BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN

PREVENCIÓN DE LOS RIESGOS DE ATAQUES CIBERNÉTICOS POR PHISHING

T E S I S

Tesis presentada para obtener el grado de:

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

Presenta:

ROSA SUAREZ CALDERON

Asesor 1 de tesis:

M.C. ADRIANA HERNÁNDEZ BERISTAÍN

Asesor 2 de tesis:

DRA. Erika Annabel Martínez Mirón

Puebla, Puebla **OCTUBRE, 2024**

Agradecimientos

1. A mis padres y familia

Principalmente, agradezco profundamente a mis padres el Sr. Urbano Suarez Rojas y a la Sra. Piedad Calderón León por haberme brindado su apoyo y por siempre creer en mí. Gracias a ustedes y a su esfuerzo, hoy estoy aquí. Con su cariño, paciencia y valores, me han impulsado a siempre perseguir mis metas y a nunca abandonarlas pese a las adversidades. Vale decir, que este logro es por y para ustedes, puesto que ustedes nunca me dejaron sola y siempre estuvieron apoyándome tanto moral como económicamente, teniendo en cuenta que, solo ustedes son conscientes de las dificultades que enfrentaron para que yo pudiera alcanzar este logro.

Por otro lado, agradezco a mis hermanos, cuñados y sobrinos, por brindarme su apoyo durante todo el recorrido de la carrera. En especial agradezco a mi cuñado Benito Pérez Flores y a mis hermanos Cesar Suarez Calderon, Rufina Suarez Calderon y Sandra Suarez Calderon por apoyarme tanto económicamente como moralmente. Gracias por siempre seguir mis pasos y nunca dejarme sola. Sobre todo, gracias por siempre creer y confiar en mí.

2. A mis amigos

Agradezco a mis amigos, Ana Laura Torres Marín, Alfredo de Jesús Ramos Benavides y Carlos Daniel Cruz Pino, puesto que siempre estuvimos juntos desde el inicio de la carrera hasta el final de la carrera. Gracias por no dejarme sola y siempre apoyarme. Sobre todo, por no permitir que desertara de la carrera. Gracias por sus palabras de aliento, por sus consejos y sus enseñanzas. Aprendí mucho de cada uno de ustedes. Agradezco su tiempo, las horas compartidas, los trabajos realizados en conjunto y, sobre todo, gracias por las historias vividas dentro y fuera de la Universidad.

3. A mi tutora y CO-Asesor

Agradezco profundamente a mi tutora la M.C. Adriana Hernández Beristaín por su voto de confianza para llevar a cabo este proyecto, agradezco su dedicación, paciencia y comprensión. Agradezco su apoyo durante todo el tiempo que estuve realizando mi tesis, sin sus palabras, conocimientos y correcciones no hubiese podido lograr mi objetivo. Gracias por aceptar ser mi

tutora y sobre todos, gracias por sus consejos. Es una gran persona, maestra y tutora. ¡Muchas gracias M.C. Adriana Hernández Beristaín!

Sin duda, también agradezco a la Dra. Erika Annabel Martínez Mirón, a la Dra. Guillermina Sánchez Román y al Dr. Abraham Maldonado García por ser mis revisores de tesis. Agradezco su apoyo, sin su ayuda no hubiese logrado mi objetivo. ¡Gracias!

4. A mis profesores

Fueron muchos los profesores que formaron parte de mi instancia durante la Universidad, a todos y cada uno de ellos les agradezco por ser parte esencial de mi camino y por transmitirme los conocimientos necesarios para hoy estar aquí. Gracias por sus regaños, por sus consejos y sobre todos por sus enseñanzas. ¡Muchas Gracias!

Tabla de contenido

Capítulo 1
Introducción

1. Introducción

1.1. Resumen

En el presente proyecto de tesis se muestra la funcionalidad de un ataque por phishing, se configura un dominio de correo electrónico para simular de manera precisa como se le envía a un usuario un correo apócrifo y como este lo recibe, logrando así un ataque focalizado; el documento se encuentra redactado de la siguiente forma, se puede observar la descripción de los capítulos en el siguiente orden y contenido.

En el capítulo 1 se encuentra el planteamiento del problema, justificación, objetivo general y objetivos específicos.

En el capítulo 2 se considera el estado del arte, donde se presentan las diferentes estadísticas de los ataques de phishing, según las organizaciones de EasyDMARC, Condusef, McAfee y Banca Santander. También se habla sobre la comparación de las tendencias de ataques por phishing mediante un cuadro comparativo y los métodos utilizados en los ataques de phishing. Se explican también las diferencias entre las técnicas de suplantación de identidad mediante un cuadro comparativo y se describen los ataques de phishing. Por último, el capítulo muestra un cuadro comparativo con las diferencias existentes entre los tipos de ataques de phishing.

En el capítulo 3 se muestra la metodología de Srum utilizada en el proyecto de tesis y los requerimientos de hardware y software. También se habla sobre la distribución de Kali Linux utilizada, la herramienta de Gophish y por último se mencionan las ventajas y desventajas de la herramienta utilizada para el ataque focalizado.

En el capítulo 4 se explican las etapas de análisis y diseño, se instala Kali Linux y Windows 11, para luego usarse ambos Sistemas Operativos para simular el cliente y servidor de correos. Se diseña el formato de repositorio que será utilizado para las guías de referencia. Así, el capítulo muestra la creación de los 6 primeros repositorios que servirán de referencia para identificar y solucionar los ataques mediante phishing.

En el capítulo 5 se muestran las pruebas consideradas para el funcionamiento de la campaña por phishing de la empresa de Afore Rosa ficticia que se utiliza para el ataque focalizado, este capítulo también muestra los resultados obtenidos con la campaña de manera funcional y satisfactoria.

En el capítulo 6 se exponen las conclusiones tras realizar el proyecto y haber cumplido los objetivos específicos y generales del proyecto de tesis, se representan las opciones de trabajo a futuro para quien desee continuar el proyecto, pueda realizar mejoras u otras opciones de campaña.

En el capítulo 7 se expone la bibliografía de apoyo utilizada para la investigación del proyecto de tesis.

1.2. Planteamiento del problema

En el mundo entero el phishing sigue siendo uno de los principales vectores de amenaza que los Ciberdelincuentes utilizan para introducirse en organizaciones de todo el mundo. Este tipo de ataques experimento un aumento del casi 50% a lo largo del 2022. Los sectores más afectados fueron educación, finanzas y gobierno. El ranking del país que más phishing reciben lo encabeza Estados Unidos. [1].

En América Latina también se presentan ataques por phishing. El phishing se sextuplico en América Latina con el reinicio de la actividad económica y el apoyo de la IA. El panorama de amenazas para el 2023 de Kaspersky también revela un aumento del 50% en los ataques de troyanos bancarios en la región, lo que equivale a 5 ataques por minuto. [2].

El reciente panorama de amenazas para América Latina de Kaspersky (que analizo datos de junio de 2022 a Julio de 2023 y junio de 2021 a Julio de 2023) muestra que, la actividad delictiva en la región se mantiene estable mientras que los ataques de malware de computadoras y dispositivos móviles han experimentado un aumento del 61.7% y del 50% en cuanto intentos de ataques por phishing y troyanos bancarios, respectivamente. Los sectores de gobierno y finanzas son los más afectados, al igual que los internautas. [2].

En México también se presentan ataques por phishing. México es uno de los países que recibe la mayor cantidad de ataques Cibernéticos en América Latina. De hecho, las estadísticas muestran un

crecimiento histórico: en 2022 hubo 187,000 millones de intentos de ciberataques, un crecimiento de 20% frente a 2021. En 2023 en México se incrementaron 63% los ataques Ransomware. De acuerdo con un informe de Apolo Alto Networks, en el país se cometieron 42 ataques Ransomware en 2023, 16 más que el año anterior, representando un crecimiento del 61.5%, siendo el principal responsable de estos ataques en grupo criminal de hackers Lokbit 3.0. [2].

De acuerdo con el estudio sobre el estado global de la ciberseguridad de 2023: México, de Inflobox, las Ciberamenazas más urgentes en los próximos 12 meses en el país serán:

- Fugas de datos (51%).
- Ataques directos a través de servicios en la nube (43%).
- Ataques a través de desconexiones de trabajadores remotos (35%).
- Amenazas avanzadas persistentes (27%).
- Ataques a través de IoT en la Red (21%).

El reporte de Infoblox también encontró que son tres principales vectores de ataque a Organizaciones: Correo electrónico/Phishing (59%); Ransomware (54%) y terceros/Cadena de Suministro (56%). [2].

En Puebla los reportes sobre delitos cibernéticos aumentaron un 22.2% en 2022, más que en 2021, de acuerdo a los resultados del Censo Nacional de Seguridad Pública Estatal 2023. 450 personas señalaron suplantación de identidad. [3].

Por otra parte, fueron identificados 3 mil 896 sitios web y se gestionó su desactivación, debido a que en 784 sitios web se detectó que cometían fraude en compras por internet. Otros eran sitios phishing que robaban información y propagaban códigos maliciosos, en 78 sitios web robaban datos financieros y personales. 65 sitios web eran de fraudes nigeriano. Este último consiste en que delincuentes envían mensajes vía correo electrónico, haciéndose pasar por integrantes de la realeza de Nigeria y piden dinero para poder sacar su supuesta fortuna de ese país. También se detectaron 49 páginas que cometían fraude por tramite de documentos, como actas de nacimiento, cartillas y pasaporte; y otras más propagaban códigos maliciosos y perpetuaban fraude por contratación de

servicios e inmuebles ficticios. En la actualidad Puebla se ubica en el quinto lugar con un total de 8 mil delitos cibernéticos. [3].

En la Comunidad Universitaria de la Facultad Ciencias de la Computación y público en general, por lo menos, tres de cada setenta y cinco personas han sido víctimas de ataques por phishing. Para obtener estos resultados se realizó dos encuestas, ambas tituladas con el mismo nombre “Ataques por Phishing”, con la diferencia de que una se realizó con el correo de Gmail y la otra con el correo Institucional de la Universidad. Una vez, realizadas las encuestas, se generaron dos QR´s, los cuales posteriormente se compartieron a la Comunidad Universitaria y público en general. Los resultados obtenidos se encuentran de la página 118 a la página 123 de este documento.

Esta problemática se presenta porque a menudo los usuarios no están enterados que han sido víctimas de ataques por phishing, esto puede ser porque no conocen de esta palabra o el significado de esta. [4]. Otra razón es porque los usuarios no saben a quién o con quien acudir cuando les ocurre este suceso o porque no saben si dicho ataque se debe de denunciar y, por lo tanto, terminan por dejar la situación por la paz.

Si esta situación continua, lo que se espera es que seguirán día a día incrementando los ataques por phishing y los ciberdelincuentes seguirán suplantando la identidad de los usuarios con mayor facilidad y cada día serán más personas estafadas.

Se pretende dar una solución para mitigar los ataques por phishing y ofrecer a la Comunidad Universitaria de la Facultada Ciencias de la Computación y público en general una serie de pasos que apoyen a la prevención de ataques de este tipo, esto a través de la concientización de la existencia de este tipo de ataque, los riesgos que genera al no contar con la información puntual y significante, conocer cómo se lleva a cabo un ataque de este tipo y así poder evitar a lo más posible caer en un ataque por phishing, se presenta en las Redes Sociales de la Academia de Cisco BUAP capsulas informativas, formularios e información referente, esto es un periodo de tiempo desde el inicio del proyecto de tesis y de manera fija.

1.3. Justificación

El objetivo principal es analizar un ataque cibernético por phishing a partir de un ataque focalizado, usando Kali Linux y otras herramientas de ciberseguridad que tiene como fin concientizar y mejorar las técnicas de mitigación, considerando que el alcance de esta concientización sea para cualquier miembro de la comunidad BUAP o sociedad en general.

Por otro lado, se considera que cualquier usuario que no sea profesional del área de Ciencias de la Computación o áreas afines pueda apoyarse con la campaña de concientización.

“Debido a que el phishing es un problema que afecta a todo tipo de usuarios en la red ya que es un método de engaño para hacer que compartas contraseñas, número de tarjetas de crédito y otro tipo de información confidencial, haciéndose pasar por una identidad de confianza mediante un correo electrónico o bien un mensaje de texto” (Malware bytes, 2019). Se requiere que los estudiantes de la Facultad Ciencias de la Computación o cualquier estudiante de la Comunidad BUAP tengan información preventiva, y conozca cómo se realiza un ataque real, pero en un ambiente focalizado y al mismo tiempo ser parte de apoyo para la sociedad en general para reducir las estadísticas de este tipo de ataque cibernético.

En todo el país y el mundo entero las víctimas de phishing reciben un mensaje de correo o un mensaje de texto que suplanta la identidad de un persona u organización principalmente de confianza, como un banco diciendo **¡Felicidades, has sido ganador de un préstamo, para más información da clic aquí!** Formando parte de una sociedad responsable, se desea que, de manera real como se lleva un ataque que al igual que este ejemplo, pero haciéndose pasar por una organización bancaria, se comprenda como se genera esta gran estafa que los delincuentes cibernéticos realizan.

1.4. Objetivo general y específicos del proyecto

1.4.1. Objetivo General

Analizar un ataque cibernético por phishing a partir de un ataque focalizado, usando Kali Linux con el fin de concientizar y mejorar las técnicas de concientización.

1.4.2. Objetivos Específicos

- Identificar y analizar los conceptos de ataques por phishing.
- Realizar un estudio acerca de las principales técnicas de ataque por phishing.
- Generar un ataque focalizado usando Linux para mostrar su ejecución.
- Identificar las herramientas y procedimientos a seguir cuando ocurre un ataque de phishing.
- Elaborar un repositorio de guía que sirva de referencia para la identificación y solución de los ataques mediante phishing.

Capítulo 2
Estado del Arte

2. Alcance

“El avance tecnológico ha facilitado la vida en muchos aspectos, ya que gracias a la tecnología se pueden hacer cosas muy simples como video llamadas con personas al otro lado del mundo, chatear con amigos, investigar sobre temas desconocidos, hasta cosas muy complejas como operar pacientes desde un ordenador o ver satélites orbitando alrededor de la tierra”, (Orliman, O, 2018) hoy en día también se pueden realizar operaciones bancarias sin la necesidad de salir de casa, pero no esto es felicidad. Lo cierto es que, con los avances tecnológicos se han modernizado también los fraudes financieros y el robo de identidad. [5].

A continuación, se presentan las estadísticas según las organizaciones, EasyDMARC, Condusef, McAfee y Banca Santander.

2.1. Estadísticas de las organizaciones gubernamentales y privadas.

Para poder conocer cuál es la realidad alarmante de este tipo de ataques cibernéticos que se hacen en contra de toda la sociedad, este apartado presenta estadísticas formales que las organizaciones interesadas en hacer conciencia realizan con el objetivo de evitar se realicen acciones que pongan en riesgo la identidad, datos sensibles e integridad de los usuarios que diariamente hacen unos de la red de internet sin tomar en cuenta consideraciones de seguridad.

Las estadísticas de las empresas y organizaciones que se analizan son las siguientes, primeramente, es oportuno hablar de quienes son las organizaciones y empresas.

1) **EasyDMARC:** Proveedor líder de DMARC con oficinas en EE. UU., Países Bajos y Armenia estamos comprometidos a garantizar la seguridad de las empresas en el Ciberespacio. [6].
2) **(CONDUSEF): La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros**, es el organismo público descentralizado de la Administración Pública Federal encargado de la protección y defensa de los derechos e intereses del público usuario de los servicios financieros, que presentan las instituciones públicas, privadas y del sector social debidamente autorizadas, así como de regular la organización, procedimiento y funcionamiento de la entidad pública encargada de dichas funciones. [7].

3) **Banco Santander:** Santander México es uno de los grupos financieros líderes en el país, centrado en la transformación comercial y en la innovación. Su negocio está enfocado en una Banca Minorista, con fuerte integración con Banca Mayorista, lo que se suma al impulso de los negocios de Banca Privada, Gestión de Activos y Seguros. [8].
4) **McAfee:** McAfee, LLC. Es una compañía de software especializada en seguridad informática cuya sede se encuentra en Santa Clara, California. Su producto más conocido es el antivirus. [9].

2.1.1. Estadísticas sobre los ataques de phishing por EasyDMARC

El phishing lidera la lista de los ataques cibernéticos tanto en volumen, como en tasa de éxito, de acuerdo con las **estadísticas de phishing** de la empresa Verizon.

1) El 93% de los ataques en línea exitosas comienzan con un ataque de phishing selectivo. El 96% de todos los ataques de este tipo llegan por mensaje de correo electrónico.
2) Durante la primera mitad del año 2022, la plataforma de EasyDMARC bloque más de 90 millones de ataques de phishing. El 89% de sus clientes informaron haber experimentado ataques de phishing en el mismo periodo.
3) La industria financiera es la más atacada a nivel mundial, con un aumento trimestral del 5.8% en el número de ataques.
4) Holanda lidera la lista de países que está bajo la mira de ataques de phishing, le sigue Rusia, Moldavia, Estados Unidos y Tailandia.
5) El porcentaje de ataques por phishing detectados por EasyDMARC aumento un 62,9% en comparación con el año 2021, lo cual representa un aumento trimestral del 30%.
6) EasyDMARC puso más de 20 millones de correos electrónicos en cuarentena en 2022. (EasyDMARC, 2022). [10].
7) A nivel mundial, de los ataques de phishing en 2023 se realizaron a través de correo electrónico. Ocasionalmente utilizando otros métodos de comunicación, como mensajes de texto, teléfono o redes sociales. [11].

2.1.2. Estadísticas sobre ataques de phishing emitidos por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)

De acuerdo con la Asociación de Bancos de México (ABM), los casos de **robo de identidad**, a través de suplantación de páginas digitales de las instituciones financieras, han tenido un crecimiento importante y son las personas adultas mayores, las más vulnerables.

1) El **robo de identidad** en personas adultas mayores representa el 35% de los casos, y es que, informes de la ABM, este tipo de ataque está más enfocado en los usuarios que en las instituciones.
2) El registro de reclamaciones por este tipo de fraudes en la CONDUSEF, fue de 49 mil 871 en 2021, lo que representa el 1% del total de las quejas registradas en ese año.
3) Representa un 54% sobre este tipo de estafa, respecto al periodo del 2020. (CONDUSEF, 2022).
4) De 2020 a finales de 2022, la CONDUSEF registró un total de 391 mil 182 controversias por posible fraude, deteniendo un incremento en el fraude cibernético, el cual, podría derivarse principalmente por el aumento del comercio electrónico y las transferencias vía electrónica.
5) Tan solo, durante 2022, el 62.3% de las controversias correspondieron a la banca múltiple (134,433). –De esa cifra, 30.5% fueron asuntos presentados por personas adultas mayores (41,051) y de éstos, el 50.5% (20,745) se originaron por un posible fraude. [12].
6) La CONDUSEF informa que durante febrero y marzo de 2023, 32 instituciones financieras debidamente constituidas e inscritas en el SIPRES, fueron víctimas de suplantación de identidad. [13].

2.1.3. Estadísticas sobre los ataques de phishing según Banca Santander

Una parte importante de la digitalización es la ciberseguridad: La capacidad de protegerse, detectar y responder a los ciberataques que suceden a diario. Estos ataques pueden ir dirigidos a los ordenadores, servidores, redes, sistemas, etc. Para conseguir información

muy valiosa para la empresa, obtener beneficios financieros o simplemente para atemorizar e impedir el correcto funcionamiento de estas.

Unos datos muy interesantes que sirven para entender mejor la situación de seguridad online de las **pymes** y ponerlo en perspectiva son las siguientes:

1) El 70% de los ciberataques en España van dirigidos a pymes.
2) Las pymes tardan en promedio de 212 días en identificar un ataque y 75 días más en contenerlo.
3) El costo promedio de un ciberataque es España es de 35.000€.
4) El 60% de las pymes víctimas de ciberataques severos desaparecen en los 6 meses posteriormente incidente.
5) El 99.8% de las pymes españolas no se consideran n objetivo atractivo para ciberataque.
6) El 91% de los ciberataques comienzan por un email de phishing.
7) En 2021 se alcanzó un pico histórico según los registros de informe Phishing **Activity de APWG**, con 245.771 páginas fraudulentas utilizadas para estafas de phishing detectadas en un mismo mes. A demás, se mantiene una curva ascendente y continua en estas actividades maliciosas.
8) Por otra parte, según el informe **Attack Landscape Q1 2021 de F-Secure** el sector financiero es el más afectado: en conjunto, cerca de un 40% de los ataques fueron dirigidos contra bancos, sistema de pago y comercios online. [14].
9) Para 2024 más de 3 mil millones de personas utilizan la banca online con la tranquilidad de que la criptografía, algoritmos altamente complejos que encriptan los datos, mantengan segura su información personal y financiera. Sin embargo, los estándares de encriptación actuales podrían volverse obsoletos pronto. Santander, la banca financiera está entre los líderes de un empuje global para elevar la seguridad online a un nuevo nivel de sofisticación. [15].

2.1.4. Estadísticas sobre los ataques de phishing McAfee

El tema predominante en 2022 es, sin duda, la magnitud y el impacto que los ataques contra la ciberseguridad han tenido en nuestra sociedad en general.

1) El informe sobre amenazas de McAfee Labs de abril de 2021 reveló que, las detecciones de ciberataques relativos a la COVID aumentaron un 114% en el tercer y cuarto trimestre de 2020.
2) La investigación también muestra que los intentos de phishing relacionados con este tema aumentaron un 33% en junio del 2022.
3) McAfee Labs contabilizó 458 incidentes de seguridad hechos públicos en el primer trimestre de 2020, incluidos los que no se distinguía la región atacada, lo que supone un aumento del 41% respecto al 4° trimestre de 2019.
4) Los incidentes que afectaron a Norteamérica aumentaron un 60% respecto al trimestre anterior, mientras que en Europa descendieron un 7%.
5) Los incidentes que afectaron a Estados Unidos durante el 1.er trimestre de 2020 aumentaron un 61%, en Reino Unido descendieron un 55% y en Canadá aumentaron un 50% respecto al trimestre anterior.
6) Los incidentes comunicados durante el primer trimestre de 2020 que afectaron a varios sectores aumentaron un 94%.
7) El sector público experimento un aumento del 73%, el sector de particulares a autónomos un 59%, y el de la fabricación un 44%, mientras que los incidentes en el sector de ciencia y tecnología descendieron un 19%. [16].
8) En el año 2024 ha continuado la evolución de las estafas informáticas, que probablemente no se ralentizará, así como una mayor adopción de Chrome como Sistema Operativo. La introducción de herramientas de inteligencia artificial (IA) fáciles y accesibles para prácticamente cualquiera que tenga un celular o una computadora portátil. [17].

2.2. Comparación de las tendencias de ataques de phishing

Muchas de las organizaciones tanto en México como en el mundo están interesadas en aportar información referente a las tendencias actuales. La tabla 1 muestra algunas de las más importantes técnicas de ataques por phishing.

Tabla 1. Técnica de comparación de ataques de phishing

No.	Nombre de las Organizaciones Gubernamentales y Privadas	Comparativa Tipología de Incidencias
1	EasyDMARC	Ataques en línea/Ataques por mensajes de correo electrónico/La industria financiera es la más atacada a nivel mundial.
2	Condusef	Ataques a través de suplantación de páginas digitales/Robo de identidad a personas mayores/Fraudes cibernéticos.
3	Banca Santander	Ataques a las Pymes/Ataques por mensajes de correo electrónico/Ataques por pago y compras Online.
4	McAfee	Ataques a público en general/Ataques por fraude.

Nota. Tabla construida a partir de la técnica de comparación de ataques de phishing (2024).

2.3. Métodos utilizados en el ataque de phishing

Tendencias y técnicas de suplantación de identidad (Phishing)

"Los ataques de suplantación de identidad son estafas que a menudo usan los ciberdelincuentes como señuelo y así robar su identidad. La comunidad de apariencia legitima es normalmente mediante el correo electrónico, ya que este se vincula a un sitio de suplantación de identidad (phishing). Un sitio de suplantación de identidad suele imitar las páginas de inicio de sesión, la cual requiere que los usuarios escriban credenciales e información de la cuenta" (Aarp, 2018). A continuación, el sitio de suplantación de identidad de captura la información confidencial en cuanto

el usuario la proporciona, y esto hace que los ataques tengan acceso a la información. [18]. Esto acontecía en 2018. Hoy las cosas han ido cambiando.

A continuación, se muestran ocho técnicas de suplantación de identidad más comunes que los atacantes emplean hoy en día, para intentar robar información u obtener acceso a los dispositivos.

2.3.1. Suplantación de identidad de factura

En esta estafa, el atacante intenta atraerle con un correo electrónico como su nombre lo indica, que tiene una factura pendiente por pagar ya sea de un proveedor o una empresa conocida. A continuación, proporciona un vínculo para que pueda acceder a la factura y pagarla. Cuando accede al sitio, el atacante estará listo para robar su información personal y fondos. [19].

2.3.2. Estafa de pago/entrega

En este método de ataque se pide que proporcione una tarjeta de crédito, débito u otra información personal y así su información de pago se pueda actualizar con un proveedor conocido comúnmente. Después se solicita la información para que se puede realizar la entrega de la mercancía ordenada. Puede que se familiarice con una empresa y haya hecho negocios con ellos en algún momento. Sin embargo, no es consciente de los artículos que compró recientemente. [20].

2.3.3. Estafas de phishing con temáticas fiscal

Una estafa de suplantación de identidad común del Servicio Interno de Rentas (IRS) se realiza mediante una carta de correo electrónico urgente que indica que debe dinero al IRS. A menudo, el correo electrónico amenaza con acciones legales si no accede al sitio a la brevedad y paga sus impuestos. Al acceder al sitio, los atacantes roban su número de tarjeta de crédito personal o incluso roban su información bancaria y purgar sus cuentas. [21].

2.3.4. Descargas

En este método un atacante envía un correo electrónico fraudulento el cual solicita que abra o descargue los datos adjuntos de un documento, como por ejemplo un PDF. Lo cual estos

datos adjuntos suelen contener un mensaje el cual pide que inicie sesión en otro sitio web, como por ejemplo sitios web de correos electrónicos o de uso compartido de archivos, para así abrir el documento. Cuando se accede a estos sitios de suplantación de identidad con sus credenciales de inicio de sesión, el atacante tiene acceso a su información y puede obtener información personal o adicional. [22].

2.3.5. Correos electrónicos de suplantación de identidad que proporcionan otras amenazas

Los correos electrónicos de suplantación de identidad suelen ser eficaces, por lo que los atacantes a veces los usan para distribuir ransomware a través de vínculos o datos adjuntos en los correos electrónicos. Cuando se ejecuta, el ransomware cifra los archivos y muestra una nota de rescate, la cual le pide que pague una suma de dinero para acceder a sus archivos.

Se han visto correos electrónicos de phishing los cuales tienen vínculos a sitios web de estafa de soporte técnico. Estos sitios web usan varias técnicas de miedo para engañar y así llamar a las líneas de acceso directo y pagar “servicio de soporte técnico” innecesarios que supuestamente corrigen problemas derivados de dispositivos, plataformas o software. [23].

2.3.6. Phishing de objetivos definido

El phishing de lanza es un ataque dirigido que implica contenido de señuelo personalizado. Normalmente, los atacantes realizan un trabajo de reconocimiento mediante una encuesta de redes sociales y otros orígenes de información sobre su objetivo previsto.

El phishing de lanza implica engañar a los usuarios para que inicien sesión en sitios falsos y divulgue credenciales. También, puede atraer a abrir documentos haciendo clic en los vínculos que instalan automáticamente malware. Con este malware instalado en su equipo de cómputo, los atacantes pueden manipular de forma remota el equipo infectado.

El malware implantado sirve como punto de entrega para un ataque más sofisticado, conocido como una amenaza persistente avanzada (APT). Las API están diseñadas para

establecer el control y robar datos durante periodos prolongados. Por lo que, los atacantes pueden intentar implementar herramientas de piratería más encubiertas, moverse literalmente a otros equipos de cómputo, poner en peligro o crear cuentas con privilegios y filtrar periódicamente información de redes en peligro. [24].

2.3.7. Ballenas

La caza de ballenas es una forma de suplantación de identidad dirigidas a ejecutivos de alto nivel o altos ejecutivos dentro de empresas específicas para obtener acceso a sus credenciales o información bancaria. El contenido de correo electrónico puede escribirse como una situación legal, una queja del cliente u otro problema ejecutivo. Este ataque también puede dar lugar a un ataque APT en una organización. [25].

2.3.8. Compromiso de correo electrónico empresarial

El compromiso por correo electrónico empresarial (BEC) es una estafa sofisticada que se dirige a empresas que con frecuencia trabajan con proveedores extranjeros o realizan transferencias bancarias. Uno de los esquemas más comunes utilizados por los atacantes de BEC implica obtener acceso a la red de una empresa a través de un ataque de phishing de lanza. El atacante crea un dominio similar a la empresa a la que se dirige, o suplanta su correo electrónico a los usuarios estafados para que liberen información de la cuenta personal para transferencias de dinero. [25].

2.4. Diferencias entre técnicas de suplantación de identidad

Actualmente un ciberdelincuente usa las técnicas de suplantación antes mencionadas, en la tabla 2 se presentan las frecuencias de uso de dichas técnicas.

