UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2021 – ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS Y SIMULACIÓN DE UN ATAQUE DE PHISHING EN EL USO DE UN FRAMEWORK GOPHISH EN LA COOPERATIVA DE TAXIS “SAN FERNANDO DE BABAHOYO”, DEL 2022.

ESTUDIANTE:

LISBETH DAYANA BAÑOS GALEAS

TUTOR:

ING. NELLY KARINA ESPARZA CRUZ

AÑO 2022

RESUMEN

El presente estudio de caso denominado: Análisis y simulación de un ataque de phishing en el uso de un framework gophish en la cooperativa de taxis “San Fernando de Babahoyo”, del 2022. Aplica la simulación de un ataque phishing en el uso de un framework gophish por lo cual es una herramienta que ayuda a conocer un método de ataque a la seguridad informática como es el phishing, además es un delito informático muy peligroso que puede llegar a exponer datos sensibles de una entidad a través de correos electrónicos, falsificando la identidad de alguna empresa de confianza para que algún usuario ingrese sus datos. Hoy en día existen varias herramientas informáticas tanto de paga como gratuitos para realizar algún ataque phishing, al emplear técnicas para este tipo de ataques lo recomendable es hacer uso de la ingeniera social en donde el atacante se hace pasar por una entidad oficial y envía mensajes que llame la atención de la víctima a través de correos electrónicos, un ejemplo de los mensajes de comunicación puede ser “regalo de un iPhone”, “actualización de contraseñas” entre otros , por lo cual los usuarios deben saber reconocer las paginas reales de las fraudulentas. El proceso de la investigación se realizó de manera eficiente y eficaz por lo tanto en el proceso del estudio de caso se empleó la metodología de investigación exploratoria por medio de la observación con enfoque experimental, del mismo modo el uso de técnicas de recolección de datos por lo que se utilizaron entrevistas.

PALABRAS CLAVES: Phishing, Servidor, Dominio, Ingeniería Social, Spam, Framework Gophish.

PLANTEAMIENTO DEL PROBLEMA

La problemática radica en que la cooperativa de taxis “San Fernando de Babahoyo” no cuenta con herramientas tecnológicas que proporcionen seguridad por lo que el uso de internet los datos quedan expuestos a cualquier amenaza o ataques por medio de sitios web.

En los últimos años los ataques phishing aumentaron significativamente a nivel mundial alcanzando los 245.771 de páginas fraudulentas por tanto puede variar la cifra dependiendo los meses y años debido a la actividad de los ataques (Harán, 2021). Ecuador no es la excepción en 2020 y 2021 se encuentra en 5to lugar entre los países que más se practica este tipo de ataques en Latinoamérica (Pichincha, 2022) . De tal manera el gobierno manifestó comunicados de alerta para prevenir el phishing, en vista de que se alteró la integridad de los usuarios. (Ecuador, 2021)

En la actualidad phishing es el ataque más frecuente donde se utiliza ingeniería social o suplantación de identidad. Busca obtener información personal por medio de servicios de mensajería, llamadas, mensajes cortos en redes sociales que maneja cualquier tipo de empresa u organización y al no tener conocimiento sobre cómo prevenirlo o cómo actuar en caso de que suceda este tipo de ataque puede ser perjudicial para la cooperativa de taxis “San Fernando de Babahoyo”, ya que sus datos personales quedan expuestos y puede ser utilizados con fines maliciosos.

Con este estudio de caso se pretende establecer una perspectiva de usuario al momento de realizar la simulación de ataque phishing para reconocer los mensajes reales de los mensajes fraudulentos y como evitarlos. Y utilizar herramientas que nos permitan mantener la información segura y prevenir posibles pérdidas.

El desconocimiento sobre seguridad informática en varias empresas, organizaciones o en la vida diaria permite confiar en mensajes que son creados para causar daño. La cooperativa de taxis “San Fernando de Babahoyo” tiene varios problemas entre ellos está la inseguridad física y la inseguridad informática. Por lo que se pretende utilizar la inseguridad informática ya que es una problemática existente en el campo tecnológico para enfocarlo hacia la cooperativa de servicios dedicada al transporte privado.

En las prácticas pre-profesionales se pudo evidenciar la falta de varias herramientas y sistemas de información para realizar procesos que beneficien a la cooperativa por otra parte, no se utilizan técnicas ni programas que proveen de seguridad hacia los datos e información confidencial.

Por lo tanto, se debe analizar la simulación de un ataque de phishing a través del uso de un framework GoPhish en la cooperativa “San Fernando de Babahoyo”, del año 2022. De manera que los usuarios puedan adquirir conocimiento sobre este tipo de ataque y tomar las medidas necesarias en caso de que se utilice phishing con spam los llamados correos no deseados que son recibidos varias veces.

Para reconocer un ataque phishing se considera el dominio ya que se denomina como irrepetible. Además, se emplean varias preguntas como: ¿De dónde proviene? si el correo es de alguna institución, empresa u organización existente, ¿Por qué razón? asimismo, si dicha persona solícito alguna ayuda o requiere una confirmación de empleo o información necesaria.

Con el paso del tiempo las nuevas tecnologías han evolucionado y también las nuevas técnicas de engañar a los usuarios y vulnerar la seguridad para así obtener información confidencial.

JUSTIFICACIÓN

La presente investigación está enfocado en la seguridad informática ya que vivimos en la era tecnológica de manera que los ataques son muy comunes y la inseguridad informática desempeña un rol importante en la accesibilidad, hoy en día los usuarios ingresan una gran cantidad de datos a sitios desconocidos por lo que existen un extenso número de ataques como malware, baiting, ddos, entre ellas está el phishing que buscan obtener información confidencial de los usuarios.

Phishing utiliza técnicas de camuflaje su diseño suele ser irreconocible para el usuario se manifiesta por medio de correo electrónico como Gmail, Outlook o Yahoo!, llamadas telefónicas o mensajes de texto, con enlaces que están vinculados a una página fraudulenta con el objetivo de extraer información personal de los usuarios utilizando herramientas para vulnerar la seguridad de los mismos.

El framework GoPhish open-source de código abierto, nos permite crear una simulación sobre este ataque de Phishing conectando con el servidor https://127.0.0.1:3333 en el puerto https://0.0.0.0:80 como usuario administrador.

En la cooperativa de taxis San Fernando de Babahoyo al utilizar constantemente el correo electrónico para recibir documentos importantes, está expuesta a que ingrese este tipo de ataques en la red por lo que todo el personal de la cooperativa de taxis necesita estar preparado para cualquier tipo de ataque que trate de violentar la integridad de la información de la cooperativa de servicios de transporte privado y de sus socios.

Por consiguiente estos ataques son utilizados en: paginas privadas de empresas u organizaciones, páginas de pago para el uso de tarjetas de crédito, páginas de juegos, páginas de compra y venta, páginas de empleo, mensajes de soporte técnico en distintas redes sociales.

OBJETIVOS

OBJETIVO GENERAL

Aplicar la simulación de un ataque de phishing en el uso de un framework Gophish en la cooperativa de taxis “San Fernando de Babahoyo”, del 2022.

OBJETIVOS ESPECIFICOS

- Emplear bibliográficamente estudios relacionados al ataque de phishing en el uso de un framework gophish.
- Analizar los distintos tipos de phishing y sus técnicas de manipulación.
- Definir el uso de framework gophish en los ataques de phishing.

LÍNEAS DE INVESTIGACIÒN

La línea de investigación es sistemas de información y comunicación, emprendimiento e innovación y la sublínea de investigación es redes y tecnologías inteligentes de software y hardware.

El presente estudio de caso análisis y simulación de un ataque de phishing en el uso de un framework gophish en la cooperativa de taxis “San Fernando de Babahoyo”, del 2022 está relacionado con los sistemas de información de la misma forma está enlazada con las redes y tecnologías inteligentes del software.

En las asignaturas de la malla rediseñada de sistemas información entre las cuales están: redes y comunicación, control y auditoría en las tecnologías de la información, programación avanzada, seguridad en computación se enfatizó conocimientos sobre el phishing y la interconexión en las redes que son necesarios para realizar este estudio de caso.

