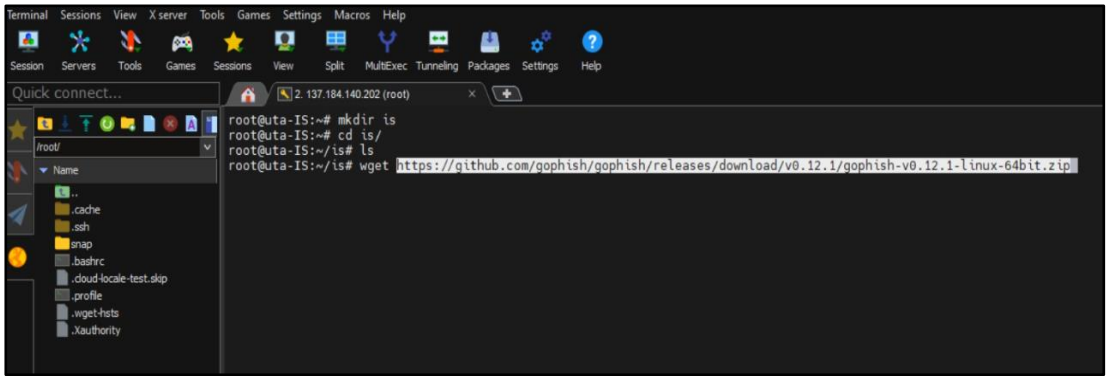


Gráfico 59. Administración Ubuntu

Elaborado por: Shirley Flores

Una vez descargado el archivo zip, se procede a descomprimir el archivo en la carpeta local en donde se está ejecutando la instalación.

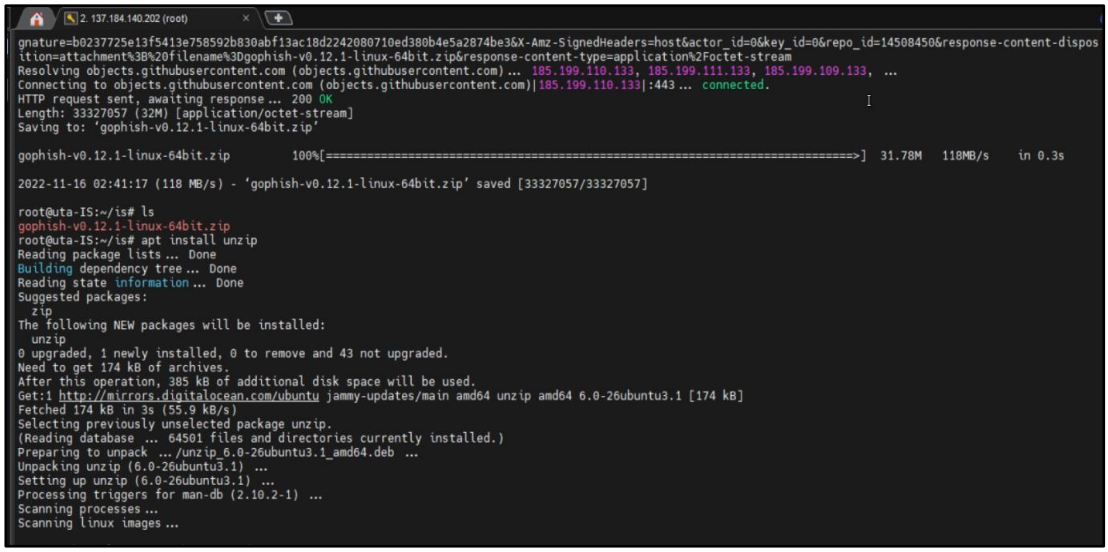


Gráfico 60. Instalación de paquetes

Elaborado por: Shirley Flores

Se continúa con la configuración del archivo config.json, en el cual se cambia la dirección de la url “0.0.0.0:8000 ”, para configurar que cualquier servidor pueda conectarse, en caso de que se tenga que levantar más servidores para las pruebas y

ejecución final o si el servidor se da de baja, pero la configuración de Gophish no cambia.

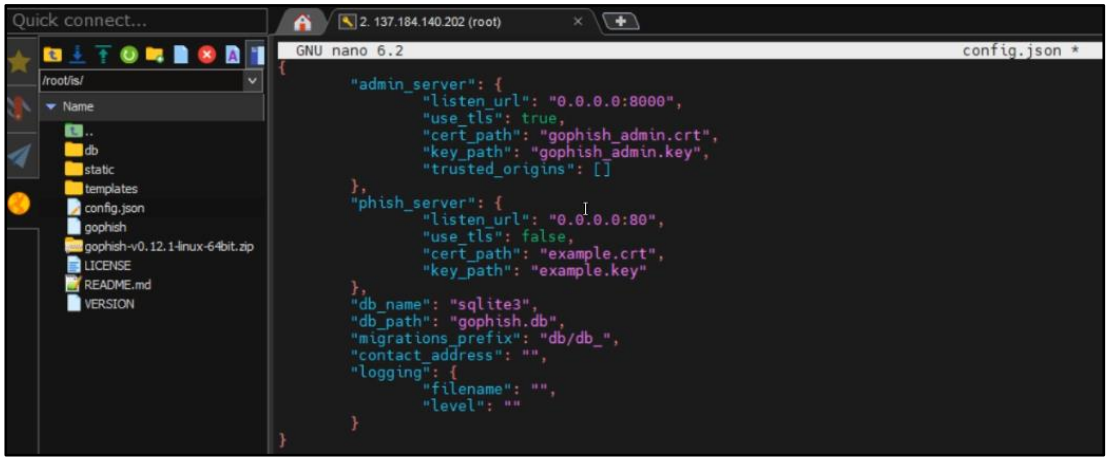


Gráfico 61. Modificación Plantilla

Elaborado por: Shirley Flores

Se revisa si Gophish cuenta con permisos de ejecución, en este caso no tiene ningún permiso, para lo cual, con el comando chmod +x se asigna el permiso de ejecución correspondiente, como se visualiza en el Gráfico 62.

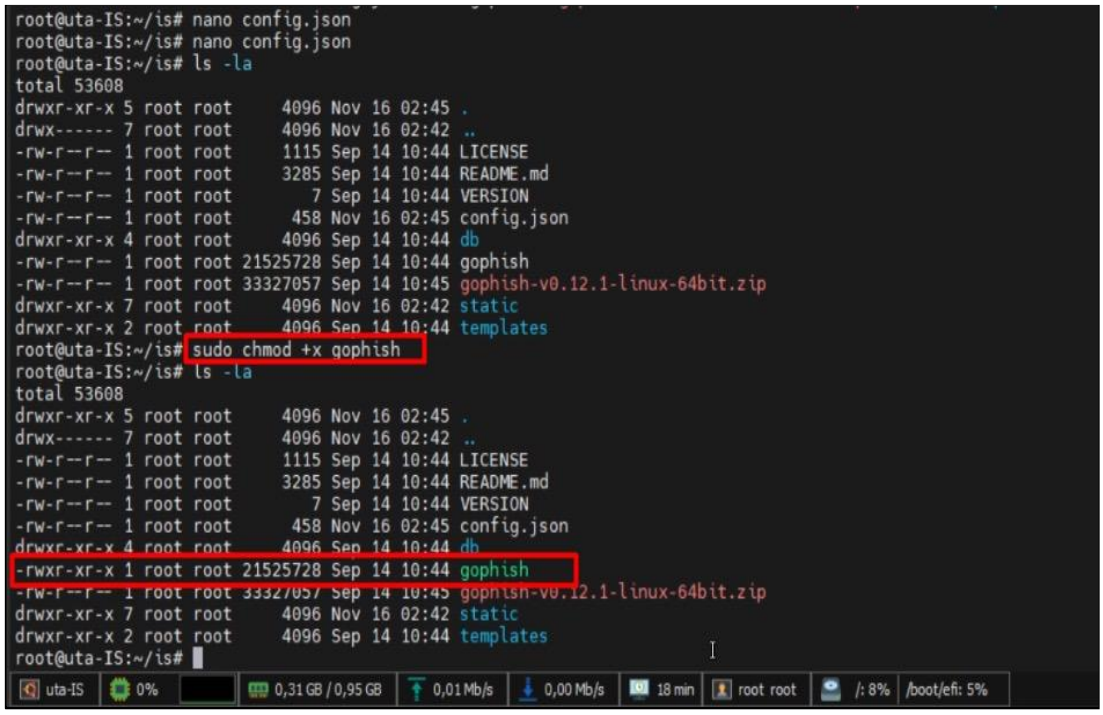


Gráfico 62. Iniciar Gophish

Elaborado por: Shirley Flores

Se ejecuta Gophish y se crea todos los archivos necesarios para que funcione correctamente la plataforma. Si no hubo ningún problema se visualiza en pantalla las credenciales de acceso por defecto al momento de levantar la herramienta, como se visualiza en el siguiente gráfico:

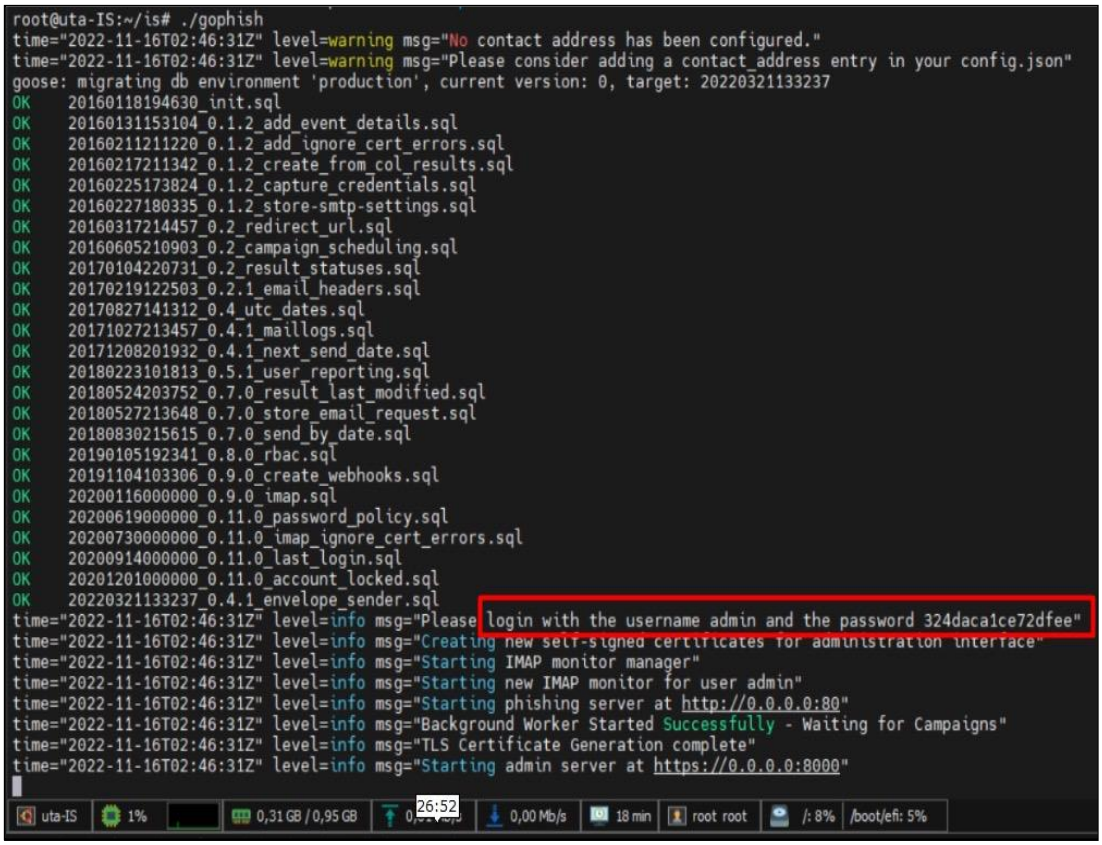


Gráfico 63. Iniciar Sesión Gophish

Elaborado por: Shirley Flores

Se abre un navegador, en la barra de direcciones se coloca la IP del servidor levantado, con el puerto configurado https://137.184.140.202:8000 y se abre la página principal del login de gophish, por consiguiente, se accede inicialmente con las credenciales por defecto.

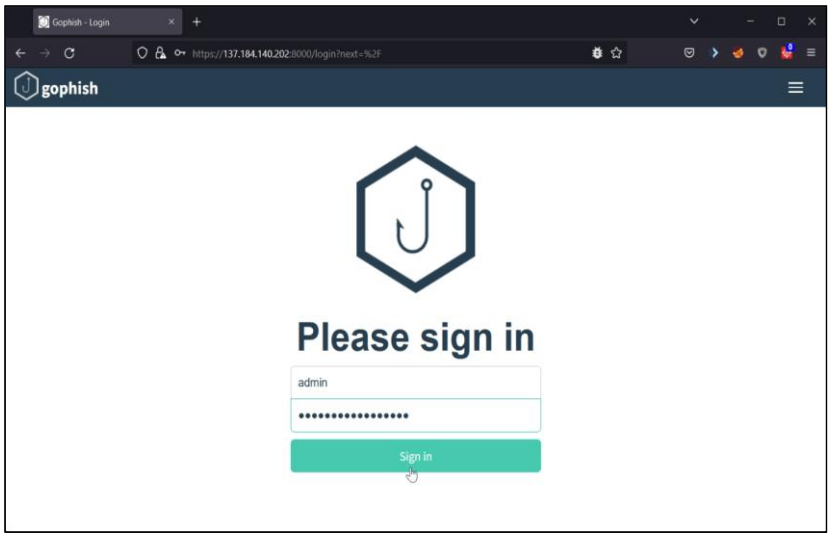


Gráfico 64. Iniciar Gophish

Elaborado por: Shirley Flores

Una vez ingresado, la plataforma solicita el cambio de contraseña, se ingresa una nueva contraseña cumpliendo con el estándar de seguridad de claves y se procede a guardar la configuración.

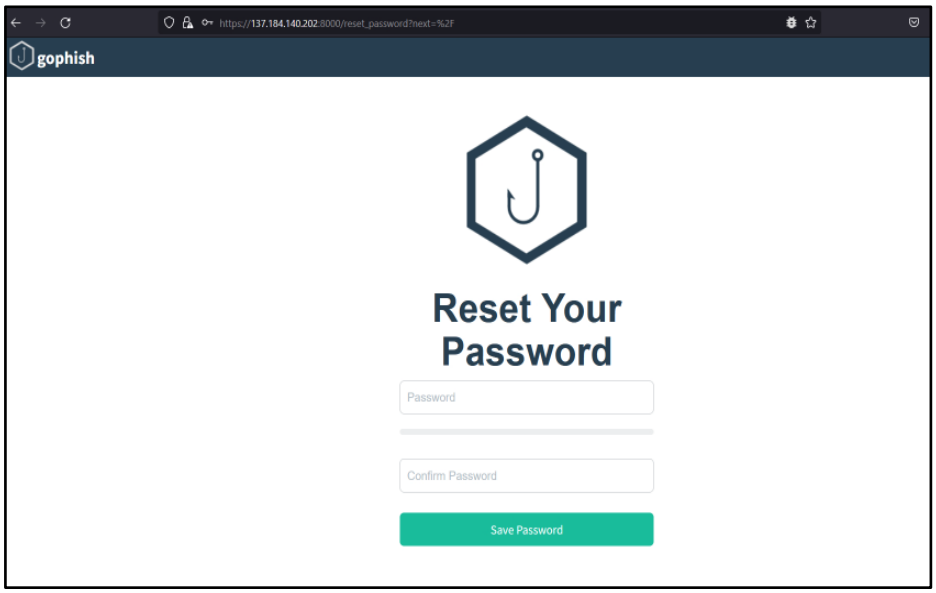


Gráfico 65. Actualización de Contraseña

Elaborado por: Shirley Flores

Cuando se haya iniciado, se encontrará con la dashboard inicial de gophish, como se visualiza en el Gráfico 66.

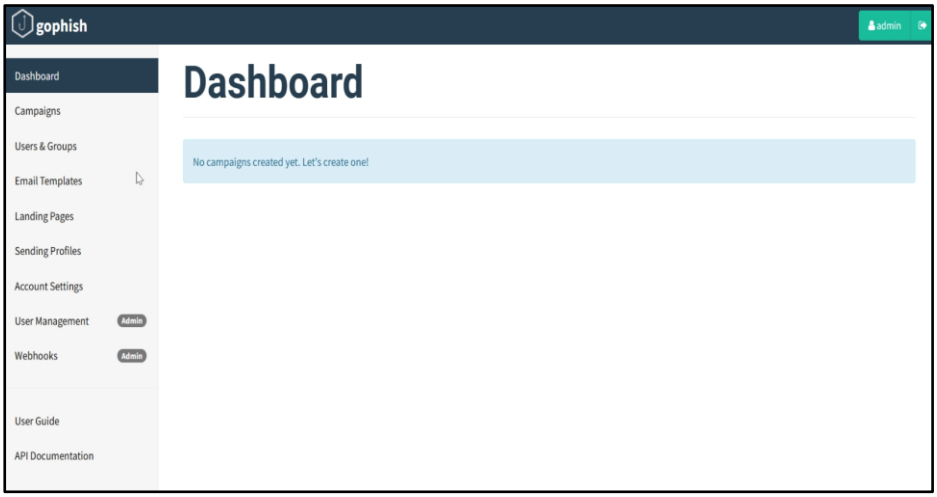


Gráfico 66. Dashboard

Elaborado por: Shirley Flores

A continuación, se procede a configurar el framework Gophish, para realizar la simulación de ataque, según lo analizado y planteado inicialmente.

3.2.4.2. Configuración de Gophish

Como primer paso, para empezar con la simulación del ataque, se debe configurar la página de envió de los perfiles, es decir analizar a quien se quiere suplantar.

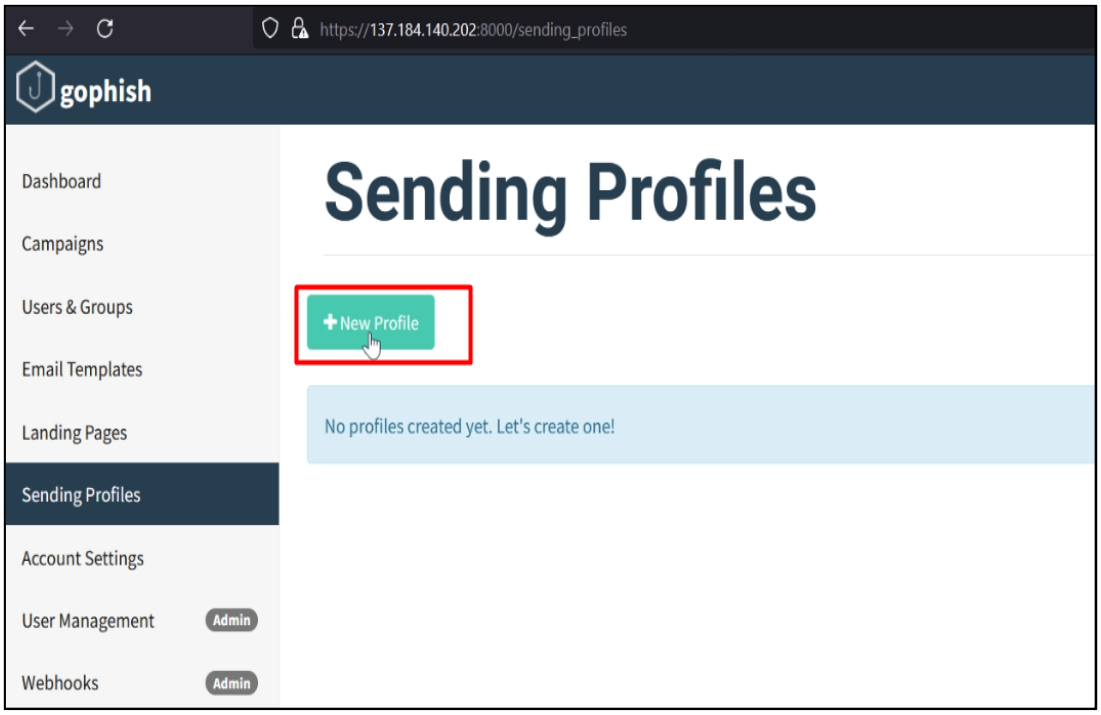


Gráfico 67. Envío de perfiles

Elaborado por: Shirley Flores

Para configurar esta página, se creó los siguientes correos en Outlook, para poder configurarlos en esta sección:

- soporte.tecnico.UTA@outlook.com
- fche.uta.univerisad@outlook.com

En el cual, el primer correo será utilizado para configurar el perfil de Docentes, y el segundo para el perfil de estudiantes de la Facultad de Ciencias Humanas y de la Educación.

3.2.4.3. Perfil Estudiantes y Docentes

En el campo Name, es el nombre que se le asigna a dicho perfil para distinguir de los demás perfiles que se vayan añadiendo.

En el apartado SMTP From, se coloca el remitente, el mismo que se visualizará en el correo que reciba la víctima. Para el envío de correos es necesario utilizar un servidor SMTP, de manera que en este caso se va a utilizar el servidor de Microsoft (smtp-mail.outlook.com:587).

Los últimos campos son el username y el password, en las cuales se ingresa las credenciales del correo real, ya antes creado en Outlook que se utilizará para la realización del envío. La configuración se muestra en el Gráfico 68 y 69.

3.2.5. Creación de Escenario 01 – Estudiantes

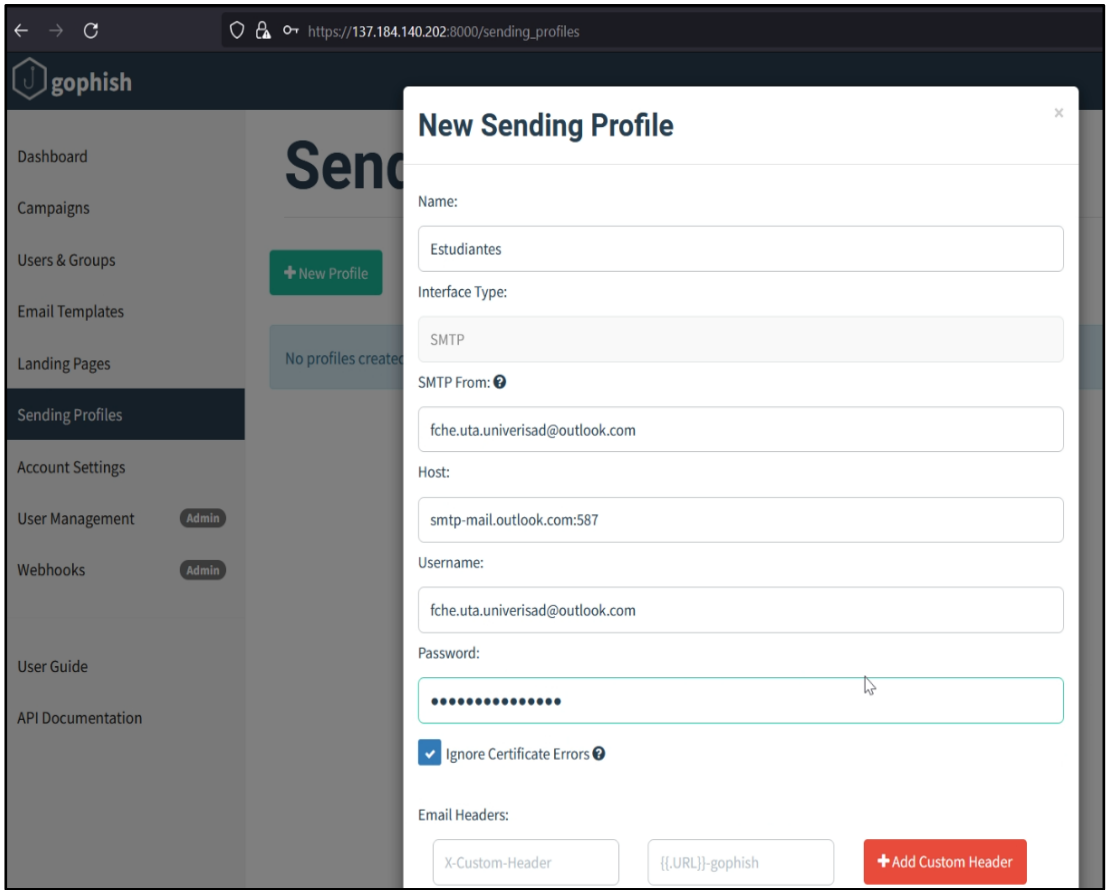


Gráfico 68. Perfil Estudiantes utilizado en la simulación en Gophish

Elaborado por: Shirley Flores

3.2.6. Creación de Escenario 02 – Docentes

Para la Creación del Escenario de Docentes, se aplica el mismo procedimiento que se realizó con el escenario de Estudiantes y se coloca el correo correspondiente con su respectiva contraseña para realizar la conexión pertinente.

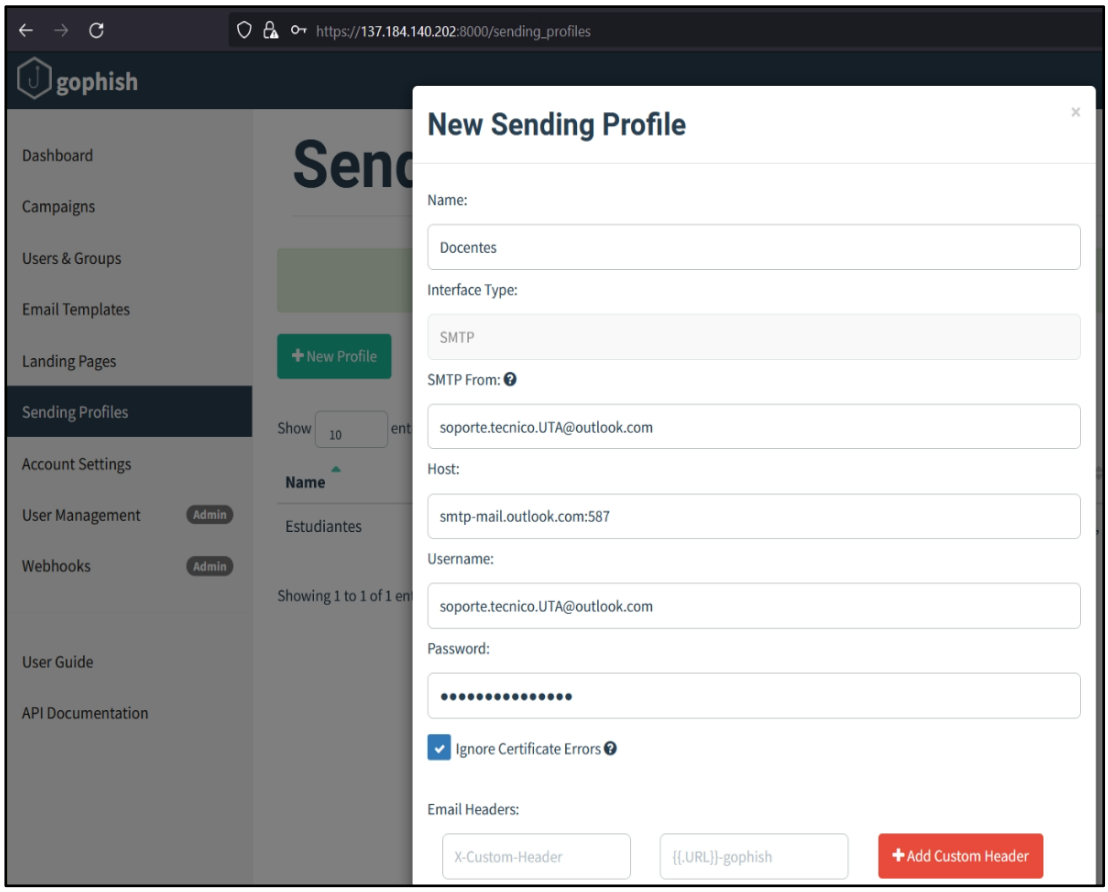


Gráfico 69. Creación de Escenario

Elaborado por: Shirley Flores

Se realizo una prueba de envío de correo con los correos configurados, para comprobar que el envío si está funcionando correctamente.

Para comprobar que existe una conexión entre la página de Gophish y el correo electrónico, se utilizó los dos correos de prueba, en el cual en el Perfil de docentes se realizó la prueba del envió del email al correo establecido para los estudiantes, como se muestra en el Gráfico.

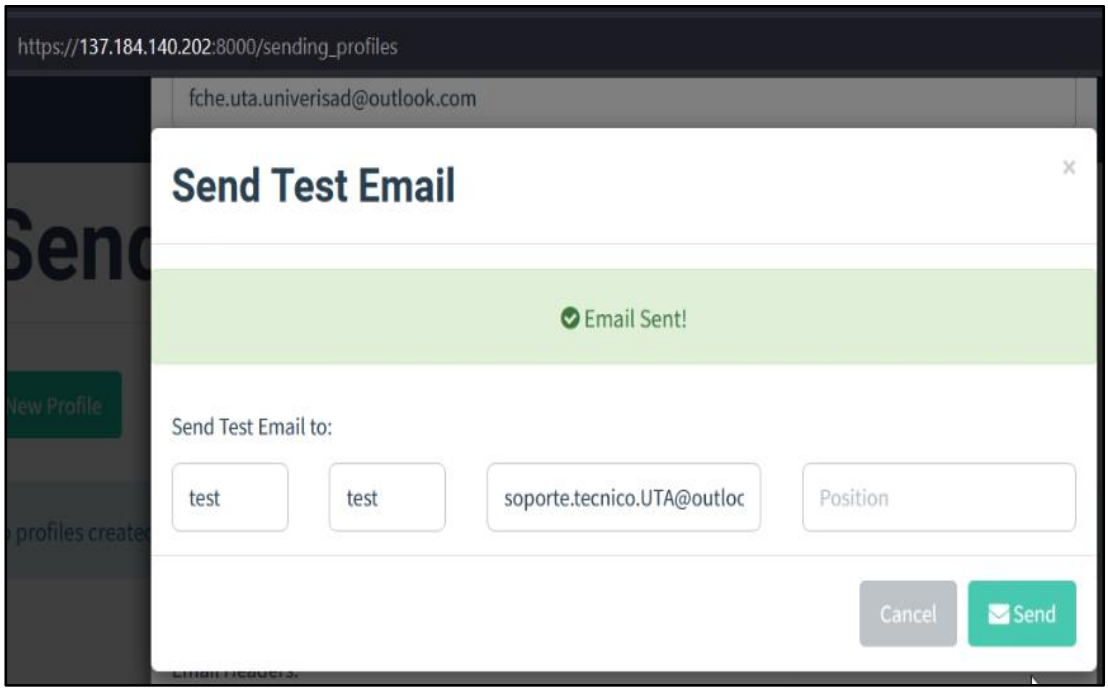


Gráfico 70. Envió de Correo Electrónico de prueba – Docentes en Gophish

Elaborado por: Shirley Flores

El correo asignado para estudiantes fche.uta.univerisad@outlook.com envió un correo electrónico de pruebas a soporte.tecnico.UTA@outlook.com el cual fue satisfactoriamente enviado y se puede comprobar que se recibió el correo como lo muestra en el Gráfico 71.