Tabla 2. Técnica de suplantación de identidad

No.	Técnica de suplantación de identidad	Frecuencia en 2022-2024	Observación
1	Suplantación de identidad	El fraude les costó a 40 millones de personas un total combinado de $43,000 millones.	Se usa comúnmente en fraudes de facturas/pagos.
2	Estafa de pago/Entrega	Reportaron $330 millones en pérdidas por estafas.	Se usa comúnmente en fraude por compras por internet.
3	Estafas de phishing con temática fiscal	El fraude provoco la pérdida de $770 millones de IRS.	Se usa comúnmente en fraude de servicio interno de rentas (ISR).
4	Descargas	Reportaron 93,1 millones de personas usuarias de internet en México, lo que represento el 78,6% de la población de 6 años o más.	Se usa comúnmente en fraudes de descargas.
5	Correos electrónicos de suplantación de identidad (Phishing) que proporcionan otras amenazas	La taza de asaltos aumento a 0.82 por cada mil buzones.	Se usa comúnmente en fraude de suplantación de correos electrónicos.
6	Phishing de objetivo definido	Los consumidores presentaron más de 95,0000 quejas de esta índole.	Se usa comúnmente a los ataques mediante una encuesta de redes sociales.
7	Ballenas	En el sistema de caza de la corte de distrito de los EEUU, 20.000 CEO´s fueron comprometidos. Aproximadamente 2,000 de ellos fueron víctimas de este esquema.	Se usa comúnmente en la suplantación de identidad dirigidas a ejecutivos de alto nivel o altos ejecutivos dentro de una empresa especifica.
8	Compromiso de correo electrónico empresarial	La frecuencia de estos asaltos aumento un impresionante 84%.	Se usa comúnmente en fraude de correos electrónicos empresariales.

Nota. En esta tabla se habla sobre las diferencias entre las técnicas de suplantación de identidad, la frecuencia y a quienes van dirigidos los ataques cibernéticos (2024).

2.5. Descripción de los ataques de phishing

A medida que la tecnología avanza y se manifiesta, aparecen nuevas técnicas las cuales son utilizadas por los atacantes y así recopilar información la cual les será útil al momento de robar su identidad y conseguir alguna retribución económica. Actualmente, se habla de un concepto denominado phishing, el cual puede ser definido como un modelo de abuso informático que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta y a través de un sistema de mensajería electrónica. Es decir, un estafador (conocido como phisher) el cual se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial con el usuario, un correo electrónico o algún sistema de mensajería instantánea.

Hace años, un correo electrónico infectado usaba trucos simples, como incorporar al correo un enlace que llevaba al lector a una dirección diferente a la indicada en su texto o una URL con errores tipográficos que lo diferenciaba del enlace original solo por un carácter o un par de caracteres transpuestos.

Actualmente, los hackers o phisher han mejorado sus técnicas para distribuir malwares o virus y ocultar sus ataques mediante una amplia variedad de herramientas y así robar datos personales y claves de acceso. En algunas oportunidades eligen un sitio, compran certificados falsos para crear el sitio (https), copian las imágenes el diseño y distribución de la página del sitio “real”, haciendo difícil que el usuario se dé cuenta de estos trucos a simple vista, logrando que las victimas hagan clic en enlaces de mensajes sin pensar. [27].

Fig. 1 Creación propia.

A continuación, se describen cuatro tipos de ataques de phishing más comunes y peligrosos.

2.5.1. Whaling

Es un tipo de phishing más focalizado y es denominado como **whaling o suplantación**, y tiene como objetivo enviar un mensaje por el cual se hace pasar por autoridad, jefe o ejecutivo importante de alguna institución. El mensaje parecerá que proviene de dicha persona, creando un contenido o historia muy realista, pero en realidad es solo una dirección falsa o una dirección que contiene una parte del nombre de dicha persona. **Por lo general, un ataque de este tipo busca dinero**, como se puede observar en la Fig. 1 el atacante pide a la víctima que transfiera fondos de la institución a la cuenta del estafador. [27].

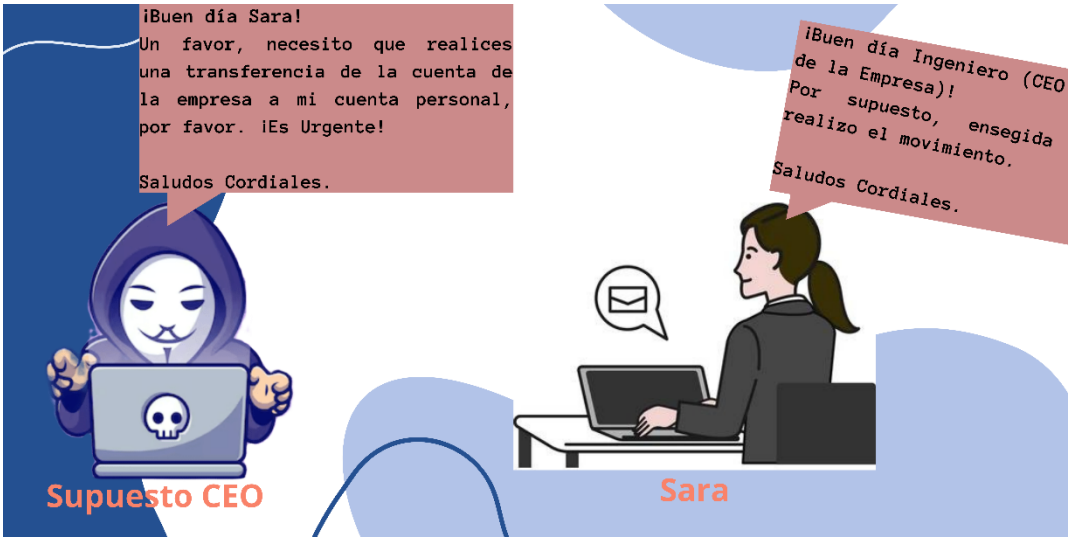

Fig. 2 Creación propia.

2.5.2. Spear phishing

Otro método es el **spear phishing**, donde una persona, hacker, phiser o estafador persigue a una persona en particular, organización o puesto muy específico dentro de una institución o empresa. El estafador incluye en el correo el nombre, la posición, la institución, el número de teléfono del trabajo y otra información del objetivo, como se puede observar en la Fig. 2 el atacante en un intento por **engañar al destinatario haciéndole creer que lo conoce o que tiene una relación existente con este, esto para ganar su confianza**. Generalmente el objetivo de atacante es buscar datos confidenciales que puedan realizar para explotar o vender en el mercado negro. [27].

Fig. 3 Creación propia.

2.5.3. Pharming

El **pharming**, es otro método, donde el tráfico de navegación, enlazado o no desde un correo recibido, se redirige para que el usuario piense que está navegando en el sitio deseado, pero en realidad está conectado al sitio web del hacker. Este ataque se utiliza para conseguir credenciales o para obtener información y así **apropiarse de la identidad de alguien**.

Una forma de identificarlo es, leer la URL antes de hacer clic en el enlace o bien instalar en el computador un antivirus actualizado que detecte y elimine el malware que está redirigiendo su navegación o que permita chequear los enlaces fraudulentos y generar una alarma antes de cargar el sitio. [27].

Fig. 4 Creación propia.

2.5.4. Smishing

Otro método es el **smishing**, es una combinación de técnicas de ingeniería social que se envían a través de mensajes de texto SMS en lugar de utilizar el correo electrónico. Los estafadores intentan hacer creer que son de confianza, como contactos de su banco, por ejemplo, para que luego proporcione datos de su cuenta. En casos recientes, un estafador lo lleva a usar la autenticación paso a paso de su banco para enviarle un texto real con una consulta de autenticación, la cual, el phiser utiliza para poner en peligro su cuenta.

Una variación de este método es el **whishing, donde se utiliza WhatsApp** como un medio de phishing, mediante el envío de mensajes rápidos para ofrecer promociones con origen de marcas conocidas. [27].

Fig. 5 Creación propia.

2.6. Diferencias entre los tipos de ataques de phishing

Actualmente un ciberdelincuente usa algunos de los diferentes tipos de ataques de suplantación antes mencionadas, en la Tabla 3 se presentan las frecuencias de uso de dichas técnicas.

Tabla 3. Usuarios vulnerables a los tipos de ataques

No.	Tipos de ataques de phishing	Tipos de usuarios vulnerables
1	Whaling	Dirigidos a corporativos/Empleados de alto nivel dentro de una empresa.
2	Spear Phishing	Dirigidos a personas/organizaciones/Empresas específicas.
3	Pharming	Dirigidas a usuarios que navegan por internet.
4	Smishing	Dirigidos a todo público en general.

Nota. En esta tabla se habla sobre los diferentes tipos de ataques de phishing y a las personas a las que van dirigidos (2024).

Capítulo 3
Marco Teórico

3.1. Metodología Scrum

El presente proyecto se implementó haciendo uso de una distribución de Linux para montar sobre el un servidor de correo electrónico, se hicieron pruebas sobre la distribución de Kali Linux y Ubuntu, tomando como decisión del uso de Kali ya que Kali es una distribución Linux basada en Debían diseñada para la auditoria de seguridad. Se utiliza como una herramienta para realizar pruebas de penetración, así como para realizar actividades relacionadas con el pentesting. Esta distribución Linux contiene una amplia gama de herramientas de seguridad, incluida Gophish motivo por el cual se decide por el uso de esta distribución

La metodología Scrum para este proyecto se basa en una investigación sobre el ataque por phishing, que consiste en técnicas combinadas con habilidades sociales, sobre plataformas tecnológicas, para una fuente confiable.

Se realiza una investigación previa para obtener información personal y/o de una organización, para así, ejecutar un ataque focalizado. Este procedimiento se ha convertido en un método de ataque frecuente para el robo de identidad y/o financiero debido a que se aprovechan del desconocimiento de la víctima en temas de seguridad, de las vulnerabilidades y combinando la facilidad de uso de herramientas disponibles para su ejecución.

La metodología Scrum es de 6 fases, cada una sustentada con un marco teórico, muestras de laboratorio y ejemplos de ataques de phishing enmarcados en repositorios guía que pretenden mitigar un ataque basado en phishing.

Fases

1) **Análisis**
    a. Se presenta la introducción, objetivos, alcance, estructura del trabajo, enfoque y relevancia del estudio.
    b. Se explican los distintos métodos utilizados en el ataque de phishing.
    c. Se describen los ataques de phishing sofisticados, basados en métodos tradicionales.

d. Se realiza una encuesta previa a nivel facultad para lograr estadísticas de conocimiento, de casos de estudio y lo referente a que tanto se tiene conocimiento de estos tipos de ataque.
e. Se realiza capacitación necesaria para lograr habilidades en el área de la ciberseguridad.
f. Se estructura de redacción del documento de tesis.

2) Planificación

a. Se planifican los tiempos de diseño para la creación de material formativo, material gráfico, repositorio ataque focalizado, implementación y entrega.
b. Se redacta el documento de tesis.

3) Formulación

a. Se realizarán entregables de avance.
b. Se instala Kali Linux.
c. Se realiza capacitación 1 sobre ataques cibernéticos (Certificación en Introducción a la Ciberseguridad de Cisco).
d. Se instala la herramienta Gophish.
e. Se configura Kali Linux.
f. Se redacta el documento de tesis.
g. Se realiza la capacitación 2 ataque por phishing (Certificación en Fundamentos del Hacking ético y Certificado de Análisis Forense Digital).
h. Se crea material formativo o repositorios 1, 2, 3.
i. Se crea material gráfico o capsula 1.
j. Se implementa el enfoque focalizado.
k. Se realiza el repositorio 4 sobre el ataque focalizado.
l. Se hacen propuestas de solución para garantizar la seguridad, por lo que se divide
m. en dos sub módulos los cuales son:
    i. Evaluación

ii. Pruebas de seguridad

n. Redacción del documento.

4) Producción

a. Se realiza diseño para los diferentes tipos de material gráfico y se comparten los resultados en redes sociales de Cisco Institucional.
b. Se desarrolla prácticas de laboratorio y se generan los repositorios 5 y 6 de las pruebas del ataque de phishing generando QR´s para la descarga pública.
c. Redacción del documento de tesis.

5) Test

a. Se genera test públicos dirigidos a la comunidad estudiantil antes y después de entregar el apoyo de mitigación de ataques por phishing.
b. Se realizan pruebas de usabilidad.
c. Se redacta el documento de tesis.

3.2. Requerimientos de hardware y software

3.2.1. Hardware

Tabla 4. Requerimientos de hardware

Nombre del Equipo	**Procesador**	**RAM**	**Sistema Operativos**	**Windows**
Lenovo	AMD A12	8.00 GB	Sistema Operativo de 64 bits, procesador basado en x64.	Windows 11 Home Single Language.

Nota. En esta tabla se muestra el hardware o especificaciones del equipo que se usó durante el proyecto de tesis (2024).

3.2.2. Software

Tabla 5. Requerimientos de Software

Software	Versión
Kali Linux	2023.2a de 64-bit
Gophish	Gophish-v0.12.1-linux-64bit

Nota. En esta tabla se muestra el software o especificaciones que se necesitó instalar, configurar y descargar para realizar el proyecto de tesis.

3.3. Sistema Operativo Kali Linux

Kali Linux es un proyecto iniciado en el año 2012, cuando Offensive Security decidió remplazar su proyecto venerable BackTrack Linux, el cual era manualmente mantenido, con algo que podría convertirse en un **derivado genuino de Debían**, completo con toda la infraestructura requerida y técnicas mejoradas para los paquetes. **Kali Linux es una distribución basada en Debían GNU/Linux diseñada para auditoria y seguridad informática**.

Desarrollo de la distribución Kali Linux

Kali Linux trae preinstalados más de 600 programas incluyendo **Nmap** (un escáner de puertos), **Wireshark** (un sniffer), **John the Ripper** (un crackeador de passwords) y la suite **Aircrackng** (software para pruebas de seguridad en redes inalámbricas). Kali se puede usar desde un CD, USB y también se puede instalar como sistema operativo principal. [28].

Tabla 6. Versiones actuales de Kali Linux

Versión	**Fecha**	**Lanzamiento**	**Núcleo**
Kali 2024.1	28 de febrero de 2024	Primer lanzamiento de Kali Rolling de 2024.	Núcleo 6.6.0, Xfce 4.18.4
Kali 2023.4	5 de diciembre de 2023	Cuarto lanzamiento de Kali Rolling 2023.	Núcleo 6.5.0, Xfce 4.18.4
Kali 2023.3	23 de agosto de 2023	Tercer lanzamiento de Kali Rolling 2023.	Núcleo 6.3.0, Xfce 4.18.4
Kali 2023.2a	6 de junio de 2023	Versión menor, soluciona el problema de UEFI en las imágenes base y corrige el sonido en las imágenes de Hyper-V.	Núcleo 6.2.0, Xfce 4.18.4
Kali 2023.2	30 de mayo de 2023	Segundo lanzamiento de Kali Rolling 2023.	Núcleo 6.1.0, Xfce 4.18.2
Kali 2023.1	13 de marzo de 2023	10 años! El primer lanzamiento de Kali Rolling 2023.	Núcleo 6.1.0, Xfce 4.18.1

Nota. En esta tabla se observan las versiones actuales de Kali Linux, para este proyecto se usó Kali 2023.2a.

3.4. Herramienta Gophish

3.4.1. Descripción de Gophish.

Gophish es una herramienta de código abierto que permite a los usuarios realizar campañas de ingeniería social con el fin de recopilar credenciales de autenticación y otros datos sensibles (phishing). Esta herramienta está diseñada para ser utilizada por los investigadores de seguridad para **mejorar la seguridad de la red**. Gophish fue creado en 2016 por Jordán Wright, un investigador de seguridad. [28].

3.4.2. Funcionamiento de Gophish

Gophish se ejecuta en un servidor, lo que significa que es necesario tener acceso a un servidor para poder usar la herramienta. Cuando la herramienta está configurada, puede usarse para crear simulacros de phishing con diferentes contenidos, como mensajes de correo electrónico, páginas web y mensajes de texto. Estos simulacros de phishing se envían a los destinatarios, que son los usuarios a los que se desea concientizar.

Los destinatarios reciben los simulacros de phishing y deben de tomar medidas para evitar caer en la trampa. Por ejemplo, algunos destinatarios pueden verificar la dirección de correo electrónico para asegurarse de que proviene de una fuente confiable. Si un destinatario cae en la trampa, Gophish registra esta información. [29].

Cuando se ejecuta la herramienta se inician dos servidores web, una base de datos y un agente en segundo plano, que gestionará el envío de correos electrónicos, como se observa en la Fig. 6 una vez que todo está disponible para iniciar basta con programar la campaña (página apócrifa donde se redirige a la víctima) y ver cuántos de empleados son “pescados”.

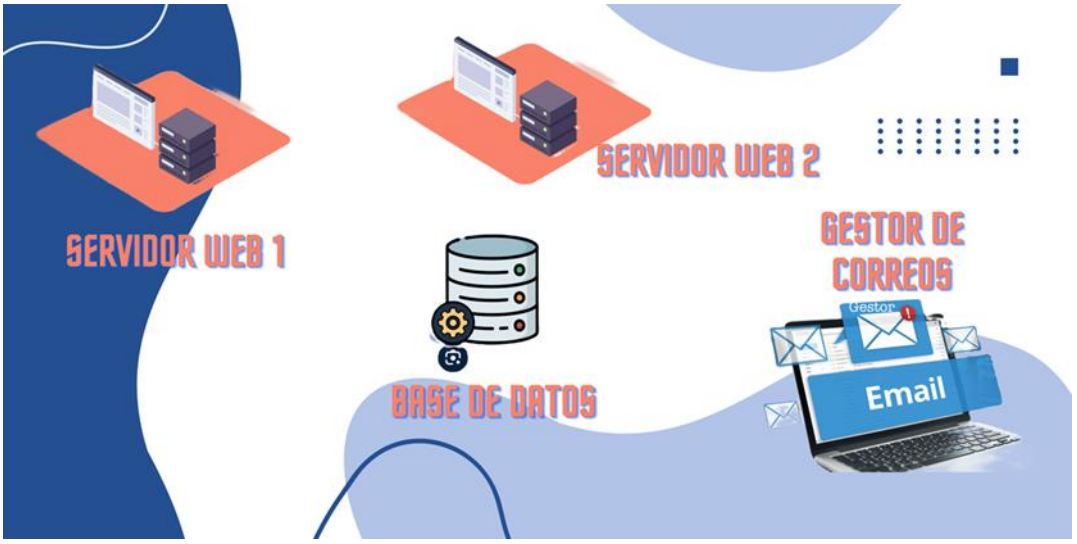

Fig. 6 Creación propia

Como se explica en los dos apartados anteriores Gophish es una herramienta valiosa y potente que sirve de prueba para los empleados de una empresa o institución que desee llevara a cabo un proceso de concientización, la herramienta lanza la simulación de ataques de phishing y con ella una empresa u organización es capaz de entregarle un entrenamiento de técnicas de Phishing al eslabón más débil que es el factor humano.

3.5. Ventajas y desventajas de Gophish

Gophish ofrece muchas ventajas a los usuarios, pero a pesar de estas, Gophish también presenta algunas desventajas. Las cuales son las siguientes:

Tabla 7. Ventajas y desventajas de Gophish

Ventajas de Gophish	**Desventajas de Gophish**
Facilidad de uso: Gophish es fácil de usar, lo que significa que los usuarios pueden comenzar a usar la herramienta con rapidez. Esto significa que los usuarios no tienen que aprender una nueva herramienta antes de poder comenzar a usarla.	Costo: Gophish es una herramienta de código abierto, pero es necesario tener acceso a un servidor para poder usar la herramienta. Esto significa que hay un costo asociado con el uso de la herramienta.
Informes de resultados: Gophish ofrece informes detallados sobre los resultados de las simulaciones de phishing. Estos informes incluyen datos sobre los destinatarios, los resultados de los simulacros y los pasos que se pueden tomar para mejorar la concienciación de la seguridad de los usuarios.	Experiencia técnica: Gophish requiere una cierta experiencia técnica para poder configurar y usar la herramienta correctamente. Esto significa que los usuarios pueden tener problemas si no tienen suficiente experiencia técnica.
Seguridad: Gophish ofrece una gran cantidad de medidas de seguridad para asegurar que los simulacros de phishing no sean detectados por los destinatarios.	Soporte limitado: Gophish es una herramienta de código abierto, por lo que no hay soporte oficial. Esto significa que los usuarios pueden tener problemas si tienen alguna pregunta o problema.

Nota. En esta tabla se muestran las ventajas y desventajas de Gophish (2024).

Capítulo 4
Análisis y Diseño

4.1. Análisis del ataque focalizado

En esta fase del proyecto de tesis se prepara el escenario del ataque focalizado de phishing, para ello se identifican las herramientas de software para ser instaladas.

Las herramientas que se instalan son las siguientes:

Tabla 8. Herramientas de Software

Sistemas Operativos	**Herramientas de Software**	**Configuración de Procesos**
Kali Linux versión 2023.2a de 64-bit	Rufus versión 4.1.2045.0	Creación de la memoria USB booteable para ejecutar imagen ISO del Sistema Operativo Kali Linux usando Rufus. Creación de la partición del disco duro para la instalación del Sistema Operativo Kali Linux.
Windows 11	Gophish version gophish-v0.12.1-linux-64bit.zip	Ejecución de la PC desde la memoria booteable de Rufus. Configuración de la herramienta de software Gophish.

Nota. En esta tabla se muestran los Sistemas Operativos, las herramientas y los procesos que se utilizaron para realizar dicho proyecto (2024).

4.1.1. Proceso de la instalación de los Sistemas Operativos

En la Fig. 7 se describe el proceso requerido para la instalación del Sistema Operativo que tiene el escenario de red para llevar a cabo el ataque focalizado.

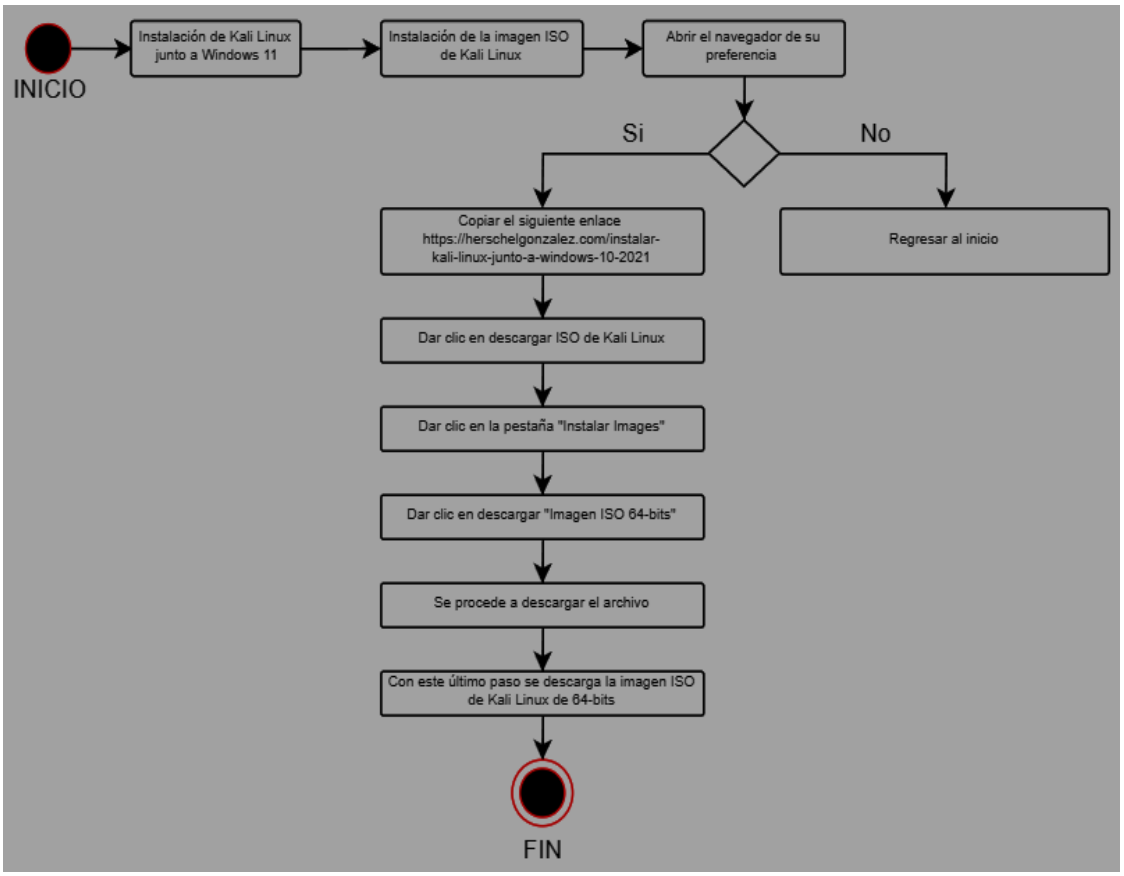

Fig. 7 Proceso de instalación de Kali Linux (2024).

4.1.2 Proceso de instalación de las herramientas de software

En la Fig. 8 se describe el proceso de requerimiento para la instalación de la herramienta de Rufus y el proceso de instalación de la herramienta de la imagen ISO de Kali Linux.

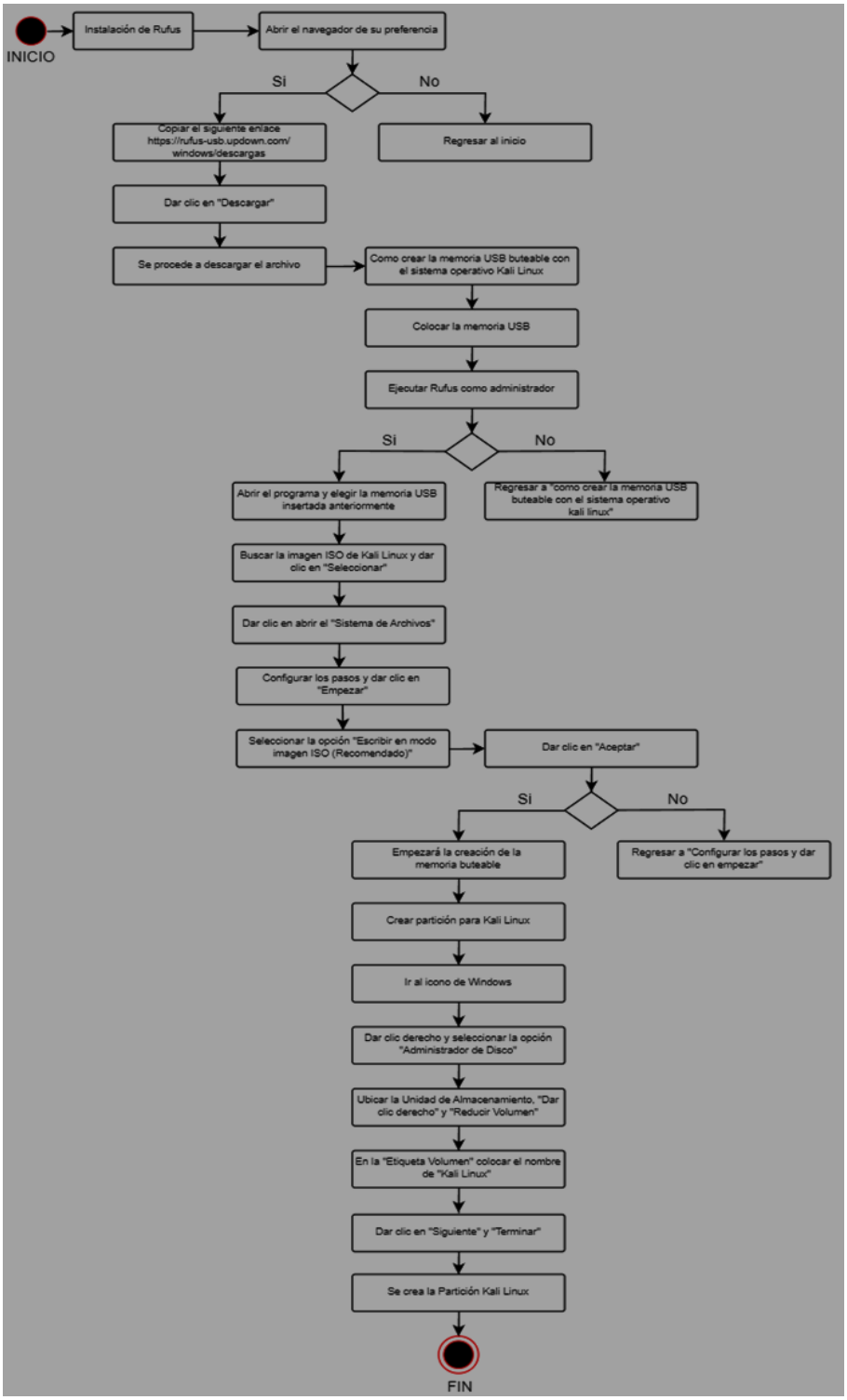

Fig. 8 Proceso de instalación de Rufus y la imagen ISO de Kali Linux (2024).

4.1.3. Procesos de configuración de procesos

En la Fig. 9 se describe el proceso de configuración e instalación de Kali Linux y el proceso de configuración e instalación de gophish.