El framework gophish fue creado desde cero con el api json que es proporcionada a los desarrolladores, administradores de sistemas por consiguiente está diseñada en lenguaje go que tiene similitud con lenguaje c está enlazada con Python por lo tanto es utilizado para realizar testing del ataque phishing desde sus inicios del año 2009 hasta la actualidad.

MARCO CONCEPTUAL

INTERNET

Internet es una red de comunicación que utiliza líneas telefónicas, cables, satélites y comunicaciones inalámbricas para conectar computadoras y otros dispositivos a la world wide web. Todas las computadoras modernas pueden conectarse a Internet, así como muchos teléfonos celulares, algunos televisores, consolas de juegos y otros dispositivos. (Delgado, 2021)

Internet es una red de comunicación que conecta computadoras y otros dispositivos a la world wide web mediante líneas telefónicas, cables, satélites y comunicaciones inalámbricas.

VENTAJAS DEL INTERNET

ACCESO A LA INFORMACIÓN

"Es que contiene una gran cantidad de información a la que se puede acceder rápidamente sin ningún conocimiento técnico especial. Con su uso se puede obtener una buena fuente de información de una manera rápida". (MarcaGo, 2022)

COMUNICACIÓN

"Siempre que ambas partes tengan acceso a Internet, puede mantenerse en contacto con cualquier persona, independientemente de la distancia entre ellos. No hay barreras que los separen. Por lo tanto, la comunicación se vuelve más fácil." (MarcaGo, 2022)

HACER QUE LAS PERSONAS TRABAJEN JUNTAS

"Internet no solo brinda acceso a la información y un medio de comunicación, sino que también proporciona un marco que permite que diferentes personas trabajen juntas para lograr un propósito particular". (MarcaGo, 2022)

PERMITE MÁS OPCIONES PARA EL APRENDIZAJE

"Además de buscar información, las redes de Internet también han creado nuevos métodos, herramientas o métodos alternativos de aprendizaje para reemplazar los métodos tradicionales". (Go, 2022)

FACILITA LA GESTIÓN Y LA ORGANIZACIÓN

"A medida que Internet ha creado mejores formas de administrar el tiempo y las actividades, hay más formas de construir una buena organización. Para planificar o buscar información sobre una determinada gestión". (MarcaGo, 2022)

DESVENTAJAS DEL INTERNET

FRAUDE Y CIBERDELINCUENCIA

El inconveniente más común del internet es el riesgo de fraude y ciberdelincuencia, ya que proporciona una gran cantidad de datos personales importantes que pueden utilizarse de manera negativa para obtener ganancias de personas externas. Estos incluyen casos de ciberacoso, amenazas, robo de información personal, fraude y robo de datos personales. (MarcaGo, 2022)

El inconveniente más frecuente que presenta el internet es la inseguridad y el peligro de que seguridad sea vulnerada, por lo que el internet hace visible cada uno de los datos personales que son importantes para las empresas, personas externas al obtenerlos pueden utilizarlos negativamente y producir ganancias .

LA PRIVACIDAD ESTÁ AMENAZADA

Internet es para que las personas se conecten, pero compartir información presenta un inconveniente porque brinda a los demás parte de la privacidad de alguien. Otro punto relacionado con esto es que a las empresas les interesan los datos de las personas y existen

empresas profesionales encargadas de recopilar datos de los internautas y venderlos a otras empresas. (MarcaGo, 2022)

Internet permite la interconexión de los usuarios pero se maneja la privacidad en lo que otras personas pueden acceder. Las empresas pueden intercambiar ese tipo de información y venderlos a la competencia.

LA INFORMACIÓN PUEDE SATURARSE

Hay mucha información a lo que puede contener datos incorrectos o fuentes defectuosas. Por lo tanto, debe tener cuidado de encontrar información realmente confiable. Otro punto relevante es la sobresaturación. Esto se debe a que tiene demasiados datos y no sabe exactamente cómo manejarlos y dónde usarlos. (MarcaGo, 2022)

En internet existen datos incorrectos por consiguiente fuentes dañadas. Por lo cual se debe tener precaución al navegar en páginas web que sean confiables, también los servidores tienden a saturarse al almacenar demasiados datos.

SERVICIOS DE INTERNET

BÚSQUEDA Y TRANSFERENCIA DE INFORMACIÓN

La información se puede encontrar y transferir fácilmente, sobre cualquier tema en cualquier momento. Esta característica ha dejado obsoletas a las enciclopedias del mismo modo a los libros físicos. Algunas búsquedas arrojan decenas de miles de coincidencias, por lo que debe acotar su búsqueda utilizando ciertos criterios y filtros que limiten el número de resultados obtenidos. (Garcia, 2019)

El uso de búsqueda por medio del internet a realizado un gran cambio significativo por lo que dejo en el pasado las enciclopedias y libros físicos a información digital. El internet permite obtener la información más relevante en menos tiempo y sin esfuerzo.

CORREO ELECTRÓNICO (E-MAIL)

"Concede a los usuarios enviar y recibir correo electrónico que contiene texto, imágenes, videos y archivos adjuntos". (Garcia, 2019)

SERVICIOS COMO FOROS, REDES SOCIALES

"Facebook, Twitter e Instagram han demostrado ser excelentes plataformas de marketing, permitiendo el rápido intercambio y difusión de información entre grupos sociales con características similares". (Garcia, 2019)

CHATS EN LÍNEA

"Chat en línea es uno de los servicios de Internet más utilizados para enviar y recibir varios tipos de mensajes electrónicos. Los mensajes pueden ser leídos por cualquiera chat público o solo por personas autorizadas chat privado". (Garcia, 2019)

COMERCIO ELECTRÓNICO

En los últimos años, la compra de productos y servicios en Internet utilizando métodos de pago electrónico como tarjetas de crédito se ha incrementado de forma espectacular. Proveedores como Amazon están transformando la forma en que hacen negocios en todo el mundo al abrir cientos de miles de productos al público a precios asequibles. (Garcia, 2019)

El internet permite realizar compra y venta de los productos con la facilidad de pagar los productos de manera digital con beneficios en distintas empresas como Amazon.

SITIO WEB

Según MSc César A y Delgado B (2021). Es una colección de páginas web agrupadas y conectadas entre sí, a menudo en el mismo dominio o subdominio. Un sitio web en internet es una colección de archivos electrónicos y páginas relacionados con un

contexto en particular, incluida la primera página de inicio, accesible a través de un nombre de dominio y una dirección de internet específica. (César, 2021)

Los sitios web es la agrupación de páginas web que mantienen conexión entre sí pueden pertenecer al mismo dominio o subdominio dependiendo de su desarrollo, utilizan contenido en particular está constituida por el dominio y la dirección especial.

SEGURIDAD INFORMATICA

Los avances en la integración de las Tecnologías de la Información y la Comunicación están revolucionando la forma de intercambiar información entre empresas. Esta transformación digital ha abierto la puerta a un tipo de ciber delincuentes con capacidad de penetrar en el sistema para secuestrar o robar información de gran valor para las empresas de todos los sectores, incluso afectar la sostenibilidad del negocio. (E&L, 2021)

Los avances en las tecnologías de información están en constante cambio e innovación en el proceso de intercambio de información a través de empresas. Este tipo de tecnología ofrece desventajas, entre ellas está la inseguridad donde intervienen los ciber delincuentes denominados como personas que intentan forzar la seguridad con el objetivo de extraer la información para causar daño.

INGENIERIA SOCIAL

La ingeniería social es la principal causa del aumento de los ciberataques es la mayor dependencia de la población en internet. La ingeniería social es la base principal de ataques como el phishing. Es un conjunto de técnicas que tienen como objetivo engañar a los usuarios con principios como la reciprocidad, la urgencia, la confianza, la autenticación social o la autoridad. Los ciberdelincuentes desarrollan una estrategia discursiva mediante la cual convencen a los usuarios para que entreguen sus datos personales. (Bello, 2021)

La ingeniería social es el factor principal del incremento de ataques informáticos que aparecen en internet. De tal manera están relacionados con el ataque phishing por lo que se utilizan técnicas con la finalidad de manipular, y antivalores además desarrollan estrategias en lo que los usuarios son engañados en las que entregan su información personal.