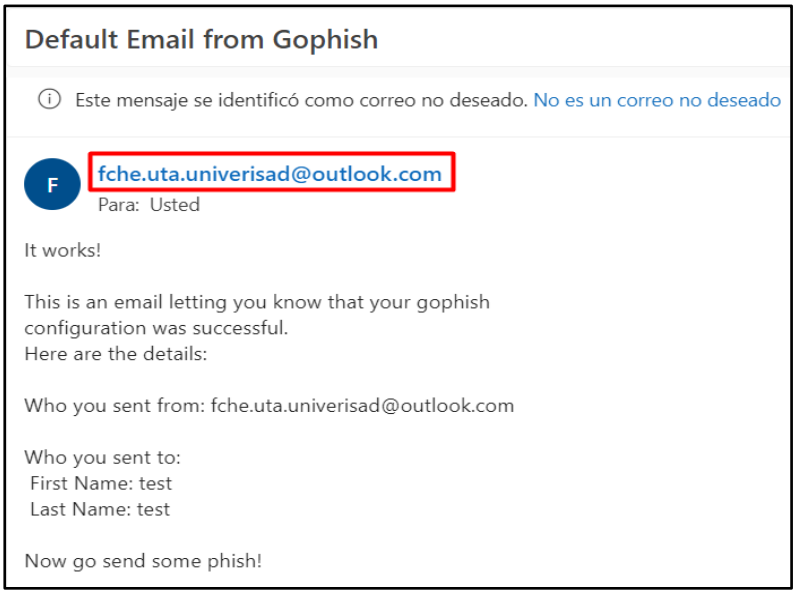


Gráfico 71. Correo recibido en la cuenta docentes de Outlook

Elaborado por: Shirley Flores

En el Perfil de estudiantes se realizó la prueba del envió del email al correo establecido para los docentes, como se muestra en el Gráfico 72.

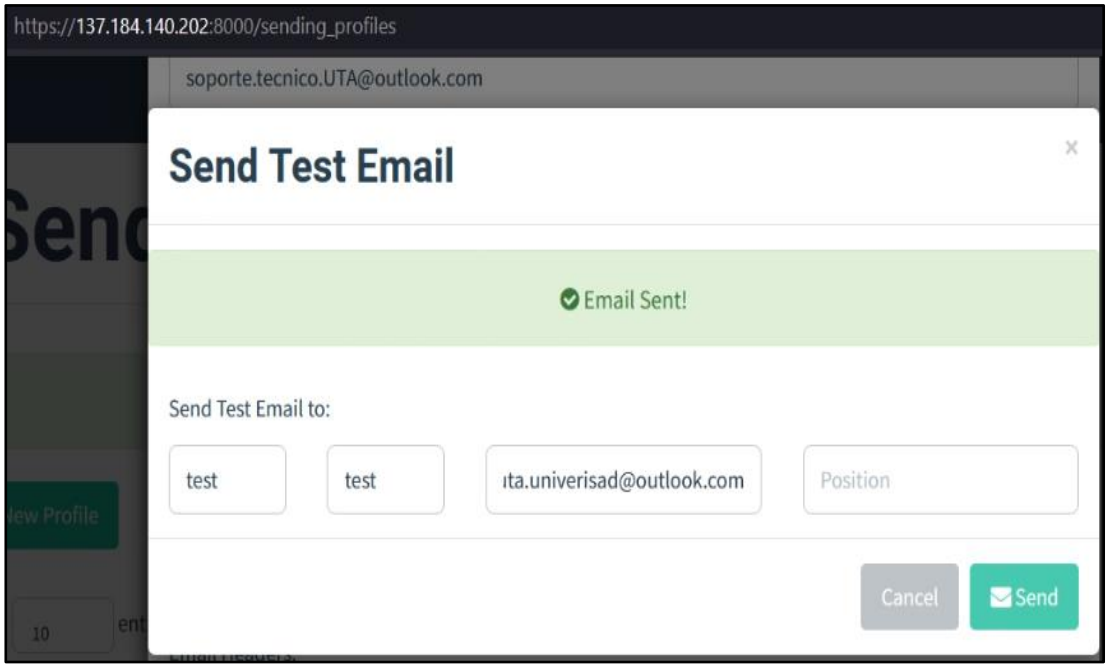


Gráfico 72. Envió de Correo Electrónico de prueba -Estudiantes en Gophish
Elaborado Por: Shirley Flores

El correo asignado para docentes soporte.tecnico.UTA@outlook.com envió un correo electrónico de pruebas a fche.uta.univerisad@outlook.com el cual fue satisfactoriamente enviado y se puede comprobar que se recibió el correo como lo muestra en el Gráfico 73.

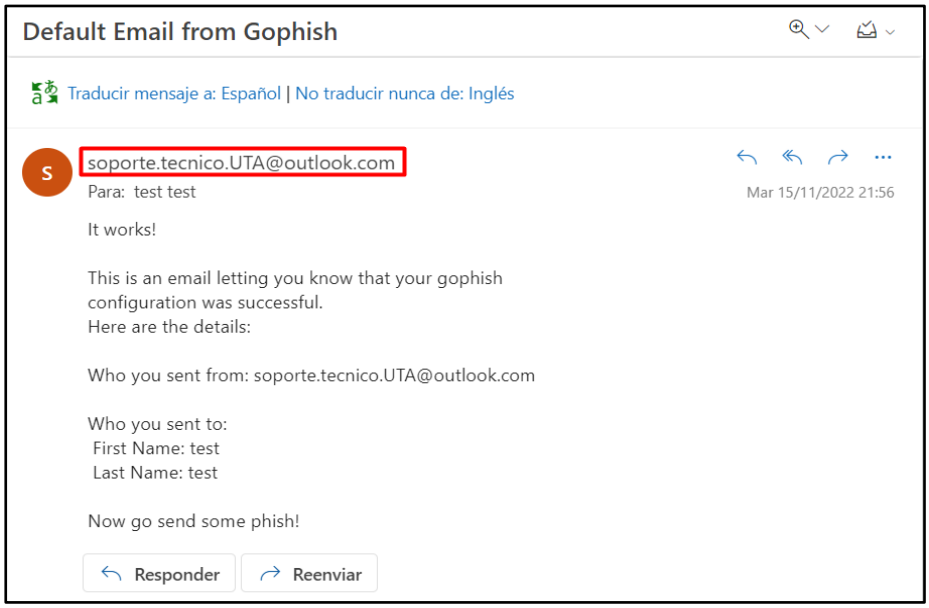


Gráfico 73. Correo recibido en la cuenta estudiantes de Outlook
Elaborado por: Shirley Flores

Una vez ya verificado los correos y que se encuentre en funcionalidad con Gophish, se guarda la configuración de los perfiles creados y se puede visualizar información acerca de la creación como el nombre del perfil con el cual se va a distinguir a la población a ser enviadas, el tipo de interface a utilizar y la fecha de creación o modificación del perfil, así como se visualiza en el Gráfico 74.

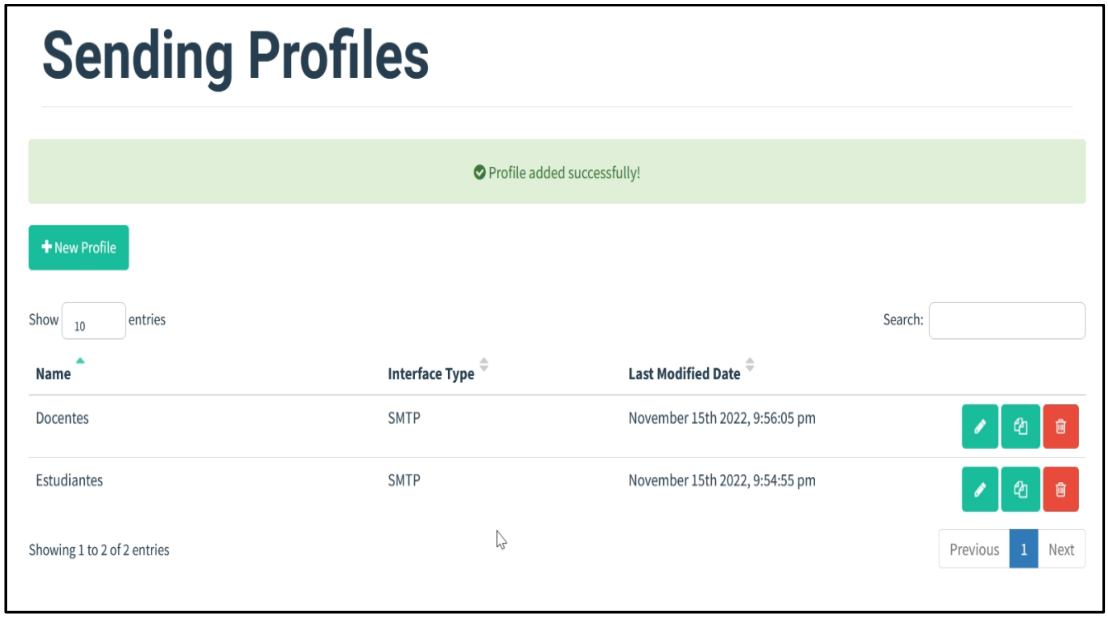


Gráfico 74. Perfiles creados en Gophish

Elaborado por: Shirley Flores

3.2.7. Creación de la Página de Destino (Landing Page)

En el menú de Gophish, se encuentra la opción de Landing Page, para crear nuevas páginas fraudulentas y estas serán la simulación de una página real, a la cual el usuario va a interactuar. Estas páginas deben estar en correspondencia con los correos en donde se enviará a las víctimas para capturar sus datos.

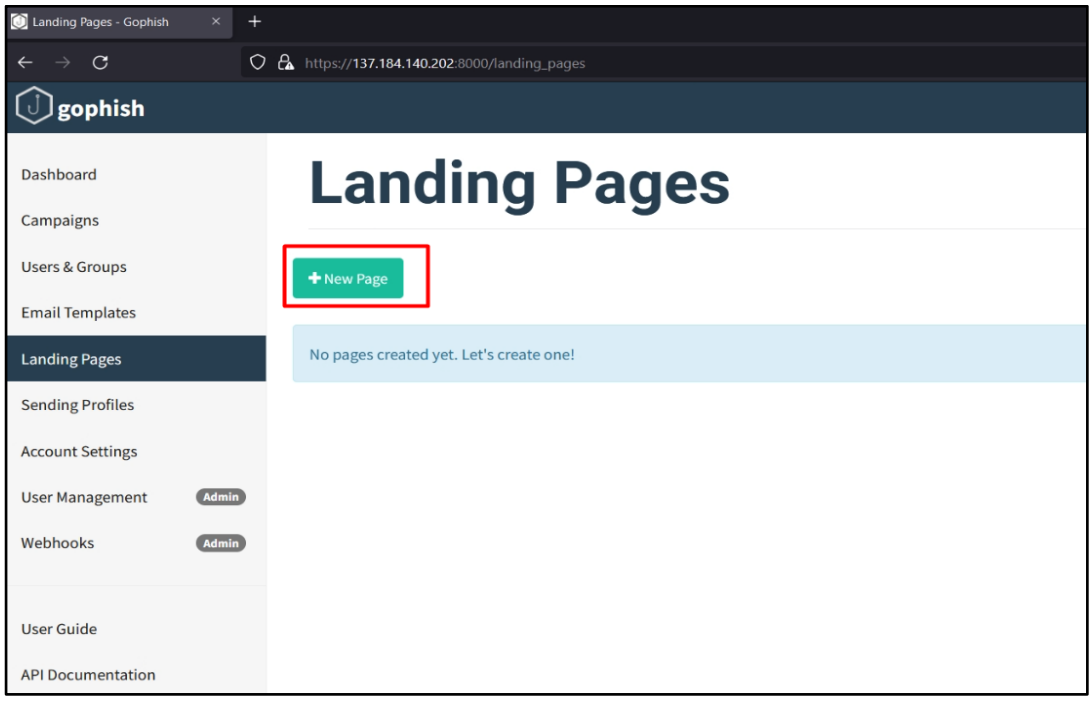


Gráfico 75. Menú de Creación de Páginas de Destino

Elaborado Por: Shirley Flores

Para crear el Landing Page, se la puede hacer de dos maneras distintas, la primera es la creación por medio de la importación de la página mediante una url desde el internet y la segunda por la implementación de código HTML. Al momento de la configuración se puede dar clic a la opción de capturar datos, es decir para capturar la información que el usuario ingrese por el landing page creado.

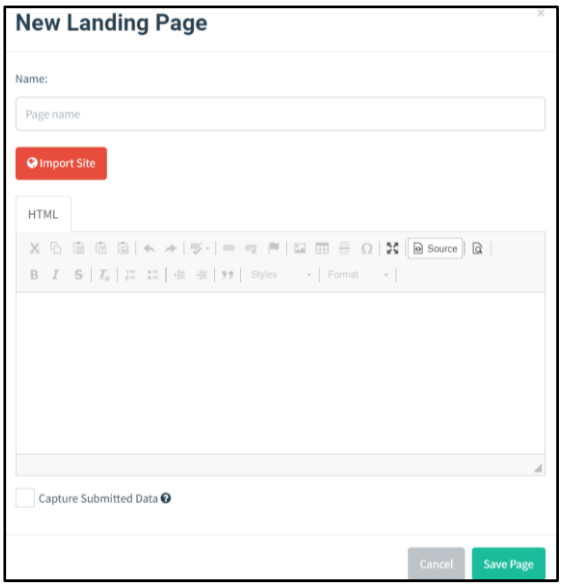


Gráfico 76. Creación de Páginas de Destino

Elaborado Por: Shirley Flores

En la opción de Source, se agrega el código creado para el diseño de la página fraudulenta. En la parte derecha del código, se encuentra la opción de visualizar, de manera que se puede observar la página como lo vería la victima de este ataque y así agregar, modificar o eliminar detalles de código.

Para culminar con la configuración de la página de destino, se va a marcar las 2 casillas, en este caso se va a capturar los datos y también las contraseñas y se va a redireccionar a la página legítima, una vez que la víctima haya iniciado sesión como se indica en el Gráfico 77.

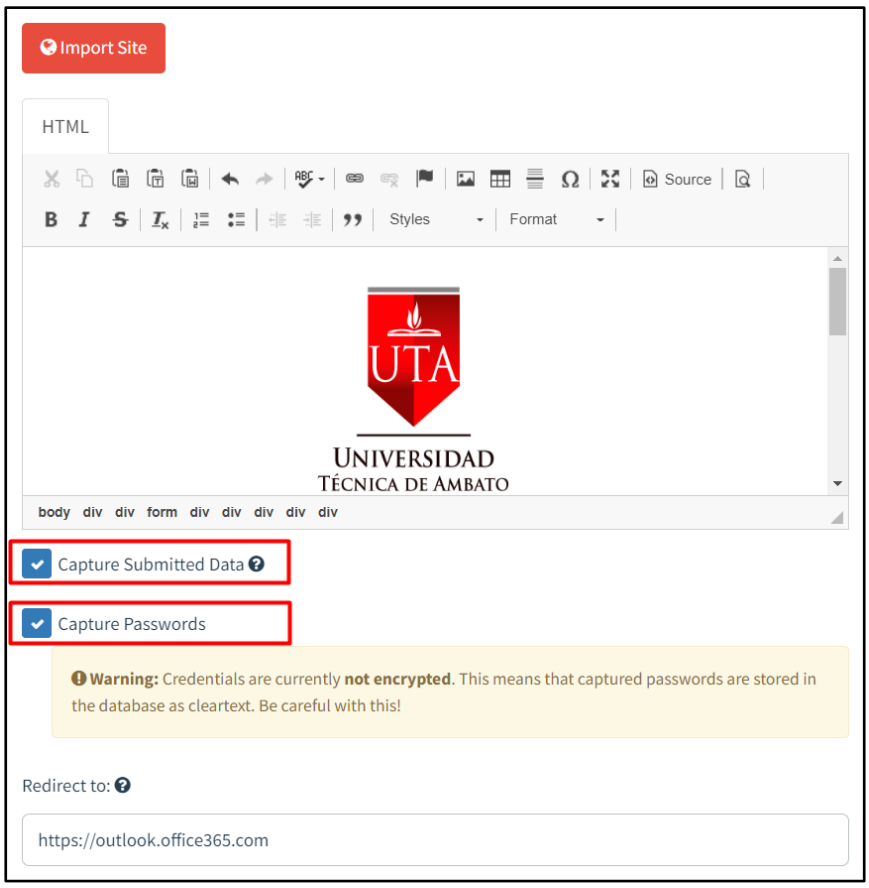


Gráfico 77. Configuración de Página de Destino UTA
Elaborado Por: Shirley Flores

En este caso se va a implementar un código HTML, similar al inicio de sesión del correo institucional, para cual se utilizó la herramienta Notepad++, y el código se lo visualiza de la siguiente manera como lo indica en el Gráfico 78.

Gráfico 78. Código HTML de Páginas de Destino UTA en Notepad++

Elaborado Por: Shirley Flores

En la opción de visualización en la página de Gophish, se muestra la página creada con el fin de confundir a la víctima en la simulación del ataque de phishing. El resultado del código HTML se muestra a continuación en el Grafico 79.

Gráfico 79. Página de Destino UTA Creada

Elaborado Por: Shirley Flores

Creación de la Plantilla de correo electrónico (Email Template)

En el panel de Gophish, para crear una plantilla de correo electrónico, se da clic en la opción Email Templates, y seguido de esa acción, se agrega una nueva plantilla como lo muestra a continuación en el Gráfico 80.

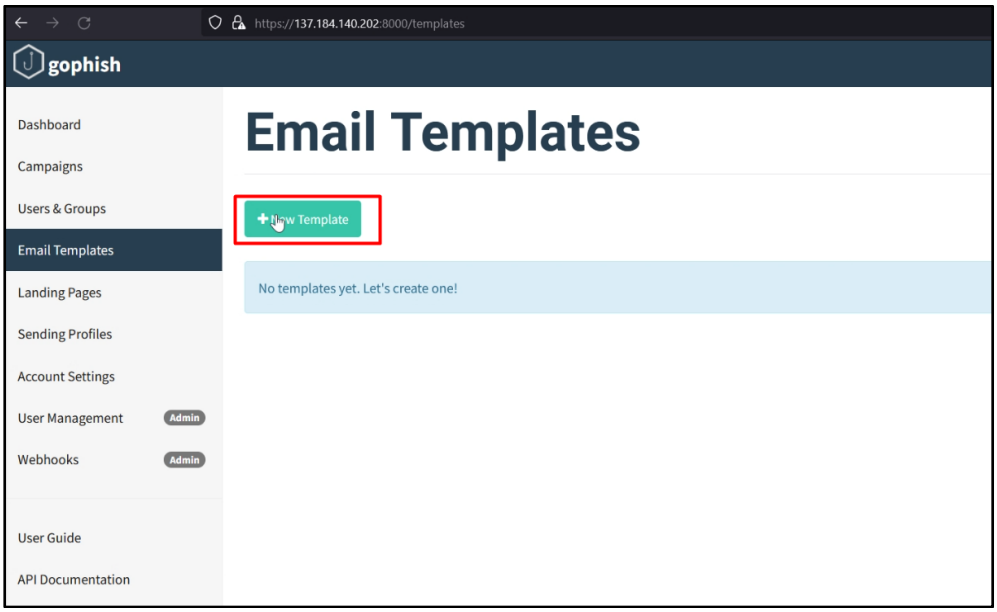


Gráfico 80. Menú de Creación de Plantilla de Correo Electrónico

Elaborado Por: Shirley Flores

Para crear una plantilla nueva, se necesita agregar información como el nombre que se va a asignar, el remitente del correo, este campo es opcional, el asunto con el cual se enviará los correos, el mismo que debe ser de gran interés y la estructura del mensaje a enviar.

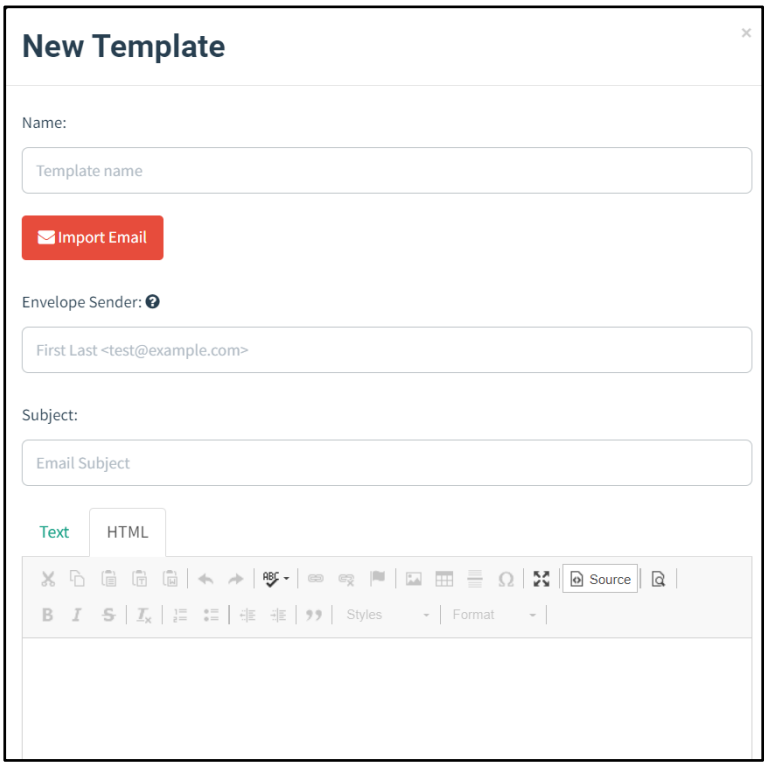


Gráfico 81. Creación de Plantilla de Correo Electrónico

Elaborado Por: Shirley Flores

Para la configuración de la plantilla de correo se configuró de la siguiente manera como lo indica el Gráfico 82:

- Nombre: AVISO UTA
- Envelope Sender: Campo Opcional – No necesario
- Asunto: Atención Estimada Comunidad Universitaria
- Código: Correo Elaborado en HTML.

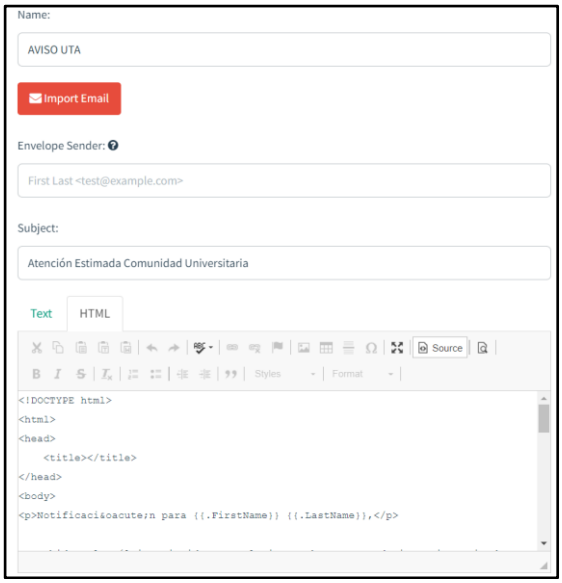


Gráfico 82. Configuración de Plantilla de Correo Electrónico

Elaborado Por: Shirley Flores

Para implementar el cuerpo del correo electrónico, se elaboró un código HTML, en el cual se detalla la información que se va a transmitir a la víctima con el fin de que el correo aparente ser un correo legítimo, para cual se utilizó la herramienta Notepad++, y el código se lo visualiza de la siguiente manera como lo indica en el Gráfico 83.

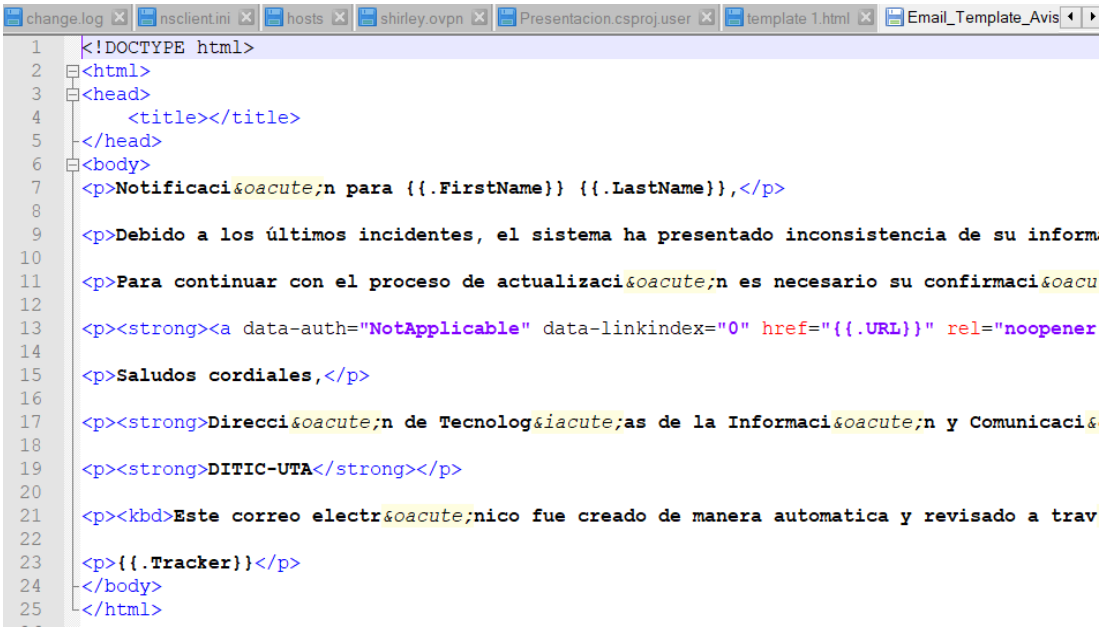


Gráfico 83. Código HTML de Plantilla de Correo Electrónico en Notepad++

Elaborado Por: Shirley Flores

En la opción de visualización de la plantilla creada, se muestra el resultado del código ejecutado en el cual se utiliza las variables permitidas en el gophish, y el enlace a redireccionar la página de destino creada anteriormente como lo indica en el Gráfico 84.

Notificación para {{.FirstName}} {{.LastName}},

Debido a los últimos incidentes, el sistema ha presentado inconsistencia de su información, el mismo no se está actualizando correctamente. La información de los correos institucionales están retenidos en nuestros filtros de seguridad ya que han superado satisfactoriamente el tiempo de **permanencia** por lo que pueden ser eliminados y esto ocasionará la perdida de su información.

Para continuar con el proceso de actualización es necesario su confirmación caso contrario el sistema de filtros de seguridad eliminará automáticamente la información de los correos retenidos en 2 horas.

Actualización de Información de su cuenta de correo

Saludos cordiales,

Dirección de Tecnologías de la Información y Comunicación UTA.

DITIC-UTA

Este correo electrónico fue creado de manera automatica y revisado a través de un sistema de detección de virus y malware.

{{.Tracker}}

Gráfico 84. Plantilla de Correo Electrónico Creada

Elaborado Por: Shirley Flores

3.2.7.1. Creación de Usuarios y Grupos (Users & Groups)

Lo último que se debe configurar, para lanzar la campaña de Phishing son los usuarios que en este caso van a ser las víctimas de la simulación de ataque. Desde el panel de Users & Groups se pueden crear distintos grupos, y en cada uno de ellos añadir las víctimas que se considere necesario.

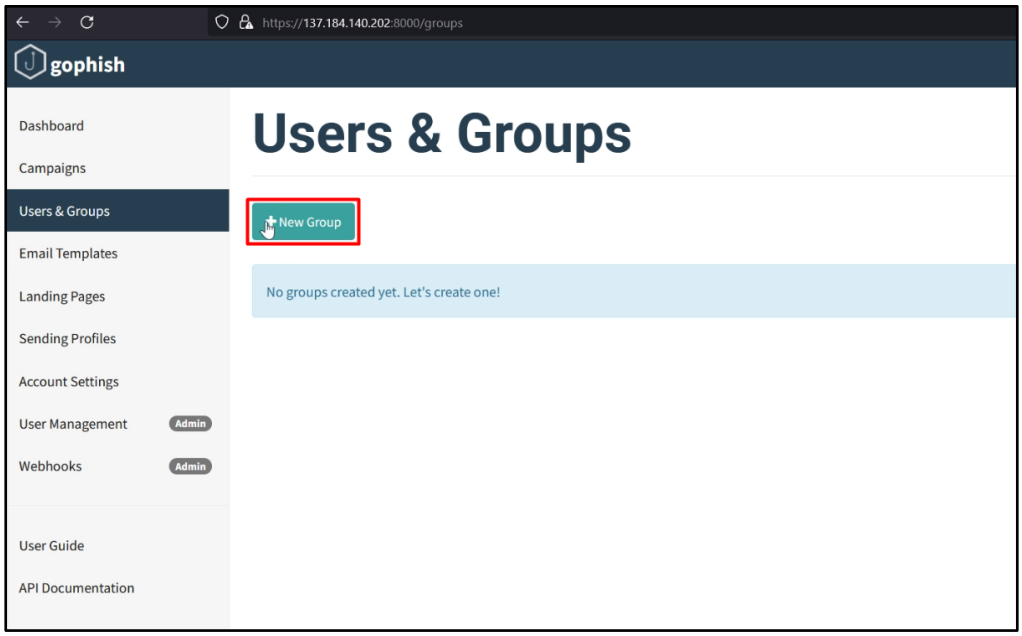


Gráfico 85. Creación de Usuarios y Grupos

Elaborado Por: Shirley Flores

Para añadir usuarios al nuevo grupo, se puede realizar manualmente, en el caso de que el número de las víctimas sean pocas, o a su vez se puede cargar los datos masivamente en formato CSV, en el caso de que el número sea considerable.