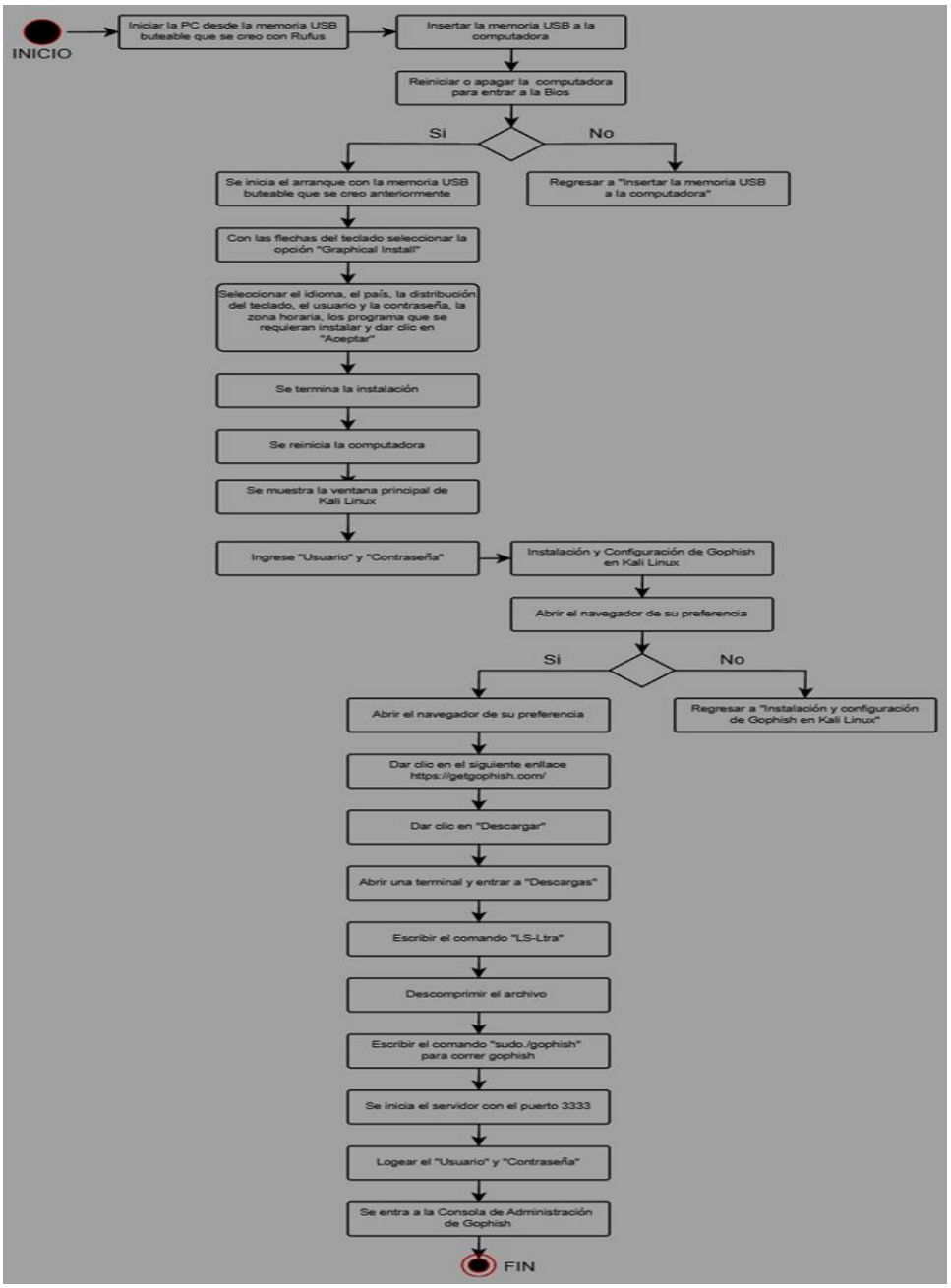

Fig. 9 Proceso de instalación y configuración de Kali Linux y Gophish (2024).

4.2. Diseño del ataque por phishing

Una vez preparado el escenario para el ataque focalizado, se procede a diseñar la campaña de phishing y su lanzamiento.

4.2.1. Creación de campaña por phishing

Una campaña de phishing es una estafa por correo electrónico, este tipo de estafa está diseñada para robar información personal de las víctimas. Los ciberdelincuentes suelen utilizar esto para obtener información confidencial como las tarjetas de crédito o las credenciales de inicio de sesión. Y para ello se disfrazan de organizaciones confiables o personas respetables por correo electrónico.

Generalmente, este tipo de campañas se lleva a cabo mediante la suplantación de identidad por correo electrónico. Este correo le indica al destinatario que ingrese información personal en un sitio web falso que es muy parecido al legítimo.

Los correos electrónicos de phishing también se utilizan para distribuir malware a través de enlaces o archivos adjuntos que pueden robar información y realizar otras tareas maliciosas. El phishing es popular entre los ciberdelincuentes; Esto se debe a que les permite robar información financiera, personal y confidencial sin tener que atravesar las defensas de seguridad de computadora o red. [30].

Básicamente una campaña de phishing no deja de ser el nombre técnico que tiene la amplia mayoría de fraudes en internet.

Mediante una campaña de phishing, lo que se busca es engañar a la víctima para que haga algo negativo (descargar y abrir un documento, insertar sus datos personales en una página, pagar por un producto en una tienda fraudulenta, enviar dinero mediante una extorsión, etc.). [31].

Una campaña de phishing utiliza técnicas de ingeniería social para atraer a los destinatarios de correo electrónico. Así ellos revelan información personal o financiera. Por ejemplo, durante las vacaciones, un correo electrónico que finge ser de una empresa conocida le dice

que vaya a su sitio web y vuelva a ingresar su información de facturación o su paquete no se enviara a tiempo para que el destinatario de su regalo. El problema aquí es que el correo electrónico te dirige a un sitio web falso, donde la información que ingrese se usará para cometer un robo de identidad, fraude y otros delitos. [32].

Para llevar a cabo este proyecto, se realizó solo una campaña de phishing a la que se le nombre "Campaña de phishig Rosa". En la cual se hizo una simulación de ataque de phishing mediante un correo de Gmail falso, el cual hacia llegar al usuario de otro correo (dicho correo creado para realizar dicha campaña) el correo clonado con información de Afore Rosa, el cual pedía ingresar los datos del usuario para poder acceder a la información más detallada de su cuenta de Afore Rosa.

4.2.2. Monitoreo previo sobre phishing

Para llevar a cabo este proyecto de tesis nombrado "Prevención de los riesgos de ataques cibernéticos por phishing". Se realizó una encuesta a los estudiantes y maestros de la Facultad Ciencias de la Computación, entre edades de los 20 y 55 años, así como público en general. En esta encuesta se plantearon preguntas sobre problemáticas que presenta la sociedad día con día. Ya sea mediante suplantación de identidad, mediante correos electrónicos, páginas de internet o sitios web falsos, etc. Dicho esto, con las respuestas obtenidas se observó que, por lo menos tres de cada sesenta y cinco personas han sido víctimas de fraudes cibernéticos. También se pudo observar que incluso había personas que no tenían ni el más mínimo conocimiento sobre el tema o incluso que ya habían sido víctimas de un ataque cibernético.

4.2.3. Lanzamiento de campaña por phishing

Para lanzar la campaña de phishing nombrada "Afore Rosa", se crearon tres correos, un correo se creó para ser el atacante y el cual enviara el correo malicioso, y los otros dos correos restantes serán las víctimas, los cuales recibirán dicho correo malicioso por el atacante.

Atacante: **rosacalderonsuarez@outlook.com**

Victima 1: **suacal99@gmail.com**

Victima 2: **rosasuarezcalderon@gmail.com**

A continuación, en la Fig. 10, se muestra el correo del usuario que juega el rol de víctima 1, el cual se creó previamente.

Fig. 10 Victima 1 (2024).

En la Fig. 11, se muestra el correo del usuario que juega el rol de victima 2, el cual se creó previamente.

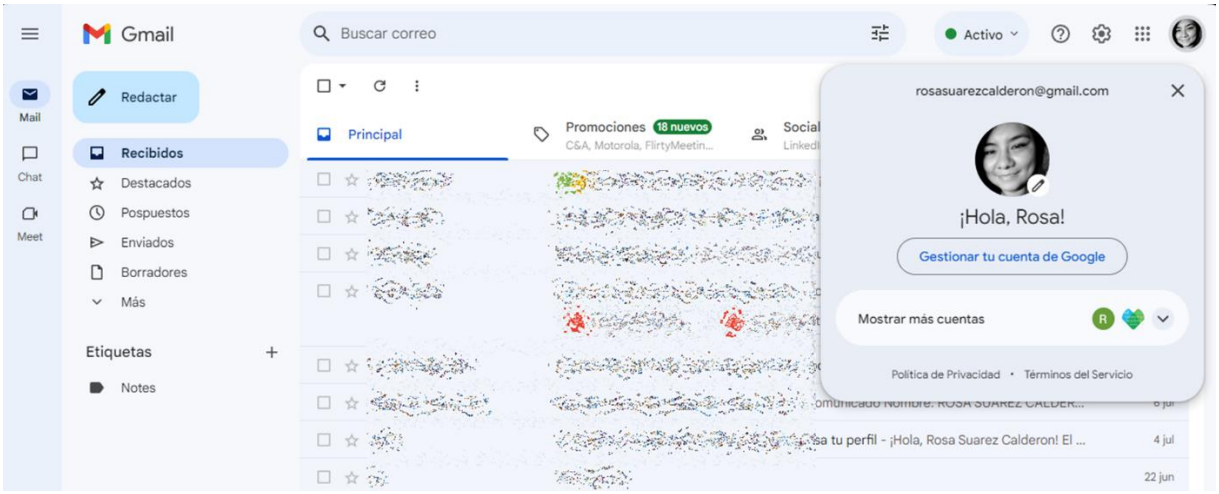

Fig. 11 Victima 2 (2024).

En la Fig. 12 se muestra el correo electrónico del atacante, el será encargado de enviar el correo malicioso o correo clonado.

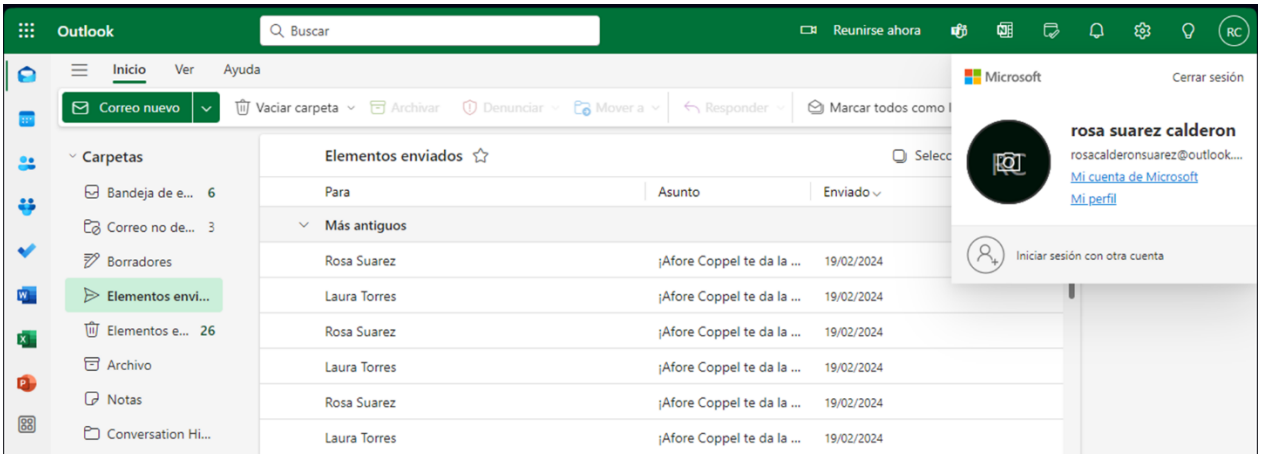

Fig. 12 Correo atacante (2024).

En la Fig. 13 se puede observar la bandeja de entrada, en la cual muestra de manera exitosa que el correo electrónico malicioso ha sido recibido en la bandeja de la víctima 1.

Nota importante. Este correo electrónico es ficticio sin daños a terceros.

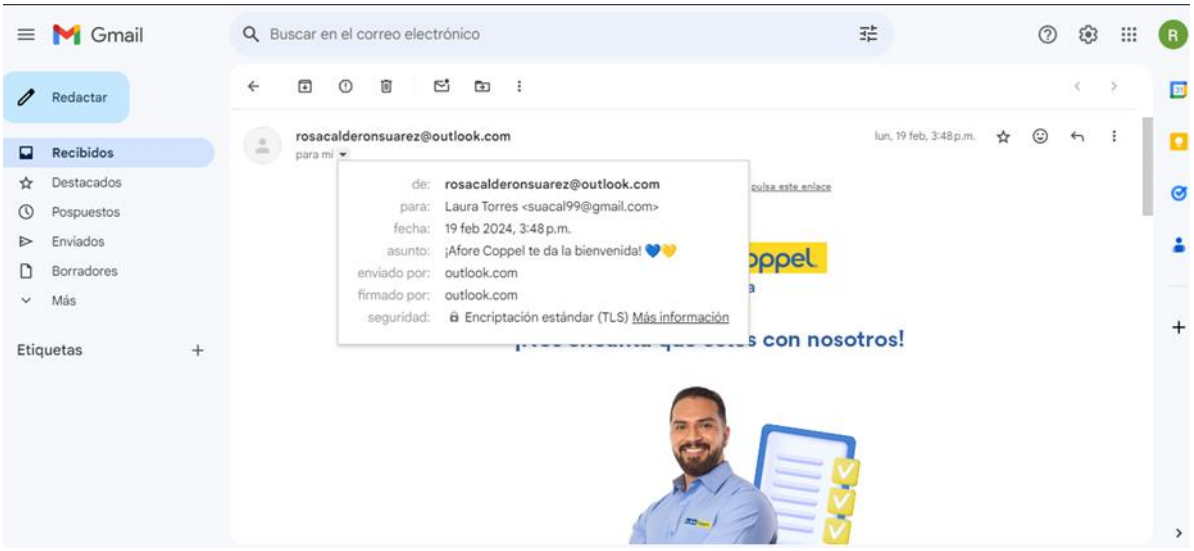

Fig. 13 Correo malicioso para victima 1 (2024).

En la Fig. 14 se muestra la bandeja de entrada, en la cual se observa que de manera exitosa llego el correo electrónico malicioso al correo dos de la víctima.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

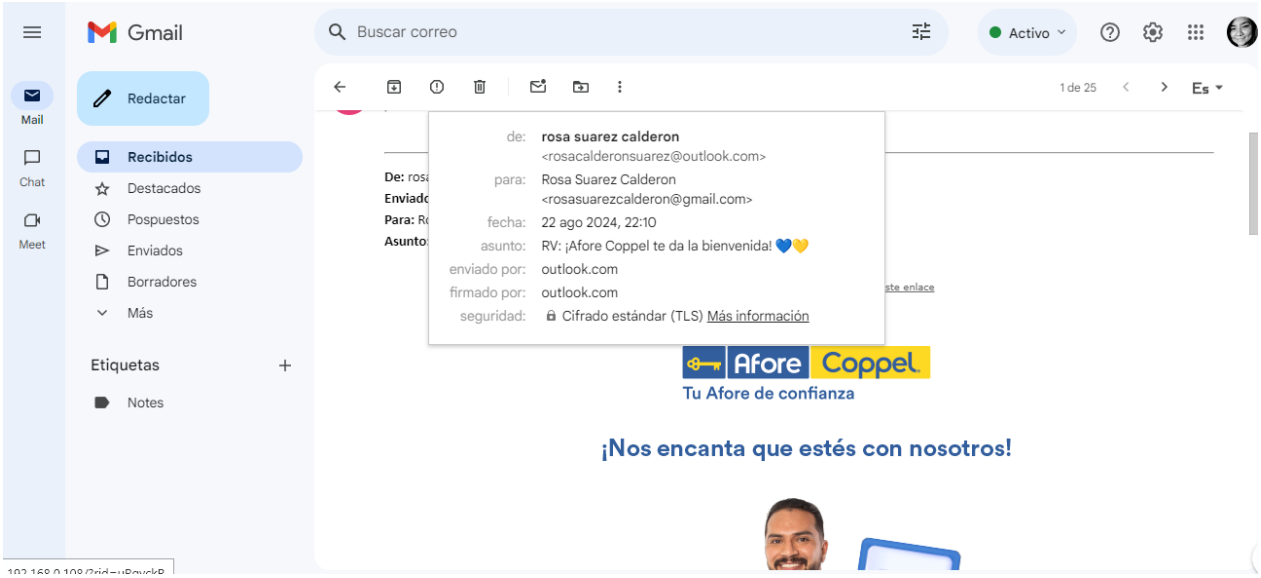

Fig. 14 Correo malicioso para la victima 2 (2024).

En la Fig. 15 se muestra la bandeja de salida del correo que se creó para que fuera la víctima. En la cual se muestran los correos electrónicos maliciosos enviados con éxito a las dos víctimas.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros

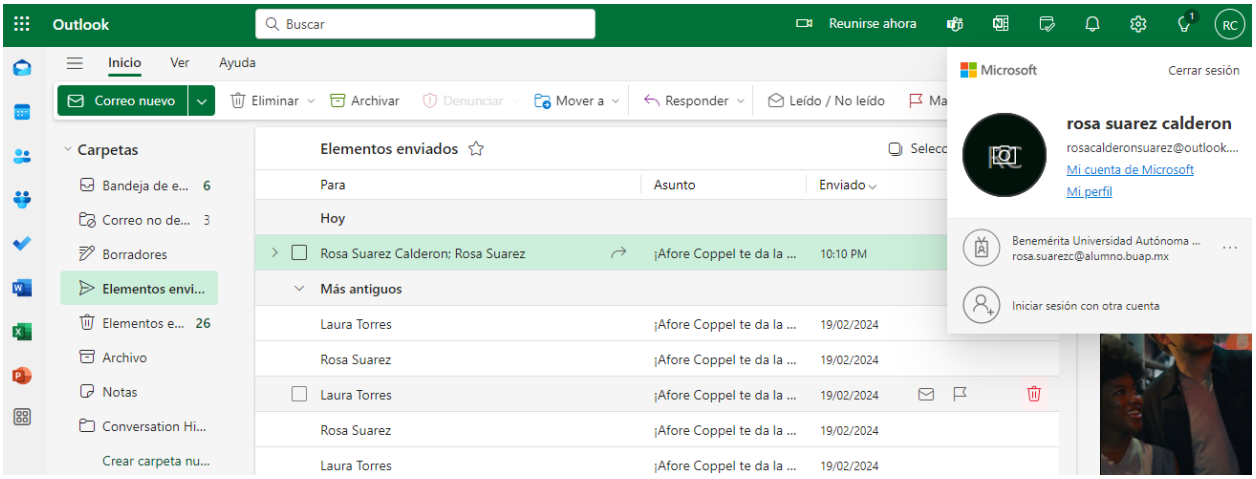

Fig. 15 Bandeja de salida (2024).

En la Fig. 16 se muestra y se describe paso a paso un modelo de procesos para crear y lanzar una campaña de phishing.

Fig. 16 Modelo de procesos para lanzar una campaña de phishing (2024).

4.2.4. Robo de identidad de la victima

Mostrar como el atacante robo la identidad de la víctima y que hará con esa información o logra el fraude.

Una vez realizado los pasos anteriores y las victimas 1 y 2 han caído en la trampa, ya que han abierto el correo electrónico malicioso en el escenario focalizado y han llenado los campos con su información, como se observa en la Fig. 17 la información de las víctimas fue capturada y guardada en la base de datos de la herramienta gophish.

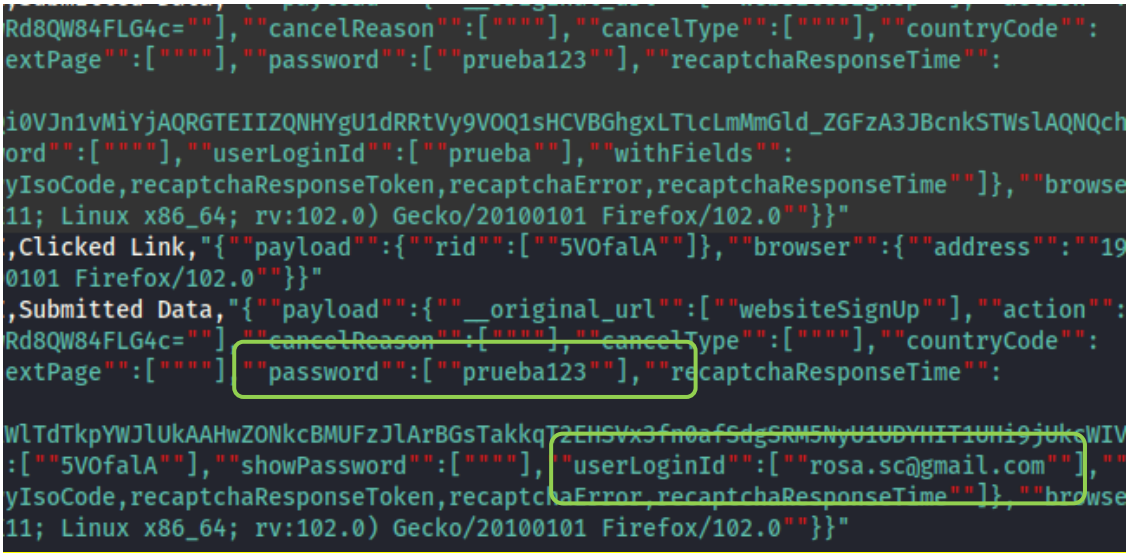

Fig. 17 Robo de identidad (2024).

Como segundo paso, es momento de entrar a la página que simula la campaña de phishing nombrada Afore Rosa, al colocar el usuario y contraseña se observa en la base de datos que la información ya fue registrada y guarda.

Nota Importante: Esta información es ficticia sin daños a terceros.

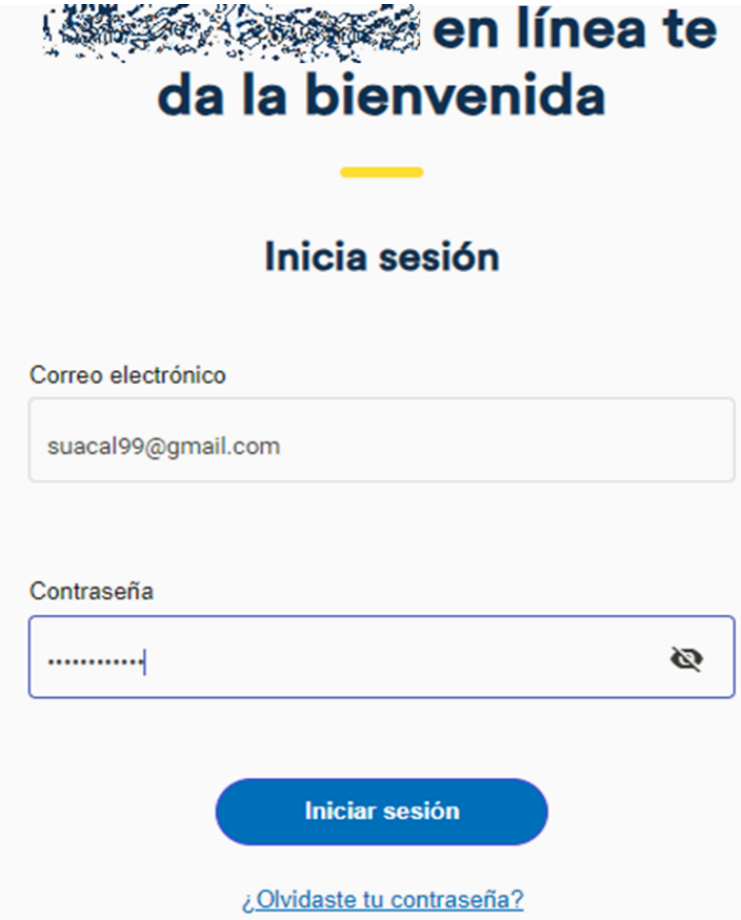

Fig. 18 Afore de Bienvenida (2024).

Una vez, llenado los campos con la información requerida se observar que accedió con éxito al estado de cuenta de la víctima 1 y por lo tanto se puede vaciar dicha cuenta si es que así se desea. Considerando que este es un escenario focalizado, no se tuvieron daños reales. Solo se presenta con el objetivo de concientizar a la población Universitaria y público en general.

Nota Importante: Esta información es ficticia sin daños a terceros.

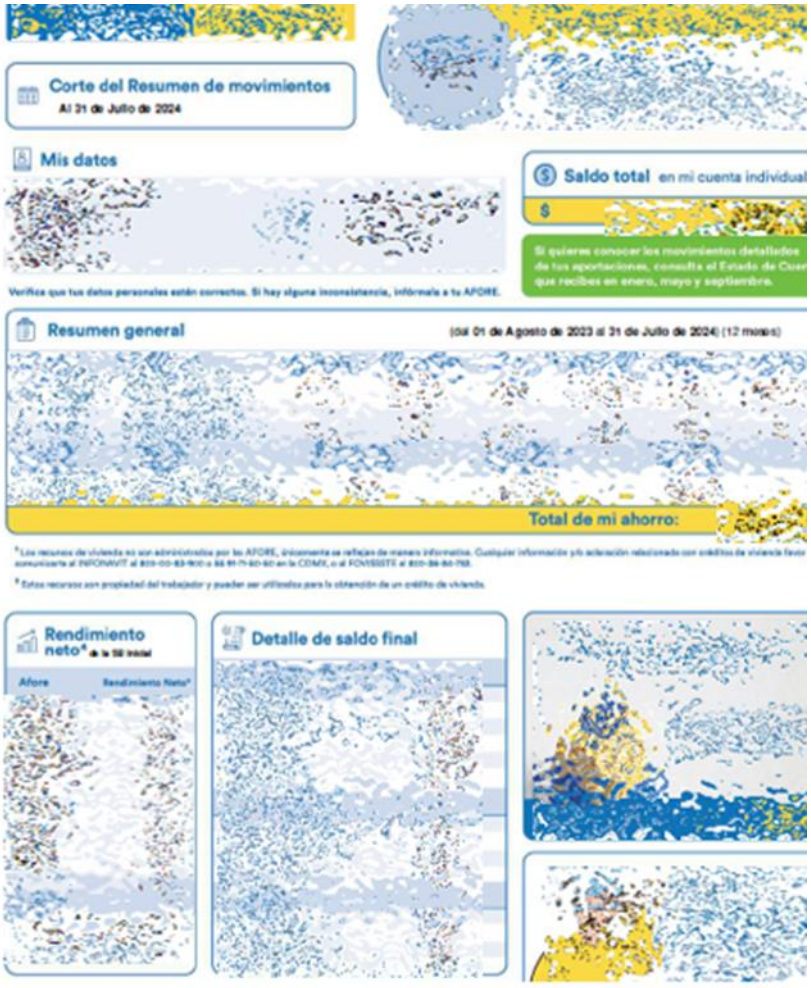

Fig. 19 Información de cuenta (2024).

4.3. Creación de material formativo y repositorios de referencia

4.3.1. Diseño de material formativo e implementación

Se generaron dos formularios, un formulario se realizó en la cuenta de Gmail y el otro formulario se realizó en la cuenta del correo institucional de la universidad (BUAP). En ambos formularios se realizaron las mismas preguntas, en las cuales se preguntaban sobre situaciones o acontecimientos que se vive día con día acerca sobre la problemática de robo de identidad. Posteriormente, se generaron dos QR´s sobre los formularios y se publicaron

en la cuenta oficial de la Academia de CISCO BUAP en Facebook. Como se puede observar en la imagen 20.

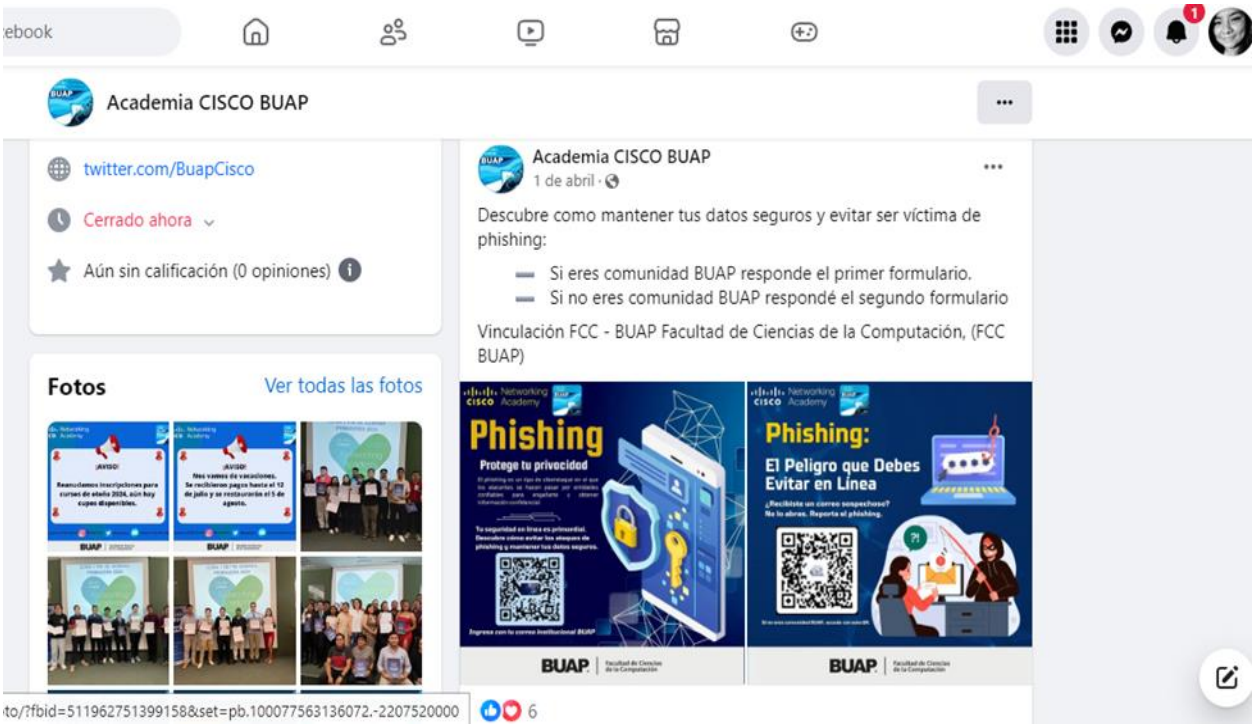

Fig. 20 Formularios publicados en la Academia de CISCO BUAP (2024).