SPAM

Spam es la palabra utilizada en el mundo para referirse a correos electrónicos no solicitados. El que envía el mismo mensaje de correo electrónico a miles o millones de personas a un costo mínimo, mucho menor que el correo tradicional, a la empresa a la que lo envía el por ello, el envío masivo de correos está a la orden del día. Si deja su dirección de correo electrónico en grupos, chats, foros de noticias es probable que su bandeja de entrada se inunde con mensajes promocionales que intentan venderle cualquier cosa. (Aranda, 2022)

Spam son correos intrusos que se realizan de forma repetitiva y son no solicitados, las empresas pagan dado que el emisor envía mensajes a un sin número de usuarios con el fin de ganar información para esa empresa. Además si el usuario mantiene su correo de manera pública en grupos, chats, foros, redes sociales es posible que aparezcan mensajes de spam de forma interminable.

DIGITALOCEAN SERVIDORES

DigitalOcean es un servicio de alojamiento y hospedaje en la nube que incluye VPS servidor privado virtual especialmente para desarrolladores. Con solo un clic, puede implementar la seguridad en su sitio web, juego o aplicación. Este servicio de alojamiento tiene un montón de características entre ellos esta: privacidad, seguridad, usabilidad y velocidad. (Smith, 2021)

En digitalocean ofrece servicios tanto para alojamiento y hospedaje mediante el cloud computing que contiene una VPS que es un servicio privado virtual para el uso de desarrolladores maneja seguridad en sitios web , en aplicaciones y también en juegos se destaca por ofrecer privacidad , usabilidad, seguridad, velocidad por lo tanto digitalocean provee de servicios de calidad para los usuarios.

DOMINIO

El término dominio como el nombre de una página web. Todos los sitios web tienen una dirección única que consta de números y una conexión al servidor que almacena los datos del sitio web; esta dirección se llama ip. (Valois, 2019)

BOTÓN DE IDENTIDAD DEL SITIO

El botón Identificación del sitio (un candado) aparece en la barra de direcciones cuando visita un sitio seguro. Puede averiguar rápida y fácilmente si la conexión al sitio está encriptada y, en algunos casos, a quién pertenece la conexión. Esta información lo ayudará a evitar sitios maliciosos que solo intentan obtener y robar su información personal. (García, 2022)

El botón de identificación del sitio es necesario direcciones en sitios, sirve para identificar según certificados si la página es segura o no cuenta con seguridad.

PHISHING

Este tipo de estafa implica el uso de varios métodos correo electrónico, sitio web, chat, para dirigir a las víctimas a un sitio web falsa y convencerlas de que están navegando en el sitio real. De esta forma, los atacantes obtienen información confidencial sobre los usuarios y sus cuentas, como números de tarjetas de crédito o débito, números de cédula de identidad o pasaporte, códigos secretos, contraseñas, dirección, número de teléfono, es decir, cualquier información útil para ellos cometer robo o fraude. Los sitios con este

ataque tienen colores, íconos y formatos similares para confundir a los usuarios. (Pichincha, 2022)

Este tipo de ataque utiliza estrategias en los que está presente en correos electrónicos, páginas web falsificadas y que los usuarios tengan la seguridad de que es auténtica. La información que es extraída pueden ser: números de cuentas de crédito, numero de cedula, códigos secretos, contraseñas, número de teléfono, dirección para estafar su diseño de la página web es irreconocible.

TIPOS DE PHISHING

PHISHING POR E-MAIL

Podría decirse que este es el tipo más común de ataque de Phishing. Este es el método tradicional de contactarse por correo electrónico. Básicamente, lo que está haciendo el atacante es hacerse pasar por una empresa u organización. Pueden utilizar direcciones de correo electrónico similares a las direcciones de correo oficiales, copiar logotipos, texto. Intentan hacer creer a la víctima que se trata de un mensaje importante y utilizan frases de advertencia para que los usuarios presten más atención y acaben visitando ese enlace malicioso. (Jiménez, redeszone, 2020)

Phishing por e-mail es el más usado en la historia del phishing en el que se hace pasar por empresas, organizaciones o instituciones importantes pero hace lo posible de que estas páginas web que empleen direcciones similares y el logo de los mismos.

VISHING

“El Vishing son ataques de voz. Allí utilizan mensajes sonoros reemplazan la identidad de una empresa u organización. Hacen que la víctima piense que está tratando con algo legítimo. De esta manera recopilarán información”. (Jiménez, redeszone, 2020)

QRISHING

Los códigos QR están muy presentes en nuestro día a día. Se utilizan para recopilar información en ciertos lugares. El problema ocurre cuando se modifica maliciosamente este código QR. Pueden ponerlo en lugares públicos donde el código suele ser legal. Al acercar el dispositivo móvil y leer este código, nos redirige a una web falsa que pone en riesgo nuestra seguridad. (Jiménez, redeszone, 2020)

QRishing es el phishing por medio de código QR que es muy común hoy en día nos permite acceder a cualquier sitio web por medio de un enlace, lo riesgoso es cuando este código QR esta enlazado a una página maliciosa.

PHISHING BASADO EN MALWARE

"El hacker agrega un archivo malicioso por lo general, reciben el correo y en lugar de un enlace a un sitio de phishing, el correo electrónico contendrá malware". (Jiménez, Redes Zone, 2020)

SIMULACIÓN DE ATAQUE PHISHING

FRAMEWORK GO PHISHING

Gophish es un software de código abierto que es completamente gratuito para que cualquiera lo use para simular un ataque phishing. Está escrito en el lenguaje de programación go esto tiene la ventaja de que los lanzamientos gophish son binarios compilados sin dependencias esto hace que la instalación sea tan simple como descargar y ejecutar esta implementado con el api json para la automatización. (Dewall, 2022)

Gophish de código abierto es un framework completamente gratuito para realizar simulación de ataque phishing, está escrito en lenguaje go y es fácil de instalar y acceder a esta herramienta tecnológica que utiliza la api json.

LENGUAJE DE PROGRAMACIÓN GO

Lenguaje de programación go también conocido como go lang es creado por Robert Griesemer, Rob Pike y Ken Thompson, con la empresa google. Es un lenguaje concurrente, hace algunos cálculos de formas diferentes sin afectar el resultado y es compilado, ya que el código fuente tiene que pasar por las etapas de traducción del código máquina para poder ser ejecutado. Aunque sus funciones son similares a la sintaxis de C. Go toma características de otros lenguajes y las implementa de una manera que hace que el código esté escrito para ser más fácil de usar. (Guerrero, 2021)

El lenguaje go es creado por Robert Griesemer, Rob Pike y Ken Thompson en conjunto con google realiza cálculos que no afectan al resultado final y se maneja la traducción de código por lo cual el lenguaje go es muy parecido a lenguaje c.

API JSON

"El api de json permite a los desarrolladores y administradores de sistemas automatizar campañas de phishing simuladas. Al ejecutarlo, se inician dos servidores web, una base de datos y agentes en segundo plano, que se encargarán de enviar correos electrónicos". (Land, 2022)

CONFIGURACIÓN (SETTINGS)

En el apartado de configuración podemos cambiar las credenciales del usuario o crear una nueva. La desventaja es que no hay un apartado donde se muestren todos los usuarios creados, por lo que para conocer este dato tendremos que acceder a la base de datos para ejecutar la consulta. También disponemos de la clave API que nos permitirá interactuar con la herramienta desde cualquier lenguaje de programación o scripting, por si preferimos utilizar otro método diferente a su interfaz web. (Rodríguez, 2018)

En la configuración se puede intercambiar credenciales del usuario o establecer una nueva se debe ingresar a la base de datos ya que no está incluido el apartado que se muestran todos los usuarios y además se tiene que poseer la clave del api que permite interrelacionarse con la herramienta a través de cualquier tipo de lenguaje de programación al utilizar otra forma de la interfaz que maneja la web.