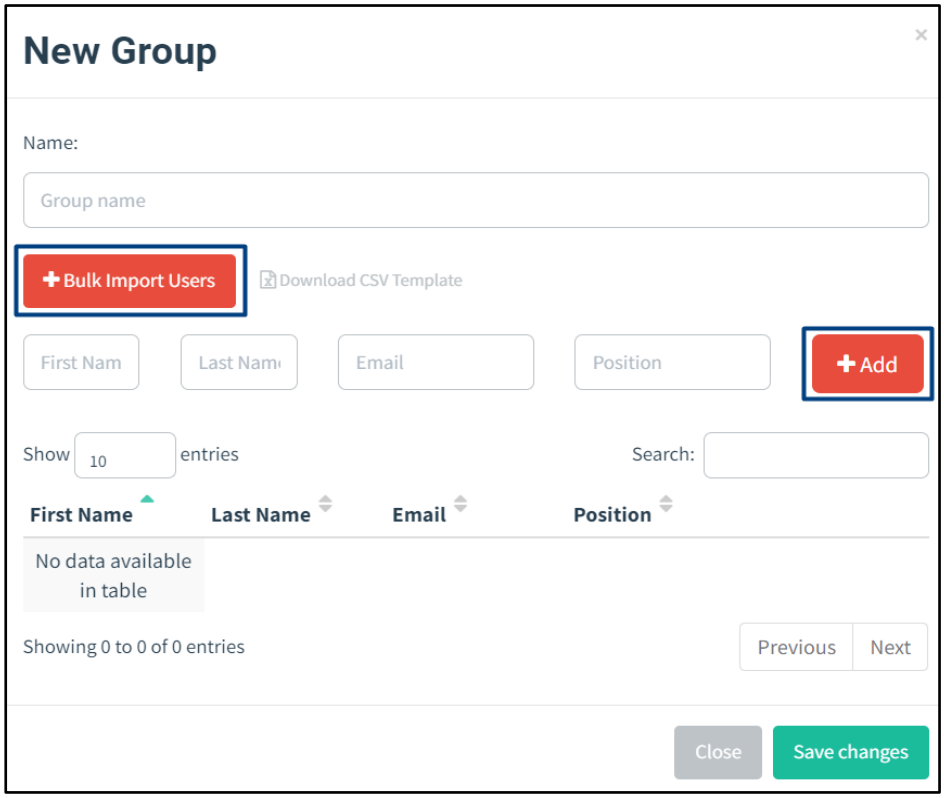


Gráfico 86. Adición de Usuarios

Elaborado Por: Shirley Flores

En este caso, se crearon 3 grupos de Docentes y 14 grupos de Estudiantes los cuales contienen entre 28 a 40 usuarios cada archivo CSV, como lo indica en el Gráfico 87 con el formato correspondiente que se puede descargar desde el Gophish.

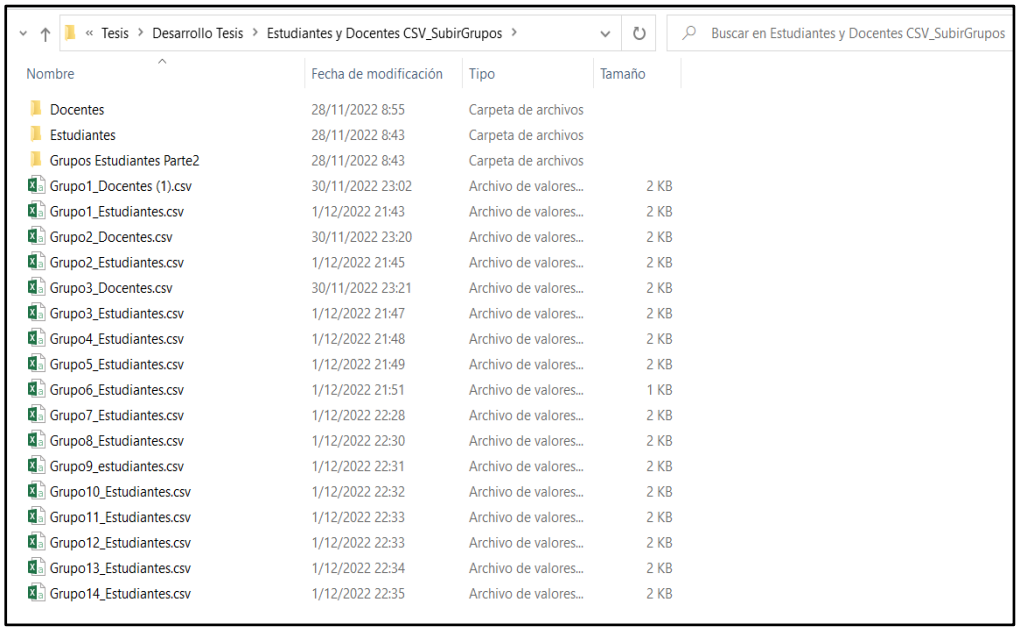
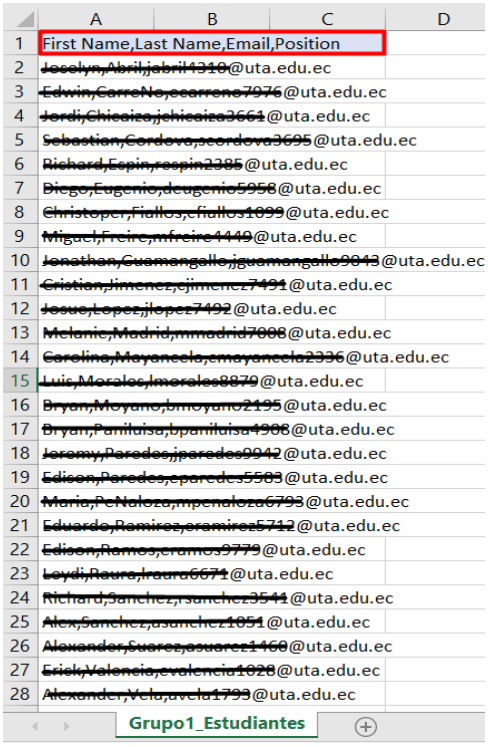


Gráfico 87. Grupos Creados en Archivo CSV

Elaborado Por: Shirley Flores

Cada uno de los archivos creados, cumplen el formato establecido para la carga correcta de los datos, en el caso de que no cumpla, Gophish no permite la carga de datos. En este caso toda la información consta de Nombre, Apellido y el correo electrónico de la víctima, el campo posición es opcional, pero si debe estar especificado en la cabecera. En el Gráfico 88, se muestra un archivo con información lista para cargar masivamente.



	A	B	C	D
1	First Name,Last Name,Email,Position			
2	Jocelyn,Abril,jabril4310@uta.edu.ec			
3	Edwin,CarreNo,ecarreno7976@uta.edu.ec			
4	Jordi,Chicaiza,jchicaiza3661@uta.edu.ec			
5	Sebastian,Cordova,scordova3695@uta.edu.ec			
6	Richard,Espin,respin2385@uta.edu.ec			
7	Diego,Eugenio,deugenio5958@uta.edu.ec			
8	Christoper,Fiallos,cfiallos1899@uta.edu.ec			
9	Miguel,Freire,mfreire4449@uta.edu.ec			
10	Jonathan,Guamangallo,jguamangallo9043@uta.edu.ec			
11	Cristian,Jimenez,cjimenez7491@uta.edu.ec			
12	Josue,Lopez,jlopez7492@uta.edu.ec			
13	Melanie,Madrid,mmadrid7008@uta.edu.ec			
14	Carolina,Mayancela,cmayancela2336@uta.edu.ec			
15	Luis,Morales,lmorales8870@uta.edu.ec			
16	Bryan,Moyano,bmoyano2195@uta.edu.ec			
17	Bryan,Paniluisa,bpaniluisa4906@uta.edu.ec			
18	Jeremy,Paredes,jparedes9942@uta.edu.ec			
19	Edison,Paredes,eparedes5583@uta.edu.ec			
20	Maria,PeNaloza,mpenaloza6793@uta.edu.ec			
21	Eduardo,Ramirez,eramirez5712@uta.edu.ec			
22	Edison,Ramos,eramos9779@uta.edu.ec			
23	Leydi,Raura,lraura6671@uta.edu.ec			
24	Richard,Sanchez,rsanchez3541@uta.edu.ec			
25	Alex,Sanchez,asanchez1051@uta.edu.ec			
26	Alexander,Suarez,asuarez1460@uta.edu.ec			
27	Erick,Valencia,evalencia1828@uta.edu.ec			
28	Alexander,Vela,avela1793@uta.edu.ec			

Grupo1_Estudiantes

Gráfico 88. Formato del Archivo CSV

Elaborado Por: Shirley Flores

En el Panel de Users & Groups, se visualizan todos los grupos que ya se han cargado la información, y se detalla el nombre del grupo, el número de miembros, la fecha de creación, en las acciones disponibles se puede modificar y eliminar los grupos de acuerdo a la necesidad, así como se visualiza en el Gráfico 89.

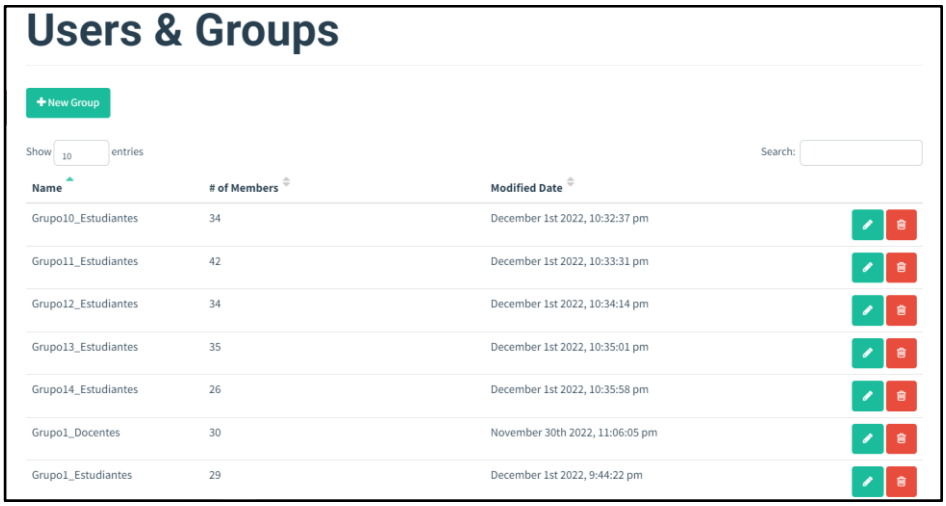


Gráfico 89. Grupos Creados con sus usuarios respectivos

Elaborado Por: Shirley Flores

3.2.8. Ejecución de Pruebas

Para la Ejecución de Pruebas, se creó una campaña en la cual se va a configurar con datos de prueba, y así poder visualizar como recibe el correo la víctima y si existe algún error al momento de ser ejecutado.

3.2.8.1. Creación de Campañas (Campaigns)

Para crear una campaña, se necesita configurar el nombre con el cual se va a identificar, se escoge la plantilla de correo electrónico creada, la página de destino a la cual va a redireccionarse la víctima, la URL del servidor, la fecha en la que se va a realizar el ataque, la misma que se puede dejar programada para que se ejecute automáticamente, se selecciona el perfil del envío y el grupo de usuarios para cual va dirigido la simulación de phishing.

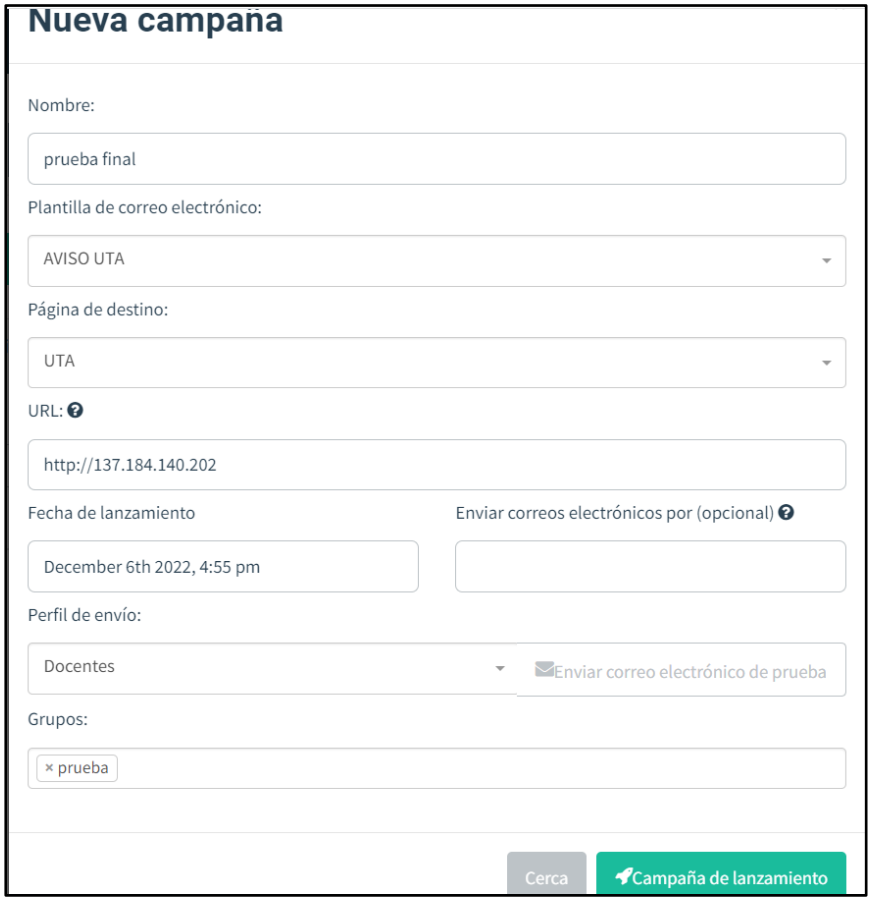


Gráfico 90. Creación de Campaña para la ejecución de Pruebas

Elaborado Por: Shirley Flores

En este caso, la ejecución de pruebas se aplicó para el grupo denominado prueba en el cual se practicó con 3 correos diferentes, 2 correos creados para la ejecución de este proyecto y 1 correo con la colaboración del docente tutor, obteniendo los siguientes resultados como se muestra en el Gráfico 91.

Gráfico 91. Estadísticas Generales de la ejecución de Pruebas

Elaborado Por: Shirley Flores

En las estadísticas generales, se puede visualizar la cantidad de correos enviados, abiertos, correos al que dieron clic en el enlace y la cantidad de usuarios que enviaron datos, así se verifica que no existió ningún error durante la ejecución de las pruebas y que los datos se almacenan correctamente.

Gráfico 92. Detalle de la ejecución de Pruebas

Elaborado Por: Shirley Flores

En el Gráfico 92 muestra el detalle de la información de la víctima que interactuó con la página creada y el estado que se encuentra, es decir a que nivel llegó la campaña de Phishing.

3.2.9. Ejecución Real

3.2.9.1. Ejecución al Grupo de Docentes

Previo a las pruebas de validación realizadas con anterioridad, se ejecutó el ataque al grupo de Docentes de la Facultad de Ciencias Humanas y de la Educación, en el cual se detalla el nombre de la campaña a crear, la plantilla de correo electrónico, la página de destino, la IP del servidor montado para el ataque real, la fecha de ejecución que en este caso fue de inmediato, el perfil y los grupos que corresponden al mismo. En el Gráfico 93 se visualiza la configuración de la campaña a ejecutar.

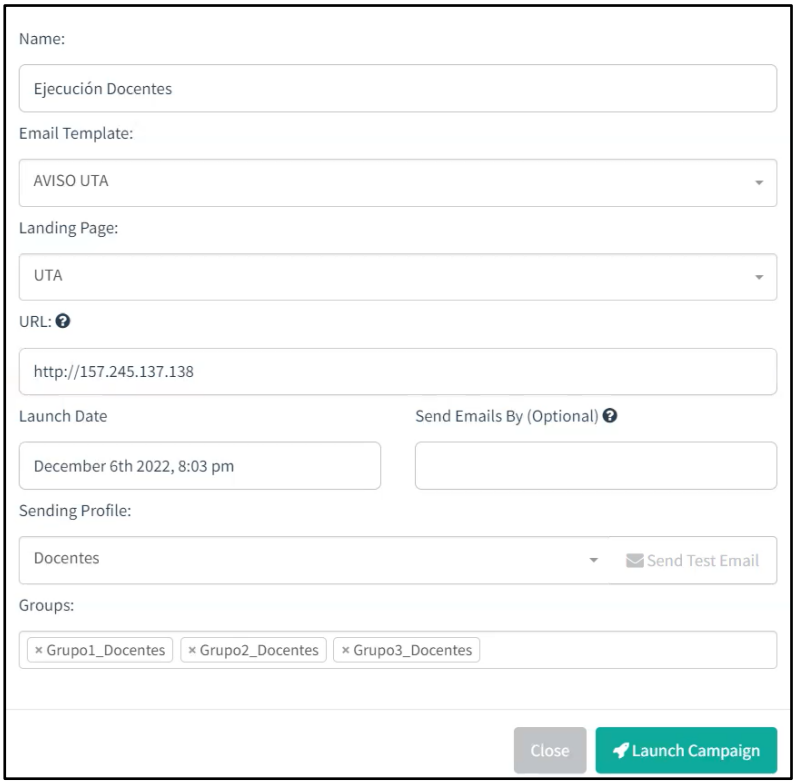


Gráfico 93. Creación de la campaña a Ejecutar de Docentes

Elaborado Por: Shirley Flores

Al momento de enviar la primera campaña, en el servidor que se levantó para esta nueva acción, la página solicita el permiso de ejecución, al ser la primera campaña al ser ejecutada, como se indica en el Gráfico 94.

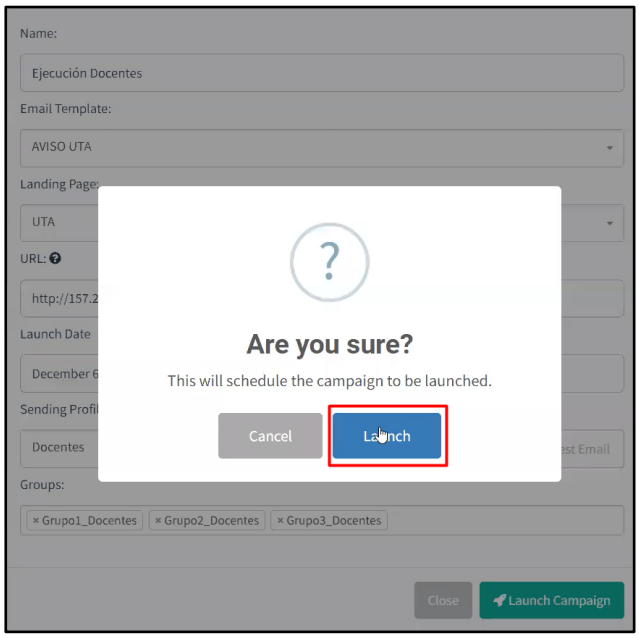


Gráfico 94. Confirmación de ejecución de la campaña a Docentes

Elaborado Por: Shirley Flores

En el Gráfico 95, se visualiza el detalle de la ejecución de la campaña Docentes.

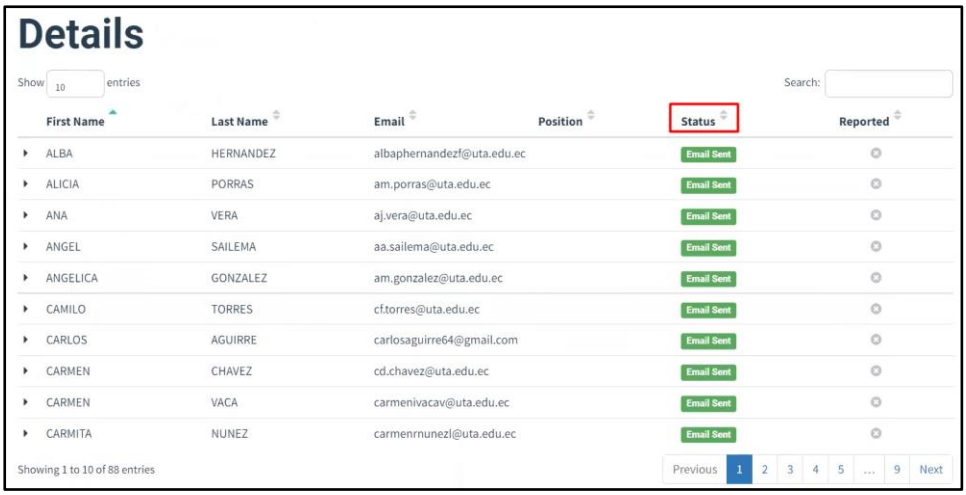


Gráfico 95. Detalles de ejecución de la campaña a Docentes

Elaborado Por: Shirley Flores

3.2.9.2. Ejecución al Grupo de Estudiantes

La ejecución para el grupo de estudiantes se la realizó en dos etapas, debido al límite de 250 correos permitidos diariamente para este tipo de ejecución y así evitar la caída del servidor o que sea declarado como spam.

Ejecución del Primer Grupo de Estudiantes

Para la ejecución de la primera parte de usuarios estudiantes, se tomó en cuenta la clasificación de grupos elaborado inicialmente, para saber con cuantos grupos de estudiantes se va a trabajar. En este caso se configuró de la misma manera que la campaña de docentes, la diferencia es que para este caso el perfil cambia a Estudiantes y los grupos que se ha utilizado para la primera ejecución se ha enumerado desde el grupo 1 al 7.

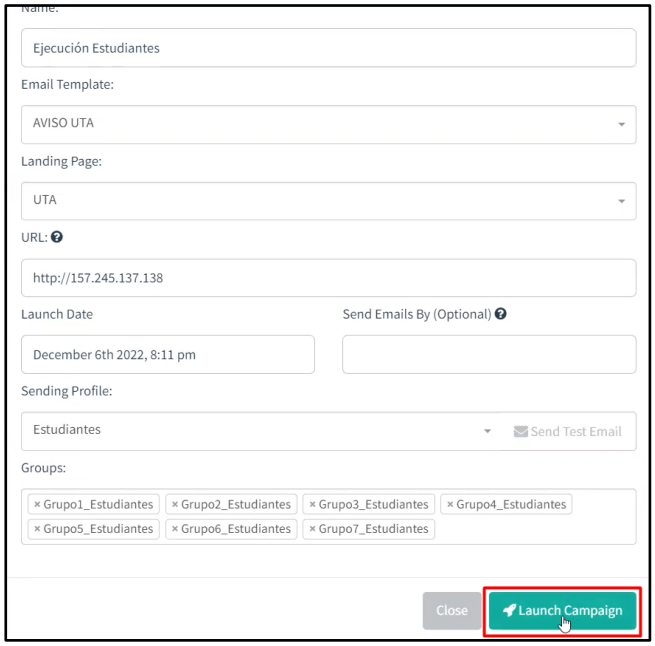


Gráfico 96. Creación de la campaña a Ejecutar de Estudiantes

Elaborado Por: Shirley Flores

Al momento de enviar la ejecución, si no existe ningún problema, el lanzamiento de la campaña fue realizada con éxito. Gophish, muestra un mensaje de confirmación y comienza a visualizarse las estadísticas generales y en detalle en el Panel de inicio.

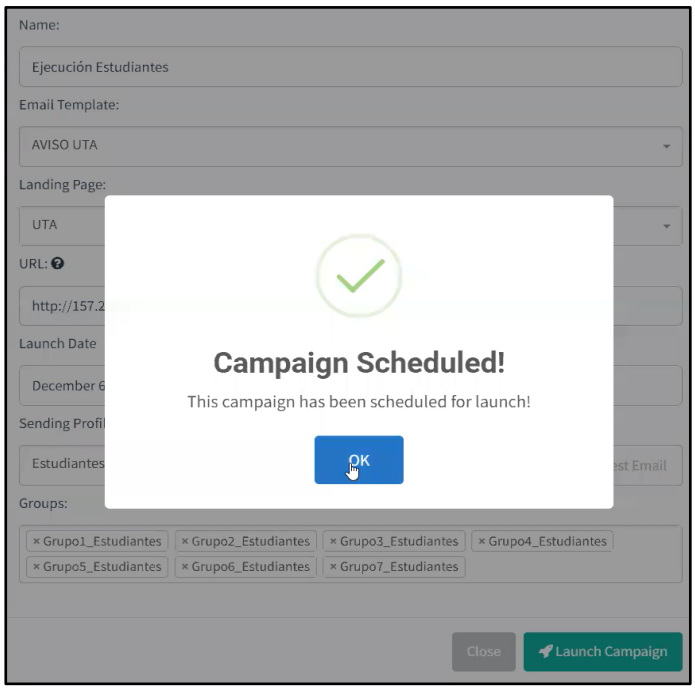


Gráfico 97. Confirmación de campaña ejecutada correctamente

Elaborado Por: Shirley Flores

Una vez ejecutada la campaña, en el panel de Gophish, se puede visualizar el progreso de los correos enviados, el estado muestra si el correo fue enviado satisfactoriamente, si se está enviando o si existió algún error con la entrega del correo, así como se visualiza en el Gráfico 98. En este caso si el correo no fue enviado, lo más probable es que ya no exista el correo al que fue enviado y por eso se emite el error.

Gráfico 98. Detalle del progreso de correos del Panel de Gophish

Elaborado Por: Shirley Flores

Una vez que la ejecución se la haya realizado el 100%, se comienza a visualizar en el Panel de Gophish el estado de cada uno de los correos que fueron enviados, para llevar un seguimiento oportuno a cada una de las acciones que se van realizando en la campaña de Phishing, como lo indica en el Gráfico 99.

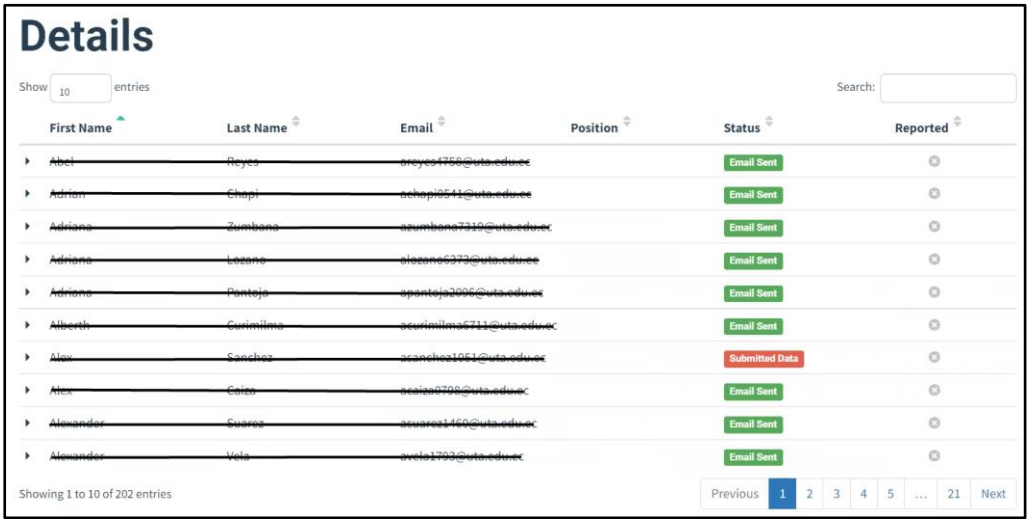


Gráfico 99. Detalle de los correos enviados y receptados

Elaborado Por: Shirley Flores

En el Panel de Campañas, se puede visualizar la información de todas las campañas que se encuentran activas en ese momento, como el nombre, la fecha de creación, el estado que se encuentra la campaña es decir si está en progreso o ya se encuentra finalizada, también se puede realizar ciertas acciones como la visualización de resultados, duplicar una campaña y eliminarla, como se puede visualizar en el Gráfico 100.

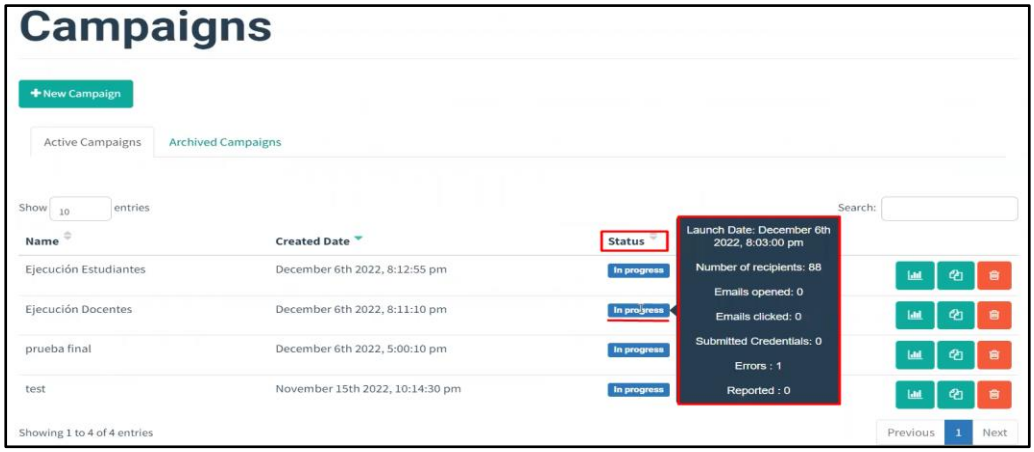


Gráfico 100. Estadísticas Generales de las Campañas realizadas
Elaborado Por: Shirley Flores

Ejecución del Segundo Grupo de Estudiantes

Para la ejecución de la segunda parte de usuarios estudiantes, se utilizó los grupos creados enumerados desde el grupo 8 al 14 y se ejecuta el mismo proceso que se aplicó para el lanzamiento de la primera campaña.

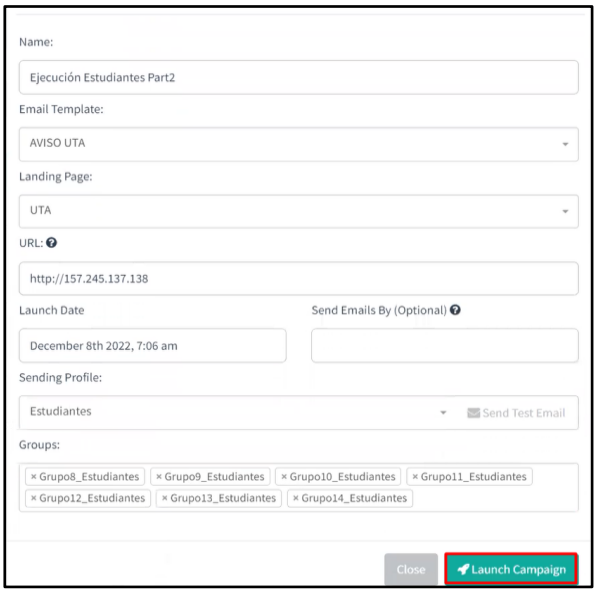


Gráfico 101. Creación de la campaña 2 a Ejecutar de Estudiantes
Elaborado Por: Shirley Flores

Al momento de enviar la ejecución, la plataforma emite un mensaje de aceptación de envío de una nueva campaña, se acepta y se ejecuta el segundo ataque simulado y empieza a enviar los correos electrónicos a los destinatarios.

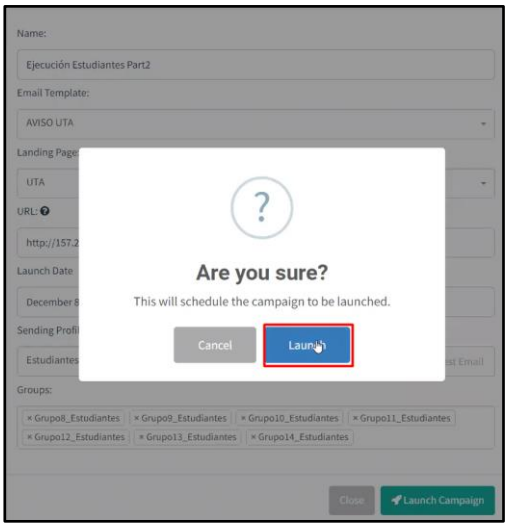


Gráfico 102. Notificación de envío de campaña

Elaborado Por: Shirley Flores

Al aceptar la ejecución, si no existe ningún problema, el lanzamiento de la campaña fue realizada con éxito. Gophish, muestra un mensaje de confirmación en este caso de la segunda campaña creada y comienza a visualizarse las estadísticas generales y en detalle en el Panel de inicio.