4.3.2. Diseño de material gráfico e implementación

Se diseñó una capsula en la cual se explican los tipos de ataques por phishing. Posteriormente, se publicaron en la cuenta oficial de la Academia de CISCO BUAP en Facebook. Como se observa en la imagen 21.

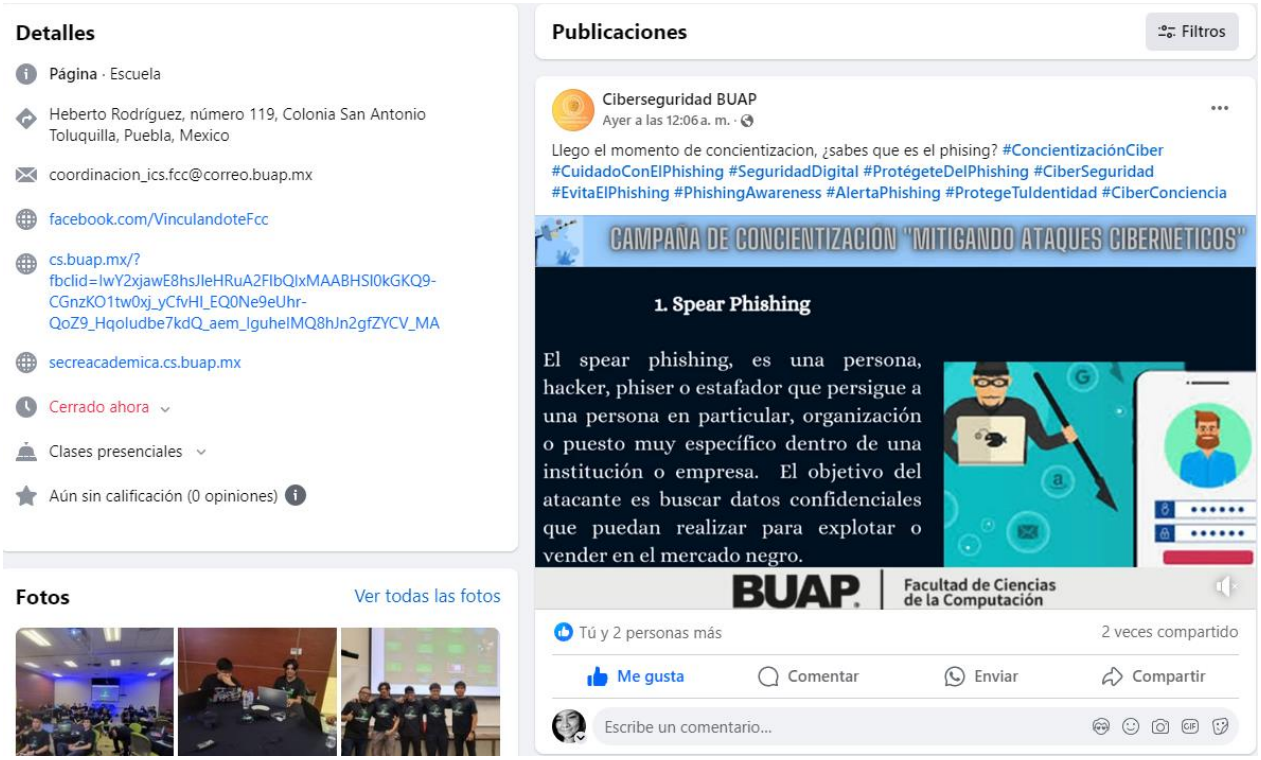

Fig. 21 Capsula publicada en la página de Ciberseguridad BUAP (2024).

4.3.3. Diseño de repositorios de referencia e implementación

Se diseñaron seis repositorios, los cuales se describen a continuación.

Repositorio No.1 Guía del proceso de instalación de la imagen ISO de Kali Linux ver. 2023.2a

El repositorio uno es una guía para instalar la imagen ISO de Kali Linux sobre Windows 11 y usar una partición del disco duro. Con esta instalación se genera un dual boot de los sistemas operativos en una misma computadora.

Repositorio No.2 Proceso de instalación de la herramienta de software Rufus.

El repositorio dos es una guía para instalar la herramienta de software de Rufus sobre Windows 11 y así obtener una memoria USB booteable con la imagen ISO de Kali Linux. Con esta instalación se crea una memoria USB booteable con Kali Linux. La cual se ocupará para instalar Kali Linux en la computadora deseada.

Repositorio No.3 Proceso de creación de la memoria USB Booteable para iniciar la imagen ISO del Sistema Operativo Kali Linux ver. 2023.2a.

El repositorio tres es una guía para llevar el proceso de creación de una memoria USB booteable para iniciar la imagen ISO en Kali Linux ver. 20023.2a sobre Windows 11. Con este proceso se iniciará la imagen ISO de Kali Linux.

Repositorio No.4 Proceso de creación de la partición para Kali Linux.

El repositorio cuatro es una guía para crear o realizar la partición del disco duro en Windows 11 y asignar dicha partición de disco duro para montar Kali Linux.

Repositorio No. 5 Proceso de inicio de una PC desde la memoria Booteable que se creó con Rufus.

El repositorio cinco es una guía para iniciar la PC desde la memoria USB booteable que se creó con Rufus sobre Windows 11 y así instalar el sistema operativo de Kali Linux.

Repositorio No. 6 Proceso de instalación y configuración de la herramienta de software Gophish en Kali Linux.

El repositorio seis es una guía para instalar y configurar la herramienta de gophish en el sistema operativo de Kali Linux. Y así, se poder crear la campaña de phishing.

Capítulo 5
Pruebas y Resultados

5. Creación de una campaña de phishing con gophish

Se creó una campaña de Phishing usando Gophish, para ello se simulo una empresa u organización que otorga servicios financieros de Afores, la empresa simulada se denominó “Afore Rosa”.

“La campaña crea en los usuarios la concientización sobre los ataques de phishing, dado que, el ataque por phishing es uno de los más populares o usados para efectuar un delito cibernético, este delito se realiza mediante la suplantación de identidad haciendo uso del envío de correos electrónicos ofreciendo algo al usuario, como puede ser una página, una red social o alguna plataforma en la cual el usuario requiere acceder” (¿Qué Es el Phishing? | IBM, s. f.).

5.1. ¿Para quién o quiénes está dirigida la campaña de pshishing?

La campaña de Phishing se dirige a la Comunidad Universitaria (BUAP) y público en general.

5.2. Que se necesita para la creación de la campaña de phishing

1) Se requiere la herramienta de Gophish de Kali Linux.
2) Se requiere un par de correos electrónicos para simular tanto el atacante, como la víctima.

En la siguiente infografía se muestran los requisitos necesarios para la creación de una campaña por phishing.

Infografía. 1 requerimientos para la creación de una campaña por phishing (2024).

5.3. Creación de la campaña de phishing Afore Rosa con gophish

Una vez realizado el proceso de instalación y configuración de Gophish, es el momento de crear los envíos de perfiles.

A continuación, del paso 1 al paso 11, se detalla la creación de los envíos de perfiles.

1) Entrar a la herramienta de gophish, como se observa en la imagen Fig. 20.

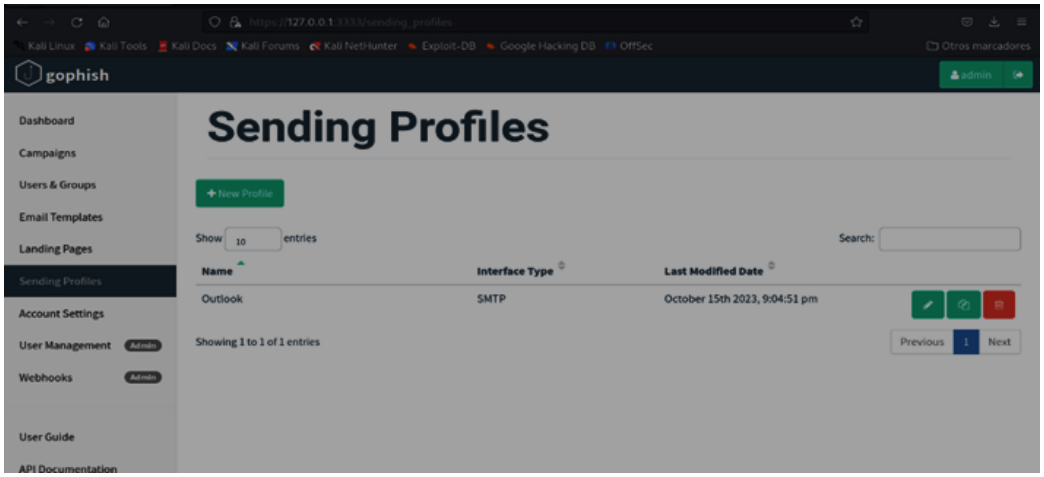

Fig. 20 Página principal de gophish (2024).

2) Configurar el servidor SMTP mediante el correo electrónico de Outlook. Dar clic en el botón de **“New Profile”**, como se observa en la Fig. 21.

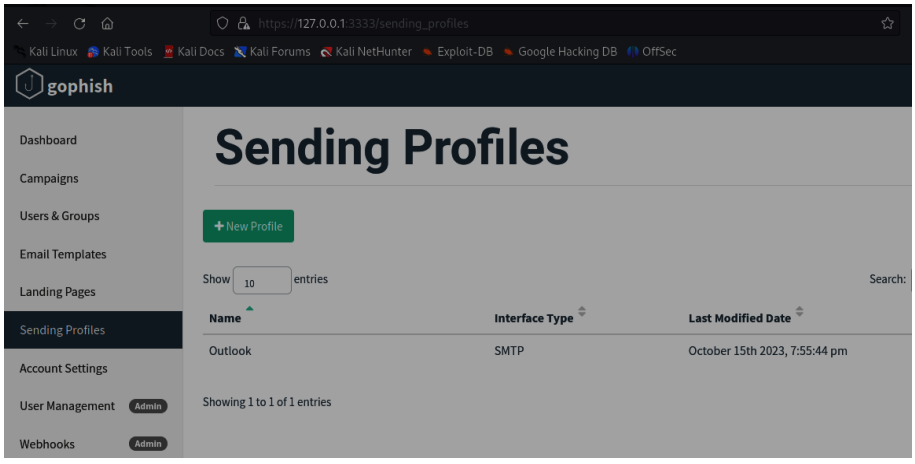

Fig. 21 New profile (2024).

3) Se observa la siguiente ventana, como se observa en la Fig. 22.

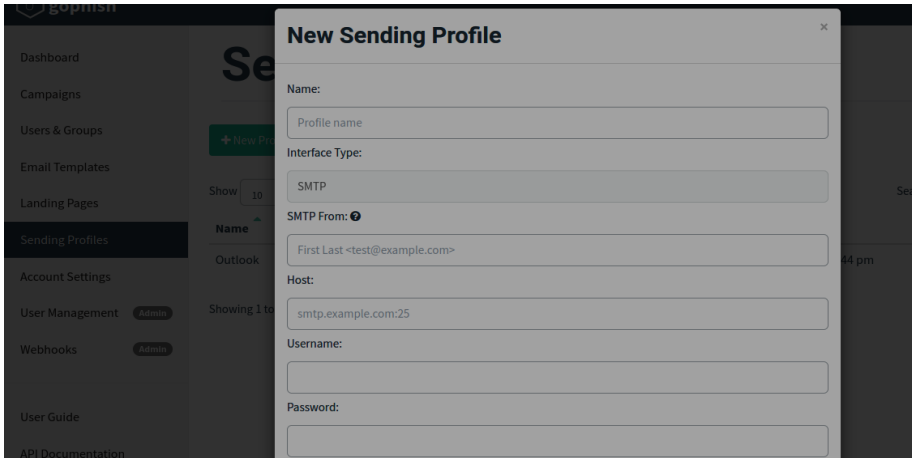

Fig. 23 New sending profile (2024).

4) Se llenan los campos solicitados, para ello se hizo uso del correo electrónico de Outlook ya que, es necesario configurar el protocolo SMTP, **(Este correo se utiliza para simular el lado del atacante)**, como se observa en la Fig. 24.

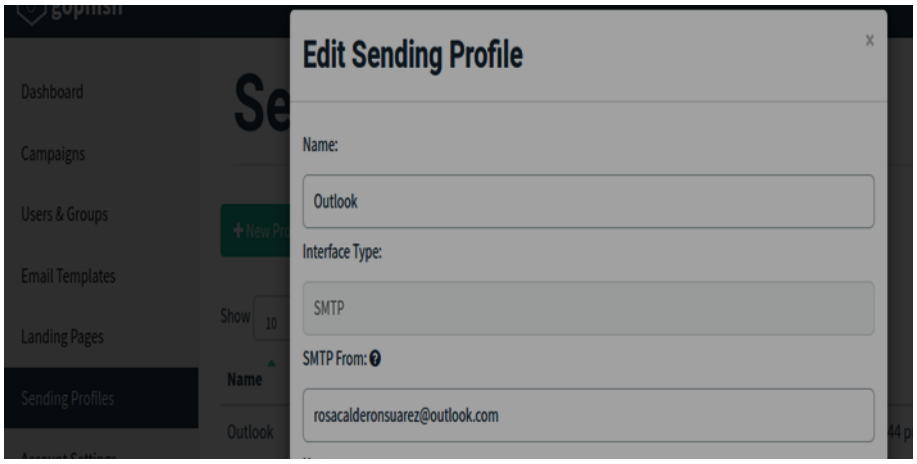

Fig. 24 Tipo de correo (2024).

5) Se requiere configurar el servidor MSTP con **el número de puerto 587**, para ello es necesario abrir el navegador de Google y escribir en el buscador **"SMTP de Outlook"**, como se observa en la Fig. 25.

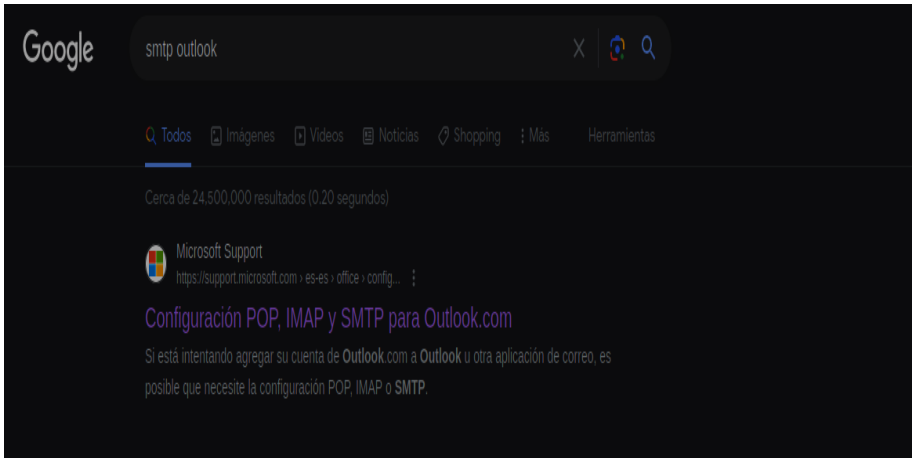

Fig. 25 SMTP Outlook (2024).

6) Dar clic en **"Configuración de Outlook.com"**, como se observa en la Fig. 26.

Fig. 26 Configuración de Outlook (2024).

7) Ir al apartado SMTP, copiar el **SMTP office365.com** y **puerto 587** del correo, como se observa en la Fig. 27.

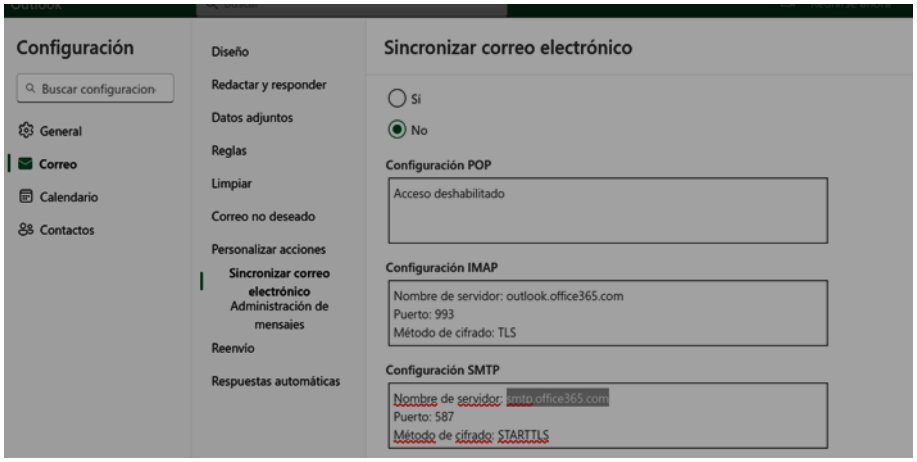

Fig. 27 SMTP y puerto (2024).

8) Una vez copiado el nombre del servidor SMTP office365.com y el puerto 587, se debe regresar a gophish y pegar lo copiado en el apartado de Host, como se observa en la Fig. 28.

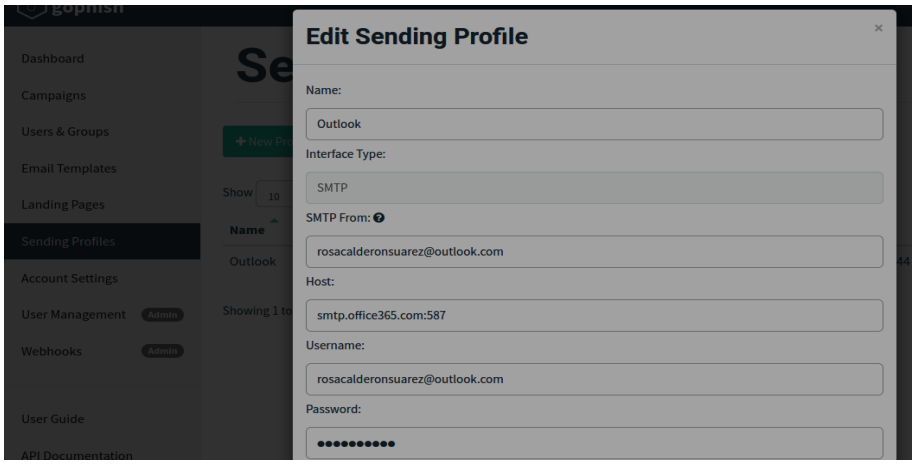

Fig. 28 SMTP (2024).

9) Ir al botón **de "Send Test Email"**, ya que este botón envía un correo de prueba utilizando el servicio de SMTP, para observar si la configuración realizada es correcta, como se observa en la Fig. 29.

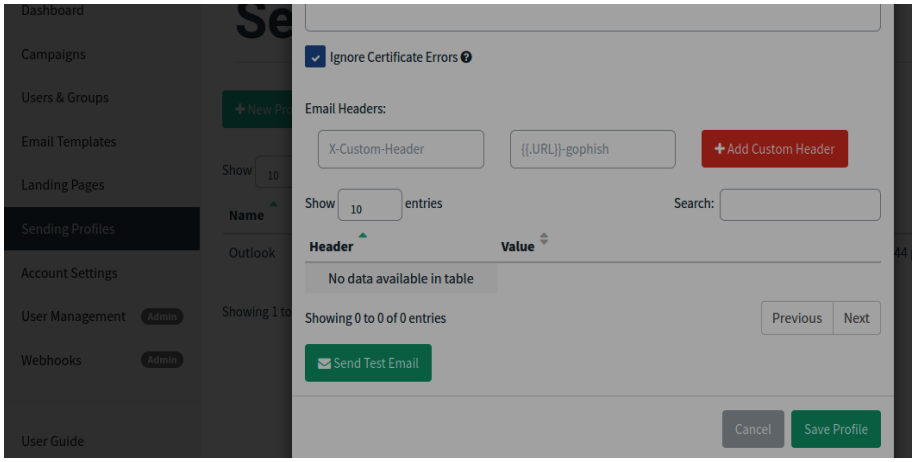

Fig. 29 Boton send test email (2024).

10) Se observa la siguiente ventana, como se observa en la Fig. 30.

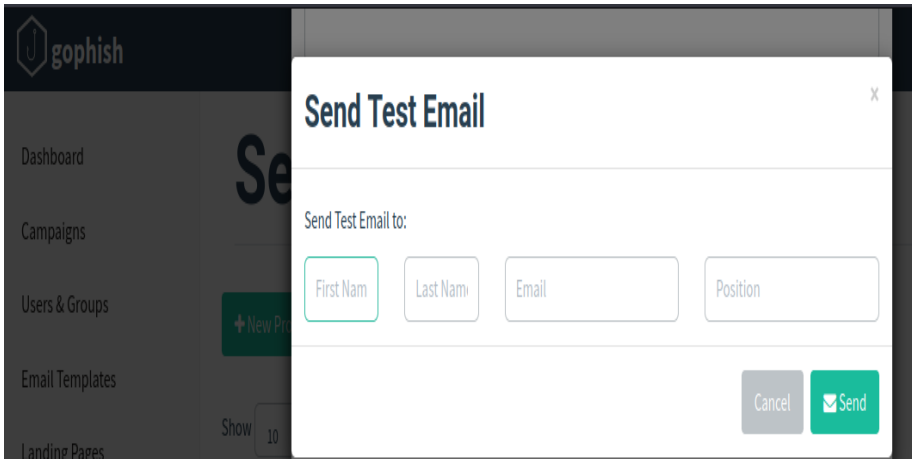

Fig. 30 Ventana send test (2024).

11) Se debe colocar el nombre y el correo de prueba y una vez llenados los datos se da clic en **“Send”** para enviar, como se observa en la Fig. 31.

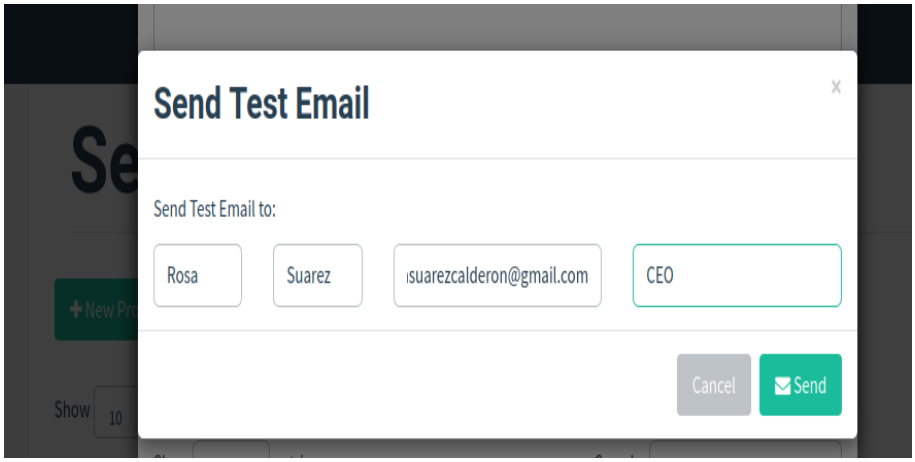

Fig. 31 Correo prueba (2024).

Una vez realizado el proceso de configuración de envió de perfiles, llega el momento de crear las páginas de destino.

A continuación, en los pasos del 12 al 22, se detalla la creación de la página de destino.

12) Terminadas las configuraciones anteriores, se muestra un mensaje indicando que todo salió con éxito, como se observa en la Fig. 32.

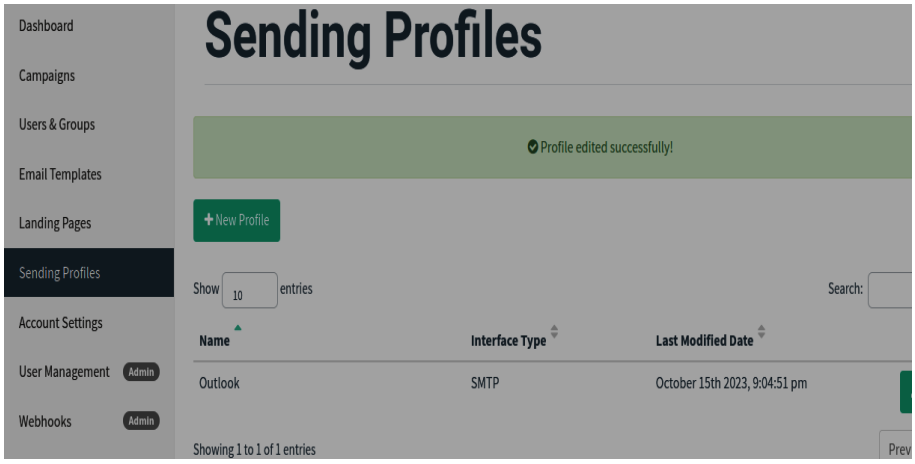

Fig. 32 Perfil exitoso (2024).

13) Se requiere Ir a la pestaña **“Landing Pages”** para crear ahora la página clonada de destino, como se observa en la Fig. 33.

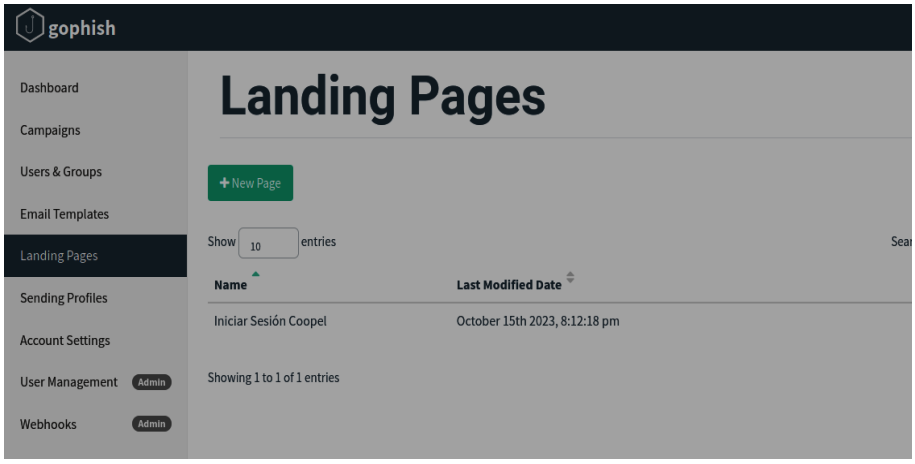

Fig. 33 Lading pages (2024).

14) Se da clic en el **“New Page”** para crear nueva página o la página clonada que se desea, como se observa en la Fig. 34.

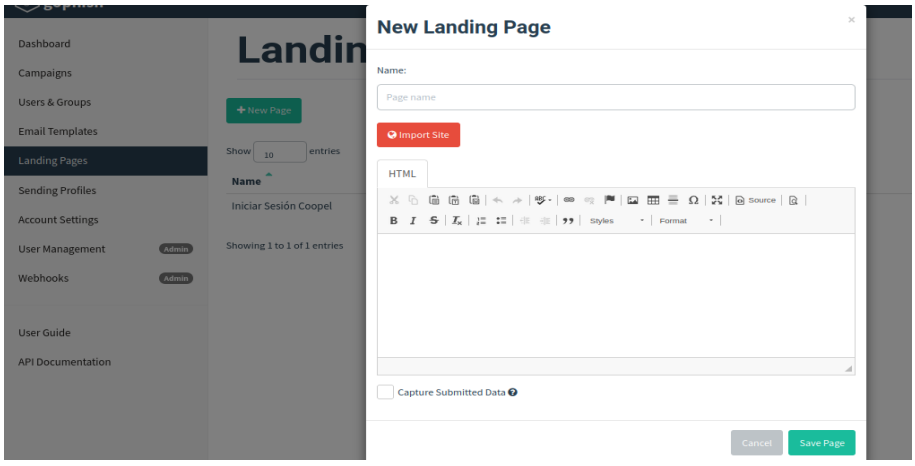

Fig. 34 New page (2024).

15) Colocar el nombre deseado para la página clonada, como se observa en la Fig. 35.