PERFILES DE ENVÍO (SENDING PROFILES)

Muestre la dirección válida en el campo from y el servidor junto al puerto al que se enviará el dispositivo. Indica si tiene un certificado de la cuenta que desea utilizar para el envío. En cambio sí utilizan el buzón o lo que devuelve sin garantía, puedes dejar dos espacios en blanco. Si hay un problema con el certificado, ya sea un certificado autofirmado, un certificado de un certificado que no es de confianza (CA) o un certificado que no es de confianza. (Rodríguez, 2018)

En los perfiles de envió se visualiza la dirección del from con el puerto que realizara él envió al dispositivo, se realizan procesos para saber si tiene certificados de cuenta que se necesita para él envió además si se usa el buzón se pueden dejar los espacios en blanco se verifica si el certificado es de confianza.

PÁGINA DESTINO (LANDING PAGE)

Es aconsejable crear una página lo más parecida posible a la que pretendemos reemplazar hay una opción para importar páginas. Esta página se almacena en la base de datos configurada en el sistema, asignándole un id, parámetro rid para crear la URL completa que utilizaremos en las campañas en las que participe. (Rodríguez, 2018)

En la opción landing page se debe crear una página web con un diseño parecido al original por lo cual se almacena en la base de datos que se configura en el sistema se

le asigna un id y parámetro rid para poder crear un enlace que esté vinculado a esta página para crear este tipo de ataque para los usuarios.

PLANTILLA DE EMAIL (EMAIL TEMPLATE)

"En esta sección, deberá crear un correo electrónico para enviar a las víctimas. Este correo electrónico contiene una enlace que redirige a la página donde tenemos el formulario para obtener la información de inicio de sesión de la víctima". (Rodríguez, 2018)

USUARIOS Y GRUPOS (USERS & GROUPS)

En esta sección, se registra el grupo de víctimas que serán objeto de la simulación. La información opcional a completar es: nombre, apellido, puesto en la empresa. y el campo obligatorio es correo electrónico, ya que sin él no permitirá la creación de un usuario o grupo. (Rodríguez, 2018)

En la parte de user & groups se agregan el grupo de victimas que se utilizaran en la simulación del ataque phishing. La información que se debe colocar es nombre, apellido, puesto de la empresa, correo electrónico que es el más importante para realizar esta simulación.

CAMPAÑAS (CAMPAIGNS)

En esta sección crearemos una campaña para enviar. Nombre de campaña, plantilla de envío de campaña creada previamente. Solíamos crear un sitio web donde se redirige a la víctima para recuperar sus datos. Programación si queremos enviar una campaña opcionalmente, se anuncia la última fecha y hora de envío para que el sistema programe los envíos en el período de tiempo que se muestra entre este y la fecha de inicio. Envía el perfil al servidor de correo electrónico que se usa para la campaña. (Bastian, 2018)

En esta opción de campaigns se registra una campaña para enviar a las víctimas. Es necesario registrar nombre de la campaña, colocar una plantilla que se desarrolla para realizar la simulación que tiene que tener su diseño igual a la página real, se utiliza programación para enviar la campaña y colocan las respectivas fechas.

ESTADÍSTICAS DE LAS CAMPAÑAS

Una vez que se crea la campaña, puede acceder a los eventos para ver si la víctima abrió el mensaje, ingresa a la página del enlace y envíe el formulario con la información que tiene que llenar la víctima. La opción de publicidad por correo electrónico está en versión beta y tiene como objetivo proporcionar un contexto para que las víctimas las alerten sobre el phishing y se aseguren de que estén al tanto de este riesgo. (Bastian, 2018)

Por consiguiente después de crear la campaña se verifica si el usuario ingreso al enlace y lleno el formulario correspondiente. La publicidad por el correo electrónico su objetivo es advertir a los usuario sobre el phishing.

PANEL (DASHBOARD)

“En esta sección puede encontrar una recopilación de todas las configuraciones del proyecto, ya sea completada o no, así como datos internacionales para cada torneo. Además se puede modificar las estadísticas para cada campaña”. (Bastian, 2018)

MARCO METODOLÓGICO

En la presente investigación se utilizó la metodología de enfoque experimental ya que se evaluarán aspectos de la simulación de un ataque phishing en la cooperativa de taxis San Fernando de Babahoyo, por medio de la observación y problemática existente se validará el tema mediante cuestionarios estadísticos.

Además, se requiere de una investigación exploratoria donde se toman en cuenta varios puntos importantes en la investigación, por tanto, se analiza el planteamiento del problema de la cooperativa, objetivos, y los procesos que debe realizar. La población es todos usuarios que conforman la cooperativa de taxis San Fernando que está conformado por el presidente, gerente, secretaria, comisiones especiales, consejo de administración, socios.

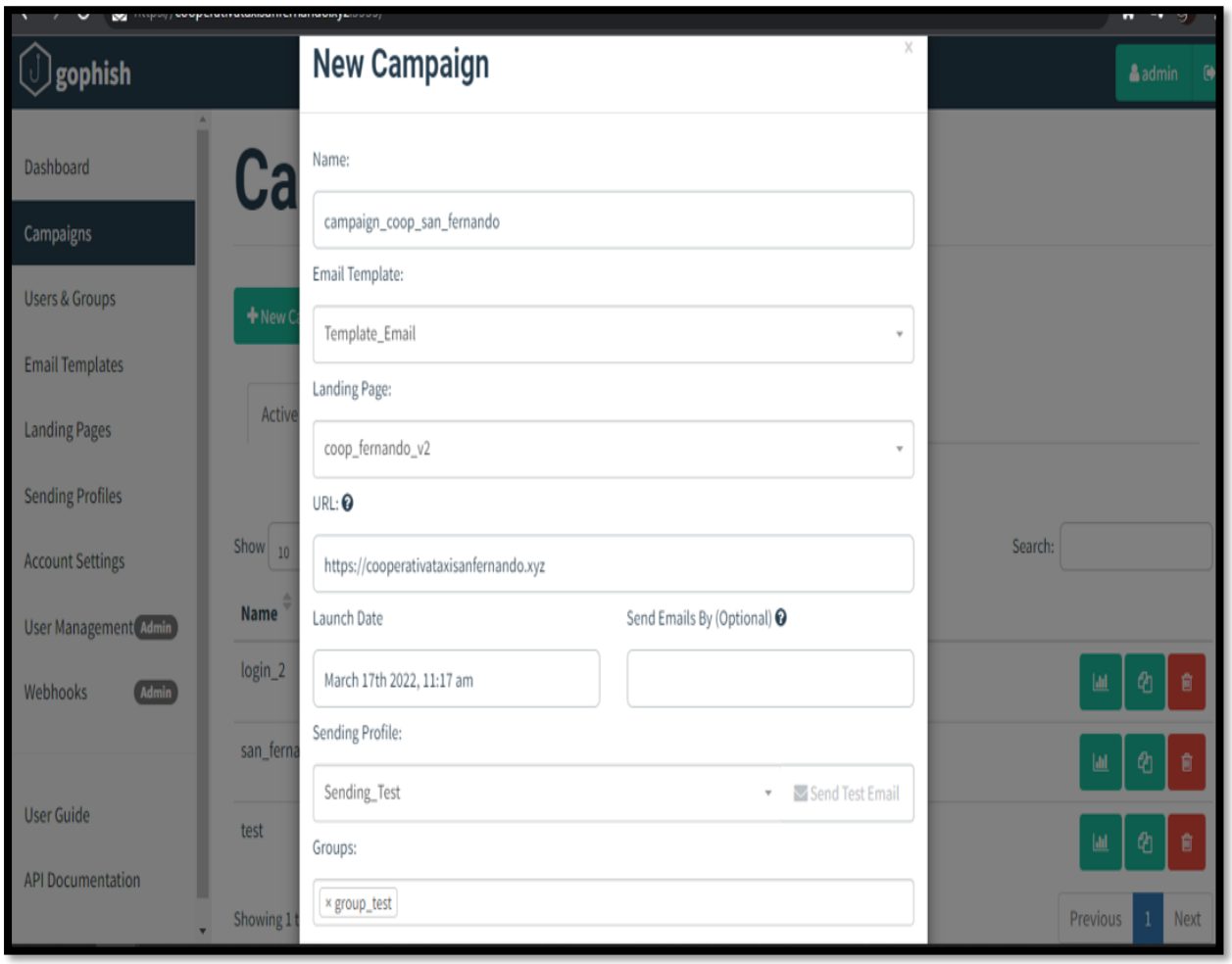
Las técnicas que se utilizo fue la recolección de datos por lo que se usó la entrevista desde el inicio del proceso de titulación solicitando por cada una de las actividades que se efectúan en el cronograma previsto por la unidad de titulación Fafi y la observación que es necesaria en la ejecución de la simulación de un ataque phishing en la cooperativa de taxis San Fernando de Babahoyo.