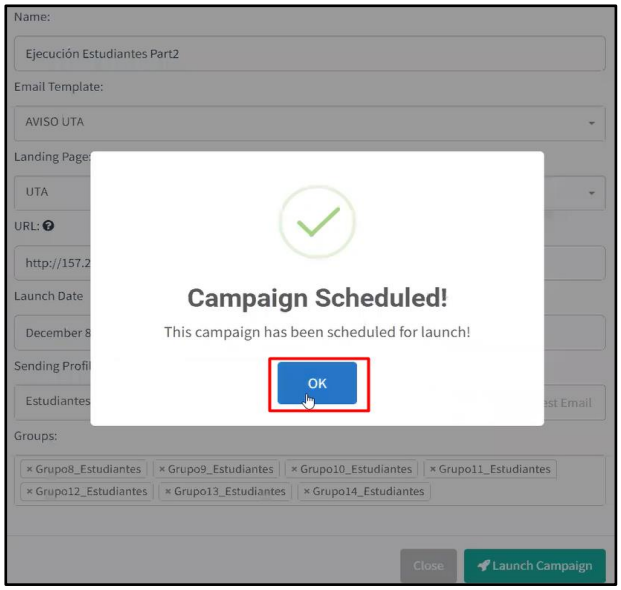


Gráfico 103. Detalle del progreso de correos del Panel de Gophish campaña 2

Elaborado Por: Shirley Flores

En el transcurso de la ejecución, se puede visualizar información de los usuarios que fueron víctimas en la campaña de phishing, y el estado de los correos que se encuentra en ese momento, en la opción de Status como lo indica en el Gráfico 104.

Gráfico 104. Detalle del progreso de correos del Panel de Gophish campaña 2

Elaborado Por: Shirley Flores

Para verificar que la conexión entre el servidor de correo electrónico y el servidor que aloja la página de gophish, se encuentra en funcionalidad, se recomienda recargar la misma y visualizar los datos que se van actualizando, según las acciones que el usuario realice con la página fraudulenta.

Gráfico 105. Detalle de los correos enviados y receptados de la segunda campaña

Elaborado Por: Shirley Flores

3.2.10. Ejecución de Ataque de Phishing con simulación de Página Facebook

Se realizó varias ejecuciones con el objetivo de llegar a la mayor cantidad de víctimas, tal cual se lo realiza en una campaña real. Para lo cual se analizó que la mayor cantidad de usuarios de Facebook, no tienen enlazada la cuenta de esta red social con un correo institucional, sino con un correo personal. Para esta ejecución se utilizó los correos personales de los estudiantes, que fueron entregados mediante la técnica de ingeniería social Pretexting en la cual no se validó la información y fue entregada una base con información confidencial y personal.

Para realizar esta ejecución se debe levantar un nuevo servidor, ya que, para este tipo de ataques de Ingeniería Social, no es recomendable tener mucho tiempo levantado el servidor, mientras más tiempo se conserva el servidor, menos será la confiabilidad de la página, debido a que la seguridad de los servidores de correo lo detectan y emiten mensajes de alerta.

3.2.10.1. Creación de un nuevo Servidor

Para crear un nuevo servidor, se accede a la página de DigitalOcean, en el proyecto denominado UTA, se da clic en la opción de Create y se despliegan las opciones a crear.

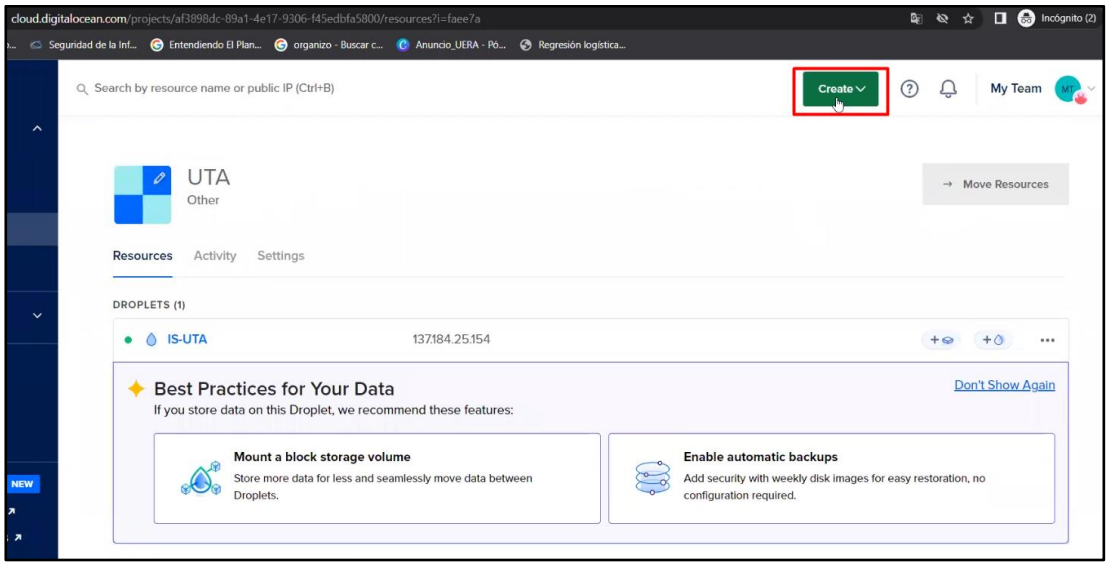


Gráfico 106. Menú del Proyecto UTA en DigitalOcean

Elaborado Por: Shirley Flores

Se necesita crear un Droplet con todas las características de un servidor, para ello se selecciona en el menú desplegable como se muestra a continuación en el Gráfico 107.

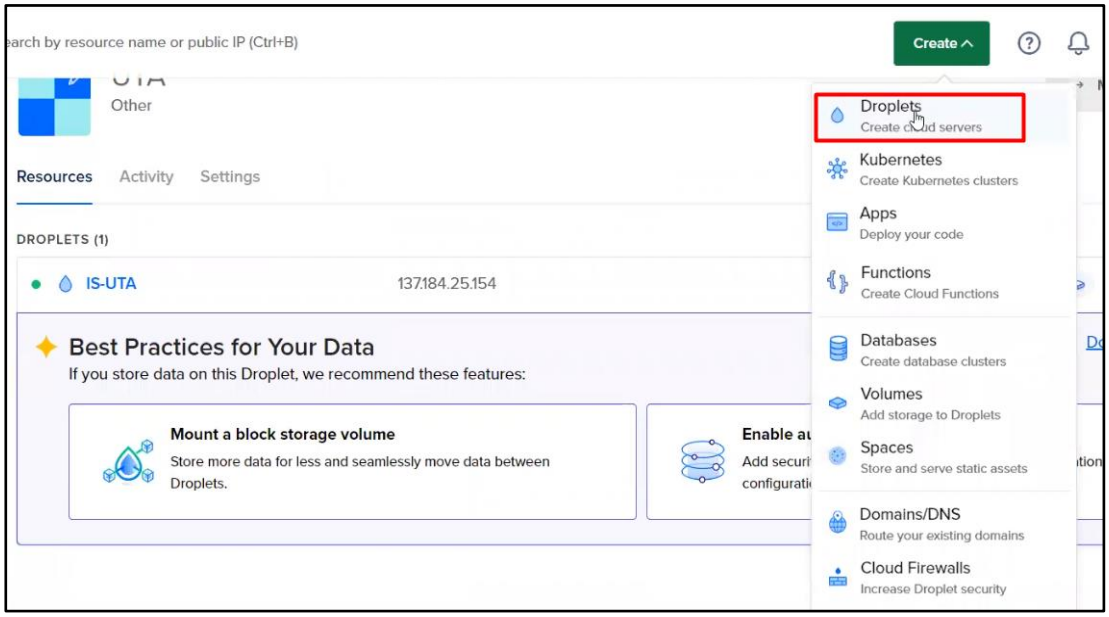


Gráfico 107. Opciones de Creación del Proyecto UTA en DigitalOcean

Elaborado Por: Shirley Flores

Para iniciar con la creación del nuevo servidor, se selecciona la región de New York, y se actualiza automáticamente el Datacenter en el cual será ejecutado.

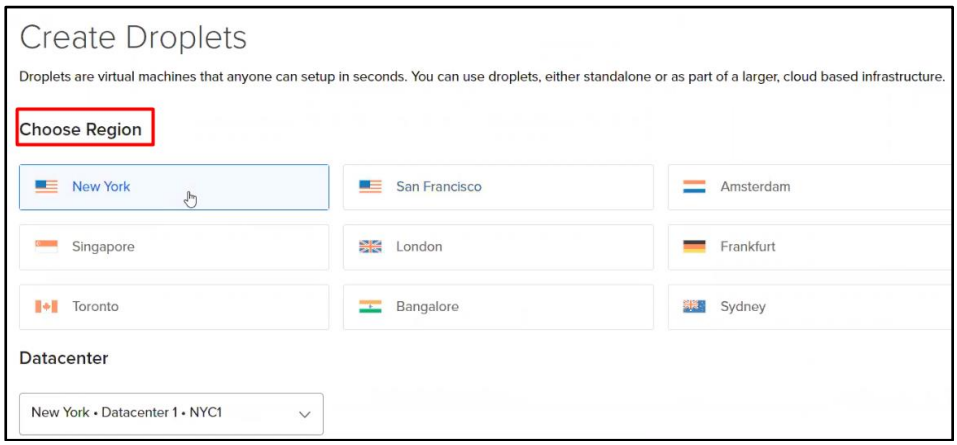


Gráfico 108. Opciones de Región Geográfica y Data Center

Elaborado Por: Shirley Flores

Una vez configurado el servidor, con las mismas características que poseía el servidor inicial, se procede a confirmar la creación del Droplet con el nombre IS-UTA, con el costo de $4.00 por mes, lo cual depende de las características que se requiera para la ejecución, en este caso el requerimiento es el mínimo.

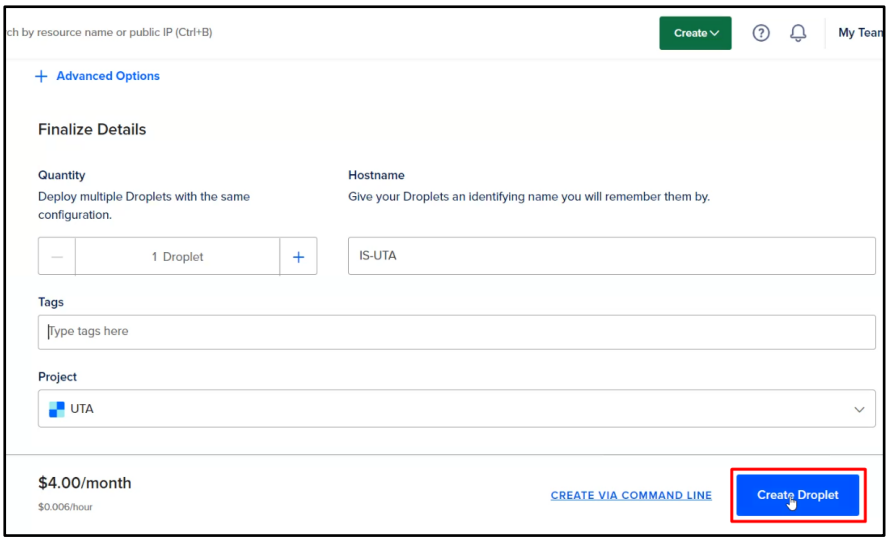


Gráfico 109. Creación del Servidor

Elaborado Por: Shirley Flores

Se puede visualizar el progreso de la creación del servidor como lo indica en el Gráfico 110.

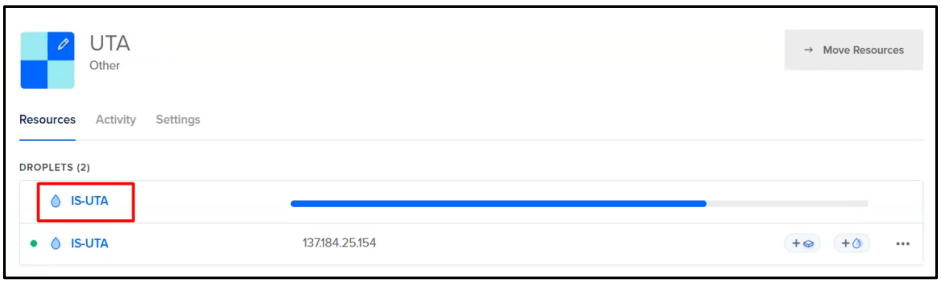


Gráfico 110. Progreso de la Creación del Servidor

Elaborado Por: Shirley Flores

Una vez cargado el Droplet al proyecto UTA, se puede visualizar la IP generada, para la utilización del nuevo servidor, las características y las opciones disponibles para el mismo. Para iniciar con la configuración se puede acceder desde la consola de Acceso como lo indica en el Gráfico 111.

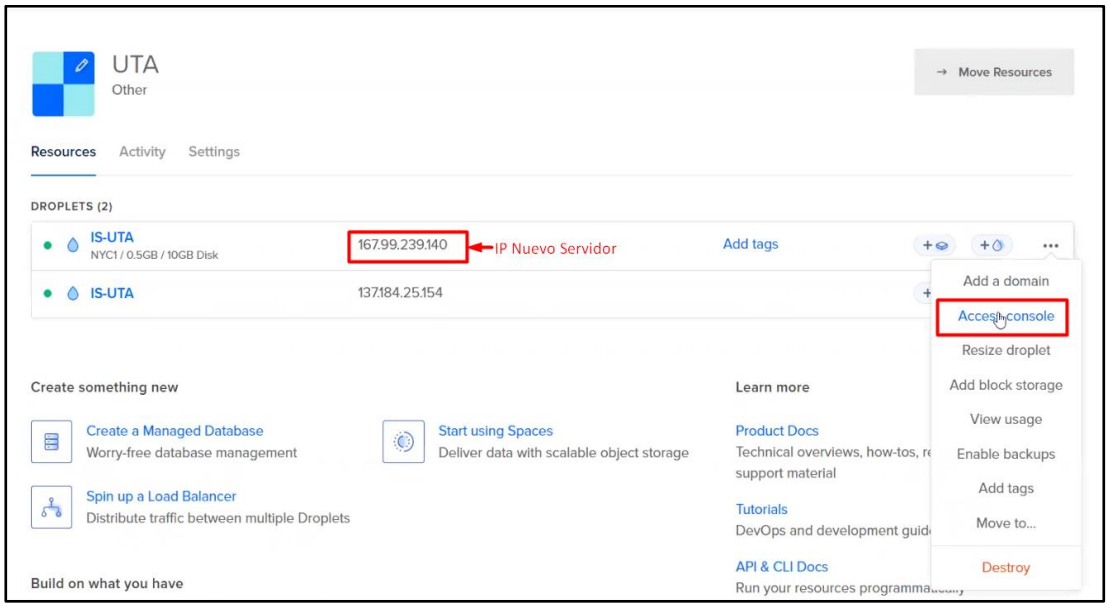


Gráfico 111. Recursos Activos en el proyecto UTA

Elaborado Por: Shirley Flores

Para abrir el terminal de acceso, desde el navegador, se ingresa como usuario root y se ejecuta en la opción Launch Droplet Console.

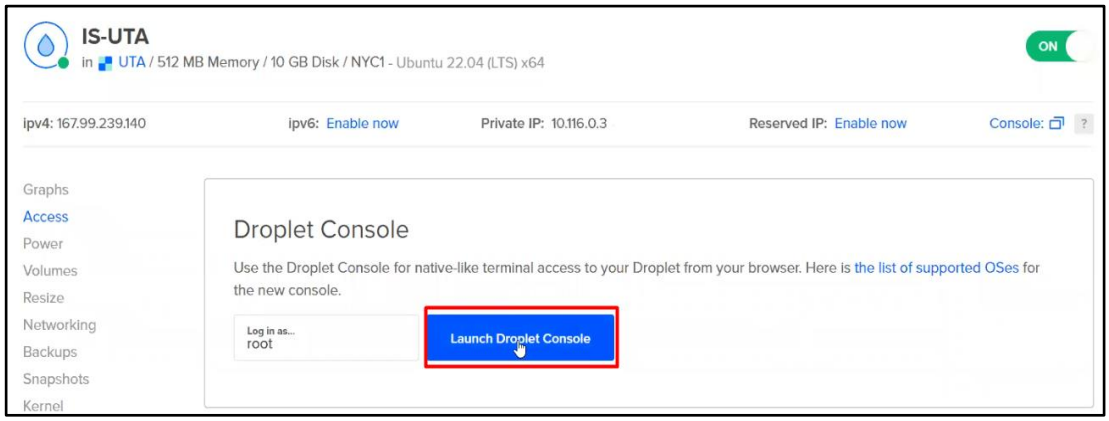


Gráfico 112. Ejecutar la consola de Acceso del servidor

Elaborado Por: Shirley Flores

3.2.10.2. Respaldo del Servidor

Antes de inhabilitar el servidor, se procede a sacar un respaldo al servidor inicial, y esta información se subirá en el nuevo servidor, para evitar la pérdida de información, y garantizar que se genere un historial de campañas ejecutadas en la página de Gophish.

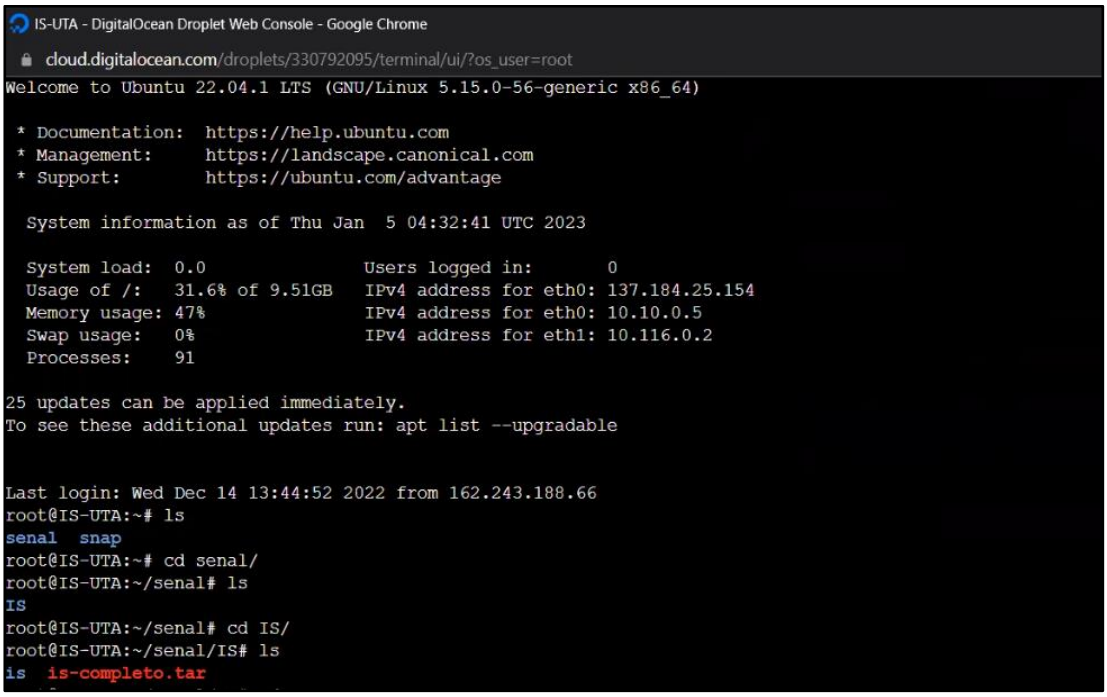


Gráfico 113. Consola de Acceso del servidor

Elaborado Por: Shirley Flores

Para instalar el paquete Net-tools en el servidor de Ubuntu, se ejecuta el siguiente comando: apt install net-tools, con el cual se podrá visualizar la configuración de red, estadísticas, conexiones entre otros, como se indica en el Gráfico 114.

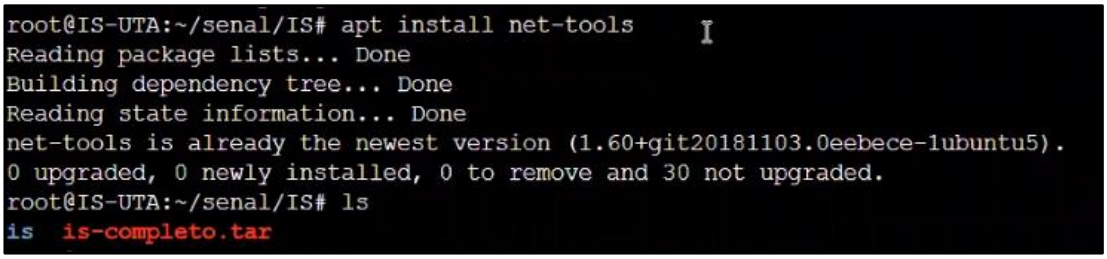


Gráfico 114. Instalación de Paquetes para la configuración del servidor

Elaborado Por: Shirley Flores

Se enlista las carpetas que existen en el servidor antiguo, en el cual contiene la configuración de la página de gophish y la información almacenada en el servidor. Se crea un archivo comprimido con el comando tar -cvf el nombre del archivo a crear y la carpeta que se necesita que sea comprimida, tal cual lo indica en el Gráfico 115.

```
root@IS-UTA:~# ls
senal  snap
root@IS-UTA:~# tar -cvf senal.tar senal/
```

Gráfico 115. Comando para la Creación de un archivo comprimido

Elaborado Por: Shirley Flores

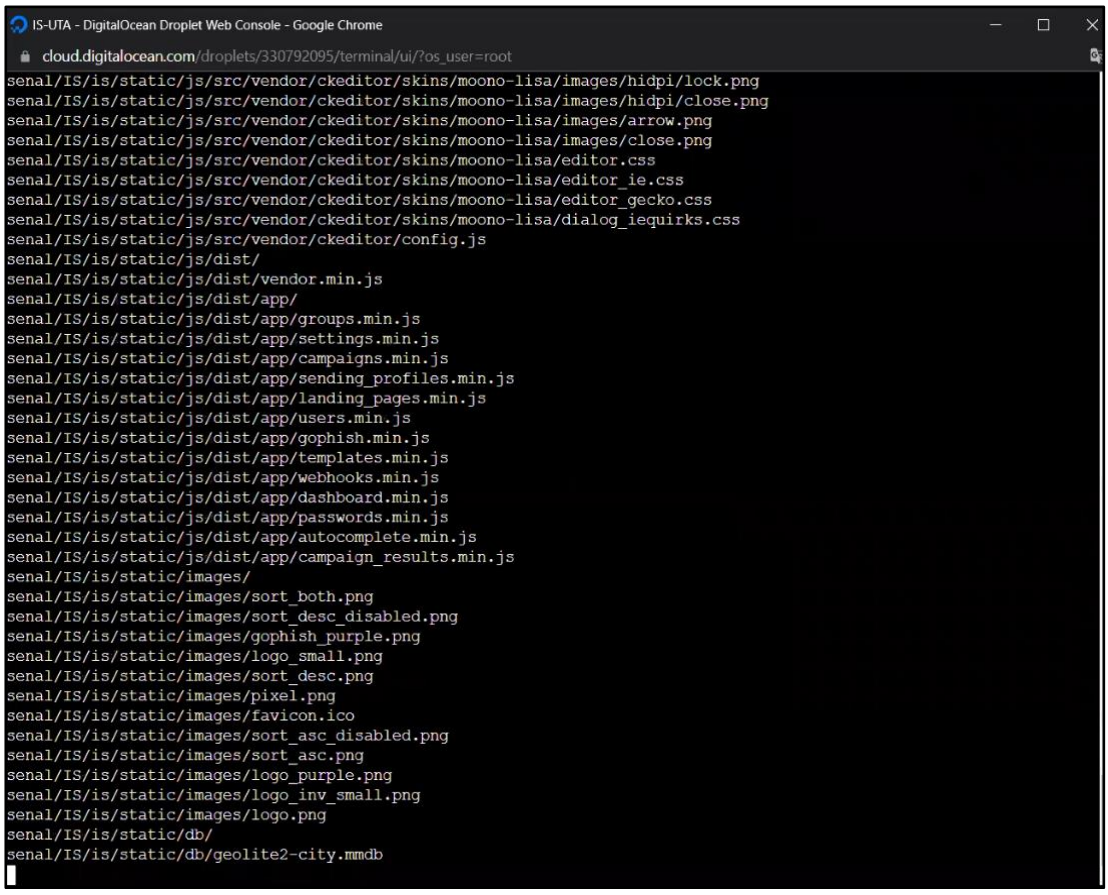


Gráfico 116. Ejecución del Comando en Ubuntu

Elaborado Por: Shirley Flores

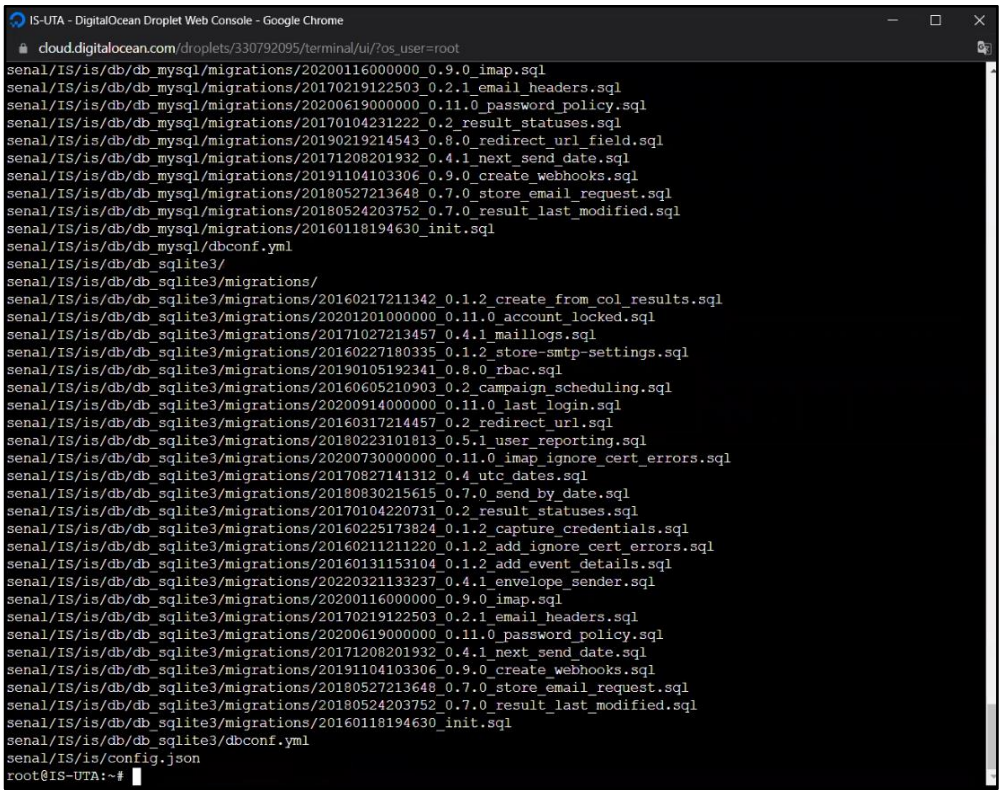


Gráfico 117. Finalización de la ejecución del Comando en Ubuntu

Elaborado Por: Shirley Flores

Se comprueba que el archivo .tar ya se encuentra creado en el servidor y se invoca el servidor http. server directamente utilizando el modificador -m con un argumento, que es el número de puerto 8181.

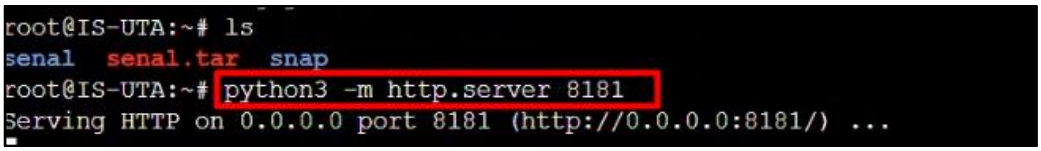


Gráfico 118. Ejecución del servidor http. server

Elaborado Por: Shirley Flores

En un navegador web, se accede a la IP del servidor que se está respaldando que en este caso es la 137.184.25.154 con el puerto 8181. En esa dirección aparece una lista de archivos, se coloca encima del archivo .tar creado, clic derecho y se copia la dirección de enlace, en este caso en un bloc de notas.

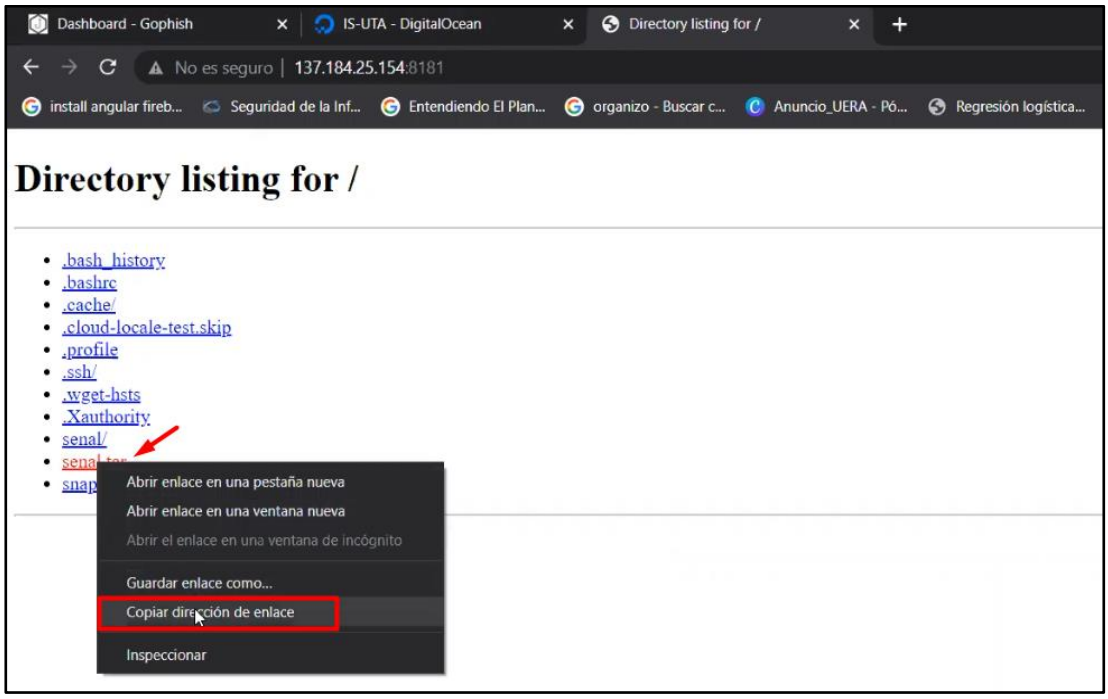


Gráfico 119. Lista de Archivos del servidor

Elaborado Por: Shirley Flores

3.2.10.3. Cargar Respaldo al nuevo servidor creado

Se ejecuta la consola de acceso del nuevo servidor, al inicio se puede visualizar información del sistema y se comprueba el número de IP generado al momento de la creación. A continuación, se crea una carpeta denominada senal, con el comando mkdir en la cual se va a descomprimir el archivo del respaldo del otro servidor.