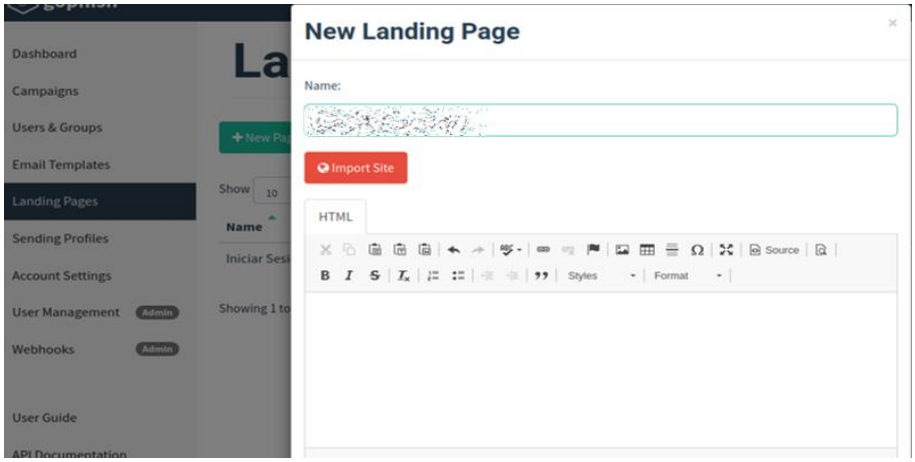

Fig. 35 Nombre de la página (2024).

16) Dar clic en **"Import Site"** para ir al sitio de importación, se abre la siguiente ventana, como se observa en la Fig. 36.

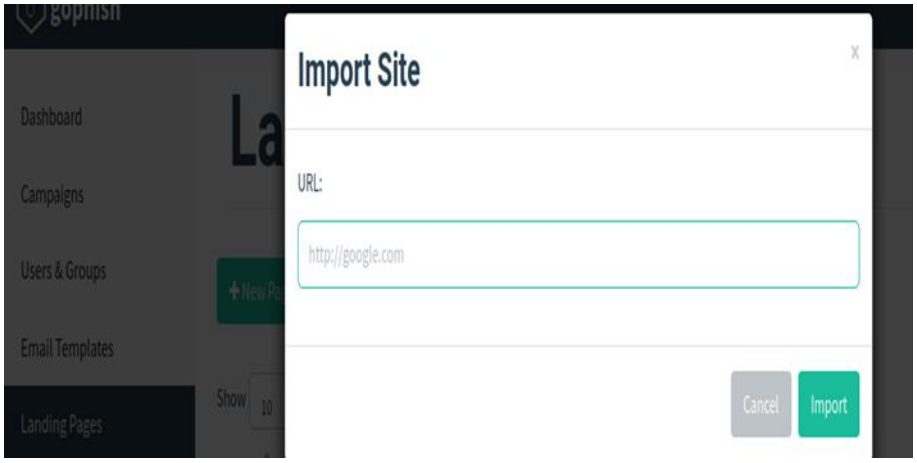

Fig. 36 Import site (2024).

17) Colocar el URL de la página que se requiera clonar, para ello se debe abrir el navegador. En este caso se clonará la página de login Copel Rosa, como se observa en la Fig. 37.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

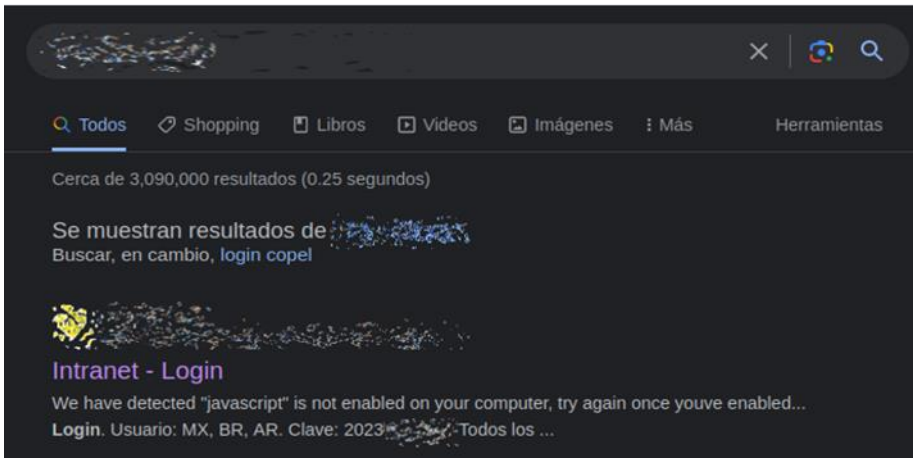

Fig. 37 Login Coppel Rosa (2024).

18) Se debe abrir la página y después copiar el URL de dicha página, como se observa en la Fig. 38.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

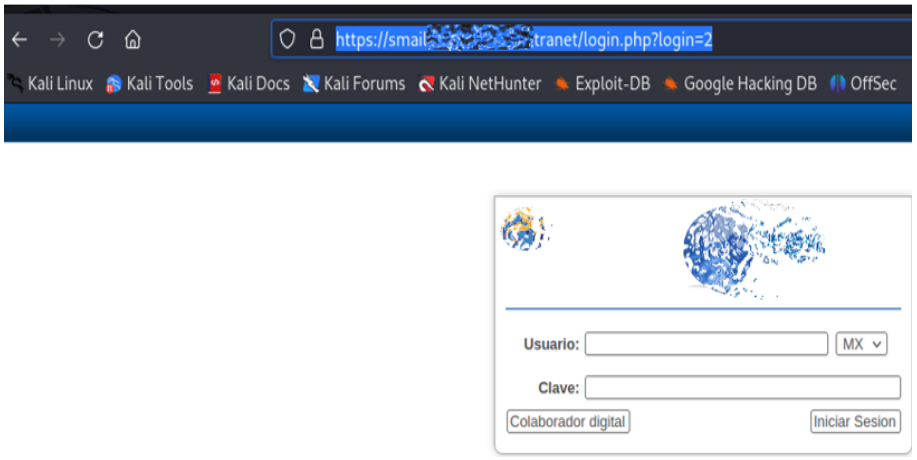

Fig. 38 URL login Coppel Rosa (2024).

19) Regresar a la herramienta de gophish y pegar en el apartado el enlace, dar clic en el botón de **"import"** para importar la página clonada, como se observa en la Fig. 39.

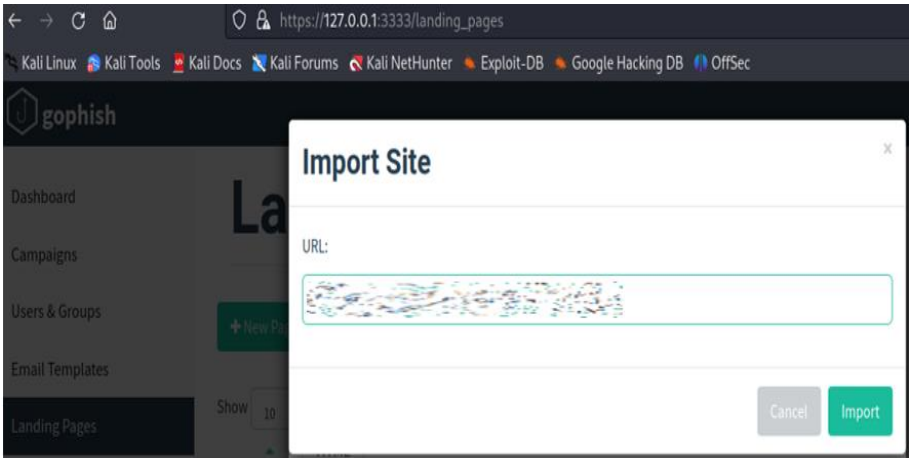

Fig. 39 Import site (2024).

20) Se muestra la página clonada, como se observa en la Fig. 40.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

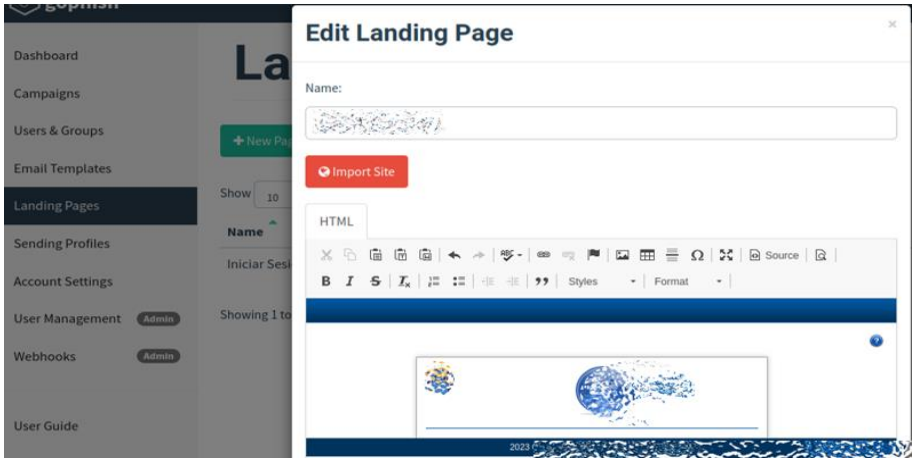

Fig. 40 Página clonada (2024).

21) Seleccionar las dos casillas, las cuales indican si se requiere observar el usuario y contraseña de la víctima. Seleccionar ambas casillas para observar dicho usuario y contraseña, clic en **"Save Page"** para guardar la página clonada, como se observa en la Fig. 41.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

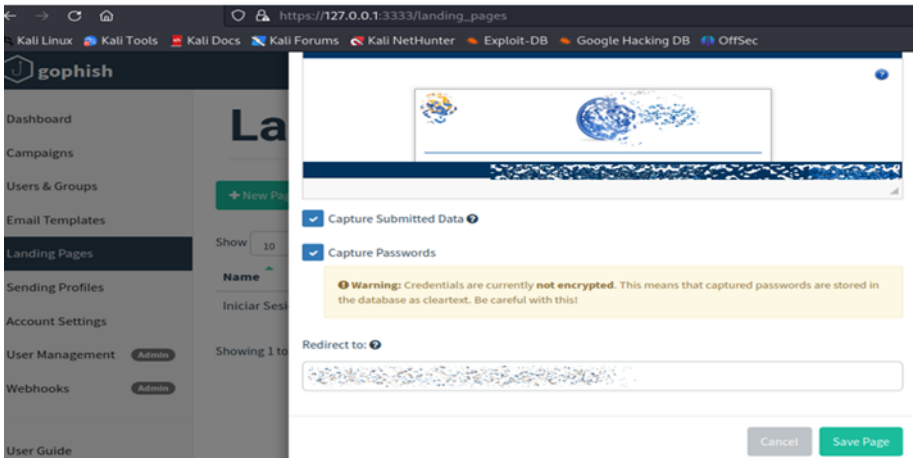

Fig. 42 Save page (2024).

22) Se observa que la configuración de Landing Pages fue exitosa, como se observa en la Fig. 43.

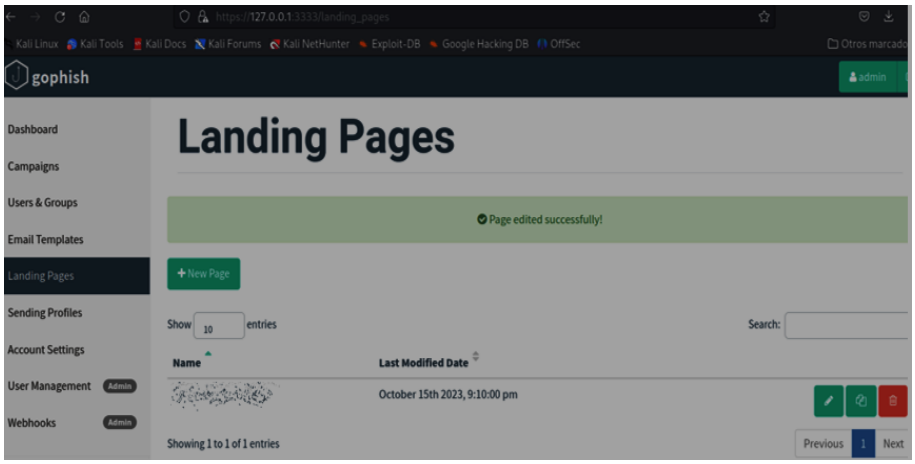

Fig. 43 Lading pages exitosa (2024).

Una vez realizado el proceso de configuración de páginas de destino, llega el momento de crear la plantilla de correo electrónico clonado.

A continuación, en los pasos del 23 al 31, se detalla la creación de la plantilla de correo electrónico clonado.

23) Ir a la pestaña **“Email Templates”** para crear la plantilla del correo electrónico malicioso, como se observa en la Fig. 44.

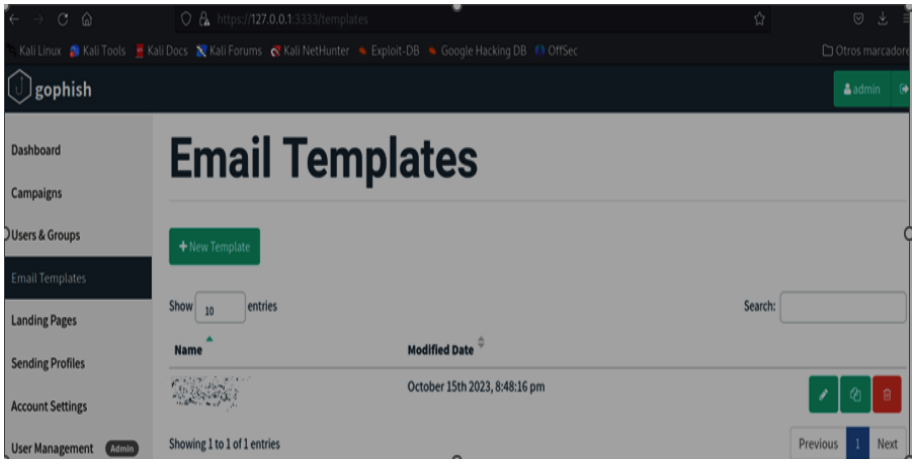

Fig. 44 Email templates (2024).

24) Dar clic en **“New Template”** para crear la plantilla, como se observa en la Fig. 45.

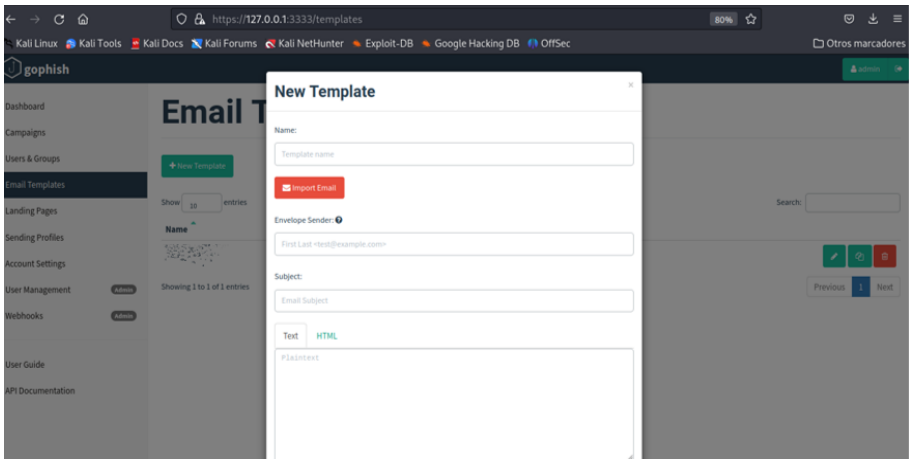

Fig. 45 New template (2024).

25) Se debe escribir el nombre del correo que se desee, como se observa en la Fig. 46.

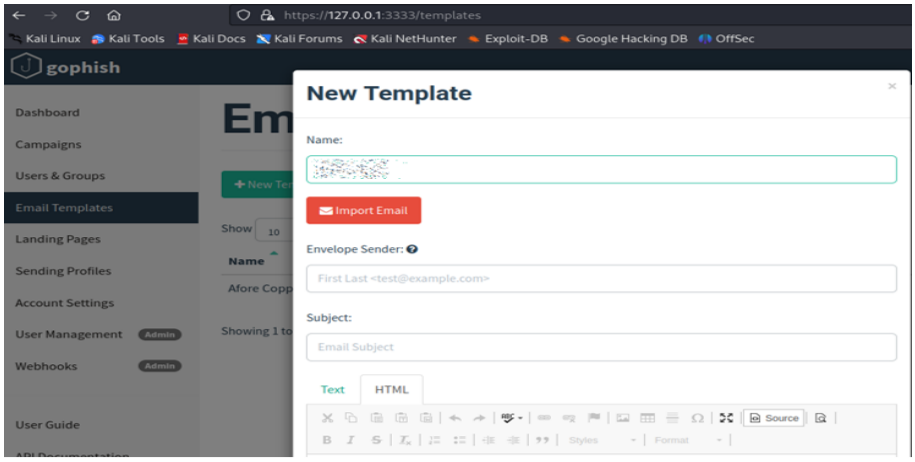

Fig. 46 Afore Rosa (202).

26) Dar clic en el botón **“Import Email”** para importar el correo. Aquí se coloca el código del correo que se desea clonar, como se observa en la Fig. 47.

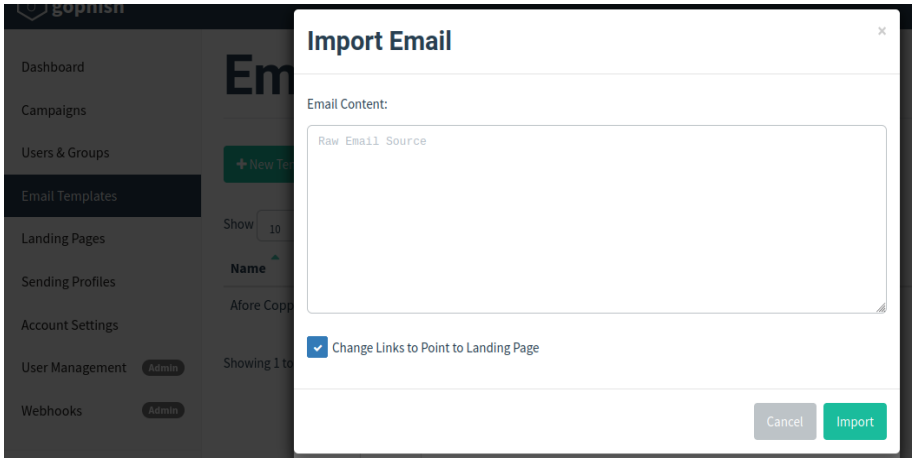

Fig. 47 Import email (2024).

27) Se debe ir a la bandeja de entrada de correo electrónico deseado. Buscar el correo que se requiera clonar, una vez encontrado dicho correo, ir al apartado de los tres puntitos y buscar la opción **“Mostrar original”**, como se observa en la Fig. 48.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

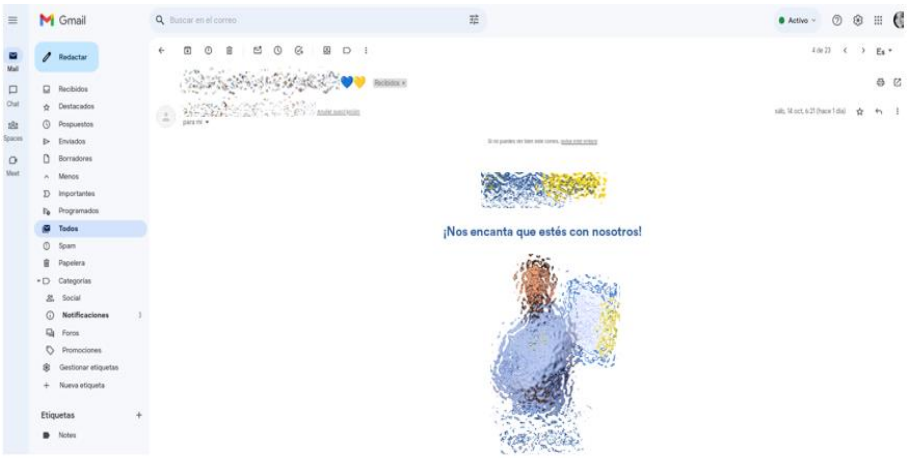

Fig. 48 Correo (2024).

28) Aparece la siguiente página, dar clic en **"Copiar en el portapapeles"**, como se observa en la Fig. 49.

Fig. 49 Copiar en el portapapeles (2024).

29) Regresar a la herramienta de Gophish y pegar el código en el apartado. Dar clic en **"Import"** para importar el código de dicho correo, como se observa en la Fig. 50.

Fig. 50 Import correo (2024).

30) El correo será clonado exitosamente. Dar clic en **"Save Template"** para guardar la plantilla, como se observa en la Fig. 51.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

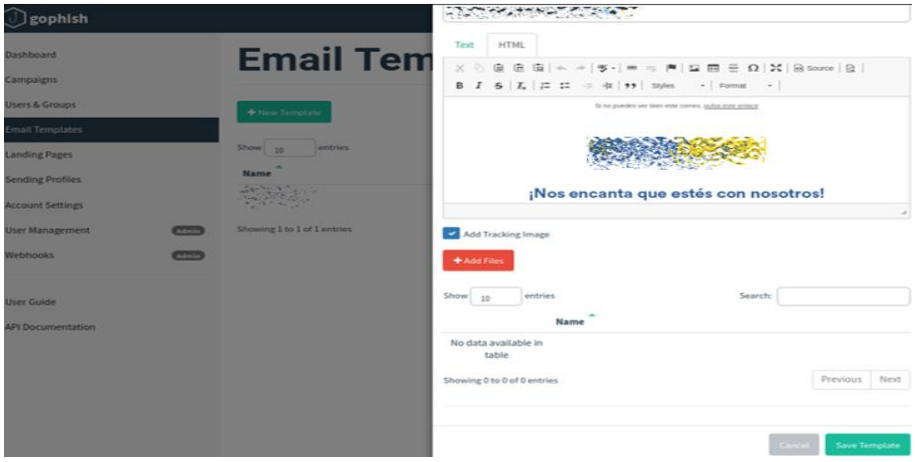

Fig. 51 Correo (2024).

31) La configuración será exitosa, como se observa en la Fig. 52.

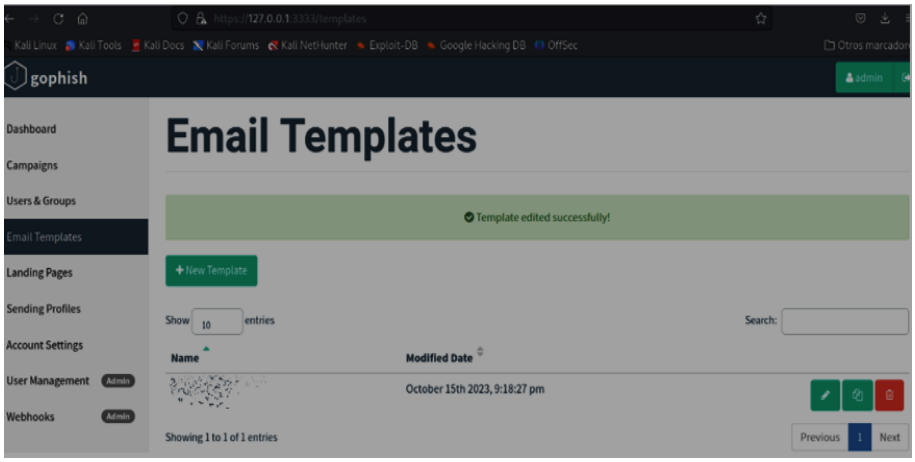

Fig. 52 Email exitosa (2024).

Una vez realizado el proceso de configuración de la plantilla de correo electrónico clonado, llega el momento de crear los usuarios y grupos.

A continuación, en los pasos del 32 al 36, se detalla la creación de los usuarios y grupos creados.

32) Se debe ir a la pestaña de **Users & Groups**, como se observa en la Fig. 53.

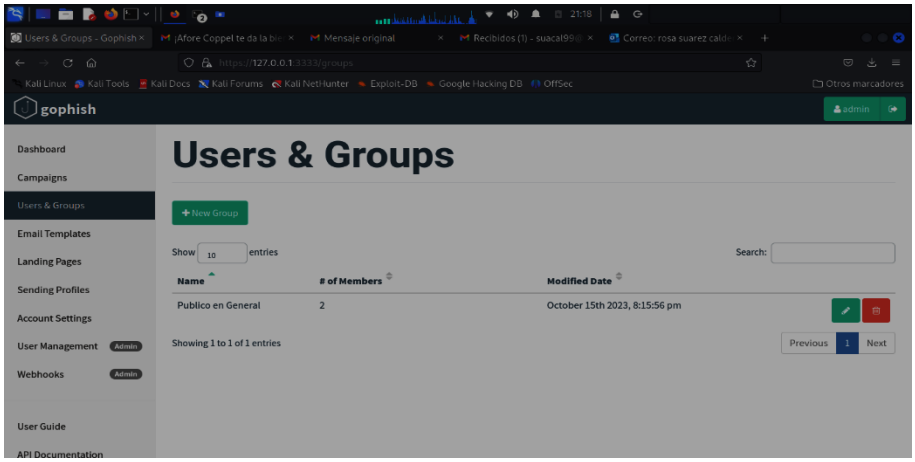

Fig. 54 Users & groups

33) Clic en **"New Group"** para crear un nuevo grupo. Se muestra la siguiente ventana, como se observa en la Fig. 55.

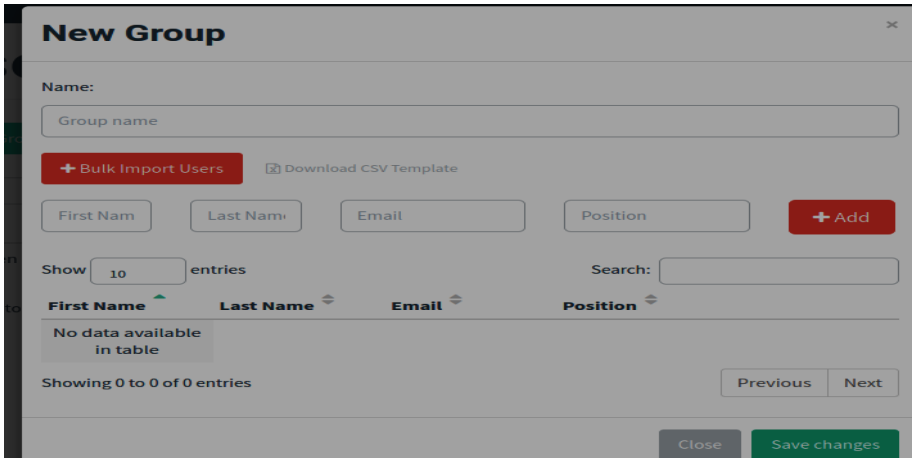

Fig. 55 New group (2024).

34) Colocar los nombres y correos electrónicos de las víctimas, llenar los campos con la información correcta. Dar clic en el botón **"Add"** para agregar. Se guardan los datos, como se observa en la Fig. 56.

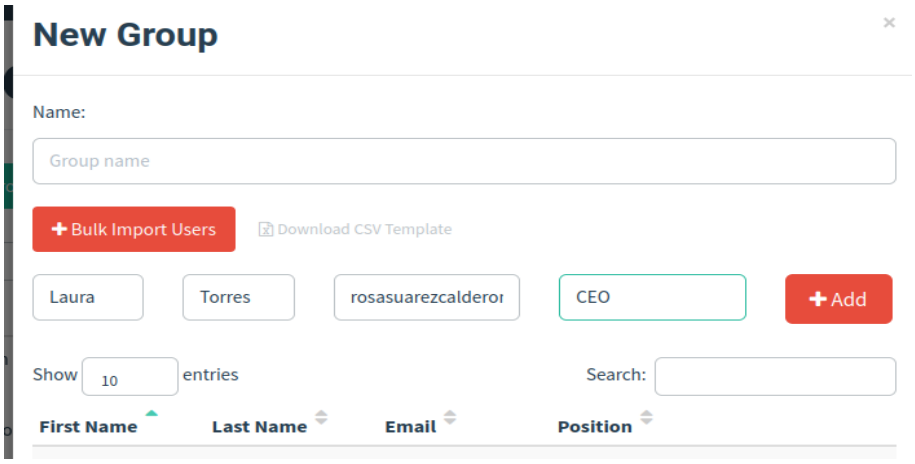

Fig. 56 Información de las víctimas (2024).

35) Los datos de las víctimas se guardan. Clic en **"Save Changes"** para guardar cambios, como se observa en la Fig. 57.

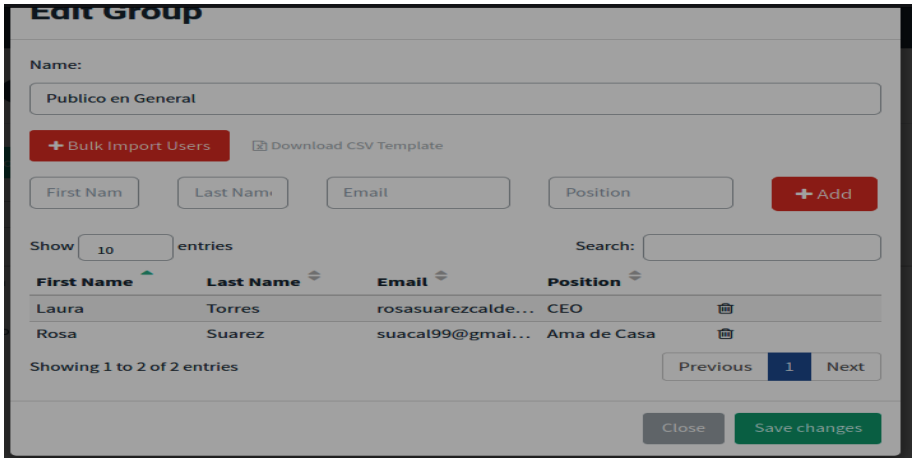

Fig. 57 Save changes (2024).