RESULTADOS

En las siguientes imágenes se puede observar el proceso de la simulación de un ataque phishing en la cooperativa por lo cual resultaron de manera eficiente y eficaz, en efecto el desconocimiento sobre seguridad hace que la cooperativa sean muy vulnerables en este tipo de ataques.

Figura 1

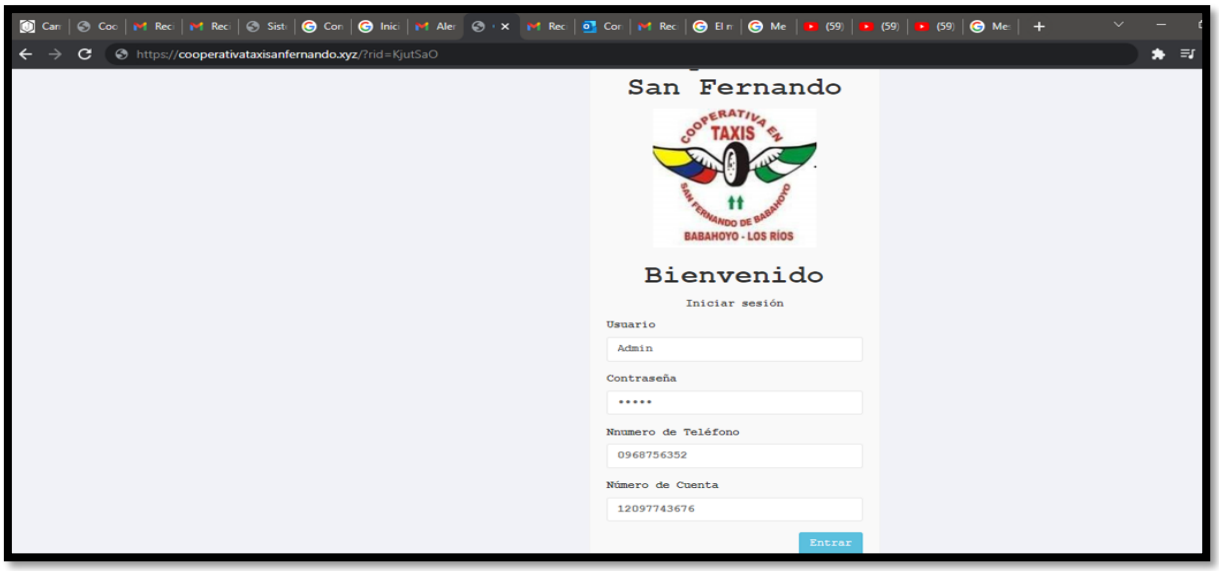
Realizar una campaña de phishing con el siguiente grupo de correos.



Nota: El grafico por elaboración propia represente el proceso de configurar el framework gophish en la opción de nueva campaña.

Figura 2

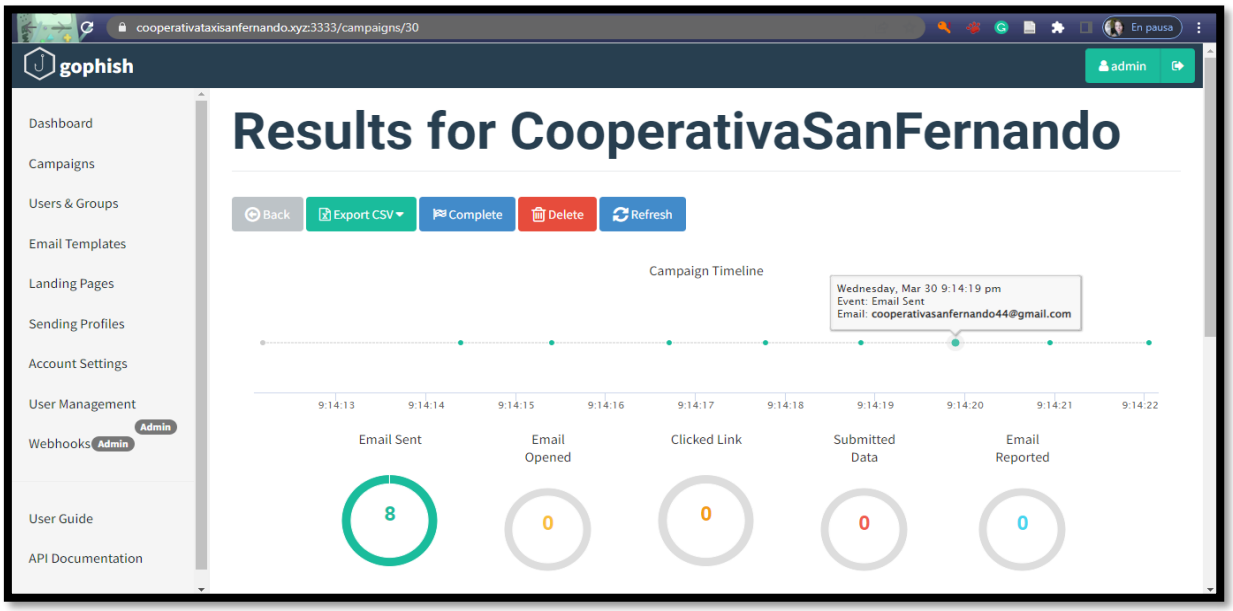
Utilizando el url se duplica la página real a una página fraudulenta.



Nota: El grafico por elaboración propia representa el login de la página fraudulenta donde los usuarios ingresan sus datos para así realizar el ataque phishing.

Figura 3

Se visualizan los resultados de los grupos de e-mail enviados al personal de la cooperativa de taxis.



Nota: El grafico por elaboración propia representa los resultados favorables de ataque phishing.

DISCUSIÓN DE RESULTADOS

El proceso de la investigación se realizó de manera eficiente y eficaz por lo tanto en el ciclo de la investigación se detectaron contratiempos que no permitían continuar con este proceso de investigación que utiliza la metodología de investigación descriptiva por medio de la observación , del mismo modo se emplearon técnicas de recolección de datos por medio de entrevistas que se realizaron según el cronograma académico de la unidad de titulación de la facultad Administración Finanzas e Informática en la carrera de ingeniería en sistemas de información y la comunicación cumpliendo con los horarios acordados.

Los contratiempos que presento el análisis y simulación de un ataque de phishing en el uso de un framework gophish en la cooperativa San Fernando de Babahoyo, del 2022. Fueron que al realizar de manera local no logro funcionar correctamente y es necesario que la web donde se aloja el framework gophish sea de origen seguro con protocolos ssl para permitir hacer las campañas o ataques a los usuarios.

Por lo tanto se requirió de un servidor privado en digitalocean en la fue necesario una cuenta bancaria para poder acceder a los servicios de un servidor, en este caso se utilizó el servidor en Ubuntu de otra manera no permite acceder sin tarjeta de crédito ya que requiere un número de tarjeta de crédito para poder continuar.