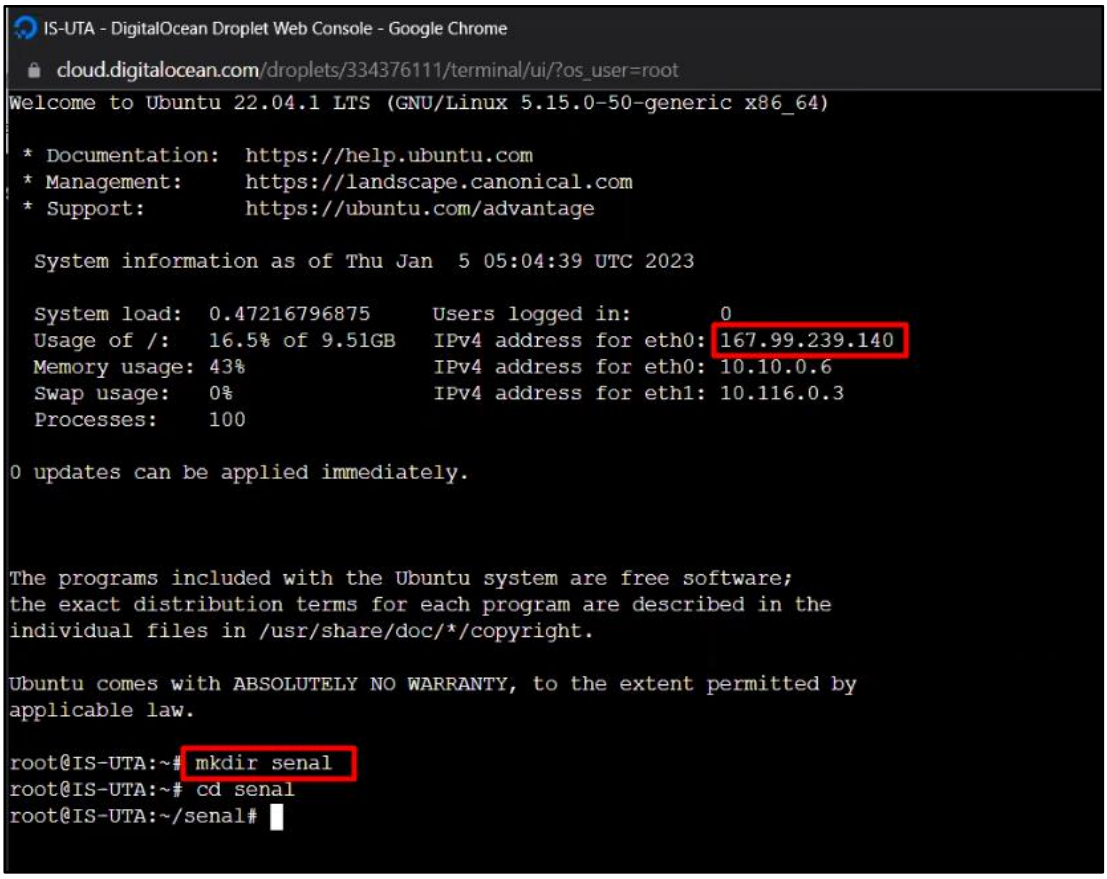


Gráfico 120. Creación de la carpeta senal

Elaborado Por: Shirley Flores

Se accede a la carpeta creada y con el comando wget se descarga el archivo .tar, copiando el enlace de la dirección de respaldo que se guardó en un bloc de notas anteriormente.

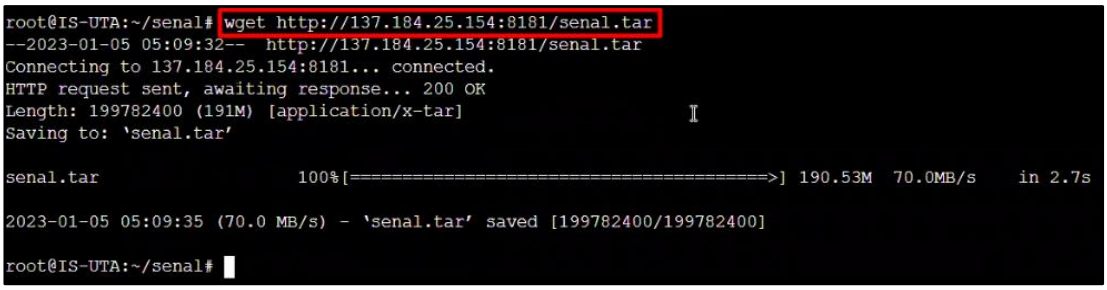


Gráfico 121. Descarga de Archivo en la carpeta creada senal

Elaborado Por: Shirley Flores

Una vez descargado el archivo, se procede a descomprimir con el comando tar -xvf y el nombre del archivo, como lo muestra en el siguiente Gráfico.

Gráfico 122. Descomprimir archivo descargado en la carpeta senal

Elaborado Por: Shirley Flores

Ya descargado el respaldo en la carpeta senal, se procede con la instalación del paquete net-tools para visualizar la configuración de red.

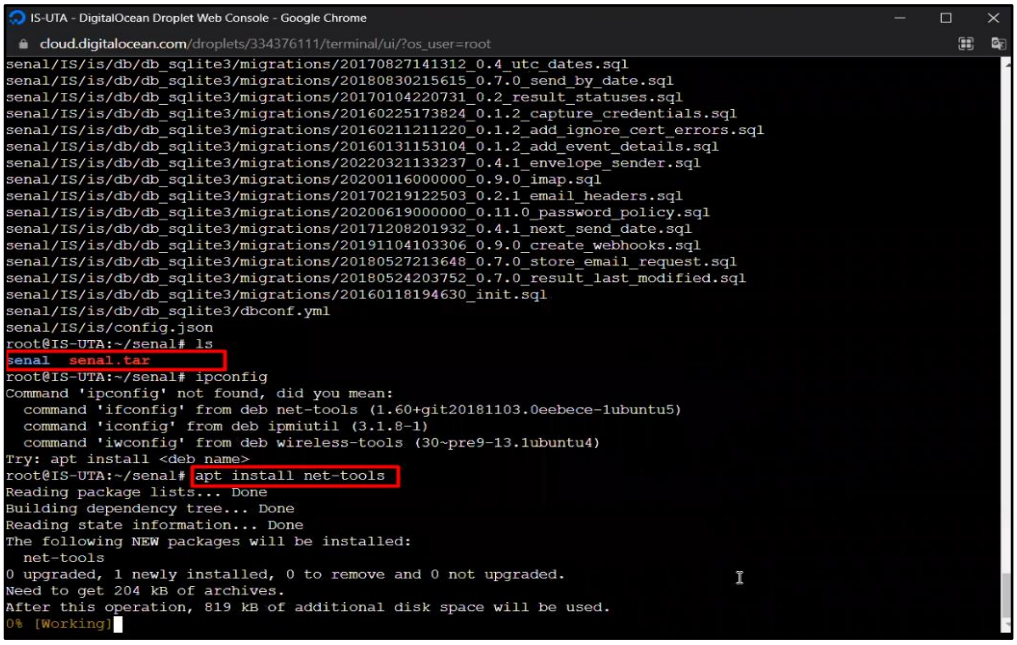


Gráfico 123. Descomprimir archivo descargado en la carpeta senal

Elaborado Por: Shirley Flores

Para verificar que el servidor este funcionando correctamente, se visualiza la IP del servidor asignada para el desarrollo de la ejecución.

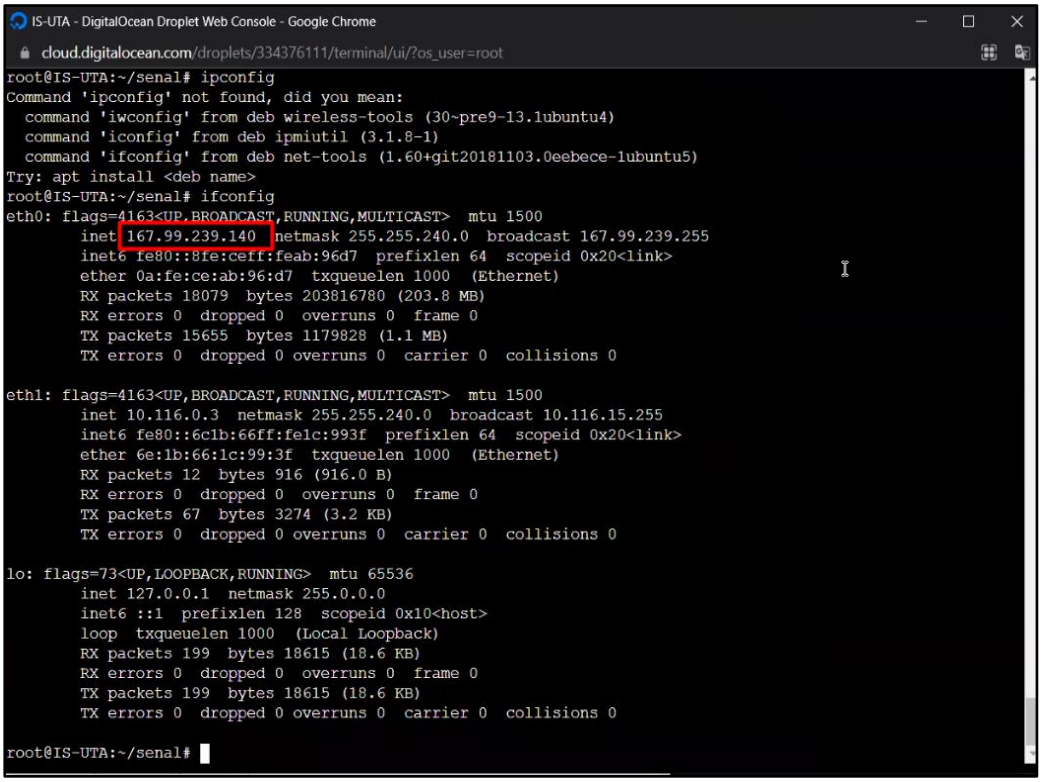


Gráfico 124. Visualización de la Red con el comando ifconfig

Elaborado Por: Shirley Flores

En el servidor inicial, se utiliza el comando ./gophish para la ejecución y se pone en segundo plano con el comando disown.

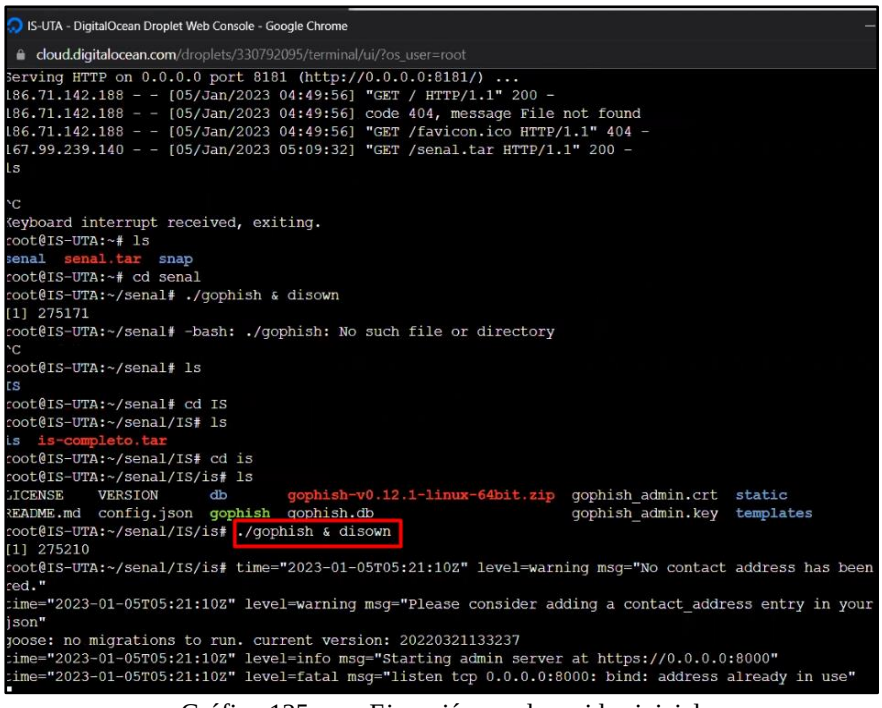


Gráfico 125. Ejecución en el servidor inicial

Elaborado Por: Shirley Flores

De igual manera, en el nuevo servidor se ingresa el comando ejecutado en el servidor inicial y se levanta el servicio de la página de gophish con su respaldo en el servidor actual.

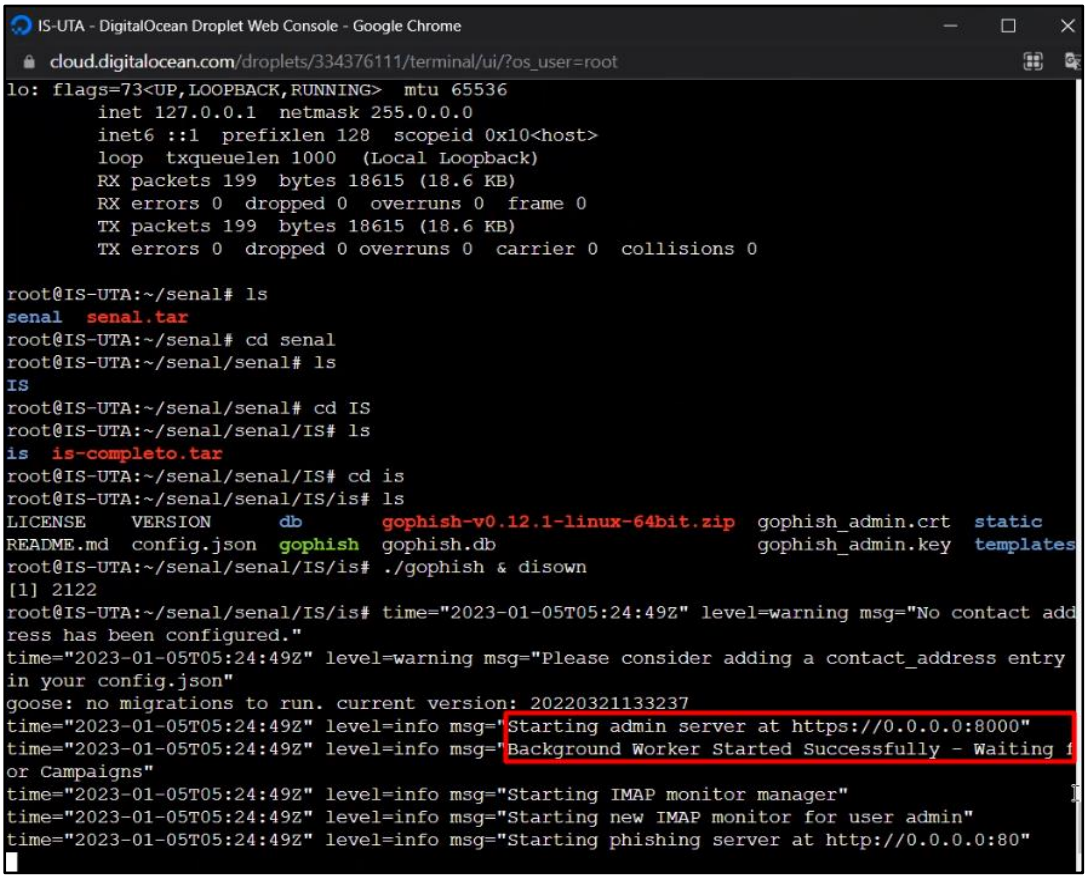


Gráfico 126. Ejecución en el servidor actual y levantamiento de servicio

Elaborado Por: Shirley Flores

Para comprobar la funcionalidad, se abre un navegador en el cual se detalla la IP del servidor creado, en este caso se ingresa a la dirección https://167.99.239.140:8000, y se visualiza la página de inicio de sesión de Gophish, en este caso, se ingresa con las credenciales correspondientes y se da clic en iniciar sesión.

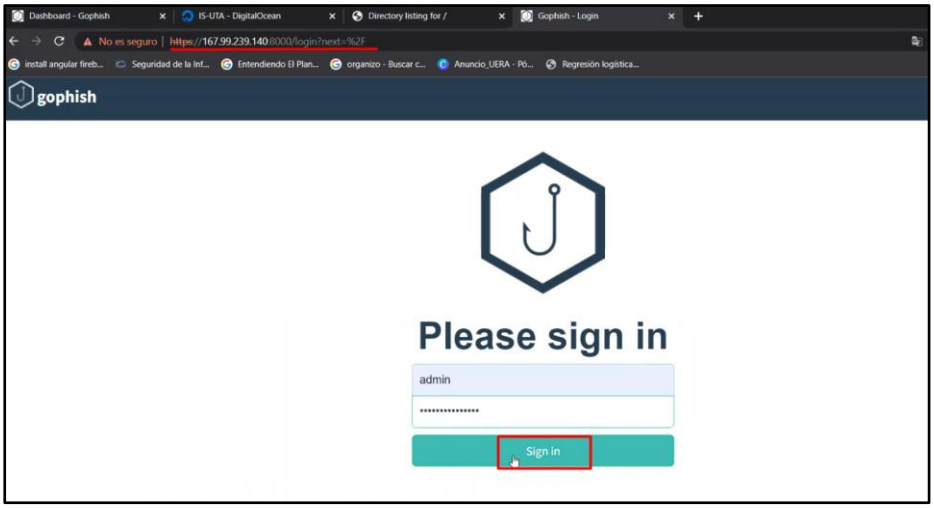


Gráfico 127. Inicio de sesión de Gophish

Elaborado Por: Shirley Flores

Al ingresar, se muestra el respaldo de la información del servidor inicial, en el nuevo servidor y se puede realizar las diferentes acciones con los diferentes módulos de la página de gophish, en este caso se comprueba la funcionalidad del servidor levantado.

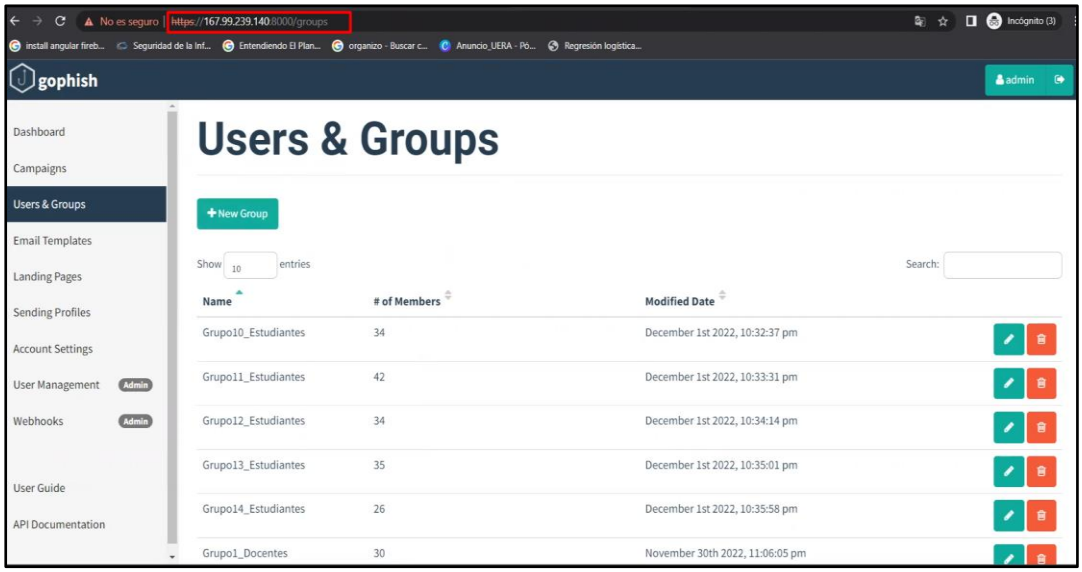


Gráfico 128. Funcionalidad de la Página de Gophish

Elaborado Por: Shirley Flores

3.2.10.4. Ataque de Phishing con la simulación de la página de la Red Social Facebook

Para el lanzamiento de esta ejecución, se realizó en dos grupos, debido a que esta ejecución va dirigido a correos personales, de dominio gmail, yahoo, hotmail, etc. Esto

implica que la seguridad de los correos, detectan más rápido que se trata de un ataque de phishing y alertan al usuario de este caso con un mensaje de alerta o el correo es enviado directamente a spam.

3.2.10.5. Configuración de Gophish

Creación de Correos

Para ello se creó dos cuentas de correo electrónico en Outlook, para realizar la configuración en él envió de perfiles, en este caso se va a trabajar con los siguientes correos:

- es.la-facebook@hotmail.com
- es.seguridad-facebook@outlook.com

Users & Groups

Para la creación del grupo, se necesita subir la lista de usuarios con los correos electrónicos, para este caso se elaboró un archivo .csv con el formato correspondiente para la importación de usuarios directamente desde la página de gophish, así como lo indica en el Gráfico 129.

	A	B	C	D	E
1	First Name,Last Name,Email,Position				
2	[redacted]				
3	[redacted]				
4	[redacted]				
5	[redacted]				
6	[redacted]				
7	[redacted]				
8	[redacted]				
9	[redacted]				
10	[redacted]_@hotmail.com				
11	[redacted]@gmail.com				
12	[redacted]@hotmail.com				
13	[redacted]@yahoo.com				
14	[redacted]@gmail.com				
15	[redacted]@gmail.com				
16	[redacted]@hotmail.com				
17	[redacted]@gmail.com				
18	[redacted]@gmail.com				
19	[redacted]@gmail.com				
20	[redacted]@gmail.com				
21	[redacted]@gmail.com				
22	[redacted]@gmail.com				
23	[redacted]@gmail.com				
24	[redacted]@gmail.com				
25	[redacted]@gmail.com				
26	[redacted]@hotmail.com				

Gráfico 129. Formato del Archivo CSV de correos personales

Elaborado Por: Shirley Flores

Para configurar el grupo, se asigna un nombre para identificación entre los demás grupos existentes y se importa el archivo en formato .CSV creado, si no existe ningún problema la lista de víctimas es cargada con éxito a la página.

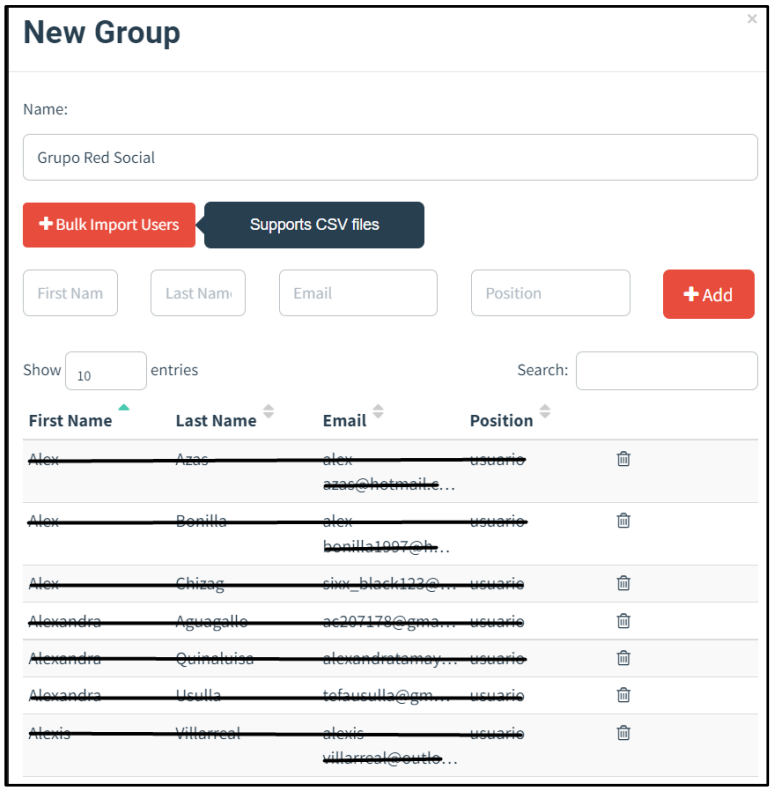


Gráfico 130. Formato del Archivo CSV de correos personales

Elaborado Por: Shirley Flores

Email Templates – Ejecución Facebook

Se creo una nueva plantilla de correo, para esta ejecución se configuro con el nombre de Advertencia Facebook, y el asunto como Advertencia, para el cuerpo del texto del correo electrónico se implementó un código en HTML, el resultado del nuevo email template se lo visualiza en el Gráfico 131.

Notificación para {{.FirstName}} {{.LastName}},

Alguien más está intentando acceder a tu cuenta de Facebook. Un dispositivo desconocido intento acceder a tu cuenta recientemente. Para mejorar la seguridad de tu cuenta de Facebook, puedes elegir recibir una alerta cuando alguien intente iniciar sesión desde un dispositivo o navegador web que no reconozcamos .

Estas alertas te indicarán que dispositivo intentó iniciar sesión y su ubicación.

Inicia Sesión para activar estas alertas.

Activación de Alertas

Este mensaje se ha enviado a {{.Email}}. Si no deseas recibir estos mensajes de correo electrónico de Meta en el futuro, cancela la suscripción. Meta Platforms, Inc., Attention: Community Support, 1 Facebook Way, Menlo Park, CA 94025 A fin de proteger tu cuenta, no reenvíes este mensaje de correo electrónico. Más información

{{.Tracker}}

Gráfico 131. Resultado de la Plantilla de Correo Electrónico

Elaborado Por: Shirley Flores

3.2.10.6. Creación de Página de Destino

Para esta ejecución se utilizó el recurso de importación de gophish, con el cual facilita la creación de páginas, mediante una réplica exactamente a la original, en este caso se ingresó la url de la página de Facebook, y esta herramienta facilitó la importación y creación de una página idéntica para la ejecución de la simulación de ataque. En la configuración se activó la captura de datos y credenciales mediante la página fraudulenta y una vez que el usuario interactúe con el enlace, se redirija a la página oficial de Facebook que es https://es-la.facebook.com/.

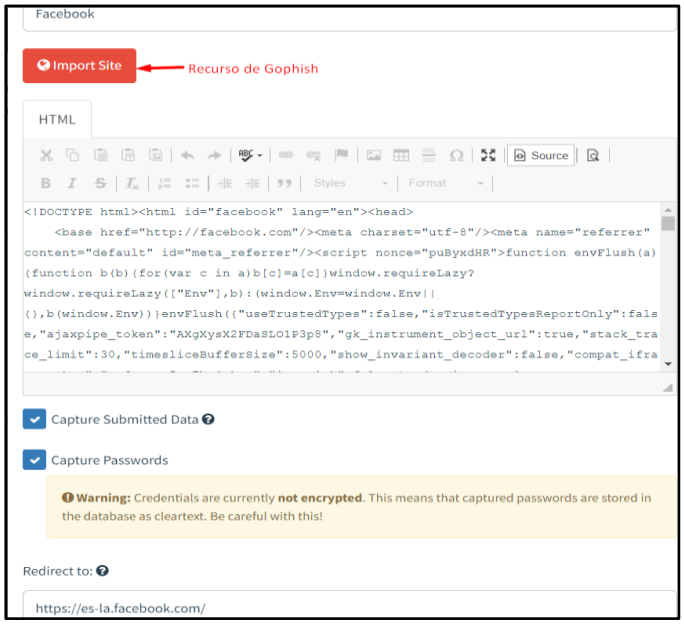


Gráfico 132. Configuración de la Página de destino Facebook

Elaborado Por: Shirley Flores

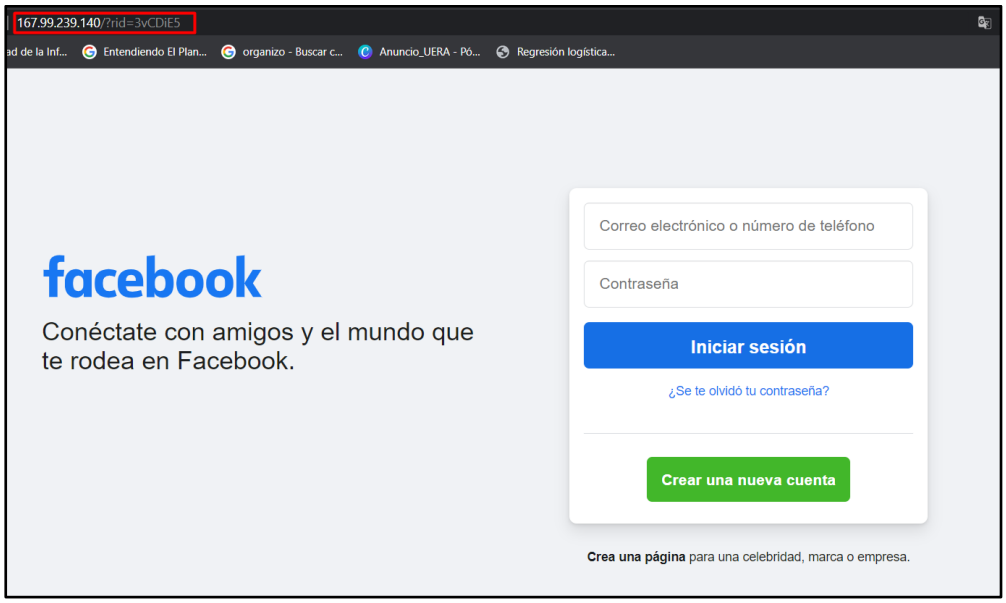


Gráfico 133. Página de Facebook replicada con Gophish

Elaborado Por: Shirley Flores

3.2.10.7. Envío de Perfiles

Se crearon dos perfiles distintos, para los diferentes grupos de ejecución y las cuentas de correo electrónico creados. Se realizo pruebas de conexión con cada uno de los perfiles, los cuales fueron satisfactorios y se procedió a la creación de las campañas.