36) La configuración es exitosa, como se observa en la Fig. 58.

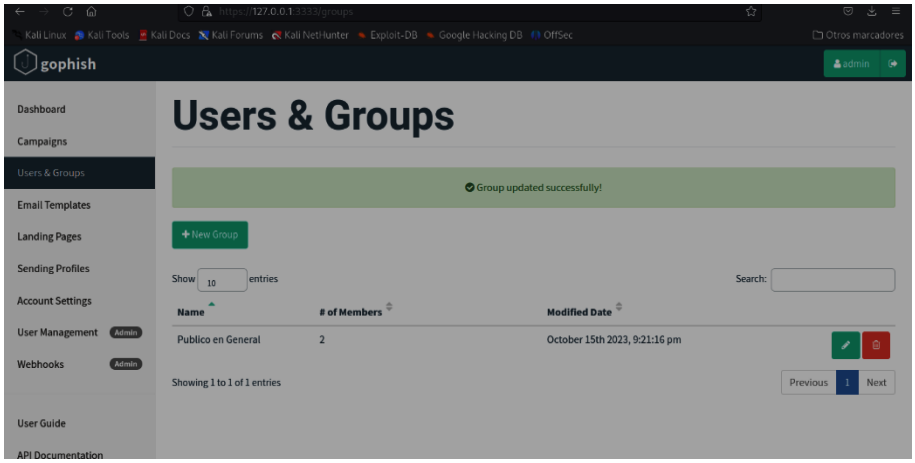

Fig. 58 User y groups exitosa (2024).

Una vez realizado el proceso de configuración de usuarios y grupos, llega el momento de crear la campaña.

A continuación, en los pasos del 37 al 43, se detalla la creación de la campaña.

37) Ir a la pestaña **"Campaigns"** para crear la campaña, dar clic en **"New Campaigns"**, como se observa en la Fig. 59.

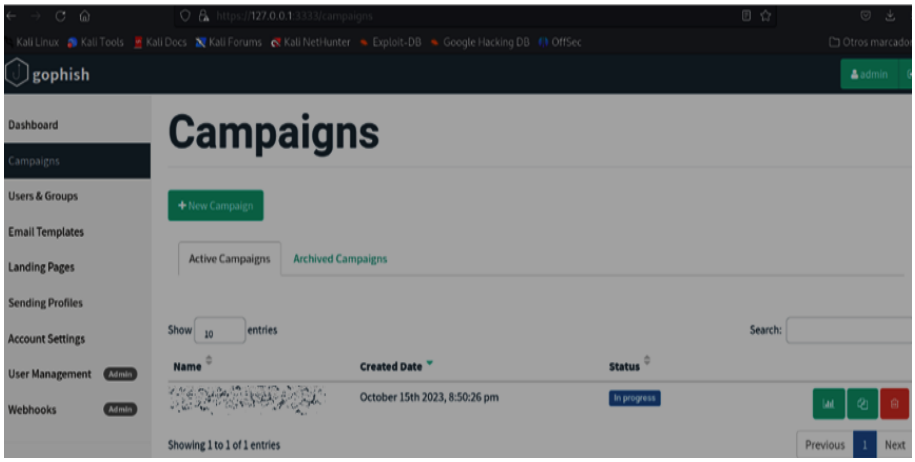

Fig. 59 Campaigns (2024).

38) Se observa la siguiente ventana, como se observa en la Fig. 60.

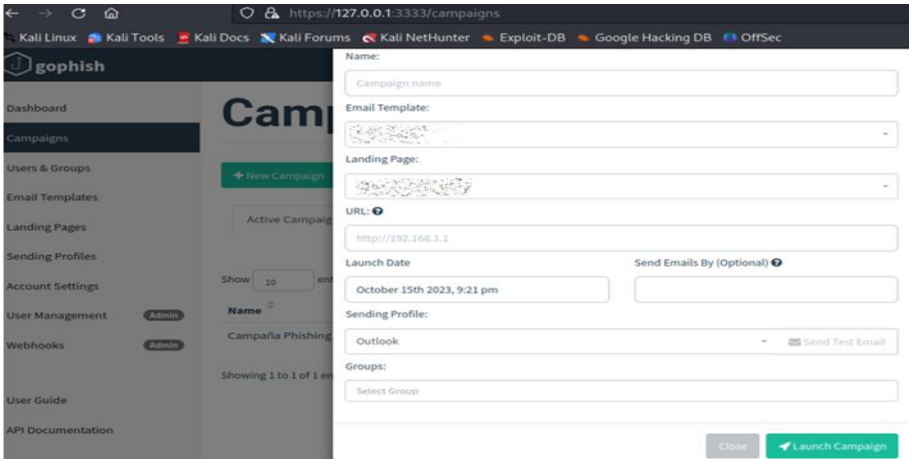

Fig. 60 New campaña (2024).

39) Llenar los campos con los datos correctos. Dar clic en **"Launch Campaign"** para crear la campaña de lanzamiento, como se observa en la Fig. 61.

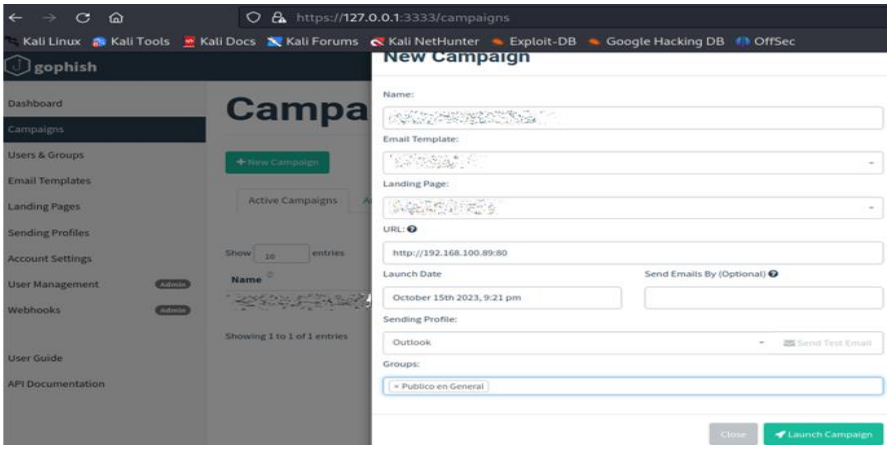

Fig. 61 Launch campaign (2024).

40) Clic en **"Launch"** para su lanzamiento, como se observa en la Fig. 62.

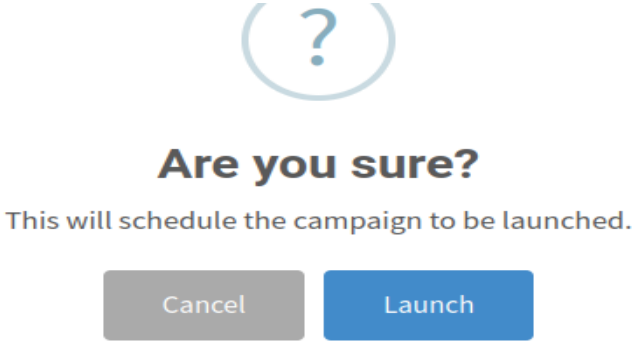

Fig. 62 Launch (2024).

41) Clic en **"OK"** para guardar la campaña, como se observa en la Fig. 63.

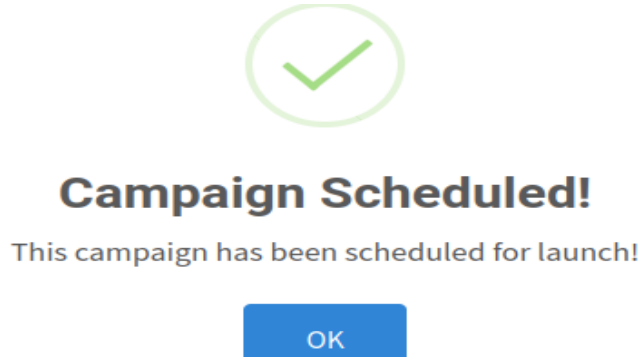

Fig. 63 OK (2024).

42) Una vez, terminado estas configuraciones aparece la página de los correos que fueron enviados, los correos que fueron abiertos, los enlaces a los que le dieron clic, la información que fue proporcionada por los usuarios y los correos que fueron reportados como posible Spam, como se observa en la Fig. 64 y 65.

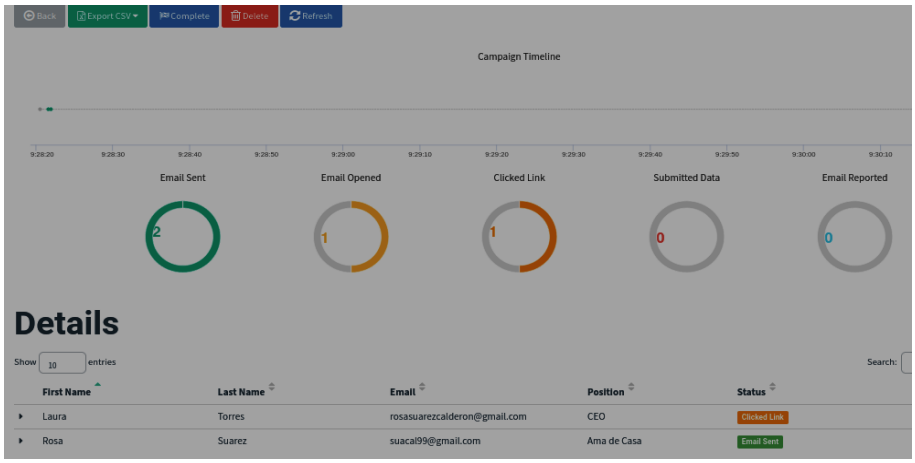

Fig. 64 Captura de resultados (2024).

Fig. 65 Captura de resultados1 (2024).

43) En la siguiente imagen se observa el usuario y contraseña ingresados por el usuario, como se observa en la Fig. 66.

Fig. 66 Captura de pantalla de resultados del usuario (2024).

En la siguiente infografía se muestra la creación de la campaña Afore Rosa.

Infografía. 2 campaña de phishing Afore Rosa (2024).

5.4. Pruebas

Una vez, realizadas las configuraciones necesarias para la creación de la campaña por Phishing Afore Rosa. Es momento de iniciar las pruebas necesarias para la realización de un ataque focalizado por phishing.

En los siguientes pasos se indica cómo realizar dicho ataque.

5.4.1. Prueba 1: Correo de suplantación Afore Rosa

Retomando los últimos pasos del 37 al 43 donde se explica cómo crear una campaña por phishing, es momento de enviar el correo de suplantación por la campaña Afore Coppel a los correos que se tienen asignados como pruebas.

Para esta prueba se utiliza el siguiente correo: suacal99@gmail.com

1) Se observa la campaña lanzada. En esta captura se observan los correos que se enviaron, los correos que fueron abiertos, los enlaces a los que se les dio clic, la información que fue interceptada y los correos que se reportaron como simple spam, como se observa en la Fig. 67.

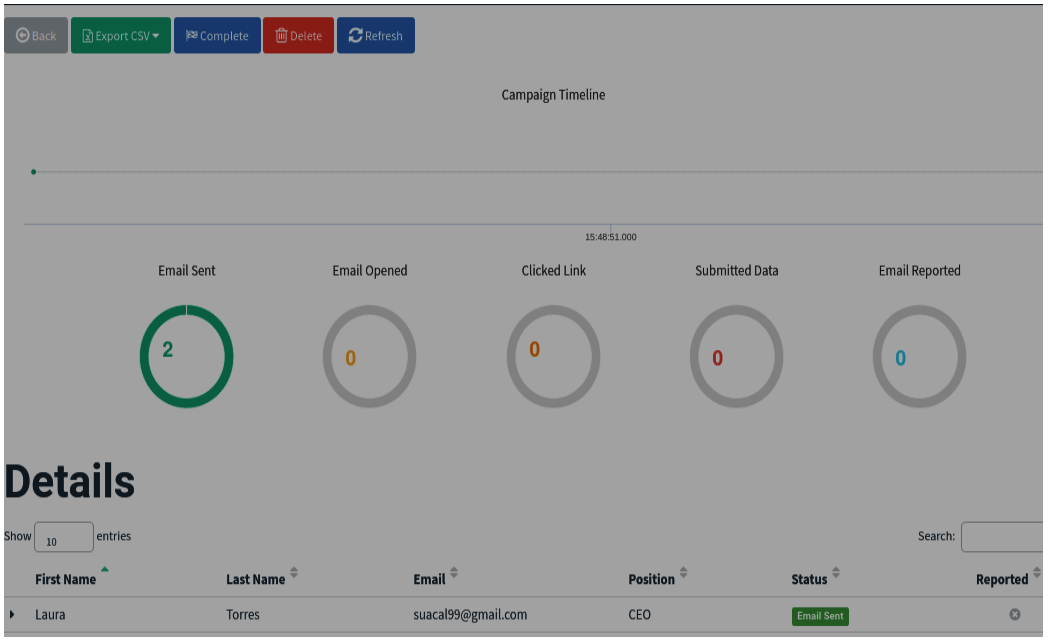

Fig. 67 Campaña lanzada Afore Rosa (2024).

2) Dar clic en **Refresh** para refrescar la página y se envié el correo clonado como se observa en la Fig. 68.

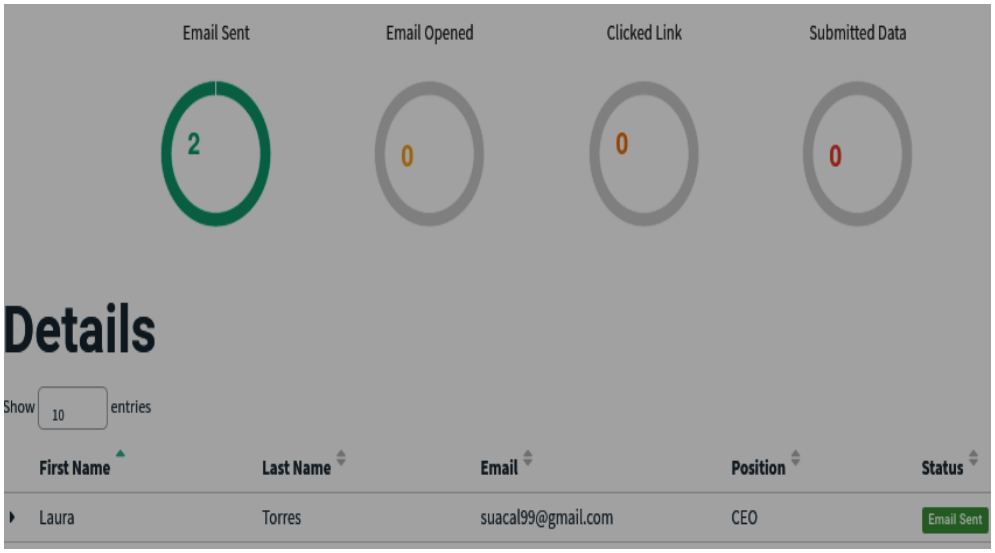

Fig. 68 Mensaje enviado (2024).

3) Ir al correo que se tiene como prueba. Se observa que el correo clonado fue llegado satisfactoriamente como se observa en la Fig. 69.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

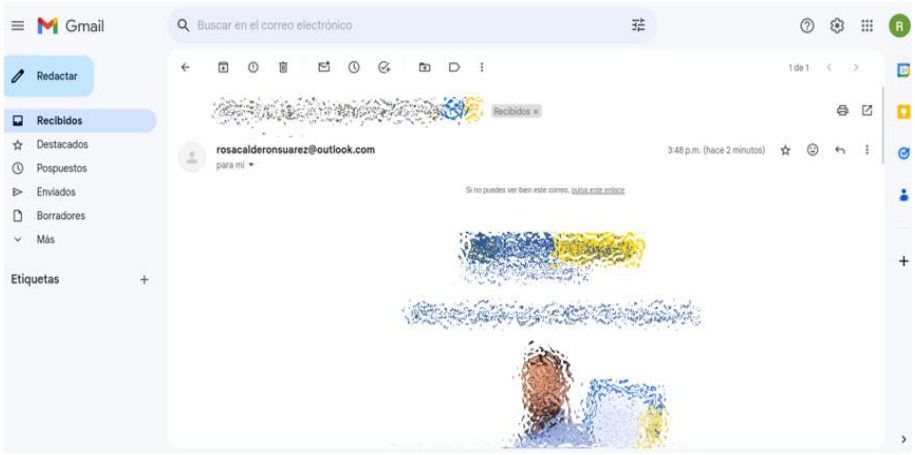

Fig. 69 Correo clonado (2024).

4) Al abrir el correo clonado, se dirige a la página principal de Afore Rosa, como se observa en la Fig. 70.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

Fig. 70 Afore Rosa (2024).

5) Una vez concluido el paso anterior, regresar a la herramienta de Gopshish. Refrescar la página y se observa que el correo y la página se han abierto exitosamente, como se observa en la Fig. 71.

Fig. 71 Herramienta gophish (2024).

6) Retomando el paso 4 donde se abre la página principal de Afore Coppel. Llenar los campos con la información requerida y dar clic en Aceptar. Al dar clic en aceptar la página cargará, pero se quedará en la misma página, ya que, en las configuraciones anteriores así se configuro. Como se observa en la Fig. 72.

Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

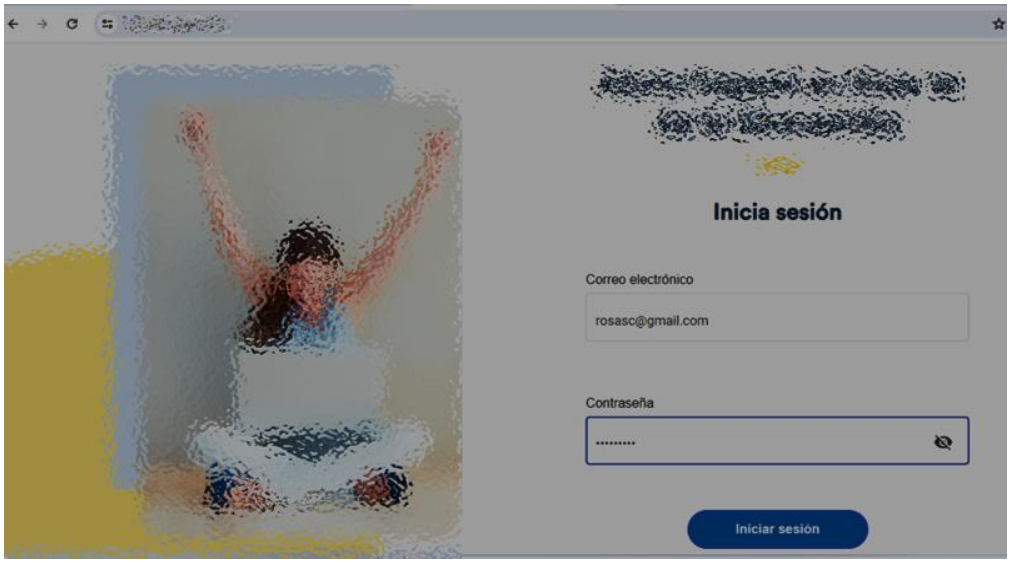

Fig. 72 rosasc@gmail.com (2024).

7) Regresar a la herramienta de Gophish, e ir a la pestaña **ExportCSV**. Dar clic en descargar. Abrir el archivo se observa el **usuario: rosasc@gmail.com** y **contraseña: Prueb@1!** ingresado. Como se observa en la Fig. 73.

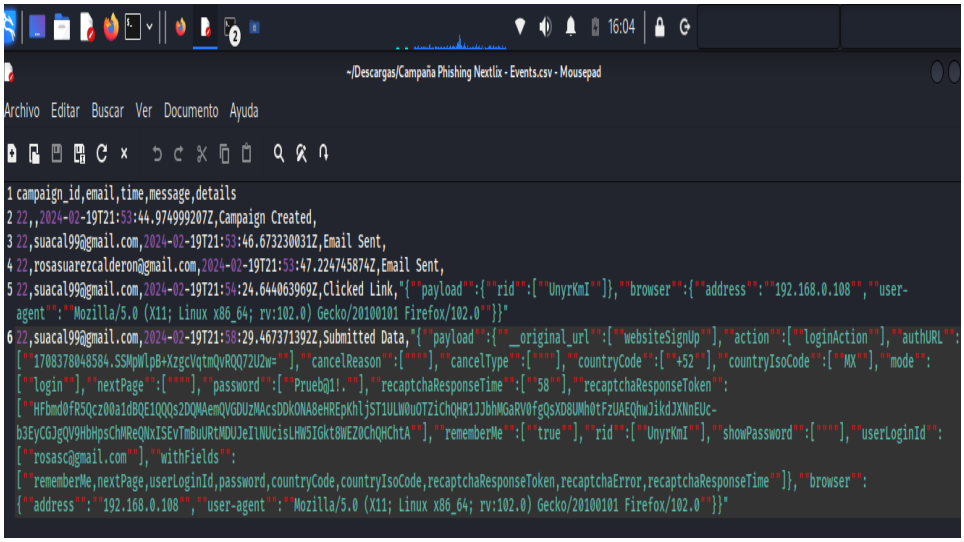

Fig. 73 Resultados del correo suacal99@gmail.com

5.4.2. Prueba 2: Correo de suplantación Afore Rosa

Para esta prueba se utiliza el siguiente correo: rosasuarezcalderon@gmail.com

1) Para la prueba 2, repetir los pasos del 1 al 5.
2) Retomando el paso 4 donde se abre la página principal de Afore Rosa. Llenar los campos con la información requerida y dar clic en Aceptar. Al dar clic en aceptar la página cargará, pero se quedará en la misma página, ya que, en las configuraciones anteriores así se configuro. Como se observa en la Fig. 74.

   Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

Fig. 74 Prueba2 (2024).

3) Regresar a la herramienta de Gophish e ir a la pestaña **ExportCSV**. Dar clic en descargar. Abrir el archivo se observa el **usuario: prueba2** y **contraseña: 12F@.\u0026#zZ.** ingresado. Como se observa en la Fig. 75.

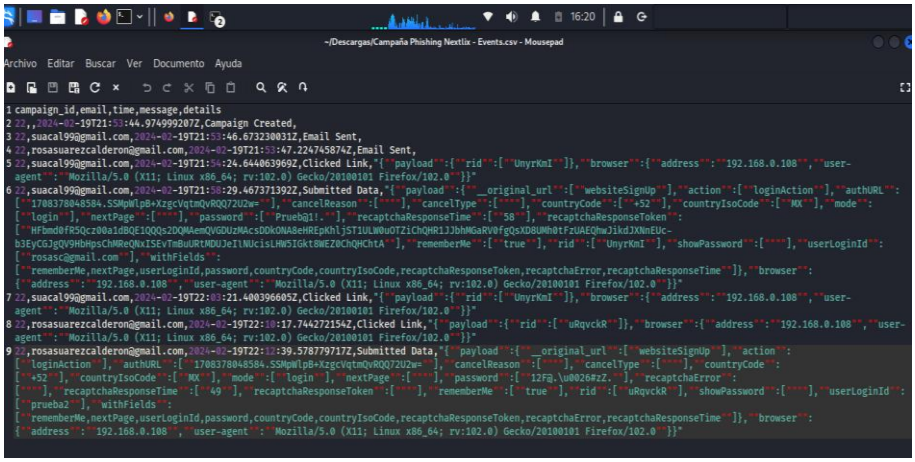

Fig. 75 Resultados del correo rosasuarezcalderon@gmail.com

5.4.3. Prueba 3: Correo de suplantación Afore Rosa

Para esta prueba se utiliza el siguiente correo: suacal99@gmail.com

1) Para la prueba 3, repetir los pasos del 1 al 5.
2) Retomando el paso 4 donde se abre la página principal de Afore Rosa. Llenar los campos con la información requerida y dar clic en Aceptar. Al dar clic en aceptar la página cargará, pero se quedará en la misma página, ya que, en las configuraciones anteriores así se configuro. Como se observa en la Fig. 76.

   Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

Fig. 76 rosa1 (2024).

3) Regresar a la herramienta de Gophish e ir a la pestaña ExportCSV. Dar clic en descargar. Abrir el archivo se observa el usuario: rosa1 y contraseña: Pros@12.! ingresado. Como se observa en la Fig. 77.

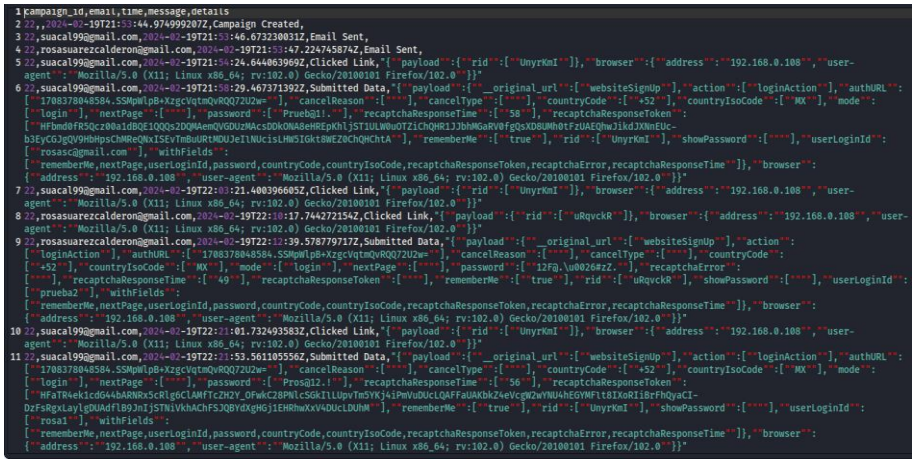

Fig. 77 Resultado2 del correo suacal99@gmail.com

5.4.4. Prueba 4: Correo de suplantación Afore Rosa

1) Para esta prueba, repetir los pasos del 1 al 5.
2) Retomando el paso 4 donde se abre la página principal de Afore Rosa. Llenar los campos con la información requerida y dar clic en Aceptar. Al dar clic en aceptar la página cargará, pero se quedará en la misma página, ya que, en las configuraciones anteriores así se configuro. Como se observa en la Fig. 78.

   Nota Importante: Este correo electrónico es ficticio sin daños a terceros.

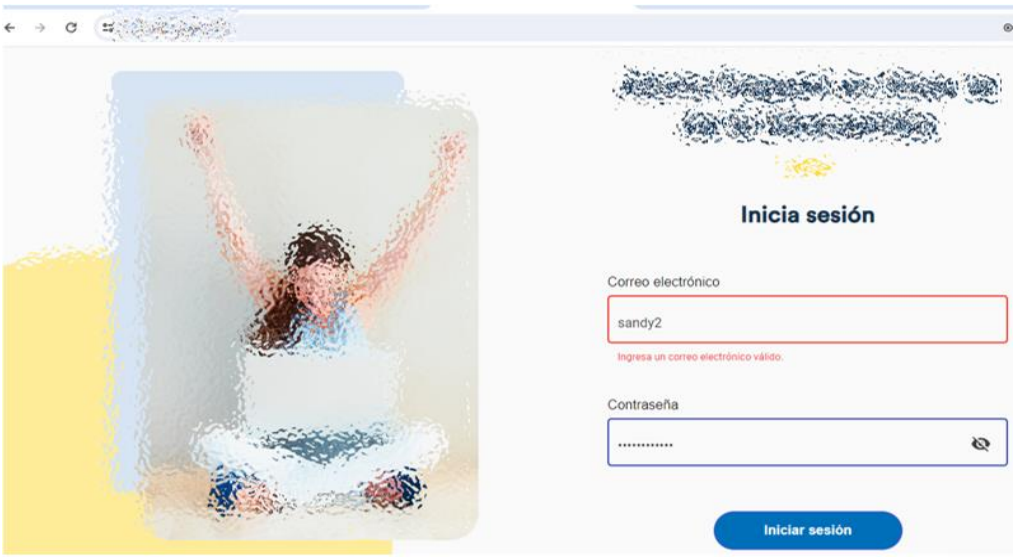

Fig. 78 sandy2 (2024).

3) Regresar a la herramienta de Gophish e ir a la pestaña **ExportCSV**. Dar clic en descargar. Abrir el archivo se observa el **usuario: sandy2** y **contraseña: @Qsandya12.¡5132.** ingresado. Como se observa en la Fig. 79.

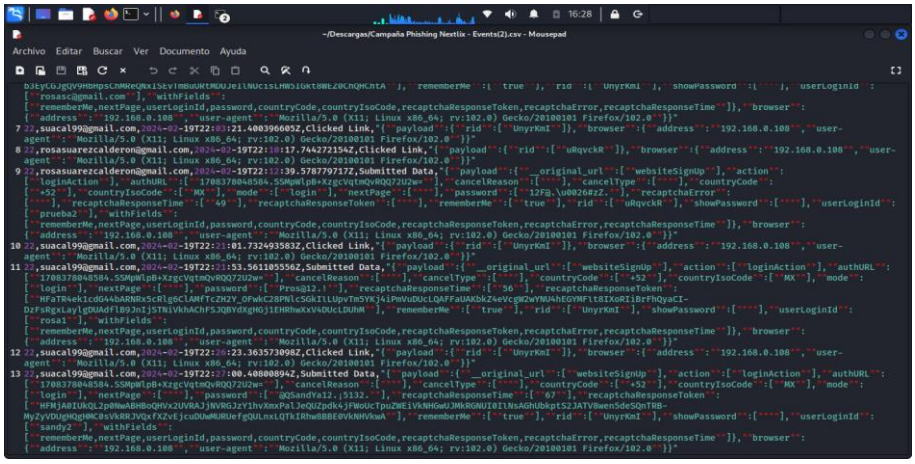

Fig. 79 Resultado del correo suacal99@gmail.com

En el siguiente diagrama se muestra cómo se realiza un ataque por phishing.