Por consiguiente al adquirir el servicio se empleó el programa putty que usualmente se lo utiliza para ejecutar servidores con distintos protocoles, por ende se realizó con el protocolo ssl, y se configuro por medio de comandos del api json así mismo para abrir los puertos necesarios, se asigna una ip de servidor para ingresar al framework gophish en la que se tiene una conexión del servidor y el framework gophish.

Además, se requirió contratar un dominio en la página de zerossl del mismo modo que en el servidor fue necesario poseer una tarjeta de crédito para poder proveer de su

servicio en la web, dependiendo el valor y el nombre de la página se coloca el .com, .xyz, .live, .art. En este caso se utilizó el http://dominio cooperativataxisanfernando.xyz. Ya obtenido el dominio configurar en el programa putty los certificados crt, , key y remplazar los puertos .

La página de la cooperativa de taxis San Fernando de Babahoyo está compuesta por panel principal, login ingresar donde los usuarios que pertenecen a la cooperativa de taxis como presidente, gerente, consejo administración, secretaria, comisiones especiales, socios ingresaran a su cuenta que contiene todos sus datos confidenciales. Al utilizar esta página web se le coloco un dominio http://dominio cooperativataxisanfernando.xyz y poderla suplantar en vista de que el usuario no sospechen de su autenticación y se configura los parámetros de gophish.

En la opción de campaings se llenaron los datos necesarios y se colocó el url de la página de la cooperativa de taxis San Fernando de Babahoyo donde visualiza una página exactamente igual pero de origen desconocido.

Al realizar distintas pruebas los resultaros fueron óptimos y eficaces al verificar que por medio de un framework gophish se puede obtener información importante de las empresas y crear un tipo de ataque como phishing para así cumplir con los objetivos planteados como resultado se puede observar el número de email enviados, opositora de email, numero de enlaces en la que se hizo click, los datos presentados, y el informe del correo electrónico.

El personal que conforman la cooperativa San Fernando destacaron que es un tema nuevo para ellos y por el cual cayeron en este tipo de ataque por ende aprendieron a identificar las paginas autentica que las fraudulentas.

CONCLUSIONES

1.- Gracias al proceso del presente estudio de caso, se logró conocer un método de ataque a la seguridad informática como es el phishing, que es un delito informático muy peligro y puede llegar a exponer datos sensibles de una entidad a través de correos electrónicos falsificando la identidad de alguna empresa de confianza para que algún usuario ingrese sus datos.

2.- El uso del framework gophish ha cumplido con la funcionabilidad de realizar las prácticas de ataques phishing incluso es una herramienta gratuita, fácil de configurar y contiene una interfaz muy intuitiva, se logró conocer el grado de impacto en la seguridad informática que existe en la cooperativa de taxis San Fernando mediante ataques phishing.

3.- En las encuestas realizadas al personal de la cooperativa de taxis San Fernando de Babahoyo se dio a conocer el porcentaje de 90% de desconocimiento sobre el ataque phishing, en un 77.5% el mal uso de sus datos privados en páginas de internet, además el porcentaje de 60% en confiar en los mensajes de correo electrónico, por lo que el porcentaje de 62.5% de socios ingresan a link de servicios de mensajería sin seguridad alguna y un porcentaje de 77.5% no confía en la seguridad de internet.

RECOMENDACIONES

- Se sugiere capacitar al personal que conforman la cooperativa de taxis San Fernando de Babahoyo, para así evitar pérdidas significativas ante los ataques de los ciberdelincuentes, en los que están expuestos al manejar el internet que proveen la tecnología actual.
- Para realizar un ataque phishing la mejor opción es el framework gophish ya que contiene una interfaz sencilla con resultados favorables en el proceso de realizar campañas para el aprendizaje de este tipo de ataque en empresas, organizaciones e instituciones.
- Se debe adquirir servicios privados en la web para así poder realizar el proceso de simulación de un ataque phishing de manera exitosa.

REFERENCIAS

Aranda, V. T. (14 de Marzo de 2022). acta.es. Obtenido de Historia y evolución del internet: https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf

Bastian, S. (Diciembre de 20 de 2018). tiraquelibras. Obtenido de https://blog.tiraquelibras.com/?p=335

Bello, E. (8 de Marzo de 2021). IEBS. Obtenido de https://www.iebschool.com/blog/ingenieria-social-tecnologia/

César, D. (14 de Marzo de 2021). upanama.e-ducativa. Obtenido de https://upanama.e-ducativa.com/archivos/repositorio/6000/6126/html/3_qu_es_.htm

Delgado, H. (8 de Junio de 2021). akus.net. Obtenido de Diseño web: https://disenowebakus.net/internet.php

Dewall, B. (5 de Enero de 2022). whiteoaksecurity. Obtenido de https://www.whiteoaksecurity.com/blog/gophish-setup-part-1/

E&L. (2021). Seguridad Informatica. Empresrial & Laboral, 1-5.

Ecuador, G. d. (7 de Enero de 2021). gobiernoelectronico. Obtenido de https://www.gobiernoelectronico.gob.ec/boletincampanasphishing/

Garcia, H. (11 de Agosto de 2019). tallerinformatica. Obtenido de http://tallerinformaticai.blogspot.com/2018/07/servicios-que-ofrece-internet.html

García, P. (24 de Marzo de 2022). support.mozilla. Obtenido de https://support.mozilla.org/es/kb/boton-de-identidad-de-sitio#:~:text=El%20bot%C3%B3n%20de%20Identidad%20del,casos%2C%20qui%C3%A9n%20es%20el%20proprietario.

Go, M. (12 de Marzo de 2022). Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

Go, M. (12 de Marzo de 2022). Marca Go. Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

Guerrero, L. E. (14 de Agosto de 2021). Programación estructurada. Obtenido de http://memoriascimted.com/wp-content/uploads/2021/08/Programacion-estructurada-en-Go-lang.pdf

Harán, J. M. (15 de Junio de 2021). welivesecurity. Obtenido de APWG: https://www.welivesecurity.com/la-es/2021/06/15/2021-registro-pico-historico-cantidad-sitios-phishing/

Jiménez, J. (30 de Marzo de 2020). Redes Zone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-phishing/

Jiménez, J. (30 de Marzo de 2020). redeszone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-phishing/

Land, H. (14 de Marzo de 2022). hacking.land. Obtenido de https://www.hacking.land/2017/05/gophishing-entrenar-usuarios-contra-el.html

MarcaGo. (12 de Marzo de 2022). Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

MarcaGo. (12 de Marzo de 2022). Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

MarcaGo. (12 de Marzo de 2022). Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

MarcaGo. (12 de Marzo de 2022). Obtenido de https://marcago.com/marketing/ventajas-y-desventajas-del-internet/

Pichincha, B. (14 de Marzo de 2022). pichincha. Obtenido de https://www.pichincha.com/portal/seguridad/internet

Rodríguez, S. B. (20 de Diciembre de 2018). Tiraquelibras. Obtenido de Ciberseguridad y TI: https://blog.tiraquelibras.com/?p=335

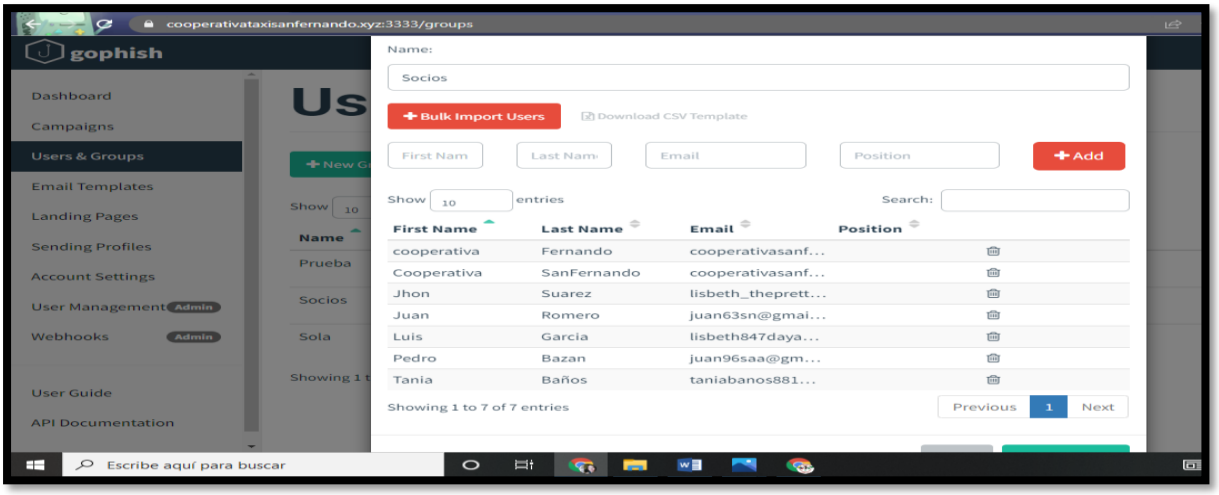
Smith, G. (24 de Marzo de 2021). hostingvictory. Obtenido de https://hostingvictory.com/es/opiniones/digitalocean/