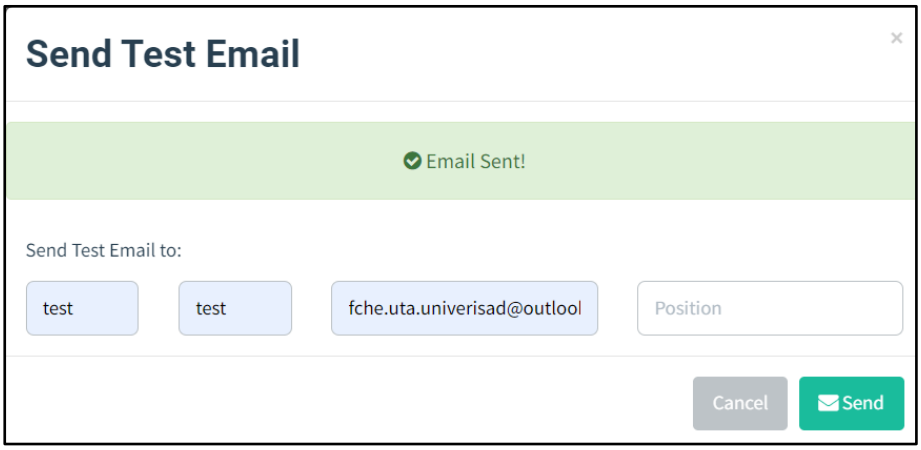


Gráfico 134. Pruebas de conexión con un correo electrónico

Elaborado Por: Shirley Flores

En la bandeja de entrada del correo que se utilizó para las pruebas de conexión, aparece el correo de prueba que se envió de la plataforma y se valida que el servicio está funcionando.

Gráfico 135. Pruebas de conexión con un correo electrónico
Elaborado Por: Shirley Flores

3.2.10.8. Creación de la Campaña para Facebook

Para la creación de la campaña se configura la información adecuada para la ejecución del ataque, esta campaña va dirigida a 238 correos personales que se encuentran configurados en el Grupo Red Social.

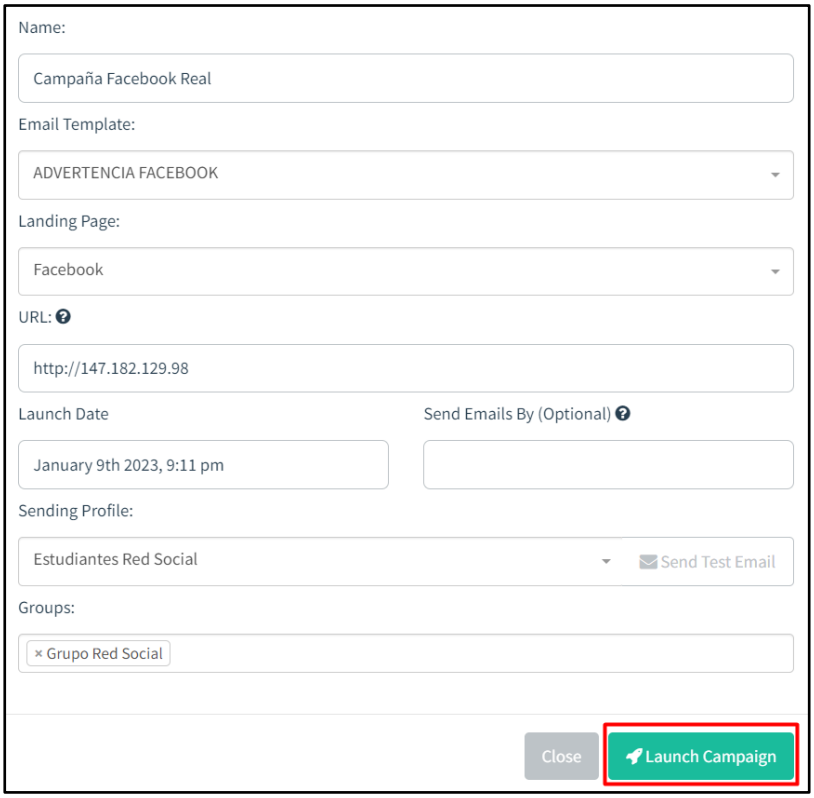


Gráfico 136. Lanzamiento de la Campaña de la Red Social

Elaborado Por: Shirley Flores

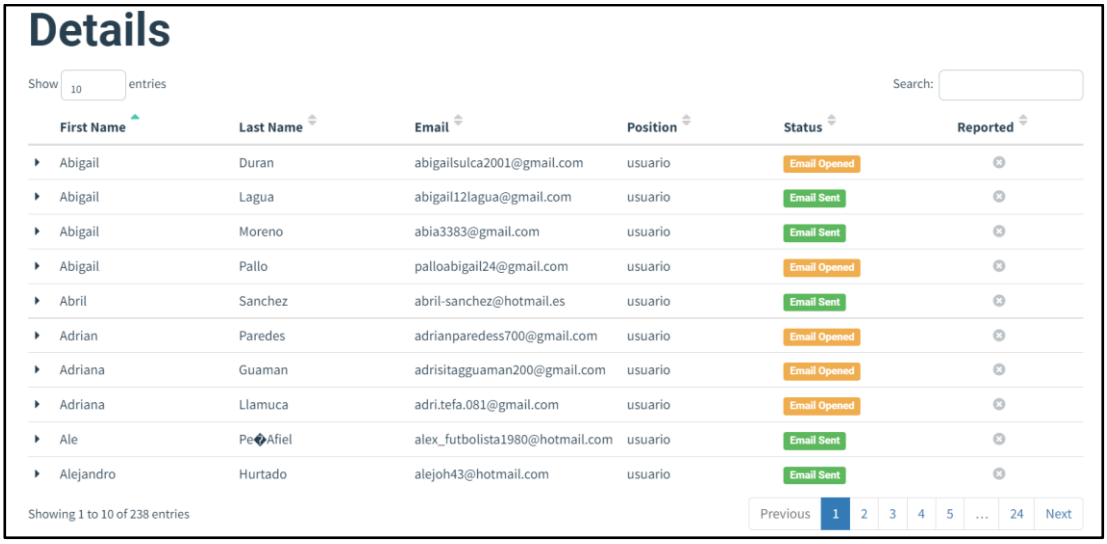


Gráfico 137. Detalle de los correos enviados a las víctimas

Elaborado Por: Shirley Flores

Al momento de la ejecución se envían 40 correos satisfactoriamente, en el progreso del ataque se da un error, ya que, al realizar una ejecución a correos personales y considerando que el correo que se envió adjuntaba una URL mencionando a una red

social, la seguridad del correo, detecta una actividad sospechosa la cual es bastante común y los correos están configurados para eso, esto provoca que se detenga la ejecución, bloqueando la cuenta que está siendo utilizada para este fin.

Gráfico 138. Bloqueo de la Cuenta de correo utilizada

Elaborado Por: Shirley Flores

Se realiza una segunda ejecución, para intentar llegar al mayor número de víctimas con correos personales, en la cual se creó un documento con formato .CSV, eliminando a los usuarios que ya fue enviado la campaña y se distribuyeron en 6 grupos de 30 a 35 usuarios con el mismo formato, para descartar que el error se haya dado por el exceso de correos.

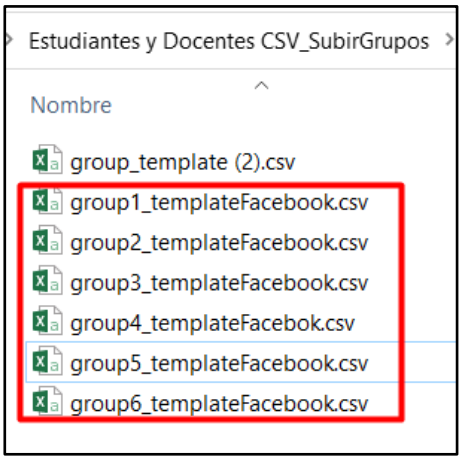


Gráfico 139. Bloqueo de la Cuenta de correo utilizada

Elaborado Por: Shirley Flores

Para la segunda ejecución, se realiza la configuración con la información de la campaña, en este caso se cambia el perfil de envío el cual está configurado con el correo es.la-facebook@hotmail.com, y se adjunta los grupos creados con los archivos importados con el formato .CSV, y se ejecuta la campaña.

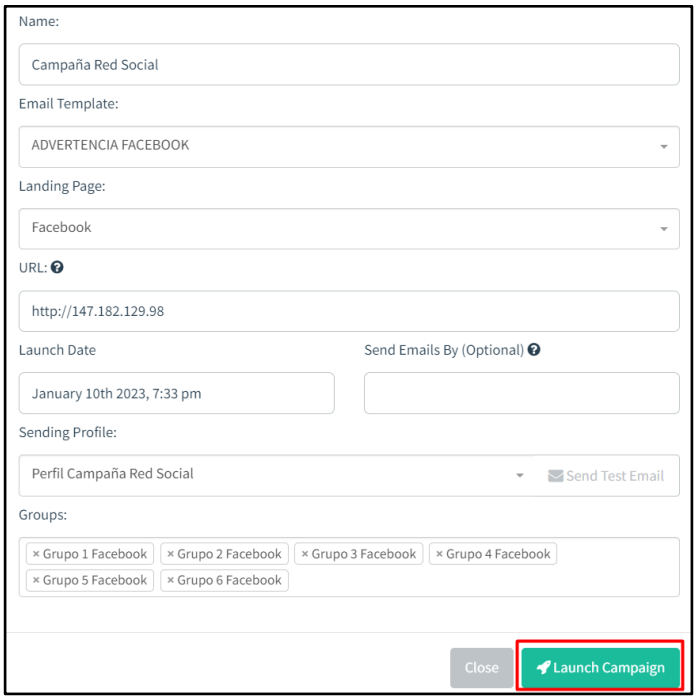


Gráfico 140. Creación de la segunda Campaña de Red Social

Elaborado Por: Shirley Flores

En el progreso de la segunda ejecución, se evidenció el mismo error, esto quiere decir que los distintos dominios de correo electrónico cuentan con la medida de seguridad de detección de spam y reconocen si se trata de un ataque de phishing, pero esta medida puede ser superada poco a poco con diferentes maneras que existen para la ejecución.

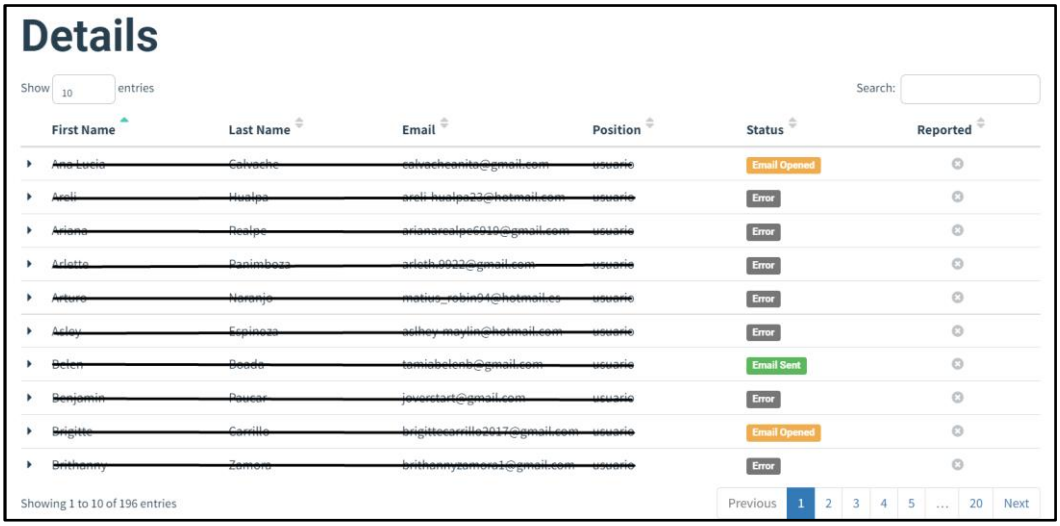


Gráfico 141. Detalles de la Ejecución Campaña 2 de Red Social

Elaborado Por: Shirley Flores

De manera inmediata, el equipo de seguridad de Outlook, envía un correo, detectando la actividad que se está realizando en ese momento como lo indica en el Gráfico 142.

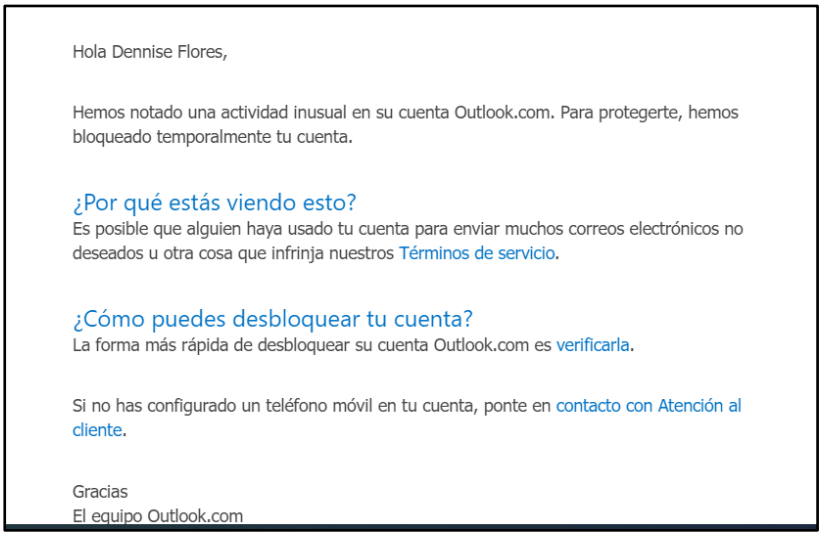


Gráfico 142. Email enviado por equipo de Outlook

Elaborado Por: Shirley Flores

3.2.11. Resultados

3.2.11.1. Análisis de Resultados

Una vez culminadas las pruebas, en esta ejecución se capturaron contraseñas, pero por políticas de seguridad no se mostrará información confidencial, pero se identificaron los usuarios que ingresaron información sobre sus accesos privados. Los resultados obtenidos se visualizan en el Gráfico 143.

3.2.11.2. Docentes

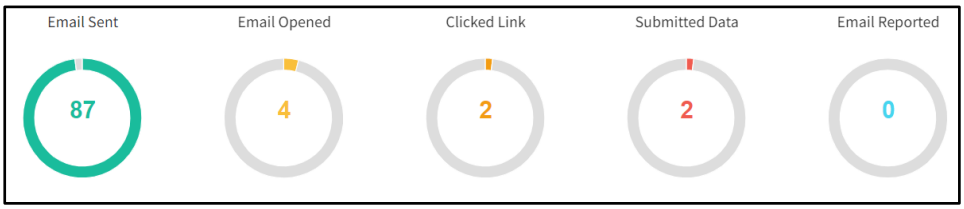


Gráfico 143. Resultados de la Interacción de IS-Docentes
Elaborado Por: Shirley Flores

En el dashboard de la campaña ejecutada se visualiza la lista de todos los usuarios que fueron víctimas a esta simulación de phishing, y los detalles de cada usuario en el cual se muestra información de los eventos realizados y la fecha de cada uno, en el caso de los usuarios que ingresaron información, se captura información del sistema operativo y el navegador con el cual iniciaron sesión, como lo indica el Gráfico 144.

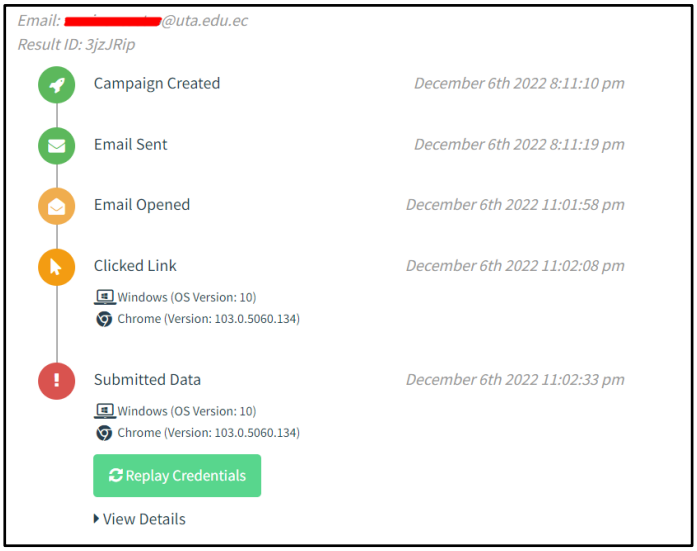


Gráfico 144. Eventos realizados en ejecución del ataque de IS-Docentes
Elaborado Por: Shirley Flores

Una vez culminado la etapa de envío de correos suplantados y recolectadas las evidencias contenidas en la Tabla 21, se analizaron y obtuvieron los resultados, mismos que se encuentran representados en el Gráfico 145.

Tabla 21. Resultados Finales IS Docentes
Elaborado Por: Shirley Flores

Correos enviados	Correos con error o no entregados	Correos abiertos	Personas que dieron clic en el enlace adjunto	Personas que ingresaron datos confidenciales (Víctimas de Phishing)
88	1	4	2	2

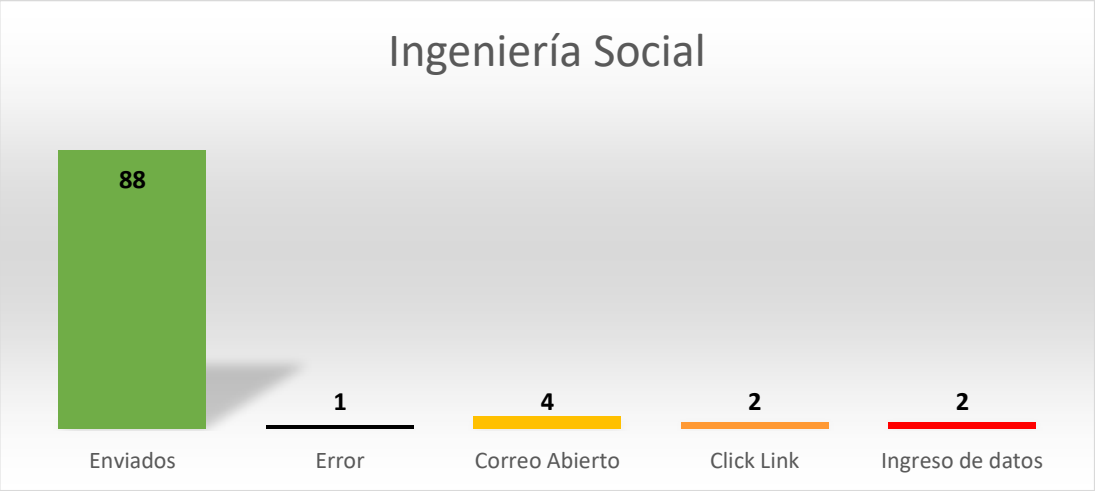


Gráfico 145. Resultados de ejecución del ataque de IS-Docentes
Elaborado Por: Shirley Flores

3.2.11.3. Estudiantes

Se analizó los resultados del ataque de phishing simulado en la plataforma de gophish, en el cual se obtuvo los siguientes resultados, el 90.99% de correos fueron enviados exitosamente, el 3.56% que representa los 17 correos abiertos, 2.56% que representa los usuario que hicieron clic en el enlace, el 1.68% que representa el número de víctimas que ingresaron datos y el 1.26% que se consideraron como error al momento de lanzar la campaña.

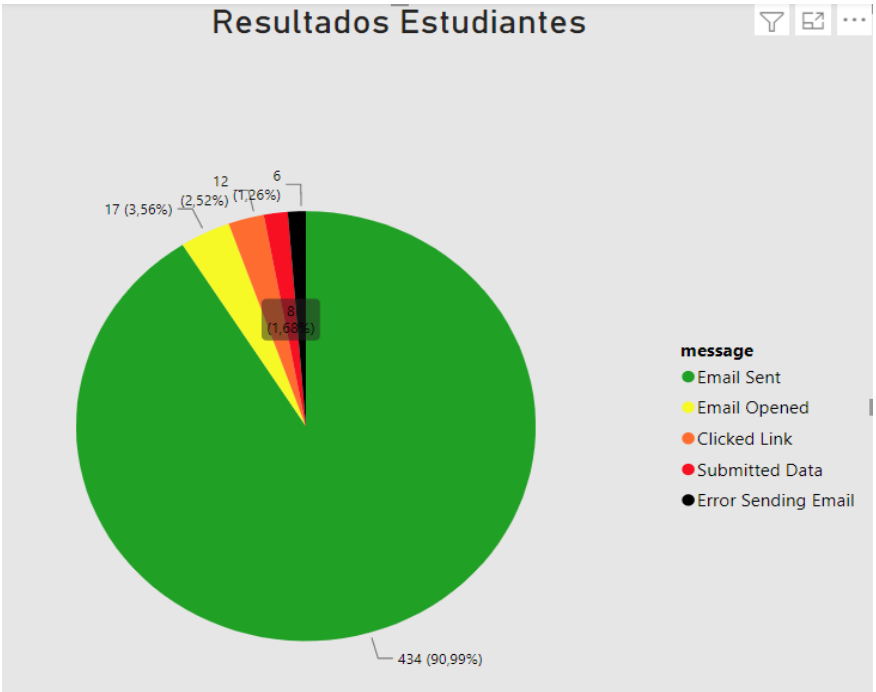


Gráfico 146. Eventos realizados en ejecución del ataque de IS-Docentes

Elaborado Por: Shirley Flores

En el detalle, que se muestra en el panel de la campaña luego de la ejecución, se puede visualizar información relevante como el número de veces que se abrió el correo, que se dio clic en el enlace adjunto, ingreso de datos, así como también se puede visualizar desde que dispositivo se accedió, y el navegador con sus respectivas versiones.

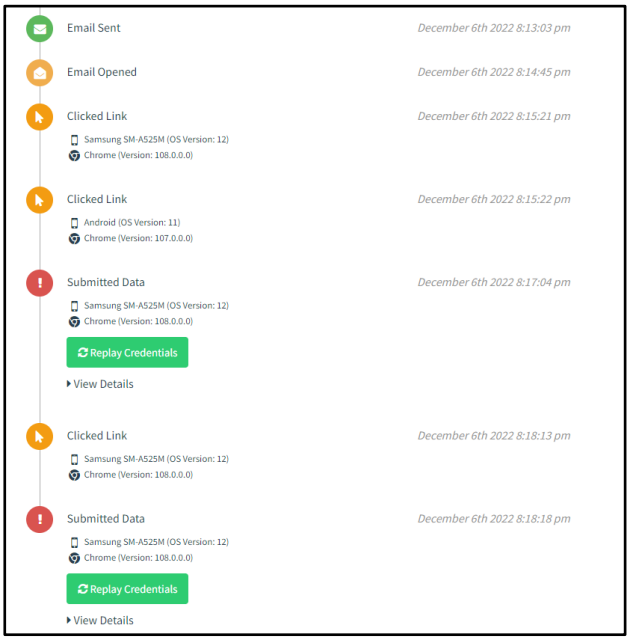


Gráfico 147. Detalle de Eventos realizados en ejecución del ataque de IS-Estudiantes

Elaborado Por: Shirley Flores

Una vez culminado la etapa de envío de correos suplantados y recolectadas las evidencias contenidas en la Tabla 22, se analizaron y obtuvieron los resultados, mismos que se encuentran representados en el Gráfico 148.

Tabla 22. Resultados Finales IS Estudiantes
Elaborado Por: Shirley Flores

Correos enviados	Correos con error o no entregados	Correos abiertos	Personas que dieron clic en el enlace adjunto	Personas que ingresaron datos confidenciales (Víctimas de Phishing)
434	6	17	12	8

La distribución de datos sobre las pruebas de phishing se detalla en el Gráfico 148, agrupando los resultados del ejercicio por evento ejecutado.

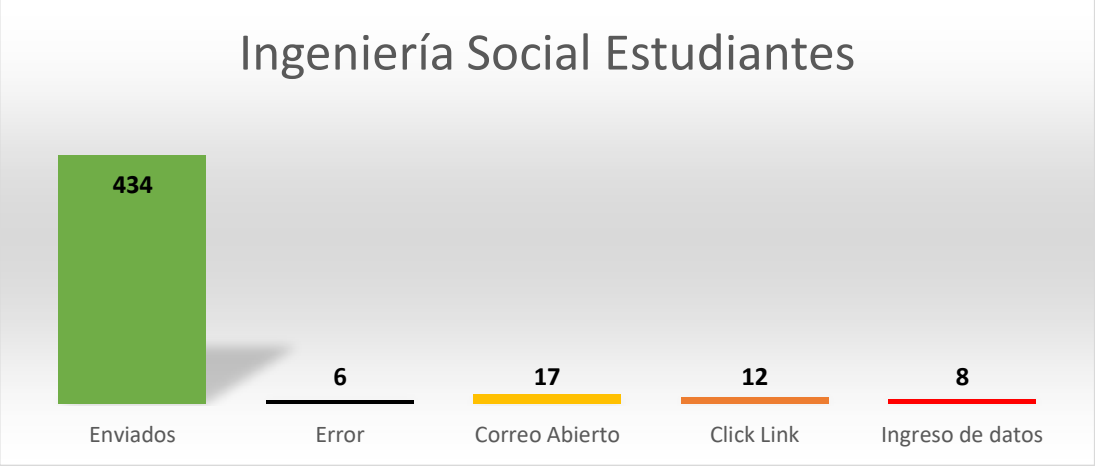


Gráfico 148. Eventos realizados en ejecución del ataque de IS-Estudiantes
Elaborado Por: Shirley Flores

Según un informe de HubSpot, los martes y el jueves es el día ideal para enviar emails, seguidos por los lunes y miércoles [40].

En base a la investigación del mejor día para enviar emails, se realizó la ejecución en los días indicados, para verificar y analizar dicho estudio. En el cual se obtuvo como resultado, que efectivamente el día martes hubo mayor interacción con la campaña ejecutada, y la mayor incidencia en la acción de abrir el correo, los resultados se visualizan en el **Gráfico 148**, que se muestra a continuación.

message	Hora	Fecha
Clicked Link	0:03:15	miércoles, 07 de diciembre de 2022
Clicked Link	7:11:05	jueves, 08 de diciembre de 2022
Clicked Link	7:12:08	jueves, 08 de diciembre de 2022
Clicked Link	7:56:08	miércoles, 07 de diciembre de 2022
Clicked Link	20:15:21	martes, 06 de diciembre de 2022
Clicked Link	20:15:22	martes, 06 de diciembre de 2022
Clicked Link	20:18:13	martes, 06 de diciembre de 2022
Clicked Link	20:21:39	martes, 06 de diciembre de 2022
Clicked Link	20:21:44	martes, 06 de diciembre de 2022
Clicked Link	20:27:16	martes, 06 de diciembre de 2022
Clicked Link	20:28:11	martes, 06 de diciembre de 2022
Email Opened	0:03:05	miércoles, 07 de diciembre de 2022
Email Opened	7:10:35	jueves, 08 de diciembre de 2022
Email Opened	7:55:36	miércoles, 07 de diciembre de 2022
Email Opened	19:39:02	jueves, 08 de diciembre de 2022
Email Opened	19:39:03	jueves, 08 de diciembre de 2022
Email Opened	20:14:45	martes, 06 de diciembre de 2022
Email Opened	20:16:36	martes, 06 de diciembre de 2022
Email Opened	20:20:53	martes, 06 de diciembre de 2022
Email Opened	20:21:30	martes, 06 de diciembre de 2022
Email Opened	20:23:07	martes, 06 de diciembre de 2022
Email Opened	20:25:28	martes, 06 de diciembre de 2022
Email Opened	20:25:39	martes, 06 de diciembre de 2022
Email Opened	20:25:49	martes, 06 de diciembre de 2022
Email Opened	20:25:56	martes, 06 de diciembre de 2022
Email Opened	20:26:41	martes, 06 de diciembre de 2022
Email Opened	20:27:40	martes, 06 de diciembre de 2022
Email Opened	20:30:26	martes, 06 de diciembre de 2022
Email Sent	7:08:40	jueves, 08 de diciembre de 2022

Gráfico 149. Análisis del Mejor día de envío de campañas ejecutadas.

Elaborado Por: Shirley Flores

En el detalle de uno de los resultados, se puede visualizar que el correo es abierto varias veces y con una diferencia de tiempo muy corta, esto quiere decir que el correo es analizado antes de que llegue a la víctima, se puede decir que se trata de la funcionalidad de un antispam.

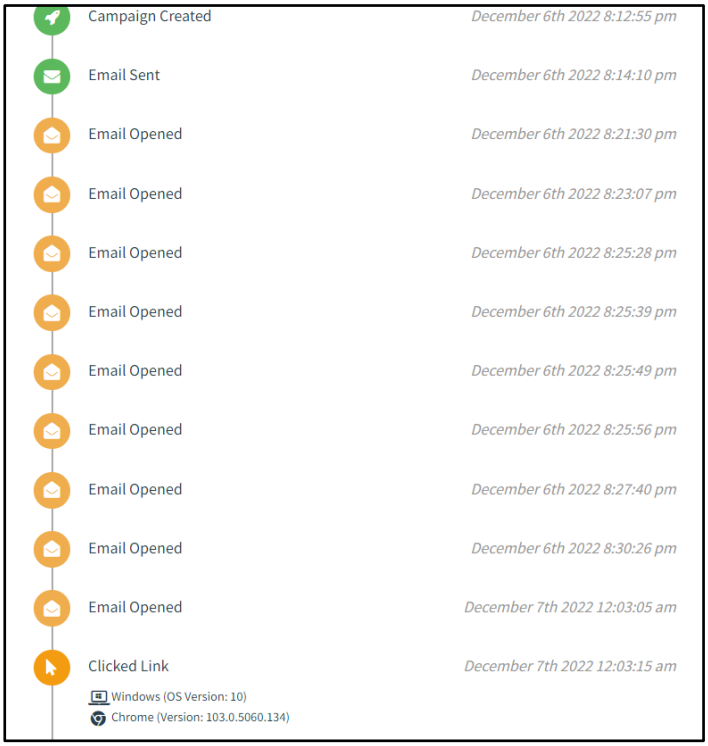


Gráfico 150. Análisis de Antispam

Elaborado Por: Shirley Flores

3.2.11.4. Red Social Facebook

Una vez concluida la campaña, de la primera ejecución con la página de Facebook en la cual se puede visualizar en la línea de tiempo él envió de correos y se muestra que los primeros correos son enviados exitosamente, a continuación, da un error ya que se bloquea la ejecución debido a que el enlace contiene una URL de Facebook, y la seguridad de los correos están configurados para detectar rápidamente ya que este tipo de ataque es muy común para fines maliciosos. Se obtiene como resultados 40 correos enviados y 24 correos abiertos como se muestra en el Gráfico 151.