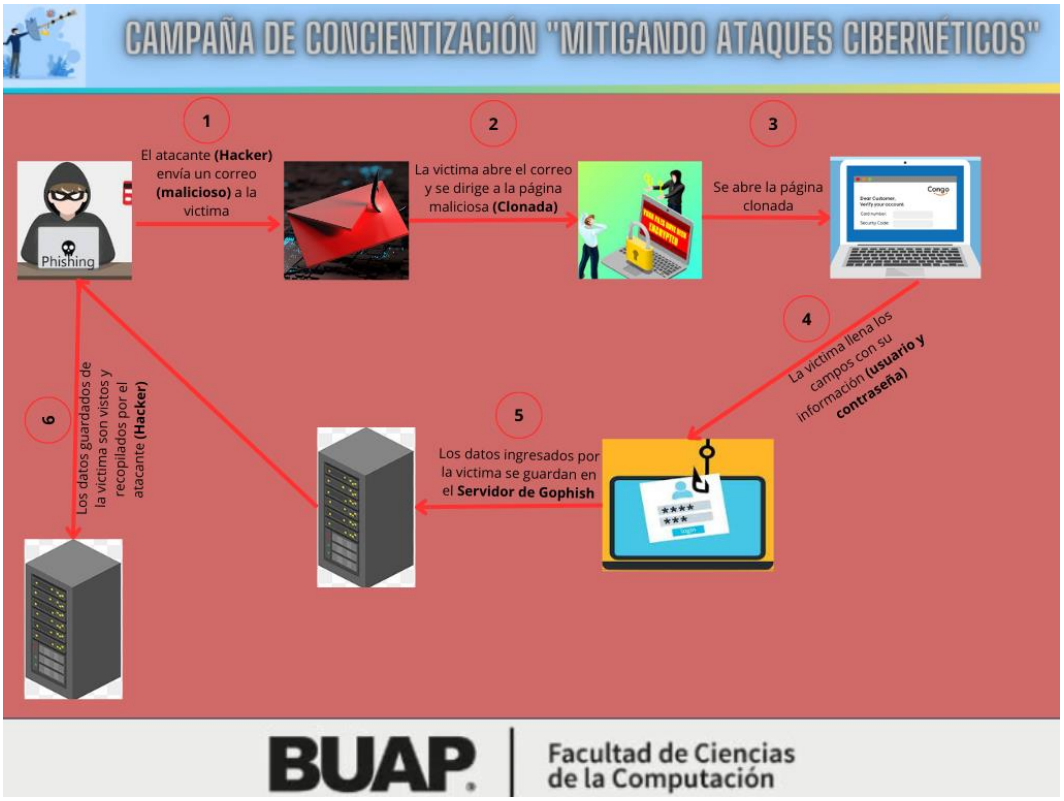

Diagrama. 1 Ejemplo de un ataque por phishing (2024).

Capítulo 6

Conclusión y Trabajo a Futuro

6. Conclusión y trabajo a futuro

En este capítulo se exponen las conclusiones a las que se llegaron tras realizar el proyecto de tesis y se presentan las opciones de trabajo a futuro que permitirán continuarlo.

6.1. Conclusiones

Hoy en día existen muchos ataques cibernéticos, pero desafortunadamente los usuarios no saben cómo reaccionar ante una situación así o con quien deben acudir para denunciar.

Con este proyecto se concluye que más personas sean conscientes del peligro al que están expuestos con el simple hecho de dar un **"solo clic"**, ya que, con esta simple decisión de dar clic y no revisar o leer lo que están aceptando podrían ser víctimas de robo de identidad.

Se concluye que, los ataques de phishing son realizados satisfactoriamente, ya que, los usuarios no verifican que las solicitudes del correo electrónico sean válidas y simplemente terminan por abrirlo.

Se concluye que los ataques por phishing se presentan porque a menudo los usuarios no están enterados si han sido víctimas de ataques por phishing, ya que ni siquiera conocen esta palabra. Otra razón es porque los usuarios no saben con quién acudir cuando les ocurre dicho suceso. También debido a que no saben si dicho ataque se debe denunciar y, por lo tanto, terminar por dejar la situación por la paz.

Por otro lado, **una regla de oro es**, si no están seguros de que la persona que envió el correo electrónico sea de un amigo, empresa o institución conocida, no lo abran.

Por último, se concluye que la **"Campaña por Phishing Afore Rosa"** fue realizada satisfactoriamente, obteniendo así los resultados esperados durante este proyecto.

6.2. Trabajo a futuro

Este proyecto puede continuar si se realizan más material de apoyo sobre los ataques cibernéticos (ataques por phishing), como, por ejemplo, pequeños videos o capsulas, exposiciones, trípticos o carteles (donde se hable sobre los ataques por phishing y los riesgos a los que están expuestos).

Otra sugerencia de trabajo a futuro es realizar platicas en escuelas (sin importar el nivel académico), al público (sin importar la edad), ya que la mayoría de los ataques por phishing se realizan satisfactoriamente a estos usuarios, ya que no cuentan con los conocimientos suficientes sobre el tema. Y por supuesto, no olvidar las pláticas a las empresas.

Por otro lado, otra sugerencia de trabajo a fututo es sobre la instalación de Gophish. La recomendación sería que al instalar Gophish se haga sobre un Servidor Web o un Servidor en la **Nube**, ya que, esto será más práctico, porque si se hace de manera local entonces se tendrá que abrir el correo electrónico(malicioso) cuando se esté conectado a la red del área local. Si no, al cargar la página creada no se verá y mostrará un mensaje que dirá que la dirección IP no se encontró.

Difundir campañas de concientización sobre todo tipo de ataques cibernéticos y orientar a dónde acudir para denunciar.

Capítulo 7
Bibliografías

7. Bibliografías

En este capítulo se presenta únicamente la bibliografía resultante de la investigación realizada para el proyecto de tesis.

7.1. Bibliografía

[1] IT Digital Media Group. (2023). Los ataques de phishing se incrementaron a nivel mundial casi un 50% en 2022 | Actualidad | IT Digital Security. https://www.itdigitalsecurity.es/actualidad/2023/04/los-ataques-de-phishing-se-incrementaron-a-nivel-mundial-casi-un-50-en-2022

[2] Nueva epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el apoyo de la IA. (2023, agosto 28). latam.kaspersky.com. https://latam.kaspersky.com/about/press-releases/2023_nueva-epidemia-el-phishing-se-sextuplico-en-america-latina-con-el-reinicio-de-la-actividad-economica-y-el-apoyo-de-la-ia

[3] Rodríguez, P. G. (2023, October 4). En 2022 crecieron 22% delitos cibernéticos, principalmente extorsión y difamación. La Jornada de Oriente. https://www.lajornadadeoriente.com.mx/noticias/economia_y_ecologia/reportes-sobre-incidentes-ciberneticos-2022-extorsion-y-difamacion/

[4] ¿Qué es el phishing? (2018, December 20). Malwarebytes. https://es.malwarebytes.com/phishing/

[5] Robo de identidad al acecho. (s/f). Gob.mx. Recuperado el 28 de octubre de 2023, de https://revista.condusef.gob.mx/2022/07/robo-de-identidad-al-acecho/

[6] About us. (s/f). EasyDMARC. Recuperado el 10 de abril de 2024, de https://easydmarc.com/about-us

[7] Condusef contenido. (s/f). Gob.mx. Recuperado el 10 de abril de 2024, de https://www.condusef.gob.mx/?p=contenido&idc=2217&idcat=1

[8] Santander México. (s/f). Santander.com. Recuperado el 10 de abril de 2024, de https://www.santander.com/es/sobre-nosotros/donde-estamos/santander-mexico

[9] About. (s/f). McAfee. Recuperado el 10 de abril de 2024, de https://www.mcafee.com/es-mx/consumer-corporate/about.html

[10] Petrosyan, K. (2022, julio 8). Estadísticas de phishing: Informe EasyDMARC [enero – junio de 2022]. EasyDMARC. https://easydmarc.com/blog/es/estadisticas-de-phishing-informe-easydmarc-enero-junio-de-2022/

[11] (S/f). Easydmarc.com. Recuperado el 10 de abril de 2024, de https://easydmarc.com/files/phishing-url-book.pdf

[12] Robo de identidad al acecho. (s/f). Gob.mx. Recuperado el 28 de octubre de 2023, de https://revista.condusef.gob.mx/2022/07/robo-de-identidad-al-acecho/

[13] Condusef contenido. (s/f). Gob.mx. Recuperado el 10 de abril de 2024, de https://www.condusef.gob.mx/?p=contenido&idc=2217&idcat=1

[14] Santander. (2022, marzo 29). Ciberseguridad para las pymes: una buena práctica que beneficia su negocio. Santander Bank. https://www.santander.com/es/sala-de-comunicacion/notas-de-prensa/2022/03/las-pymes-espanolas-ya-pueden-optar-a-las-ayudas-europeas-para-fortalecer-su-ciberseguridad

[15] El futuro de la seguridad de los datos del cliente: criptografía post-cuántica. (2024, marzo 18). Santander.com; Santander Bank. https://www.santander.com/es/stories/el-futuro-de-la-seguridad-de-los-datos-del-cliente-criptografia-post-cuantica

[16] Varadaraj, V. (2021, septiembre 3). Cómo evitar las estafas de phishing por correo electrónico. McAfee Blog; McAfee. https://www.mcafee.com/blogs/es-mx/privacy-identity-protection/como-evitar-las-estafas-de-phishing-por-correo-electronico//

[17] Labs, M. (2022, diciembre 7). Predicciones de amenazas de McAfee para 2023: evolución y explotación. McAfee Blog; McAfee. https://www.mcafee.com/blogs/es-mx/security-news/predicciones-de-amenazas-de-mcafee-para-2023-evolucion-y-explotacion//

[18] Cómo protegerte del "phishing" o suplantación de identidad. (s/f). AARP. Recuperado el 28 de octubre de 2023, de https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2019/suplantacion-de-identidad.html

[19] "Estafa CEO" y "Mail Spoofing" o suplantación de identidad por correo electrónico: las nuevas técnicas para estafar a las empresas. (s/f). Sayma. Recuperado el 28 de octubre de 2023, de https://www.sayma.es/estafa-ceo-y-mail-spoofing-o-suplantacion-de-identidad-por-correo-electronico-las-nuevas-tecnicas-para-estafar-a-las-empresas/

[20] ¿Qué es Smishing (SMS Phishing)? (s/f). Ibm.com. Recuperado el 28 de octubre de 2023, de https://www.ibm.com/mx-es/topics/smishing

[21] IRS, socios de la Cumbre de Seguridad advierten a los contribuyentes sobre una nueva estafa; correo inusual del servicio de entrega intenta engañar a las personas para que envíen fotos, información de cuentas bancarias. (s/f). Irs.gov. Recuperado el 28 de octubre de 2023, de https://www.irs.gov/es/newsroom/irs-security-summit-partners-warn-taxpayers-of-new-scam-unusual-delivery-service-mailing-tries-to-trick-people-into-sending-photos-bank-account-information

[22] Phishing: definición y métodos en un vistazo. (2023, febrero 14). IONOS Digital Guide; IONOS. https://www.ionos.mx/digitalguide/servidores/seguridad/phishing/

[23] Suplantación de identidad (phishing) y comportamiento sospechoso. (s/f). Microsoft.com. Recuperado el 29 de octubre de 2023, de https://support.microsoft.com/es-es/office/suplantaci%C3%B3n-de-identidad-phishing-y-comportamiento-sospechoso-0d882ea5-eedc-4bed-aebc-079ffa1105a3

[24] ¿Qué es el phishing? (s/f). Microsoft.com. Recuperado el 29 de octubre de 2023, de https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing

[25] ¿Qué es la caza de ballenas? (s/f). Ibm.com. Recuperado el 29 de octubre de 2023, de https://www.ibm.com/es-es/topics/whale-phishing

[26] (S/f). Cloudflare.com. Recuperado el 29 de octubre de 2023, de https://www.cloudflare.com/es-es/learning/email-security/business-email-compromise-bec/#:~:text=El%20compromiso%20de%20correo%20electr%C3%B3nico%20empresarial%20(BEC)%20es%20un%20ataque,objetivo%20estafar%20a%20sus%20v%C3%ADctimas.

[27] Dirección de Tecnologías de Información. (s/f). Uach.cl. Recuperado el 29 de octubre de 2023, de https://www.uach.cl/direccion-de-tecnologias-de-informacion/seguridad/tipos-de-phishing

[28] Algo de historia sobre Kali Linux. (s/f). Reydes.com. Recuperado el 29 de octubre de 2023, de https://www.reydes.com/d/?q=Algo_de_Historia_sobre_Kali_Linux

[29] Noel, E. P. (s/f). Gophish: Una poderosa herramienta de código abierto para simulaciones de phishing. Recuperado el 29 de octubre de 2023, de https://lignux.com/que-es-gophish/

[30] Bits Marketing. (2022, January 12). ¿Que es Phishing Campaign? Bits empresa de ti México; Bits Desarrollo e ingeniería IT sc. https://bits.com.mx/que-es-phishing-campaign/

[31] Iglesias, P. F. (2021, March 30). Campañas de phishing: ¿Cómo nos protegemos de los fraudes en Internet? CyberBrainers. https://www.cyberbrainers.com/como-protegerse-phishing-fraude/

[32] Bits Marketing. (2022, January 12). ¿Que es Phishing Campaign? Bits empresa de ti México; Bits Desarrollo e ingeniería IT sc. https://bits.com.mx/que-es-phishing-campaign/

Anexo 1. Diccionario de Términos

Definición de palabras

Phishing: Se conoce como phishing a la estrategia en la que los atacantes envían correos electrónicos malintencionados diseñados para estafar a sus víctimas.

Netmedia: Es una empresa editorial fundada en 1999 por Mónica Mistretta. **Es líder en generación de contenidos IT y medios B2B**. Es creadora de las marcas IT Masters (**Mag, Series, News y Update)** así como de **Las más innovadoras de México**.

Ransomware: El ransomware es un tipo de **malware** que bloquea los datos o dispositivos de una víctima y amenaza con mantenerlos bloqueados, a menos que la víctima pague un rescate al atacante.

Palo Alto Networks: Palo Alto Networks es una empresa de ciberseguridad que con su Plataforma de Seguridad Next Generation, está innovando y transformando por completo el mundo de la seguridad de la información para las empresas.

LockBit: Es una subclase de ransomware conocido como **«virus de cifrado»** que exige como rescate el pago de dinero a cambio de descifrar archivos. Se centra más en las empresas y organizaciones gubernamentales y no tanto en los particulares.

Inflobox: Se autodefine como la primera solución de nube que permite centralizar el control y automatizar DDI para redes híbridas y multinivel. También sostiene que simplifica y unifica los equipos de redes y seguridad en cualquier entorno.

IoT: El término IoT, o Internet de las cosas, se refiere a la red colectiva de dispositivos conectados y a la tecnología que facilita la comunicación entre los dispositivos y la nube, así como entre los propios dispositivos.

EasyDMarc: Cuyas siglas en ingles significan **“Domain-based Message Authentication, Reporting & Conformance”** o Autenticación de dominio basado en mensajes, reportes y conformidad. Es una política de autenticación para correos electrónicos que también funciona como un protocolo para generar reportes.

Condusef: La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, es un organismo efectivo para la protección y defensa de los intereses y derechos de los usuarios ante las instituciones financieras.

McAfee: Es un software **antivirus**, creado y mantenido por la empresa Intel Security, conocida anteriormente por Network Assoiates. El VirusScan Plus fue creado para uso doméstico; el VirusScan Enterprise para uso en pequeñas y medianas empresas.

Gophish: Es una herramienta de código abierto que permite a los usuarios **realizar campañas de ingeniería social** con el fin de recopilar credenciales de autenticación y otros datos sensibles (Phishing).

Ciberseguridad: La **ciberseguridad**, también denominada **seguridad de las tecnologías de información**, se centra en la protección de los sistemas informáticos, las redes y los datos frente a robos, daños o accesos no autorizados. El objetivo principal de la ciberseguridad es garantizar la confidencialidad, integridad y disponibilidad de los datos.

Kaspersky: Es antivirus propiedad de Kaspersky Lab, **una empresa centrada enteramente la ciberseguridad**. El origen de la empresa se remonta al año 1997 y su cede central se encuentra en Moscú, Rusia.

Pymes: Es el acrónimo utilizado a la hora de hablar de pequeñas y medianas empresas. Estas, generalmente suelen contar con un bajo número de trabajadores y de un volumen de negocio e ingresos moderados en comparación con grandes corporaciones industriales o mercantiles.

Ciberdelincuente: Persona que realiza actividades delictivas en internet como robar información, acceder a redes privadas, estafas y todo lo que tiene que ver con los delitos e ilegalidad.

CEO: El chief executive officer (CEO) es el máximo ejecutivo de una organización, encargado de diseñar y aplicar estrategias para lograr los objetivos.

Ataque de Phishing: Es una técnica de ingeniería social que consiste en él **envió de correos electrónicos** que suplantan la identidad de compañías u organismos públicos **y solicitan información personal y bancaria al usuario**.

Hacker: Es una persona o una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo. Los hackers también son conocidos como **"piratas informáticos".**

Pentesting: Es una abreviatura formada por dos palabras **"penetración"** y **"testing"** y es una práctica/técnica que consiste en atacar diferentes entornos o sistemas con la finalidad de encontrar y prevenir posibles fallos en el mismo.

Rufus: Es un programa que da utilidad para ayuda a las unidades de arranque flash USB de formato y crear, como llaves USB/ pendrives (Memorias Flash), tarjetas de memoria, etc. Puede ser cualquier Sistema Operativo.

Campaña de Phishing: Las campañas de simulación de phishing son un medio eficaz para enseñar a los empleados a detectar los mensajes engañosos y ayudar a combatir phishing. El éxito de estas campañas requiere planificación, comunicación y análisis.

Whaling: Es ataque de whaling es un método que usan los cibercriminales para simular ocupar cargos de nivel superior en una organización y así atacar directamente a los altos ejecutivos u otras personas importantes dentro de ella, con el objetivo de robar dinero, conseguir información confidencial u obtener acceso a sus sistemas informáticos con fines directivos.

Spear Phishing: Consiste en una modalidad phishing dirigida contra un objetivo específico, en el que los atacantes intentan, mediante un correo electrónico, conseguir información confidencial de la víctima.

Pharming: Es una combinación de los términos **“phishing”** y **“farming”,** es un tipo de cibercrimen muy semejante al phishing, en el que el tráfico de un sitio web es manipulado para permitir el robo de información confidencial. El pharming aprovecha los principios con lo que funciona la navegación por internet, es decir, la necesidad de convertir una secuencia de letras para formar una dirección de internet, como **www.google.com**, es una dirección IP por parte de un servidor DNS para establecer la conexión.

Smishing: El Smishing o fraude por mensaje de texto, es una variante de phishing en la que un atacante usa un atractivo mensaje de SMS para convencer al destinatario de que haga clic en un enlace, que le envía al atacante información privada o descarga programas malintencionados a un teléfono móvil o Smartphone.

Troyano: Es un tipo de malware que se descarga en una computadora disgrazado de programa legítimo. El método de entrega suele hacer que un atacante utilice la ingeniería social para ocultar código malicioso dentro del software legitimo para intentar obtener acceso al sistema de los usuarios con su software.

Microsoft: Es una compañía multinacional, que diseña y comercializa programas informativos y dispositivos electrónicos.

Apócrifo: Es algo que no es auténtico o no es obra de la persona a la que se atribuye.

Anexo 2. Encuesta

Se realiza realizará una encuesta a nivel facultad, universidad y público en general en la cual se realizarán un par de preguntas sobre "el tema de ataques de phishing" y así saber que tanto conocen sobre los riesgos a los que se encuentran expuestos hoy en día. Si no hacen un buen uso de la tecnología y así logar estadísticas de conocimientos.

Preguntas que se realizarán para la encuesta estudiantil y público en general:

1. Nombre Completo.
2. Esta navegando por internet y aparece un anuncio indicando; **"HAS SIDO EL GANADOR DE $100 MIL PESOS, DA CLIC EN "ACEPTAR" PARA PROPORCIONAR TUS DATOS Y HACERTE LLEGAR TU DINERO"**.

   ¿Qué haría al respecto?

   ☐ Confía en el anuncio y proporciona sus datos

   ☐ Ignora por completo el anuncio y lo cierra

   ☐ No sabe que hacer
3. Está en una red social y de repente llega un mensaje del perfil de uno de tus amigos con un enlace e indicando lo siguiente: **"TUS FOTOS APARECEN EN ESTA PAGINA Y NO SABIA COMO DECIRTELO"**.

   ¿Qué haría al respecto?

   ☐ Abre el enlace sin importar lo que pase

   ☐ Le pregunta a su amigo que fue lo que envió en realidad antes de abrir el enlace

   ☐ Ignora el mensaje y lo elimina
4. Se encuentra en su trabajo en el cual usted pertenece al área de nómina, su jefe ordena realizar unas transferencias y de pronto aparece un mensaje emergente mencionando lo siguiente: **"PARA REALIZAR MOVIMIENTOS EN TU CUENTA, DEBERAS ACTUALIZAR TUS DATOS".**

¿Qué haría al respecto?

☐ Ignora por completo el mensaje y lo cierra

☐ Da clic y hace las actualizaciones que le pide el banco

☐ Le informa a su jefa y llaman al banco para cerciorarse que la información es correcta

5. Recibe un correo electrónico del **"personal de recursos humanos"** solicitando proporciones tu documentación para el alta de seguro social, sin embargo, recuerda que ya había entregado su documentación anteriormente y no hacía falta ningún documento.

   ¿Qué haría al respecto?

   ☐ Ignora el correo y lo elimina

   ☐ Responde el correo y envía sus documentos

   ☐ No contesta el correo y busca a la persona de recursos humanos para informarle que no le hace falta ningún documento

6. Está jugando en línea y aparece un mensaje emergente de un perfil desconocido diciendo: **"ACEPTEME EN EL JUEGO, PARA HACERLO MAS DIVERTIDO"**.

   ¿Qué haría al respecto?

   ☐ Lo ignora y sigue jugando

   ☐ Lo acepta y juegan juntos

   ☐ No sabe que hacer

7. Hace uso de su equipo de cómputo y llega una notificación mencionando **"YA SE ENCUENTRA DISPONIBLE LA NUEVA VERSION DE TU ANTIVIRUS".**

   ¿Qué haría al respecto?

   ☐ Da clic sin leer antes y descarga la nueva versión

   ☐ Ignora el mensaje

   ☐ Se cerciora que la información sea correcta y después descarga la nueva versión

8. Requiere comprar cosas de la plataforma de mercado libre, al entrar de inmediato le pide que proporcione su número de tarjeta.

   ¿Qué haría al respecto?

☐ Ignora y cierra la página

☐ Se cerciora que la página a la que ingreso sea la oficial

☐ Proporciona su número de tarjeta

9. Está realizando una cita para su próxima consulta del IMSS, al ingresar a la página le pide que proporciones más datos de lo inusual.

   ¿Qué haría al respecto?

   ☐ Proporciona todos los datos aun sabiendo que antes no los requería

   ☐ Tiene duda sobre la página y mejor habla directamente a su clínica y agenda su cita

   ☐ No sabe que hacer

10. Entra en su Banca desde su aplicación móvil, de inmediato le pide que ingrese su toquen para que pueda realizar cualquier acción.

    ¿Qué haría al respecto?

    ☐ Proporciona su toquen

    ☐ No sabe que hacer

    ☐ Llama directamente al Banco para asegurarse que está acción es correcta

Una vez formuladas las preguntas, se procede a crear dos formularios con dichas preguntas, un formulario fue creado en Gmail y el otro en el Correo Institución para después pasar el enlace a los estudiantes, profesores y público en general y así responder dichas preguntas.

En las imágenes 1. y 1.1. se muestra el inicio de cómo se ven ambos formularios:

Imagen. 1 inicio del formulario creado en correo institucional (2024).

Imagen. 1.1 Inicio del formulario creado en Gmail (2024).

Para que se puedan contestar dichos formularios dar clic en el botón “Empezar ahora” que se encuentra en la parte inferior derecha

En las imágenes 2. y 2.1. se muestra el botón **“Empezar ahora”**

Imagen. 2 Clic en el botón “Empezar ahora” correo institucional (2024).

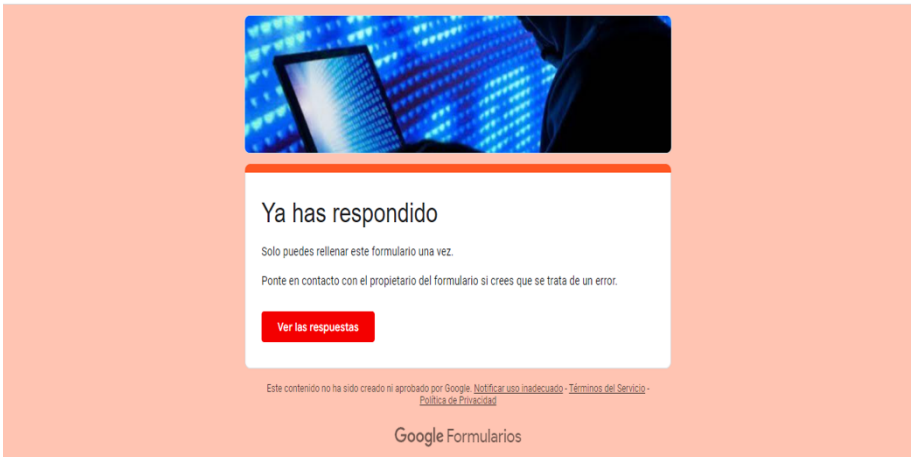

Imagen. 2.1 Clic en el botón “Empezar” Gmail (2024).

Una vez, dado clic en aceptar, se abrirán la pregunta que se deben de contestar y se observarán de la siguiente manera:

En las imágenes 3., 3.1., 4., 4.1., 5., 5.1., 6., 6.1., 7. Y 7.1. se muestran las preguntas que se deben responder:

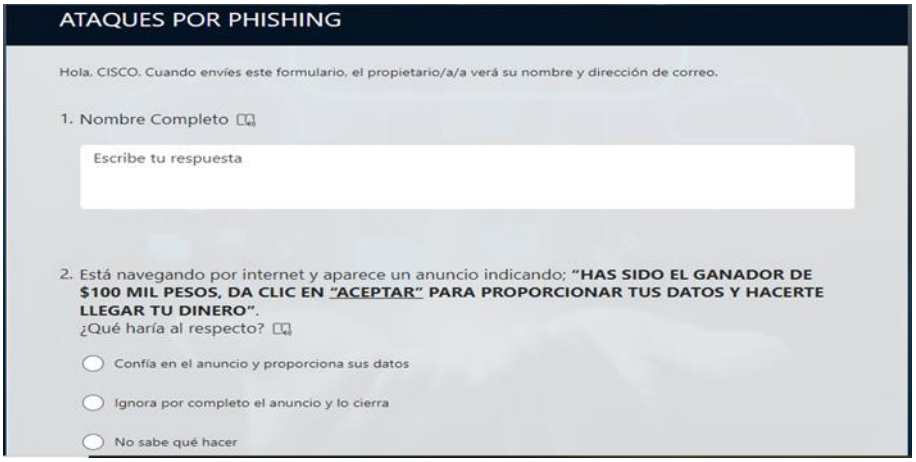

Imagen. 3 Preguntas para contestar correo institucional (2024).

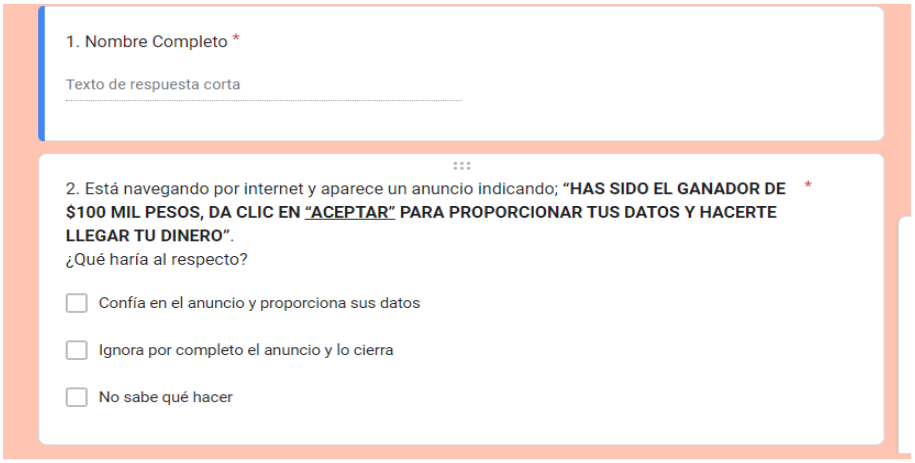

Imagen. 3.1 Preguntas para contestar Gmail (2024).