Valois, M. (16 de Mayo de 2019). hostgator. Obtenido de https://www.hostgator.mx/blog/que-es-un-dominio-en-internet/

ANEXOS

Figura 1

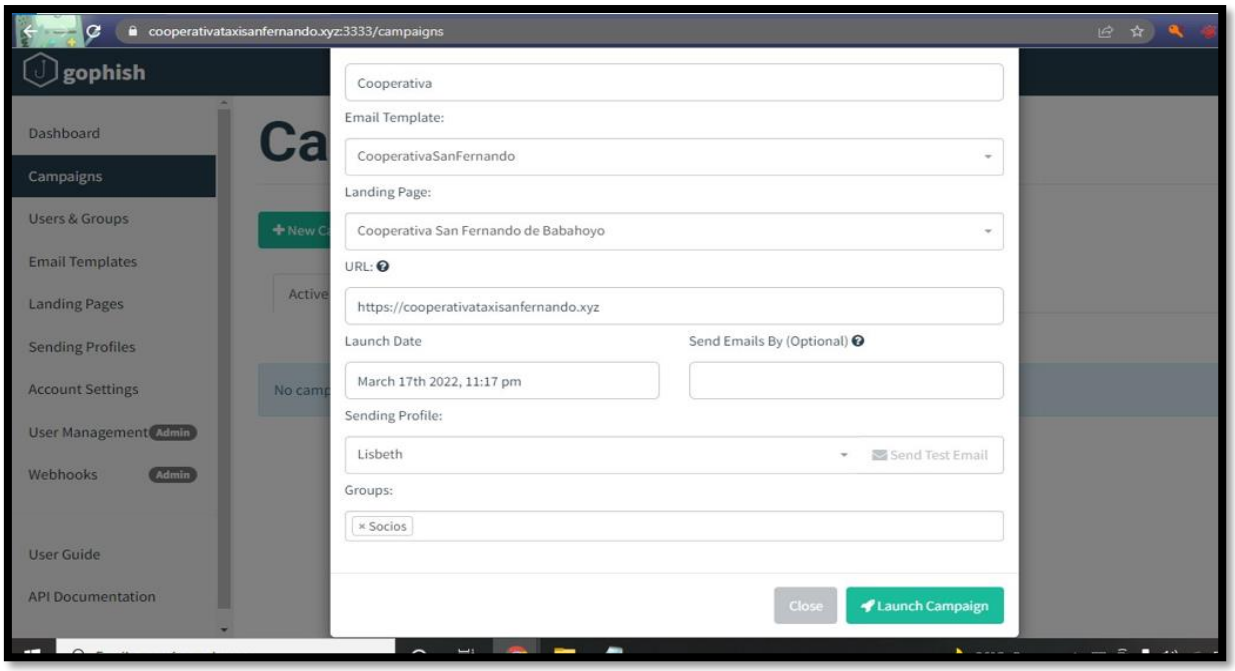
Uso de la opción de User&Groups para ingresar los email para el ataque en grupo.



Nota: El grafico por elaboración propia representa el grupo de usuarios que recibirán los correos que contienen ataque phishing.

Figura 2

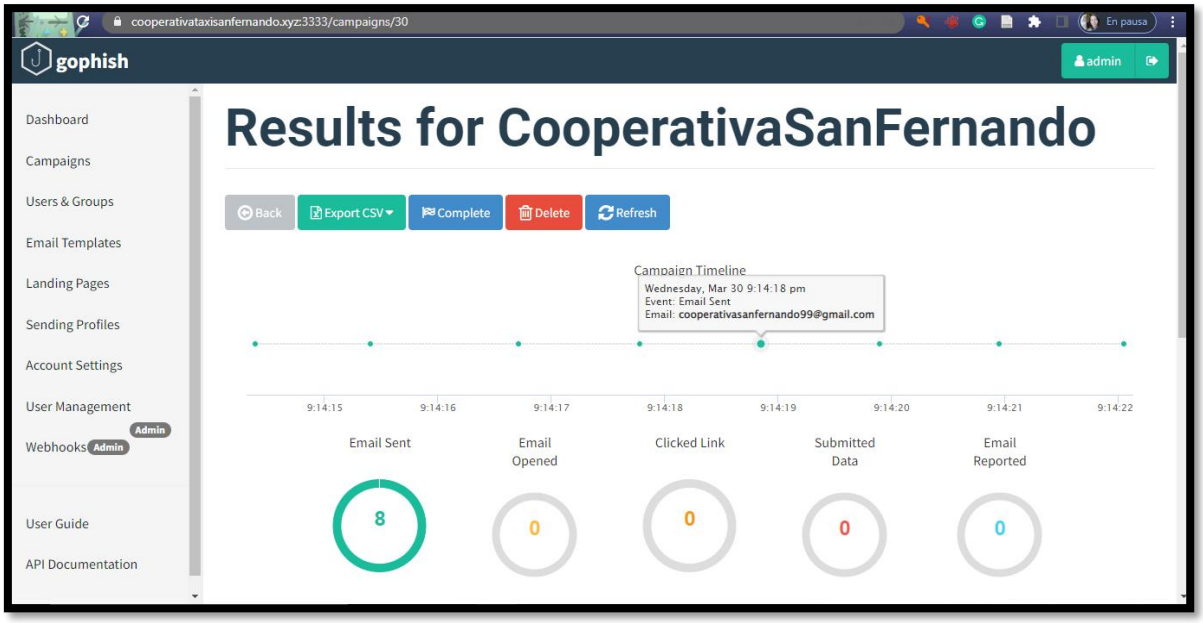
Uso de la opción campaigns para crear una campaña de phishing.



Nota: El grafico por elaboración propia representa la campaña de phishing en la cooperativa de taxis San Fernando.