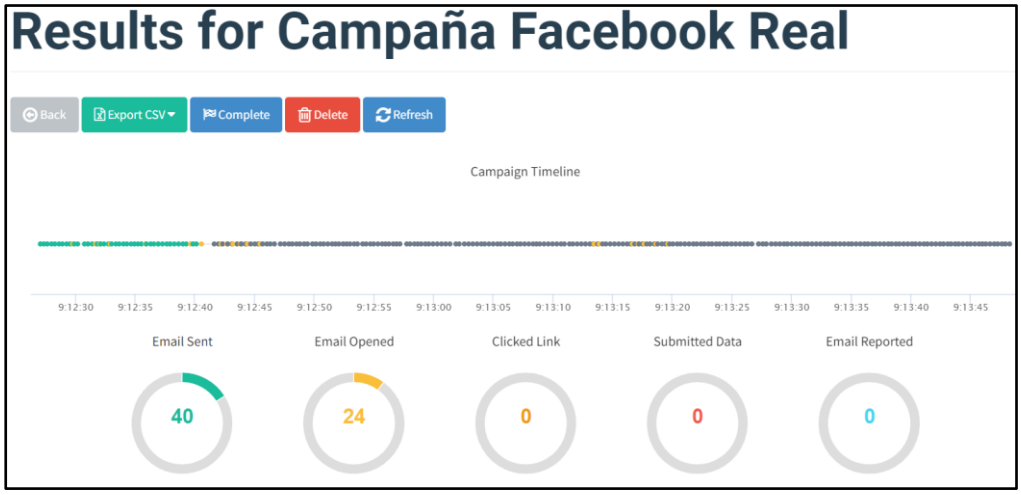


Gráfico 151. Resultados de la primera campaña de Facebook

Elaborado Por: Shirley Flores

Los resultados de la segunda ejecución de la campaña de Facebook, son similares a la de la primera, en el hecho de que se envían los primeros correos satisfactoriamente, Se obtiene como resultados 24 correos enviados y 17 correos abiertos como se muestra en el Gráfico 152.

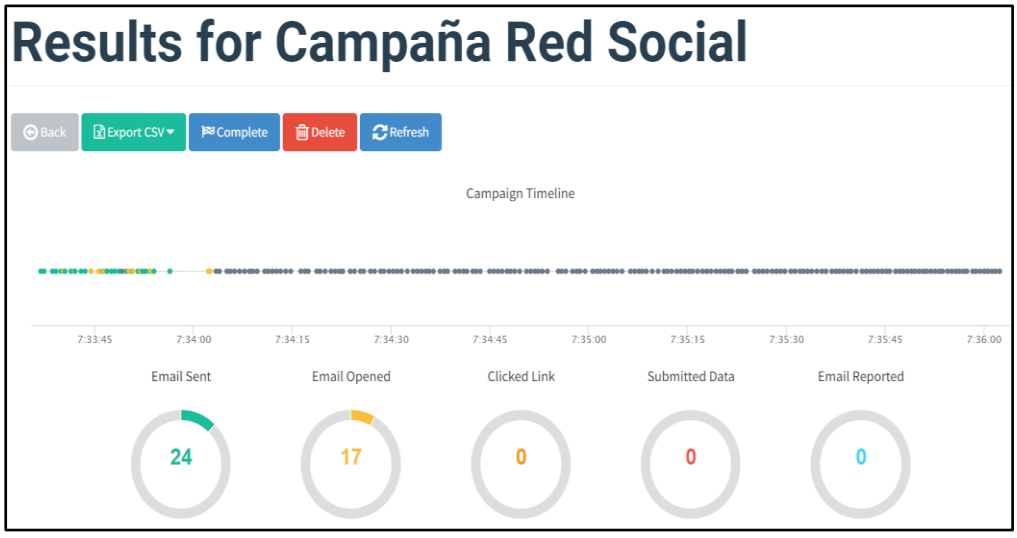


Gráfico 152. Resultados de la segunda campaña de Facebook

Elaborado Por: Shirley Flores

Se realizo un análisis total de datos de la ejecución dirigida a estudiantes con la página de red Social de Facebook, en la cual se puede afirmar que existió un total de **41** víctimas de Phishing de un universo de **64** usuarios de prueba enviados exitosamente.

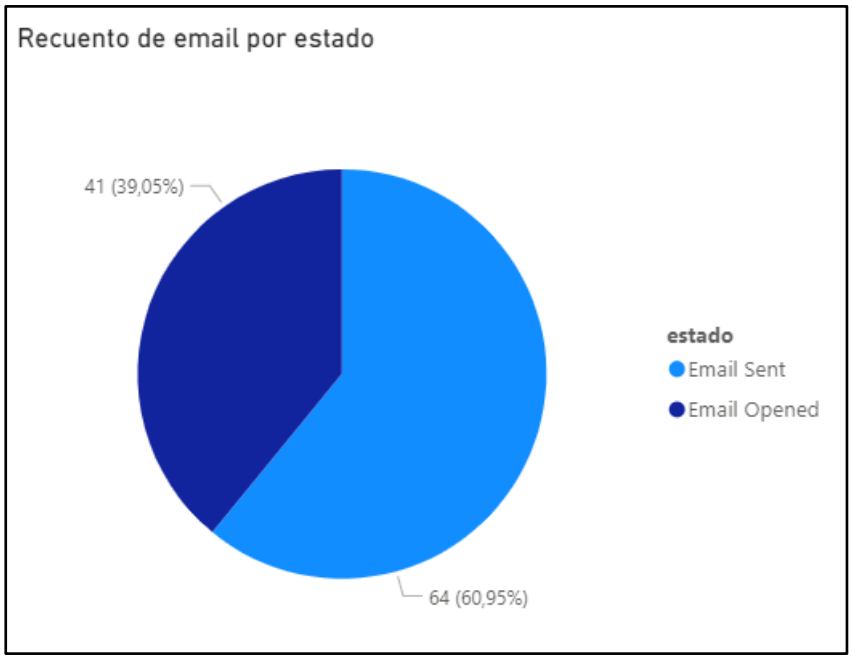


Gráfico 153. Resultado Consolidado de la ejecución de Facebook

Elaborado Por: Shirley Flores

Una vez culminado la etapa la campaña de ejecución de phishing y recolectadas las evidencias contenidas en la Tabla 23 se analizaron y obtuvieron los resultados, mismos que se encuentran representados en el Gráfico 154.

Tabla 23. Resultados Finales IS Red Social

Elaborado Por: Shirley Flores

Correos entregados	Correos con error o no entregados	Correos abiertos	Personas que dieron clic en el enlace adjunto	Personas que ingresaron datos confidenciales (Víctimas de Phishing)
64	133	41	0	0

La distribución de datos sobre las pruebas de phishing se detalla en la siguiente gráfica, agrupando los resultados del ejercicio por evento ejecutado.

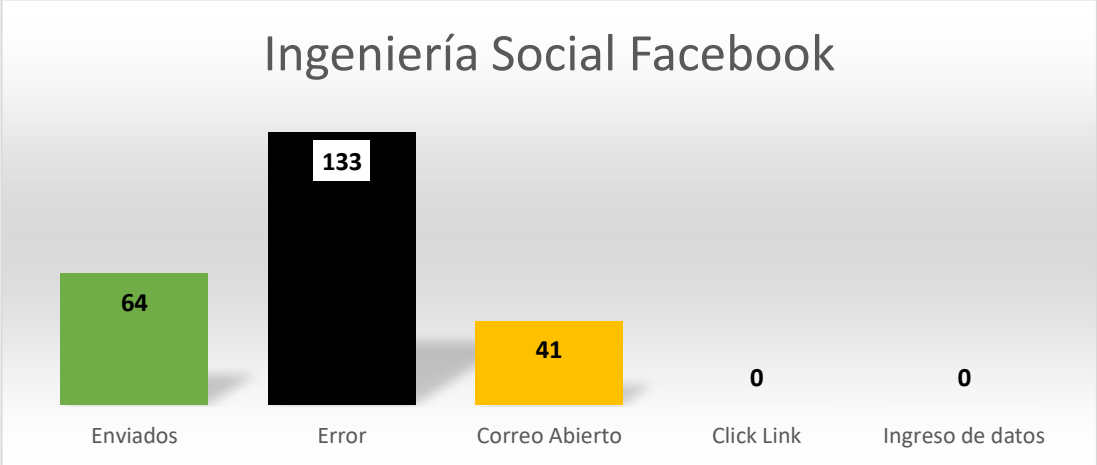


Gráfico 154. Histograma de la ejecución total de Facebook

Elaborado Por: Shirley Flores

3.3. Análisis de Brechas

Se observa que en la ejecución de los ataques dirigidos a estudiantes y docentes existe interacción con las diferentes páginas falsas, no obstante, se han considerado brechas en riesgo:

- No se reconoce una página falsa, considerando así el robo inmediato de información, afectando la brecha integridad de la información recibida.
- En el transcurso del tiempo de ejecución, se observa, que los estudiantes protegen sus redes sociales más que la información universitaria. En el caso de los docentes, es un riesgo medio ya que protegen más sus cuentas universitarias y en una brecha supuesta o esperada controlan sus cuentas bancarias.
- La pérdida de información es mediante claves y usuarios, observando así, que no existe un robustecimiento de la seguridad de los dígitos de una contraseña.
- Las filtraciones de información nacen a partir de bajo uso de antivirus, antimalware y el registro indiscriminado en cualquier página web, de esta manera estas pueden ser vendidas en la DEEP y en la DARK Web.
- Una de las brechas de seguridad, que pueden contemplarse para futuras investigaciones es los ataques de fuerza bruta, ya que obteniendo un modelo de usuario estos pueden ser atacados.

3.4. Estrategia de Capacitación

La estrategia de capacitación propuesta, está diseñada en 4 Fases las cuales se visualizan en el Gráfico 155.

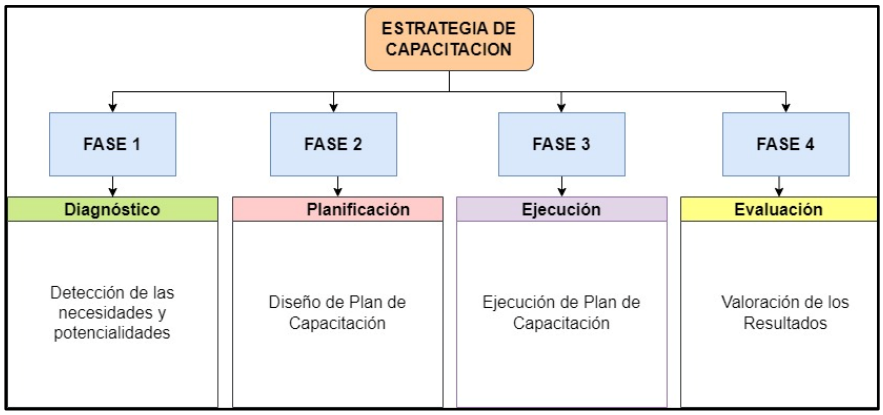


Gráfico 155. Estrategia de Capacitación

Elaborado Por: Shirley Flores

3.4.1. Diagnóstico

El diagnóstico de las necesidades se lo realizó en la encuesta inicial que fue dirigida a los estudiantes y docentes de la Facultad de Ciencias Humanas y de la Educación, en el proceso de recolección de información. De igual manera se consideró a las víctimas del ataque de simulación de phishing para que puedan ser parte de la charla de Seguridad de la Información.

3.4.2. Planificación

PLAN DE CAPACITACIÓN	
Fecha:	jueves, 2 de febrero de 2023
Hora:	9h00
Duración:	1 Hora Clase
Temas a abordar:	
• Seguridad de la Información	
• Ingeniería Social	
• Correo Electrónico	
• Ataques a través de correo electrónico	
• Cómo detectar correos fraudulentos	
• Redes Sociales y Buenas Prácticas de Redes Sociales para la seguridad de la información	
• Navegación Segura	
• Credenciales de Acceso	

Gráfico 156. Plan de Capacitación

Elaborado Por: Shirley Flores

3.4.3. Ejecución

Para la ejecución de la capacitación se elaboró material visual para la concientización en Seguridad de la Información, en el cual se incluye videos de información para captar mejor la atención del usuario. El desarrollo de la misma se realizó en el Aula Magna de la Facultad de Ciencias Humanas y de la Educación.

Gráfico 157. Material de Capacitación

Elaborado Por: Shirley Flores

3.4.4. Evaluación

Una vez culminada la capacitación, se elaboró un cuestionario interactivo en el cual se utilizó la aplicación Quizizz ya que es una herramienta de gamificación que permite evaluar de manera divertida, el mismo que se aplicó a las personas asistentes. En el cual los estudiantes y docentes pudieron identificar conceptos básicos, cuando se trata de una página oficial y una fraudulenta, reconocimiento de que se debe hacer en casos de robo de identidad, etc. En el Gráfico 158, se puede visualizar un resumen de la evaluación interactiva, la cual se visualiza los aciertos que obtuvo cada participante.

La estructura de la evaluación se encuentra detallado en el (Anexo A.3).

Gráfico 158. Resumen de Evaluación Interactiva

Elaborado Por: Shirley Flores

De igual manera, se realizó una evaluación sumativa, en la cual mediante un cuestionario de conocimientos de Google Forms (Anexo A.4), se obtuvo los siguientes resultados.

Pregunta 1: ¿Qué es la Seguridad de la Información?

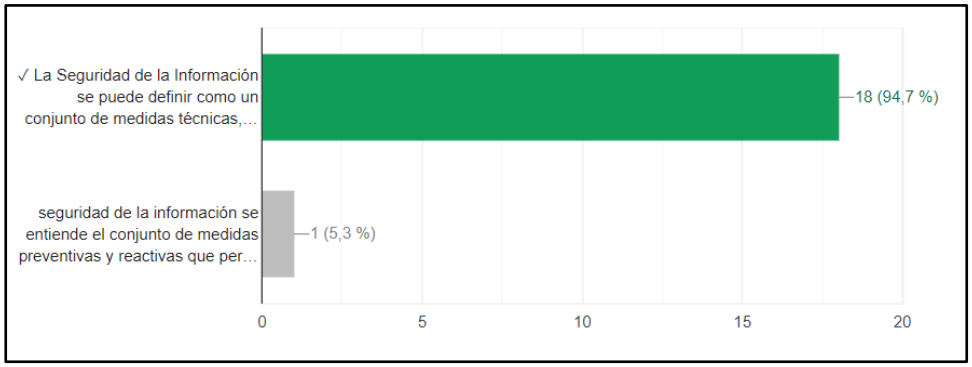


Gráfico 159. Estadísticas Pregunta 1

Elaborado Por: Shirley Flores

Pregunta 2: ¿Qué es la Ingeniería Social?

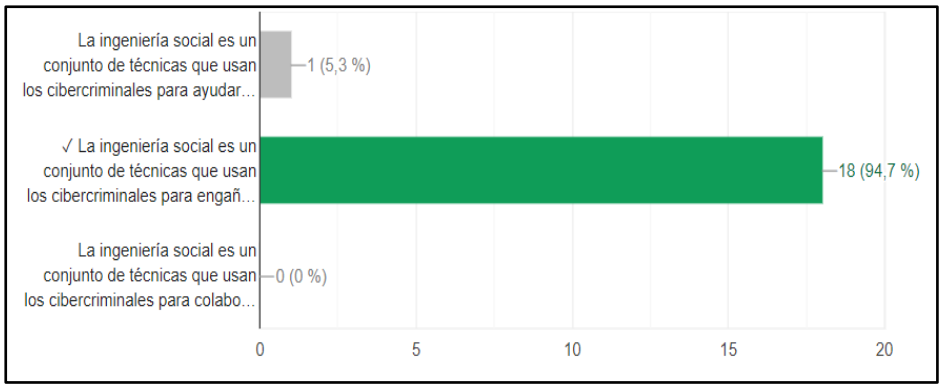


Gráfico 160. Estadísticas Pregunta 2

Elaborado Por: Shirley Flores

Pregunta 3: El envío de correos electrónicos fraudulentos para conseguir los datos bancarios de personas recibe el nombre de:

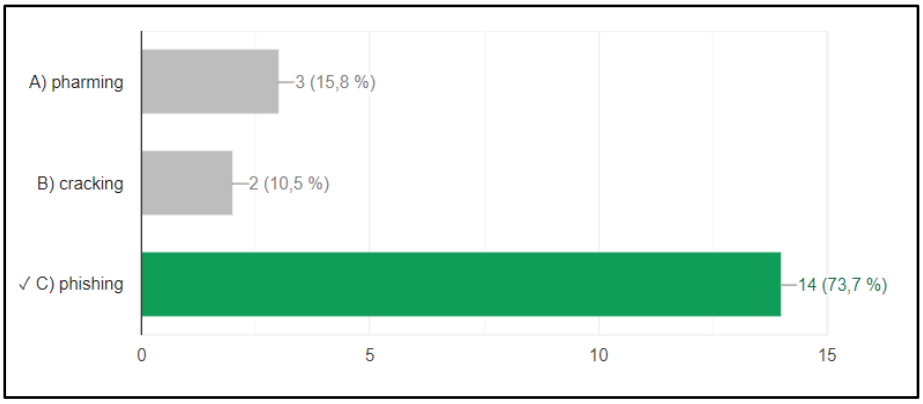


Gráfico 161. Estadísticas Pregunta 3

Elaborado Por: Shirley Flores

Pregunta 4: Las redes sociales son un servicio que te permiten estar en contacto con otras personas, por eso…

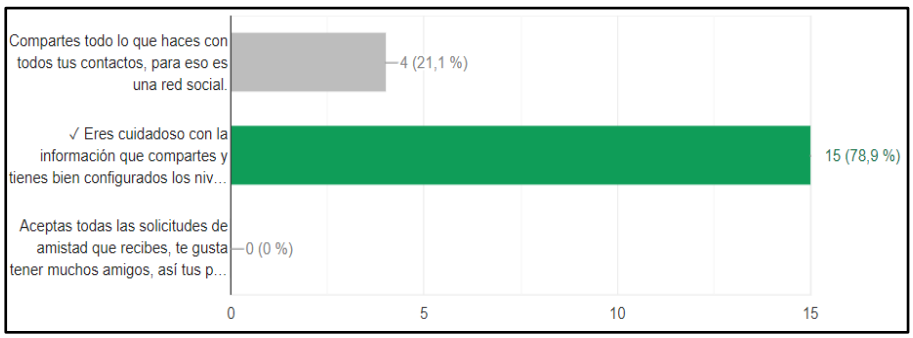


Gráfico 162. Estadísticas Pregunta 4

Elaborado Por: Shirley Flores

Pregunta 5: ¿En qué consiste la técnica del phishing?

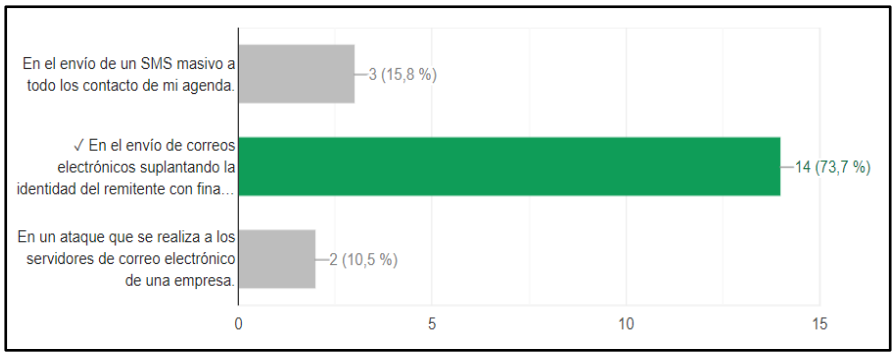


Gráfico 163. Estadísticas Pregunta 5

Elaborado Por: Shirley Flores

Pregunta 6: Los enlaces que aparecen en un phishing suelen redireccionar al usuario a páginas web falsas o descargar malware:

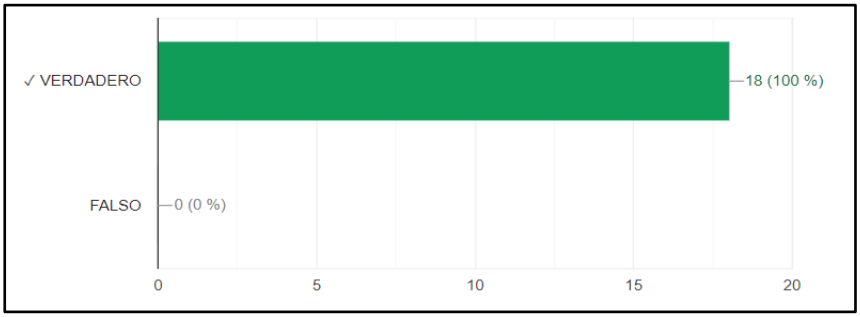


Gráfico 164. Estadísticas Pregunta 6

Elaborado Por: Shirley Flores

Pregunta 7: Entre las siguientes opciones, ¿Cuál dirías que es una contraseña robusta y segura?

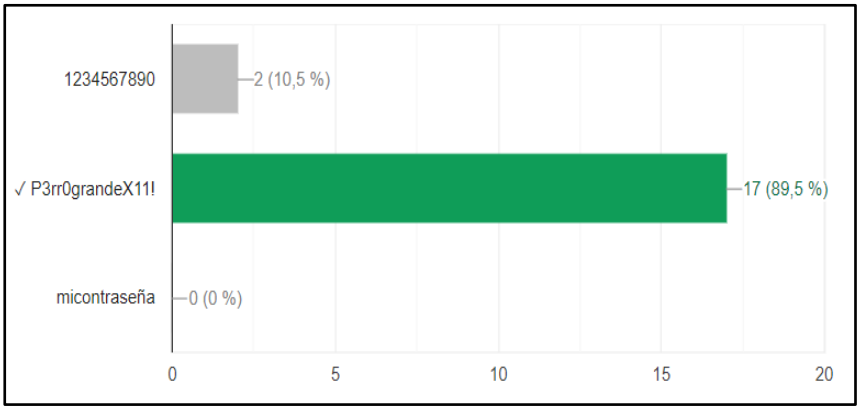


Gráfico 165. Estadísticas Pregunta 7

Elaborado Por: Shirley Flores

Pregunta 8: ¿Son importantes las URL para detectar páginas fraudulentas?

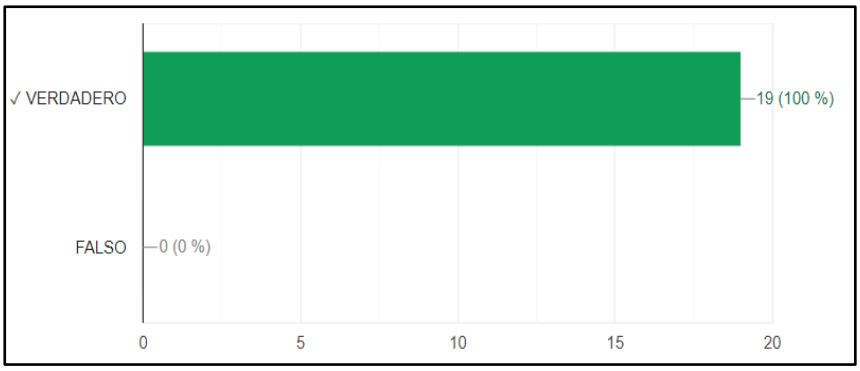


Gráfico 166. Estadísticas Pregunta 8

Elaborado Por: Shirley Flores

Pregunta 9: He recibido un mensaje privado a través de mis redes sociales, donde un desconocido me advierte de que tiene en su poder un vídeo mío comprometido junto a un enlace de descarga. Además, me pide que haga un pago o lo difundirá. ¿Qué hago?

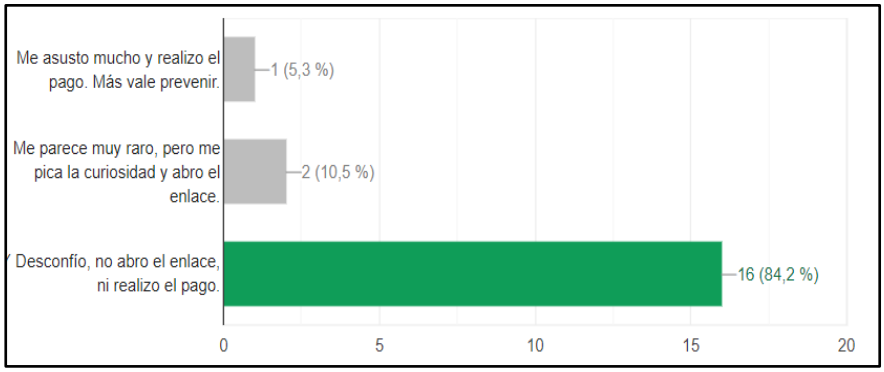


Gráfico 167. Estadísticas Pregunta 9

Elaborado Por: Shirley Flores

Pregunta 10: ¿Cuál de las siguientes opciones crees que es una web segura?

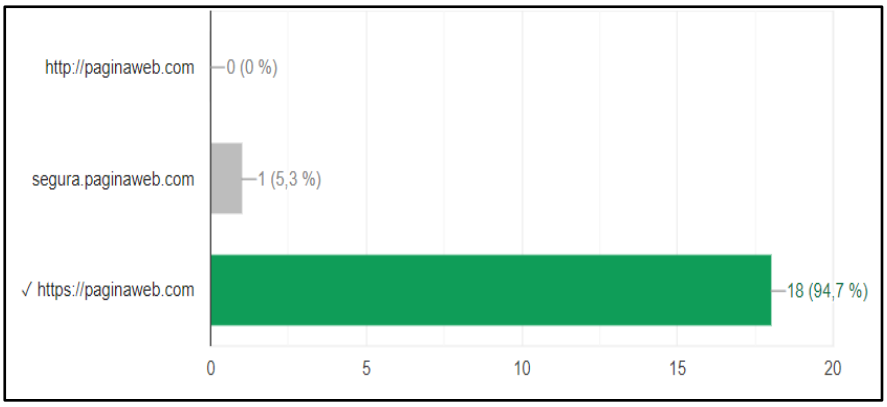


Gráfico 168. Estadísticas Pregunta 10

Elaborado Por: Shirley Flores

Se observó que antes de ejecutar la capacitación, los participantes no presentaban un sólido conocimiento de Seguridad de la Información; una vez ejecutada la charla de concientización, por medio de los resultados obtenidos de la evaluación tanto práctica como teórica, se puede comprobar que la capacitación fue exitosa, con un total de 37 participantes, de los cuales el 48.65% tuvo participación en la evaluación práctica y el 51.35% tuvo participación en la evaluación teórica o de conocimientos, se menciona que el 86,48% de asistentes reconocen páginas y enlaces fraudulentos, de esta manera se mitiga el riesgo de ataques informáticos.

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Dentro de los usuarios que fueron sujetos de las pruebas de ingeniería social existieron usuarios que al recibir las pruebas realizaron múltiples ingresos de datos incluso por 2 ocasiones.

- No se necesitó de la compra de un dominio web, ya que se analizó la cantidad de usuarios que no identifican una URL, y no verifican la dirección web, antes de interactuar con la página fraudulenta que se diseñó en la campaña de phishing.

- Dentro del análisis, se puede dilucidar que la seguridad de los correos electrónicos, se encuentran configurados para la detección de spam, mucho más si el correo electrónico que se va a enviar contiene una URL de una Red Social, es este caso fue Facebook, el cual fue detectado y no permitió completar con la ejecución a los correos personales de los estudiantes, bloqueando inmediatamente la acción.

- Las pruebas de Phishing de Ingeniería Social conllevan a determinar una vulnerabilidad presente en el comportamiento del personal que forma parte de una Institución. Dicha vulnerabilidad puede denominarse Baja concientización de seguridad de la información y debe ser tomada en cuenta al igual que un fallo presente en un dispositivo de red.

- A pesar de que existió una mayor interactividad por parte de los usuarios en la apertura del correo como vector inicial, se visualiza que 10 usuarios ingresaros datos, esto sin dejar de lado que una sola contraseña puede comprometer la institución.

- Una vez concluida la charla de concientización a los estudiantes y docentes, se puede decir que la estrategia de capacitación y la metodología de evaluación aplicada fue la adecuada, ya que se obtuvo resultados favorables de los conocimientos adquiridos acerca de la Seguridad de la Información.

4.2. Recomendaciones

- Se recomienda crear con un tiempo de anticipación considerable los correos electrónicos a utilizar para realizar el ataque, ya que el correo se valida y se verifica como más confiable, y se puede ejecutar sin ningún problema, teniendo la mayor cantidad de correos enviados, mediante la plataforma de gophish.

- Para la ejecución se recomienda mantener activo el servidor durante 4 días máximo para la Ingeniería Social, ya que mientras más tiempo se tiene operativo, menos credibilidad tendrá la página fraudulenta por los mensajes de seguridad y error de sitio no seguro.

- Preparación continua de los estudiantes y docentes de la facultad de Ciencias Humanas y de la Educación, en temas referentes a Seguridad de la Información, ya que al manejar activos importantes tales como información educativa o credenciales se convierte en una brecha de seguridad el no tomar conciencia de la protección de la información.

- Se debe proporcionar la información necesaria con respecto a las consecuencias que tiene el ser víctimas de ataques de ingeniería social, haciendo énfasis en el impacto que conlleva entregar información personal, credenciales, accesos o cualquier tipo de información relevante que pueda ser usada en su contra.

- Realizar campañas de continuo cambio de contraseñas y evitar el uso de contraseñas en las diferentes aplicaciones y redes sociales.

- Dentro de los planes académicos semestrales, se debe contemplar una capacitación o talleres obligatorios para los estudiantes y docentes de la Facultad de Ciencias de la Humanas y de la Educación, fomentando la cultura de seguridad de la información y ciberseguridad.

Bibliografía

[1] "Las Redes Sociales: una ventana de comunicación – Ministerio de Telecomunicaciones y de la Sociedad de la Información", Telecomunicaciones.gob.ec , 2022. [En línea]. Disponible: https://www.telecomunicaciones.gob.ec/las-redes-sociales-una-ventana-de-comunicacion/#:~:text=Quito.,medio%20de%20comunicaci%C3%B3n%20en%20voga

[2] Repositorio.unipiloto.edu.co , 2022. [En línea]. Disponible: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6951/Seguridad%20Aplicada%20en%20Sitios%20de%20Redes%20Sociales.pdf?sequence=1.

[3] J. P. Conde Mendoza, «Concientización en Ciberseguridad a través de Ataques de Ingeniería Social», INF-FCPN-PGI, n.º 7, pp. 62–64, nov. 2021.

[4] López Grande, C. E. (2015). Ingeniería Social: el ataque silencioso. Revista Tecnológica: no. 8.

[5] "La ciberseguridad, uno de los problemas de la vida en internet", Universidad Nacional de Loja, 2022. [En línea]. Disponible: https://www.unl.edu.ec/noticia/la-ciberseguridad-uno-de-los-problemas-de-la-vida-en-internet.

[6] "En 2020 se duplicaron las detecciones de ataques de Ingeniería Social en Latinoamérica", Eset.com, 2022. [En línea]. Disponible: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/en-2020-se-duplicaron-las-detecciones- de-ataques-de-ingenieria-social-en-latinoamerica/.

[7] R. Llumiquinga, "Ecuador es uno de los países más vulnerables para los ciberdelincuentes", prensa.ec | Portadas, boletines, entrevistas. , 2022. [En línea]. Disponible: https://prensa.ec/2022/06/22/ecuador-es-uno-de-los-paises-mas-vulnerables-para-los-ciberdelincuentes/.