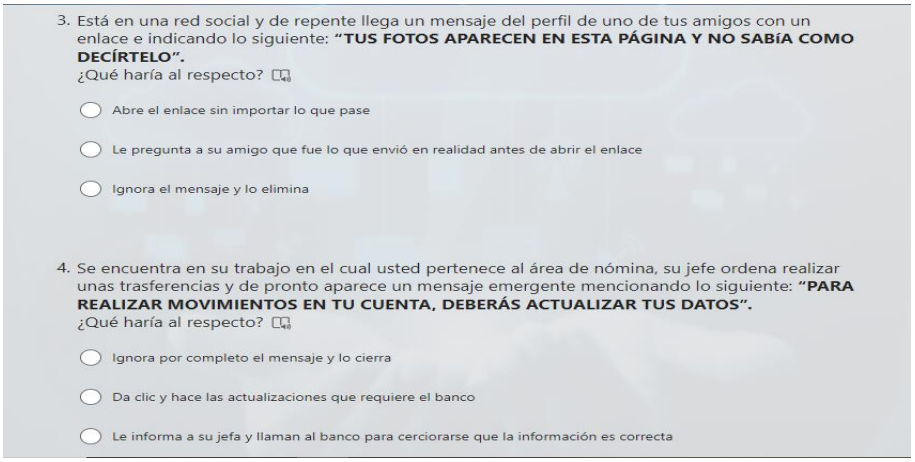

Imagen. 4 Preguntas para contestar1 correo institucional (2024).

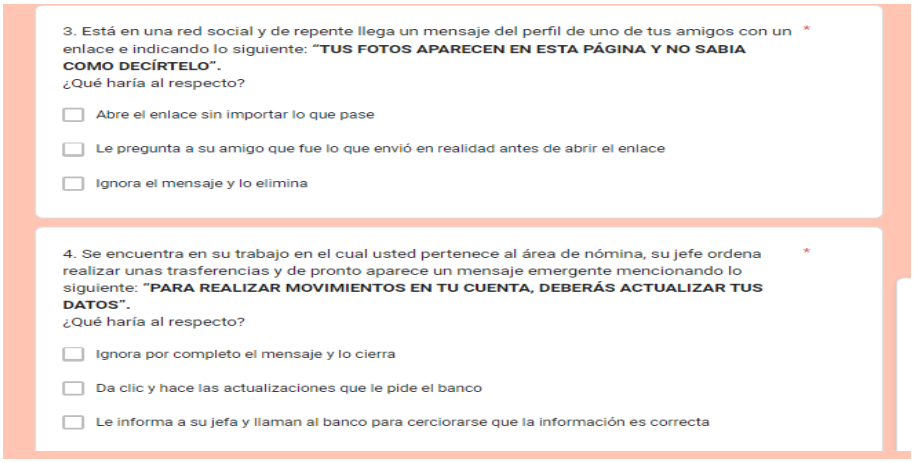

Imagen. 4.1 Preguntas para contestar1 gmail (2024).

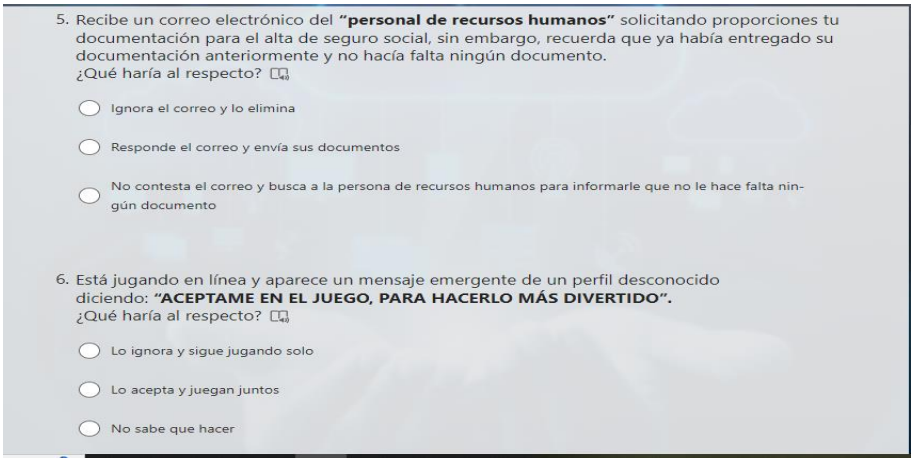

Imagen. 5 Preguntas para contestar2 correo institucional (2024).

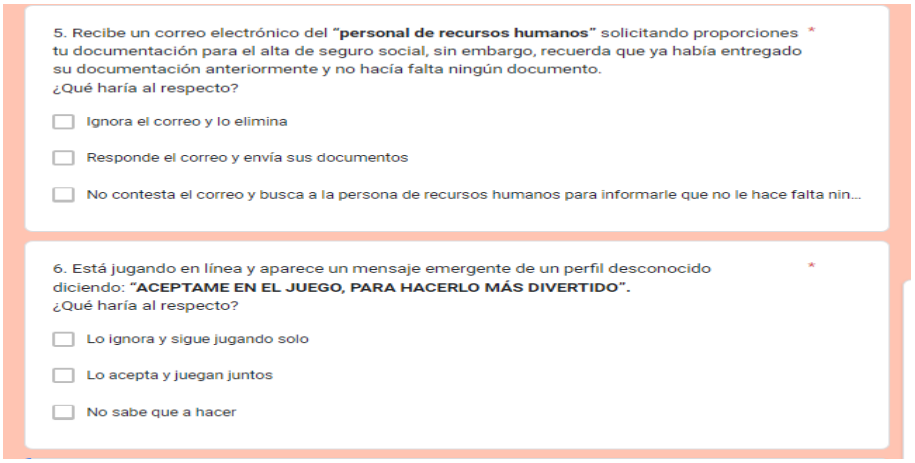

Imagen. 5.1 Preguntas para contestar2 gmail (2024).

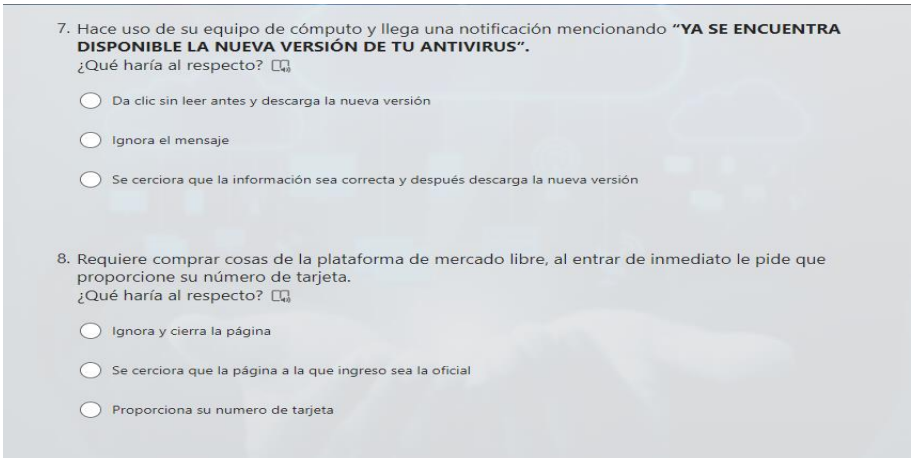

Imagen. 6 Preguntas para contestar3 correo institucional (2024).

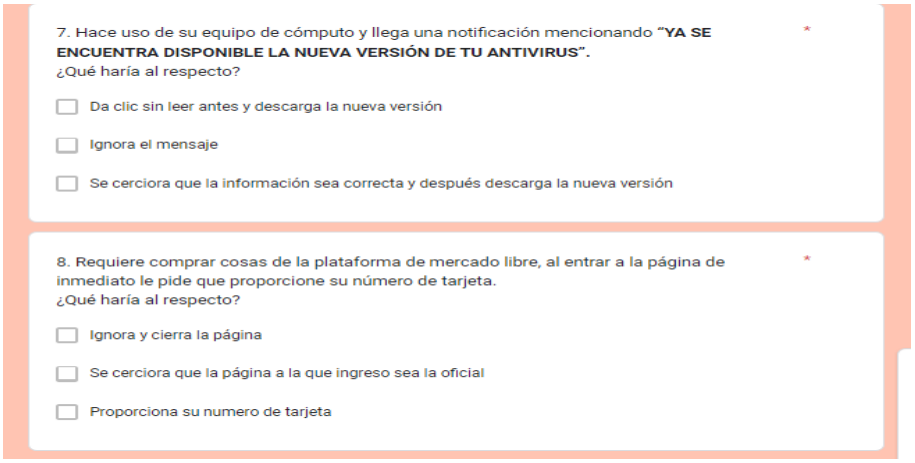

Imagen. 6.1 Preguntas para contestar3 gmail (2024).

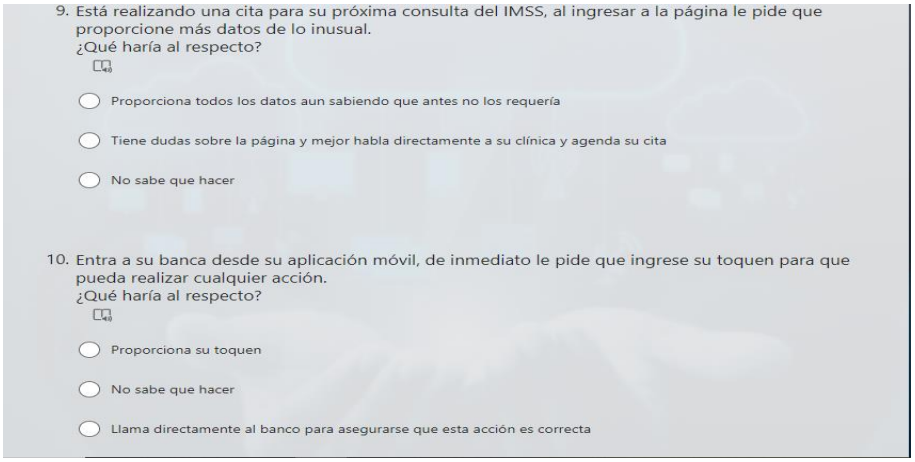

Imagen. 7 Preguntas para contestar4 correo institucional (2024).

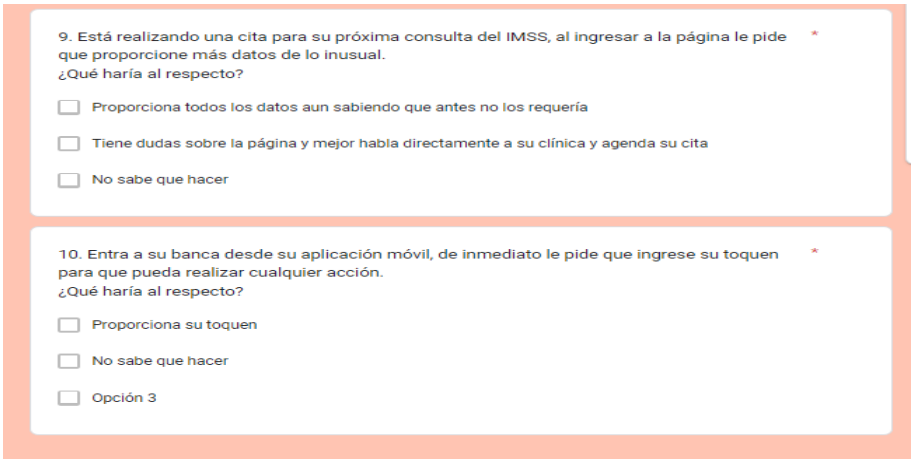

Imagen. 7.1 Preguntas para contestar4 gmail (2024).

Una vez, terminado de contestar sus preguntas, se procede a enviar sus respuestas, y una vez enviadas dichas respuestas se mostrará una ventana, la cual dirá que sus respuestas han sido enviadas correctamente.

En las imágenes 8. Y 8.1. se muestra la ventana que aparece después de enviar sus respuestas:

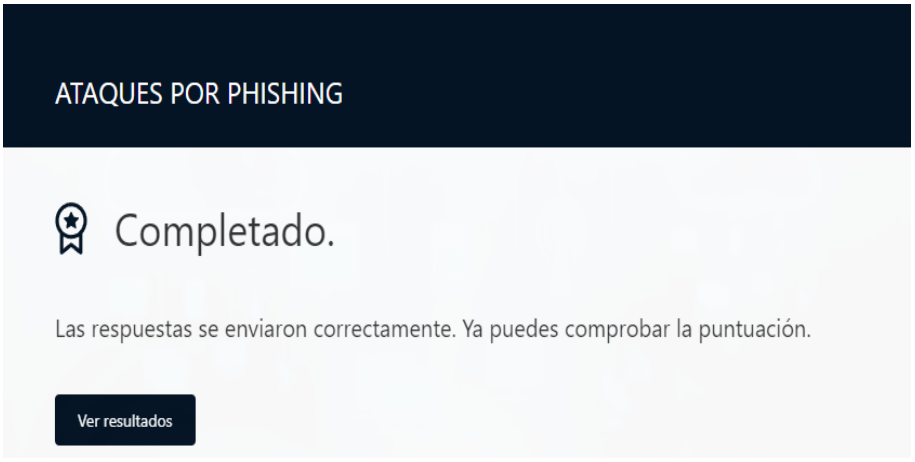

Imagen. 8 Pantalla de resultados enviados exitosamente correo institucional (2024).

Imagen. 8.1 Pantalla de resultados enviados exitosamente gmail (2024).

Resultados obtenidos

En las siguientes imágenes se muestran los resultados obtenidos después de realizar la encuesta a 75 usuarios sobre el tema ataques por phishing.

En la imagen 9 se muestra el resultado de la segunda pregunta sobre qué decisión tomarían los usuarios estando en un navegador web donde el 100% de los usuarios eligen ignorar por completo el anuncio y cerrarlo.

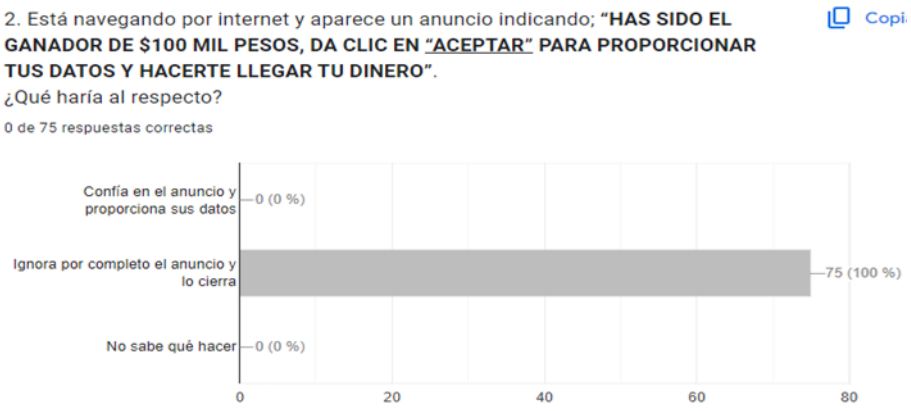

Imagen. 9 Navegando por internet (2024).

En la imagen 10 se muestra el resultado de la tercera pregunta sobre qué decisión tomarían los usuarios estando en una red social.

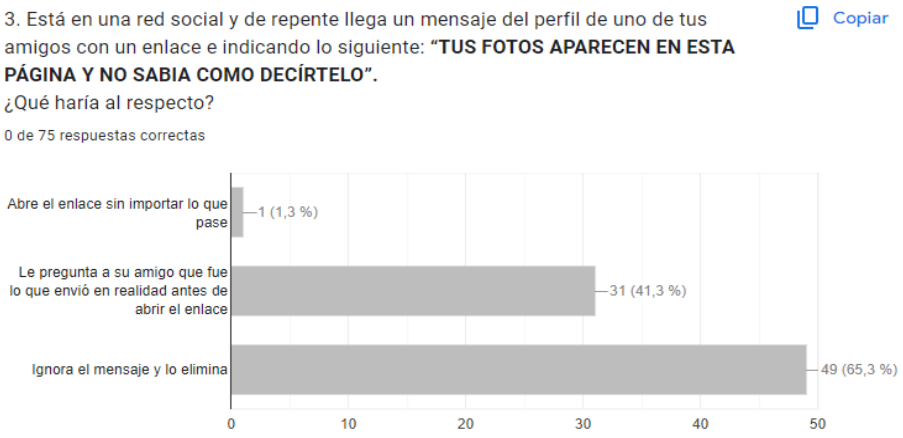

Imagen. 10 Red social (2024).

En la imagen 11 se muestra el resultado de la cuarta pregunta sobre qué decisión tomarían los usuarios estando en su trabajo y de repente les aparece un mensaje emergente.

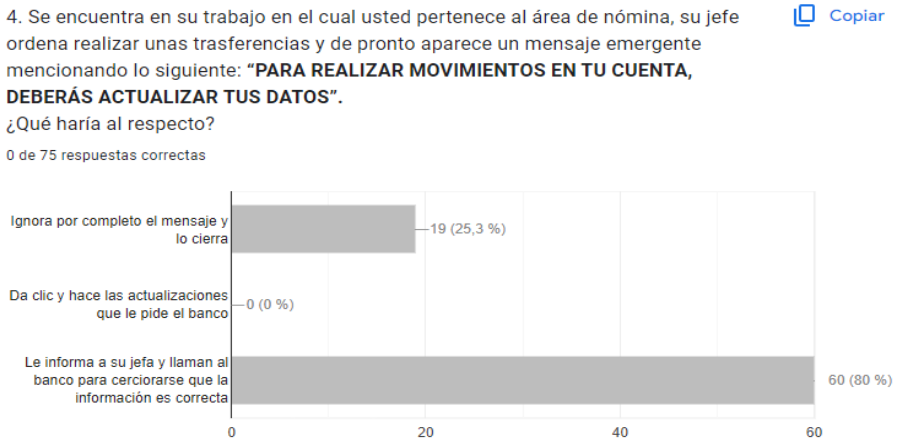

Imagen. 11 Mensaje emergente (2024).

En la imagen 12 se muestra el resultado de la quinta pregunta sobre qué decisión tomarían los usuarios al recibir un correo electrónico del área de recursos humanos solicitando sus datos personales.

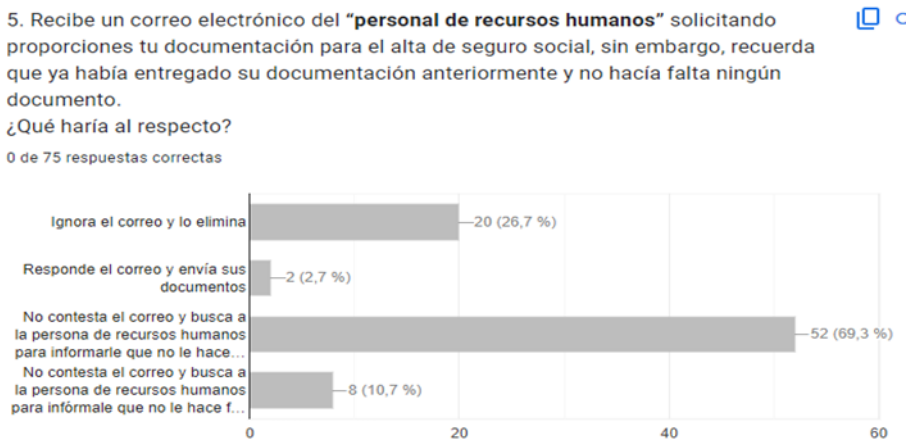

Imagen. 12 Correo electrónico (2024).

En la imagen 13 se muestra el resultado de la sexta pregunta sobre qué decisión tomarían los usuarios jugando en línea y de repente les aparece un mensaje emergente.

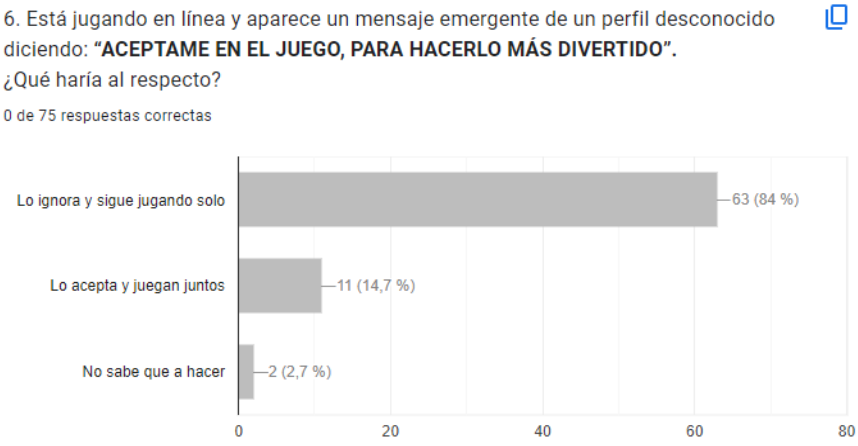

Imagen. 13 Juego en línea (2024).

En la imagen 14 se muestra el resultado de la séptima pregunta sobre qué decisión tomarían los usuarios haciendo uso de un equipo de cómputo y llega una notificación maliciosa.

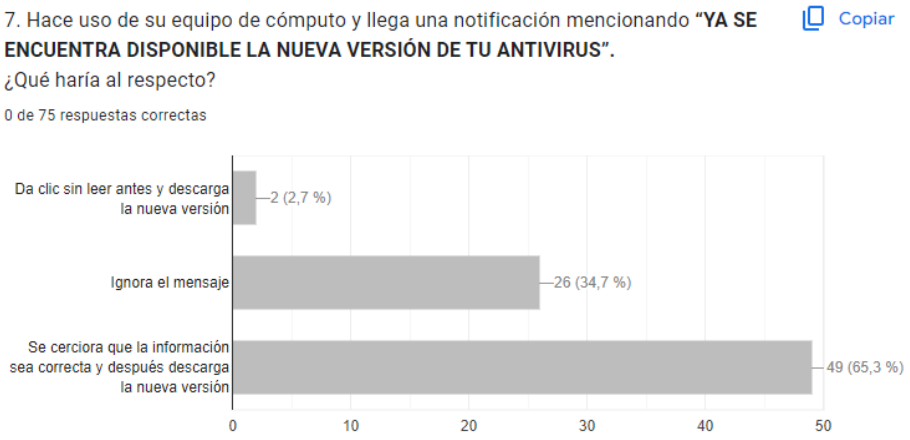

Imagen. 14 Actualización de antivirus (2024).

En la imagen 15 se muestra el resultado de la octava pregunta sobre qué decisión tomarían los usuarios cuando se encuentran comprando cosas por internet y de inmediato les piden que proporcionen su número de cuenta.

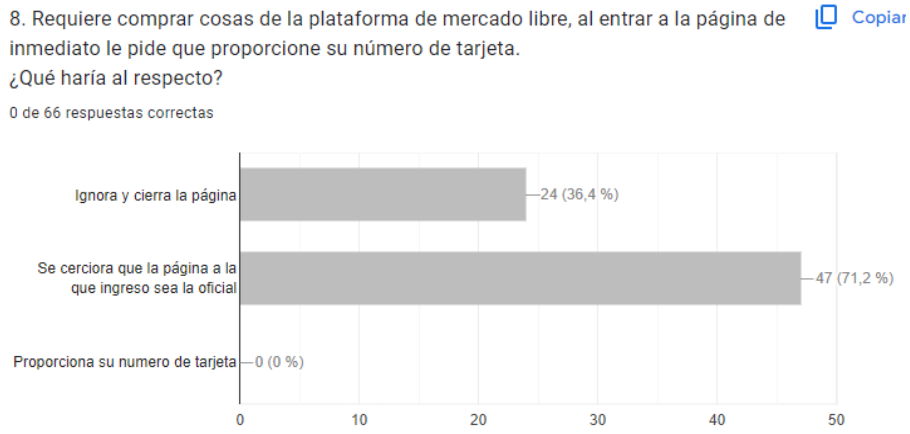

Imagen. 15 Compras por internet (2024).

En la imagen 16 se muestra el resultado de la novena pregunta sobre qué decisión tomarían los usuarios cuando se encuentra haciendo una cita por internet para su próxima consulta médica.

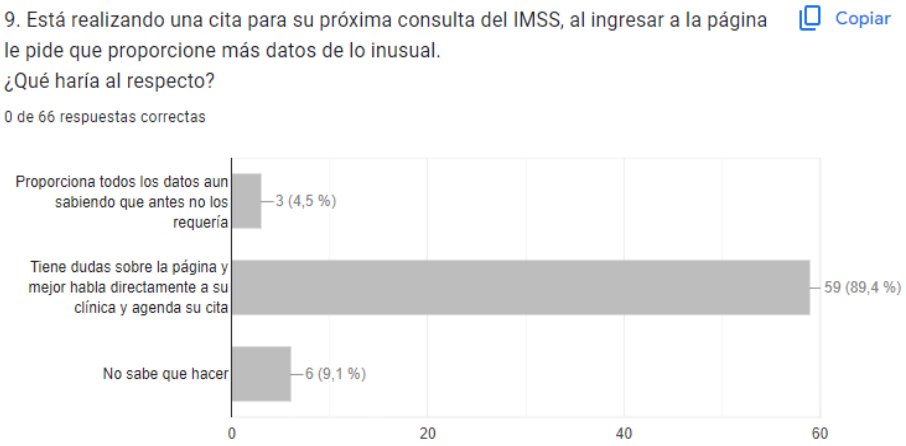

Imagen. 16 Cita médica (2024).

En la imagen 17 se muestra el resultado de la décima pregunta sobre qué decisión tomarían los usuarios cuando se encuentran en su banca por internet y de inmediato pide que proporcionen su toquen.

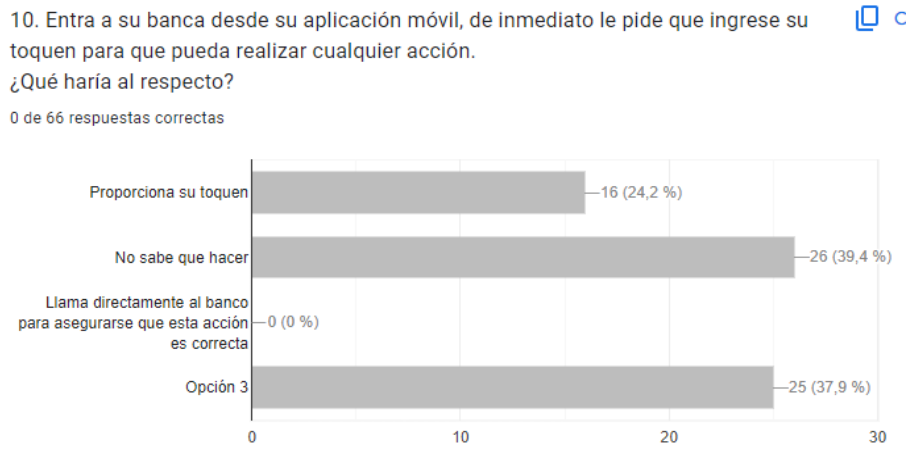

Imagen. 17 Banca por internet (2024).

Anexo 3. Repositorios

Para el presente proyecto. Se han desarrollado seis repositorios que abordan los siguientes temas de manera sistemática.

- Instalación de Kali Linux.
- Instalación de Rufus.
- Creación de una manera USB de arranque.
- Proceso de partición del disco duro.
- Arranque desde la memoria USB.
- Instalación y configuración de Gophish.

Los repositories están disponibles en la Plataforma de OneDrive.

[1] https://correobuap-my.sharepoint.com/personal/coordinacion_ics_fcc_correo_buap_mx/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing%2FRepositorio%201%29Instlacion%20Kali%20Linux%2Epdf&parent=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing

[2] https://correobuap-my.sharepoint.com/personal/coordinacion_ics_fcc_correo_buap_mx/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing%2FRepositorio%202%29Instalacion%20de%20la%20herramienta%20de%20Rufus%2Epdf&parent=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing

[3] https://correobuap-my.sharepoint.com/personal/coordinacion_ics_fcc_correo_buap_mx/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing%2FRepositorio%203%29%20Creacion%20de%20la%20memoria%20usb%20booteable%20de%20la%20imagen%20ISO%20de%20kali%20linux%2Epdf&parent=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing

[4] https://correobuap-my.sharepoint.com/personal/coordinacion_ics_fcc_correo_buap_mx/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing%2FRepositorio%204%29%20Proceso%20de%20particion%20para%20kali%20linux%2Epdf&parent=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing

[5] https://correobuap-my.sharepoint.com/personal/coordinacion_ics_fcc_correo_buap_mx/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing%2FRepositorio%205%29%20Proceso%20de%20inico%20de%20una%20PC%20desde%20una%20memoria%20booteable%2Epdf&parent=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing

[6] https://correobuap-my.sharepoint.com/personal/coordinacion_ics_fcc_correo_buap_mx/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FD

ocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing%2FRepositorio%206%29%20Proceso%20de%20instalacion%20y%20configuracion%20de%20Gophish%2Epdf&parent=%2Fpersonal%2Fcoordinacion%5Fics%5Ffcc%5Fcorreo%5Fbuap%5Fmx%2FDocuments%2FRepositorios%2F1%28Prevenci%C3%B3n%20riesgos%20Phishing