[8] 2022. [En línea]. Disponible: https://aprenderlinux.org/herramientas-de-ingenieria-social-kali-linux/.

[9] 3ciencias.com, 2022. [En línea]. Disponible: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf.

[10] "La comunidad educativa de Ambato reflexionó acerca de los riesgos de las Redes Sociales en menores gracias a la iniciativa #GOODNETIZEN", Fundación Telefónica Ecuador, 2022. [En línea]. Disponible: https://fundaciontelefonica.com.ec/noticias/la-comunidad-educativa-de-ambato-reflexiono-acerca-de-los-riesgos-de-las-redes-sociales-en-menores-gracias-a- la-iniciativa-goodnetizen/.

[11] Moyano Morales, S. A. (2015). La manipulación de la mente humana como arma blanca en la Ingeniería Social (Bachelor's thesis, Universidad Piloto de Colombia).

[12] J. Villacís Freire, "Ataques de Ingeniería Social: un estudio de mapeo sistemático", Repositorio.uta.edu.ec , 2022. [En línea]. Disponible: https://repositorio.uta.edu.ec/jspui/handle/123456789/34343.

[13] R. Rocohano Ramos and L. Silva Ordoñez, "Detección de Vulnerabilidades en el Comportamiento de las Personas para Evitar que sean Víctimas de Ataques de Ingeniería Social.", Repositorio.espe.edu.ec , 2022. [En línea]. Disponible: http://repositorio.espe.edu.ec/handle/21000/25916.

[14] J. Urrutia franco y G. Hernández Flores, "Ingeniería Social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil", Repositorio.ug.edu.ec , 2022. [En línea]. Disponible: http://repositorio.ug.edu.ec/handle/redug/10741.

[15] W. Chérrez y D. Pesantez, "Ciberseguridad en las Redes Sociales: Una revisión teórica", *Dialnet* , 2022. [En línea]. Disponible: https://dialnet.unirioja.es/servlet/articulo?codigo=8298208.

[16] L. Gil Lluís, "Estudio de los ataques y su defensa en la Ingeniería Social", *E-spacio.uned.es* , 2022. [En línea]. Disponible: http://e-spacio.uned.es/fez/view/bibliuned:master-ETSInformatica-II-Lagil.

[17] "Significado de TIC (Tecnologías de la información y la comunicación)", Significados, 2021.[Online]. Available: https://www.significados.com/tic/.

[18] "Seguridad de la Información On Premise & Off Premise – Sinetcom", *Sinetcom.com.ec*, 2022. [En línea]. Disponible: https://sinetcom.com.ec/portfolio/seguridad-de-la-informacion-on-premise-off-premise/#:~:text=La%20seguridad%20de%20la%20informaci%C3%B3n,disponibilidad%20e%20integridad%20de%20datos.

[19] E. Bello, "Ingeniería Social: ¿qué es y cómo evitarla?", *Thinking for Innovation* , 2022. [En línea]. Disponible: https://www.iebschool.com/blog/ingenieria-social-tecnologia/.

[20] 2022. [En línea]. Disponible: https://ilifebelt.com/que-es-comunicacion-digital-y-por-que-es-importante-en-las-empresas/2016/09/.

[21] "Redes Sociales - Qué son, tipos, ejemplos, ventajas y riesgos", *Concepto,* 2022. [En línea]. Disponible: https://concepto.de/redes-sociales/.

[22] "Usuario", *Economipedia*, 2022. [En línea]. Disponible: https://economipedia.com/definiciones/usuario.html.

[23] B. Santander, "Vulnerabilidad", *Banco Santander*, 2022. [En línea]. Disponible: https://www.bancosantander.es/glosario/vulnerabilidad-informatica.

[24] A. Orellana, "Riesgos de seguridad: ¿Qué factores ponen en peligro tu entorno de TI?", *GB Advisors* , 2022. [En línea]. Disponible: https://www.gb-advisors.com/es/riesgos-de-seguridad-que-factores-ponen-en-peligro-tu-entorno-de-ti/#:~:text=Los%20Riesgos%20de%20seguridad%20no,una%20p%C3%A9rdida%20para%20la%20empresa.

[25] R. Toro, "Activos de información ¿Cómo realizar un inventario?", *PMG SSI - ISO 27001*, 2022. [En línea]. Disponible: https://www.pmg-

ssi.com/2017/02/realizar-inventario-activos-de-informacion/#:~:text=Los%20activos%20de%20informaci%C3%B3n%20son,indirectamente% 2C%20con%20las%20dem%C3%A1s%20entidades.

[26] "Ciberseguridad", Infosecuritymexico.com , 2022. [En línea]. Disponible: https://www.infosecuritymexico.com/es/ciberseguridad.html#:~:text=La%20ciberseguridad%20es%20el%20conjunto,m%C3%B3viles%2C%20redes%20y%20sistemas%20electr%C3 %B3nicos.

[27] "Ciberataques: Qué son y qué tipos existen - Iberdrola", Iberdrola, 2022. [Online]. Disponible: https://www.iberdrola.com/innovacion/ciberataques.

[28] "Digital Ocean: qué es, cómo usar y qué planes tiene la herramienta". Rock Content - ES. https://rockcontent.com/es/blog/digital-ocean/.

[29] "Fedora vs. Ubuntu ¿cuál elegir y por qué? [2022]," *https://www.crehana.com*. [Online]. Available: https://www.crehana.com/blog/transformacion-digital/fedora-vs-ubuntu/.

[30] "Digitalocean Reviews 2022: Details, pricing, & features | G2." [Online]. Available: https://www.g2.com/products/digitalocean/reviews.

[31] "Monitoring metrics," *DigitalOcean Documentation*. [Online]. Available: https://docs.digitalocean.com/products/monitoring/concepts/metrics/.

[32] "The cloud for builders," *DigitalOcean*. [Online]. Available: https://www.digitalocean.com/.

[33] "Digitalocean vs google cloud," *Back4App Blog*, 18-Aug-2021. [Online]. Available: https://blog.back4app.com/es/digitalocean-vs-google-cloud/#:~:text=En%20t%C3%A9rminos%20generales%2C%20Digital%20Ocean,para%20aplicaciones%20de%20grandes%20empresas.

[34] "Seguridad Y privacidad de gmail - centro de seguridad de google," *Seguridad y privacidad de Gmail - Centro de seguridad de Google*. [Online]. Available: https://safety.google/intl/es_es/gmail/.

[35] L. Spencer, "Gmail vs. outlook: ¿cuál es el mejor servicio (gratuito) de correo electrónico?," *Business Envato Tuts+*, 23-Feb-2017. [Online]. Available: https://business.tutsplus.com/es/articles/gmail-vs-outlook-whats-the-best-free-email-service--cms-28195.

[36] J. Jiménez, “Así puedes ayudar a combatir el phishing en outlook y gmail,” *RedesZone*, 15-Nov-2020. [Online]. Available: https://www.redeszone.net/2018/08/01/ayudar-combatir-phishing-outlook-gmail/.

[37] R. Velasco, “Gophish, Una Herramienta Libre para aprender a identificar y evitar el phishing,” *RedesZone*, 06-Jun-2022. [Online]. Available: https://www.redeszone.net/2016/04/16/gophish-una-herramienta-libre-aprender-identificar-evitar-phishing/. [Accessed: 15-Dec-2022].

[38] “Digitalocean,” *Capterra*. [Online]. Available: https://www.capterra.ec/software/205055/digitalocean.

[39] “Tabla comparativa de distribuciones linux.,” *Alcance Libre*. [Online]. Available: https://blog.alcancelibre.org/staticpages/index.php/tabla-comparativa-distros-linux.

[40] A. A. Castillo, “Los Mejores Momentos para Enviar emails de marketing,” *AB Tasty*, 23-Jun-2020. [Online]. Available: https://www.abtasty.com/es/blog/mejores-momentos-emails-marketing/.

[41] Alberto FonteApasionado de la ciberseguridad en continuo aprendizaje, “OSINT, ¿Qué es? ¿Para qué sirve?,” *Derecho de la Red*, 08-Mar-2021. [Online]. Available: https://derechodelared.com/osint/.

[42] por L. I. S. A. Institute, “HUMINT: Ejemplos, tipos y motivaciones de las Fuentes Humanas,” *LISA Institute*. [Online]. Available: https://www.lisainstitute.com/blogs/blog/humint-ejemplos-tipos-fuentes-humanas.

[43] R. Velasco, “Gophish, Una Herramienta Libre para aprender a identificar y evitar el phishing,” *RedesZone*, 06-Jun-2022. [Online]. Available: https://www.redeszone.net/2016/04/16/gophish-una-herramienta-libre-aprender-identificar-evitar-phishing/.

[44] “Phishing: ¿Qué es?, cómo reconocerlo - arka tecnology,” ARKA TECNOLOGY - Tu aliado tecnológico de confianza, 28-Oct-2022. [Online]. Available: https://arkatec.com.ec/que-es-el-phishing-como-reconocerlo-y-evitarlo/#:~:text=El%20phishing%20es%20un%20ataque,robar%20su%20informaci%C3%B3n%20y%20dinero.

[45] P. Zendesk, "¿Qué es la metodología ágil? ¿Para qué sirve?," Zendesk MX, 13-Dec-2022. [Online]. Available: https://www.zendesk.com.mx/blog/metodologia-agil-que-es/.

[46] "¿Qué es kanban? Una descripción general del Método Kanban," *Digite,* 18-Aug-2021. [Online]. Available: https://www.digite.com/es/kanban/que-es-kanban/.

[47] "¿Qué es un límite wip de kanban? ¿Por qué lo necesita?: Kanbanize," Kanban Software for Agile Project Management. [Online]. Available: https://kanbanize.com/es/recursos-de-kanban/primeros-pasos/que-es-limite-wip.

[48] C. Editorial, "Hunter.io: Encuentra en Segundos Las Cuentas de Correo electrónico que necesitas," *Consejo de Redacción*. [Online]. Available: https://consejoderedaccion.org/sello-cdr/hunter-busca-correos-emails#:~:text=Hunter.io%20es%20un%20portal,solo%20introducir%20su%20p%C3%A1gina%20web.&text=Durante%20la%20investigaci%C3%B3n%20period%C3%ADstica%20es,con%20personas%20que%20no%20conocemos.

ANEXOS

A.1 Encuesta Estudiantes y Docentes De La Facultad De Ciencias Humanas y de la Educación.

Objetivo: Determinar el nivel de conocimiento que tienen los estudiantes acerca del uso seguro de las redes sociales y conceptos de ciberseguridad.

1. **¿Señale el género al que pertenece?**

   ◯ Femenino

   ◯ Masculino

2. **¿En qué rango de edad se encuentra?**

   ◯ 14-18 años

   ◯ 19-24 años

   ◯ 25-34 años

   ◯ 35-44 años

   ◯ 45-55 años

   ◯ Más de 55 años

3. **¿Con qué fin utiliza las redes sociales?**

   ◯ Entretenimiento
   ◯ Educativo
   ◯ Informativo
   ◯ Trabajo
   ◯ Todas las anteriores

4. **¿Cuántos caracteres utiliza en las contraseñas para registrarse en la cuenta de las redes sociales?**

   ◯ 5 – 8
   ◯ 9 – 12
   ◯ 13 – 16

5. **¿Qué nivel de conocimiento tiene respecto a las amenazas y los riesgos informáticos que están presentes en las redes sociales?**

   ◯ Alto
   ◯ Medio
   ◯ Bajo

6. **¿Utiliza contraseñas diferentes para sus cuentas electrónicas como redes sociales, email, aula virtual?**

   ◯ SI
   ◯ NO

7. **Asigna un valor, donde 0 es nada frecuente y 5 es muy frecuente, ¿Qué tanto utiliza las siguientes redes sociales?**

	0	**1**	**2**	**3**	**4**	**5**
Facebook	◯	◯	◯	◯	◯	◯
Twitter	◯	◯	◯	◯	◯	◯
Instagram	◯	◯	◯	◯	◯	◯
WhatsApp	◯	◯	◯	◯	◯	◯
LinkedIn	◯	◯	◯	◯	◯	◯
Tic Tok	◯	◯	◯	◯	◯	◯
Snapchat	◯	◯	◯	◯	◯	◯
Telegram	◯	◯	◯	◯	◯	◯

8. **¿Con que frecuencia publica información en sus redes sociales?**

- ◯ Todos los días
- ◯ 2 veces por semana
- ◯ 1 vez a la semana
- ◯ Al menos una vez cada 15 días
- ◯ Solo los fines de semana

9. **¿Qué tipo de Contenidos, publica con mayor frecuencia en redes sociales?**

- ☐ Solo Textos
- ☐ Texto con Imagen o Fotografía
- ☐ Solo Imágenes o Fotografías
- ☐ Videos
- ☐ Videos con Texto
- ☐ Audios
- ☐ Historias
- ☐ No publico nada

10. **¿Conoce acerca de lo qué es la Ingeniería Social?**

- ◯ SI
- ◯ NO

11. **¿Cuál de estos ciberataques conoce, y que los podría explicar a otras personas?**

- ☐ Ransomware
- ☐ Phishing
- ☐ Ataques por denegación de servicios (DDoS)
- ☐ Troyanos
- ☐ Ninguna

12. **¿Qué tipo de fraudes electrónicos le genera mayor temor?**

- ( ) Que me roben dinero de mis cuentas bancarias
- ( ) Suplantación de identidad
- ( ) Que secuestren mi WhatsApp
- ( ) Estafas en sitios web ilegítimos

13. **¿Alguna vez han vulnerado la seguridad de sus cuentas electrónicas (Redes Sociales, email, banco virtual, etc.)?**

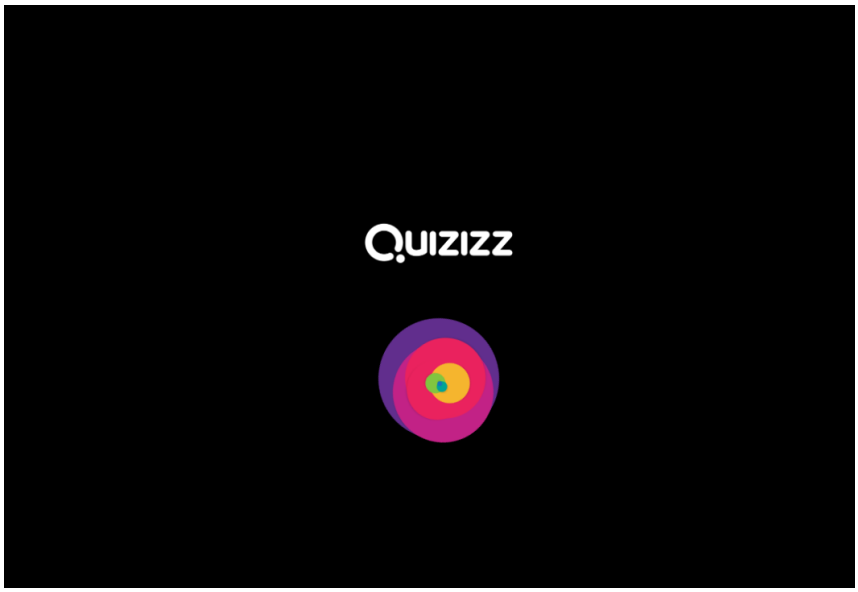
- ( ) SI
- ( ) NO

14. **¿Le gustaría formar parte de las capacitaciones de seguridad de la información?**

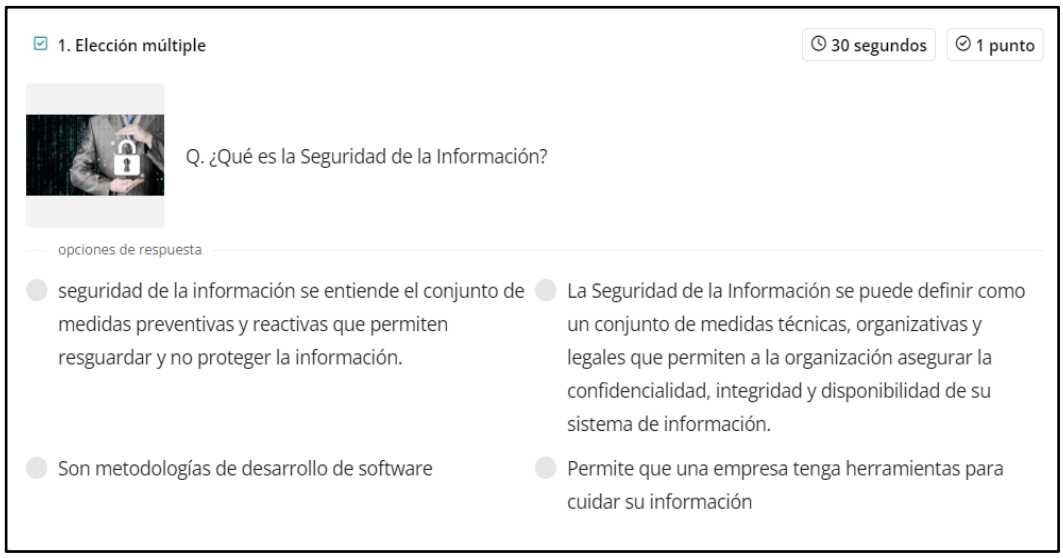
- ( ) SI
- ( ) NO

A.2 Ejecución de la Estrategia de Capacitación.

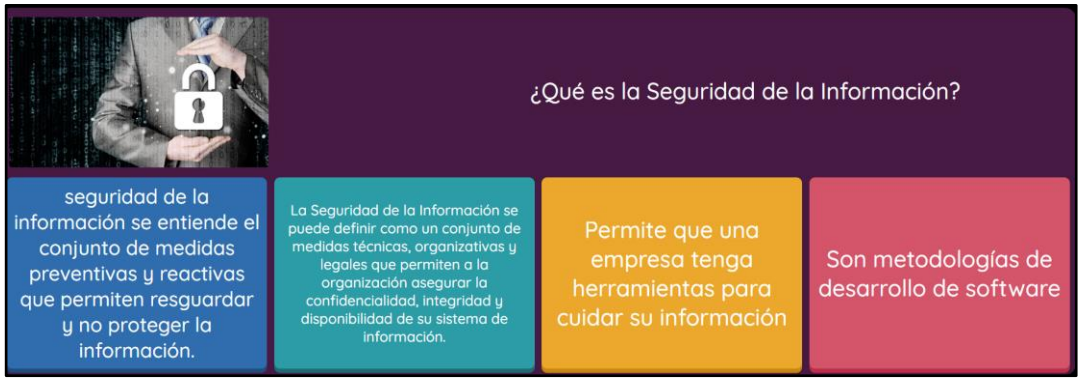
A.3 Evaluación Interactiva con la Herramienta Quizizz.



Pregunta 1



Visualización



Pregunta 2

2. Reordenar

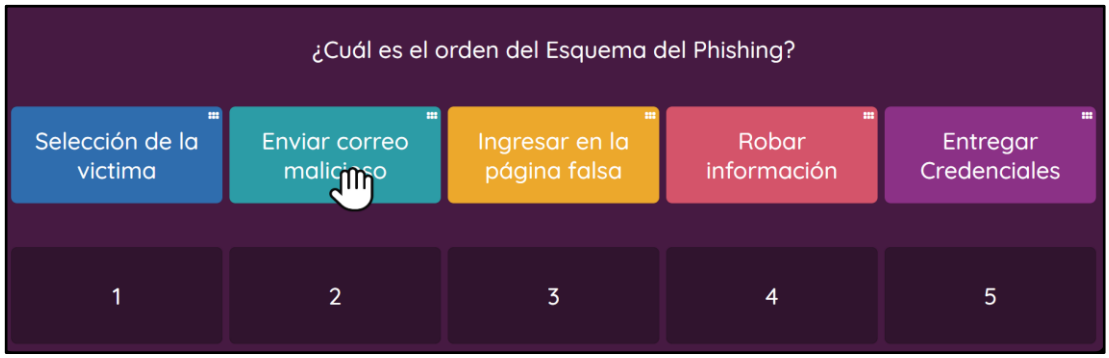
1.5 minutos | 1 punto

Q. ¿Cuál es el orden del Esquema del Phishing?

opciones de respuesta

- Selección de la victima
- Enviar correo malicioso
- Ingresar en la página falsa
- Entregar Credenciales
- Robar información

Visualización



Pregunta 3

3. Arrastra y suelta

1.5 minutos | 1 punto

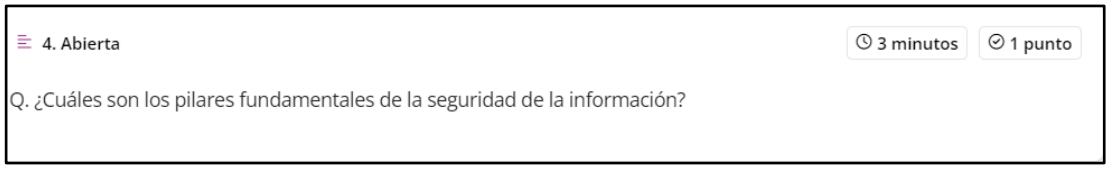
Q. La (a) _____ es un conjunto de técnicas que usan los (b) _____ para engañar a los (c) _____ incautos.

opciones de respuesta

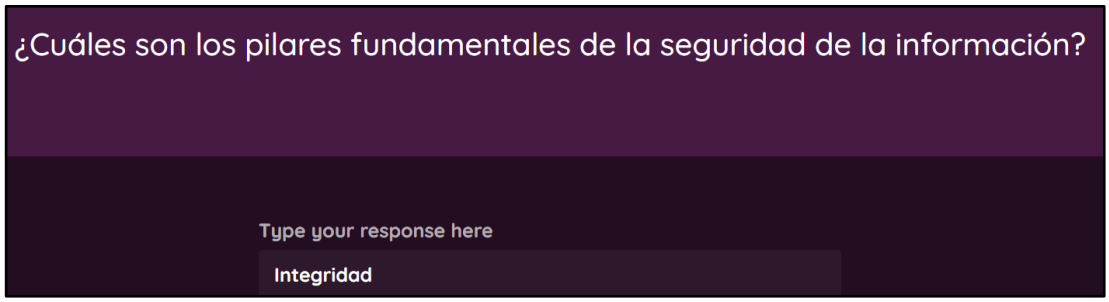
- ingeniería social
- cibercriminales
- usuarios
- investigadores

Visualización

Pregunta 4

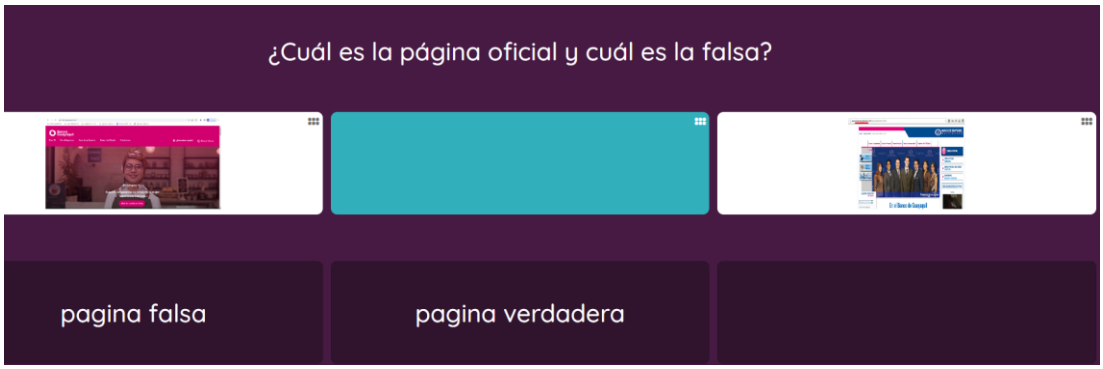


Visualización



Pregunta 5

Visualización

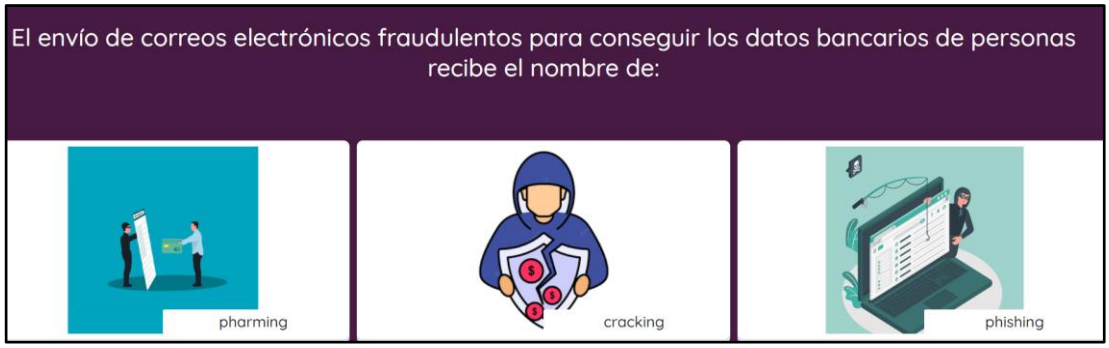


Pregunta 6

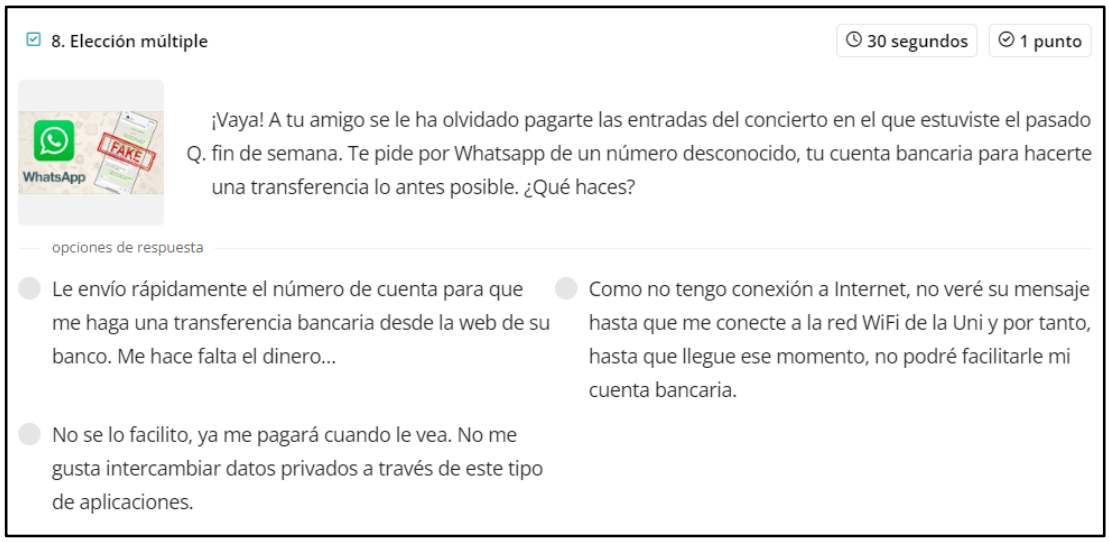
Visualización

Pregunta 7

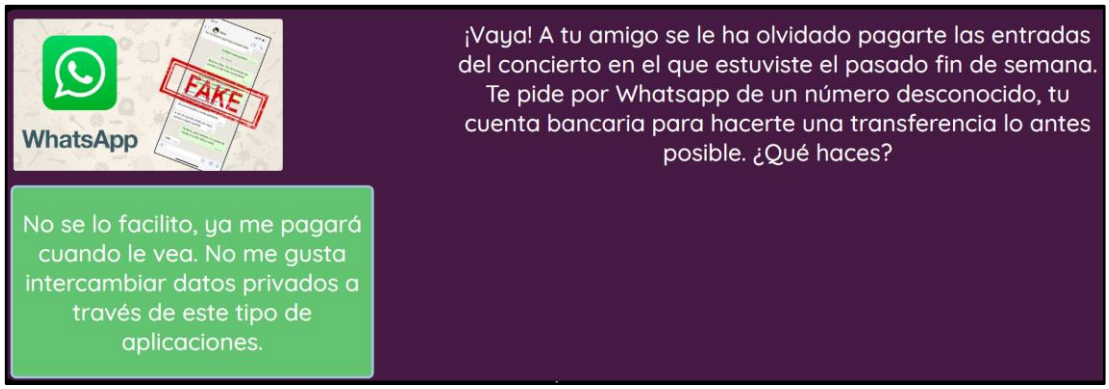
Visualización



Pregunta 8



Visualización



Pregunta 9

Visualización

Pregunta 10

Visualización

Pregunta 11

Visualización

A.4 Evaluación Teórica de Conocimientos en Google Forms.

Pregunta 1: ¿Qué es la Seguridad de la Información?

- La Seguridad de la Información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.
- Seguridad de la información se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y no proteger la información.

Pregunta 2: ¿Qué es la Ingeniería Social?

- La ingeniería social es un conjunto de técnicas que usan los cibercriminales para ayudar a los usuarios incautos.
- La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos.
- La ingeniería social es un conjunto de técnicas que usan los cibercriminales para colaborar a los usuarios incautos.

Pregunta 3: El envío de correos electrónicos fraudulentos para conseguir los datos bancarios de personas recibe el nombre de:

- Pharming
- Cracking
- Phishing

Pregunta 4: Las redes sociales son un servicio que te permite estar en contacto con otras personas, por eso…

- Compartes todo lo que haces con todos tus contactos, para eso es una red social.
- Eres cuidadoso con la información que compartes y tienes bien configurados los niveles de privacidad. No te apetece que tu vida se convierta en un "Gran Hermano".
- Aceptas todas las solicitudes de amistad que recibes, te gusta tener muchos amigos, así tus publicaciones tienen más éxito (más "me gustas", compartidos, etc.)

Pregunta 5: ¿En qué consiste la técnica del phishing?

- En el envío de un SMS masivo a todo los contacto de mi agenda.
- En el envío de correos electrónicos suplantando la identidad del remitente con finalidad de fraude.
- En un ataque que se realiza a los servidores de correo electrónico de una empresa.

Pregunta 6: Los enlaces que aparecen en un phishing suelen redireccionar al usuario a páginas web falsas o descargar malware:

- VERDADERO
- FALSO

Pregunta 7: Entre las siguientes opciones, ¿Cual dirías que es una contraseña robusta y segura?

- 1234567890
- P3rr0grandeX11!
- micontraseña

Pregunta 8: Son importantes las URL para detectar páginas fraudulentas?

- VERDADERO
- FALSO

Pregunta 9: He recibido un mensaje privado a través de mis redes sociales, donde un desconocido me advierte de que tiene en su poder un video mío comprometido junto a un enlace de descarga. Además, me pide que haga un pago o lo difundirá. ¿Qué hago?

- Me asusto mucho y realizo el pago. Más vale prevenir.
- Me parece muy raro, pero me pica la curiosidad y abro el enlace.
- Desconfío, no abro el enlace, ni realizo el pago.

Pregunta 10: ¿Cuál de las siguientes opciones crees que es una web segura?

- http://paginaweb.com
- segura.paginaweb.com
- https://paginaweb.com