Figura 3

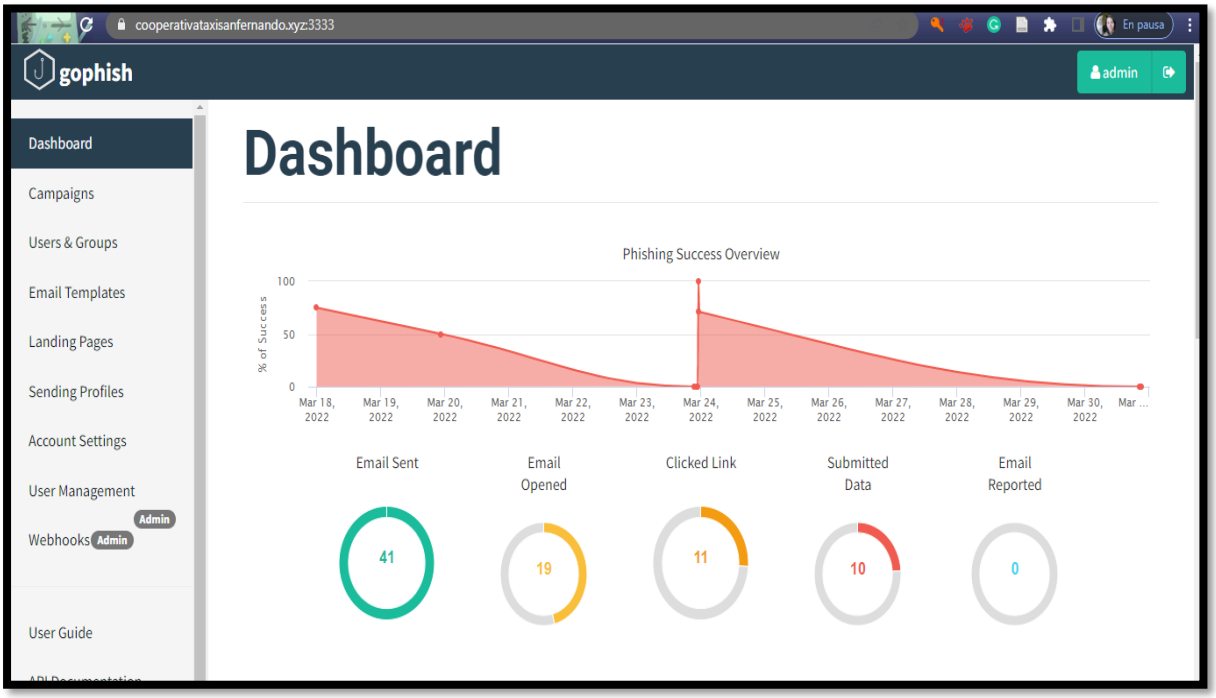
Resultados del grupo de correos que ingresaron al enlace de la página fraudulenta.



Nota: El grafico por elaboración propia representa los resultados del grupo de email enviados.

Figura 4

Dashboard refleja las veces que se realizaron los ataques phishing.



Nota: El grafico por elaboración propia representa la cantidad total de ataques realizados a los socios de la Cooperativa San Fernando de Babahoyo.

Figura 5

Utilizando el url se duplica la página real a una página fraudulenta.

Nota: El grafico por elaboración propia representa el login de la página fraudulenta donde los usuarios que ingresan sus datos y el framework gophish lo recibe.

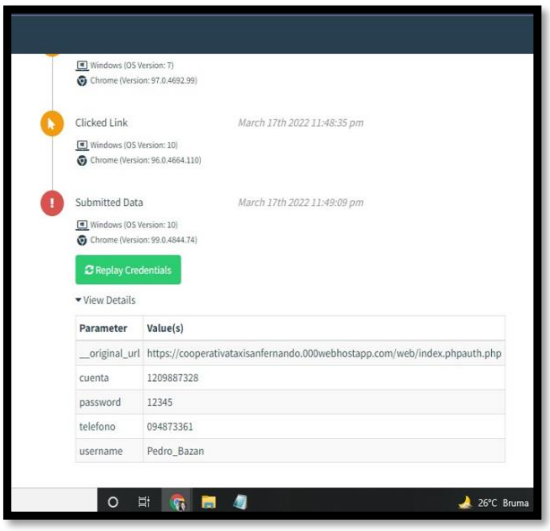
Figura 6

Página oficial de la Cooperativa San Fernando.

Nota: El grafico por elaboración propia representa la página oficial de la Cooperativa San Fernando.

Figura 7

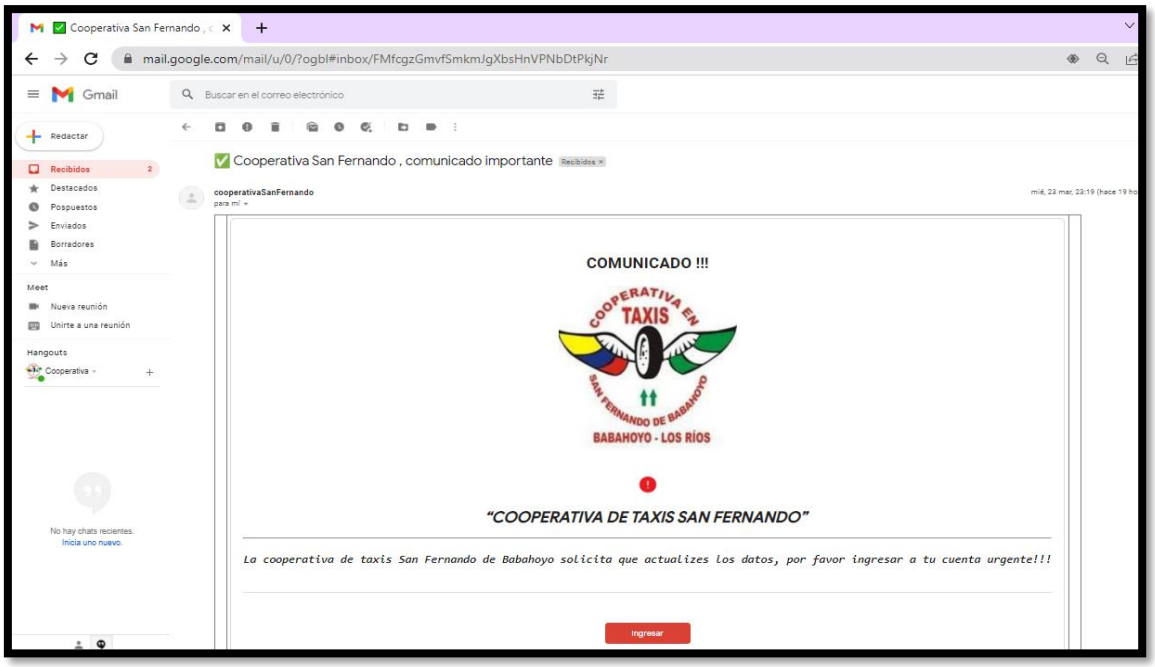
Datos obtenidos por el ataque phishing



Nota: El grafico por elaboración propia representa los datos obtenidos.

Figura 8

Mensaje recibido por el personal de la cooperativa San Fernando.

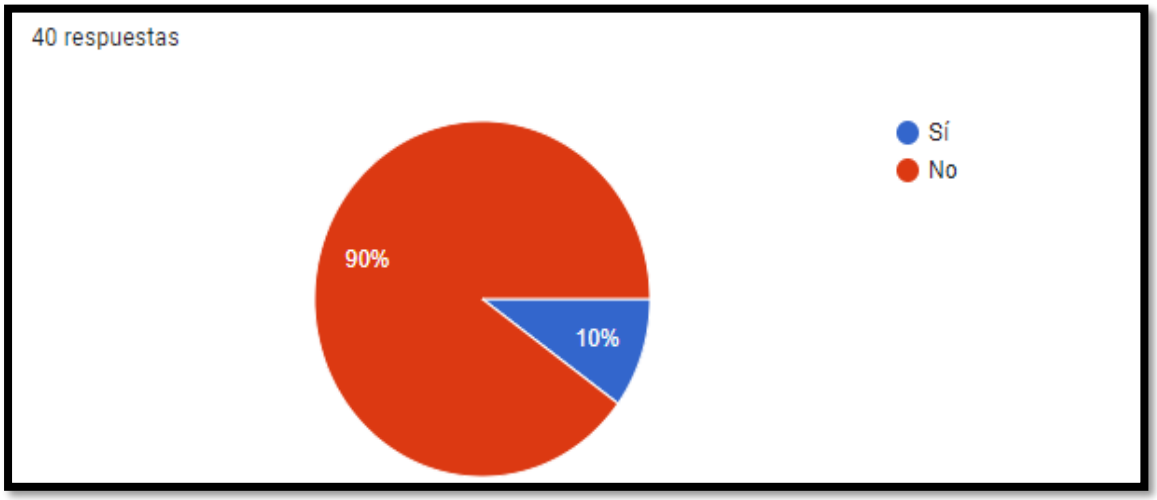


Nota: El grafico por elaboración propia representa al e-mail que contiene phishing y que los usuarios de la cooperativa San Fernando reciben con apariencia engañosa.

13. ANEXOS DE RESULTADOS DE LAS ENCUESTAS

Figura 1

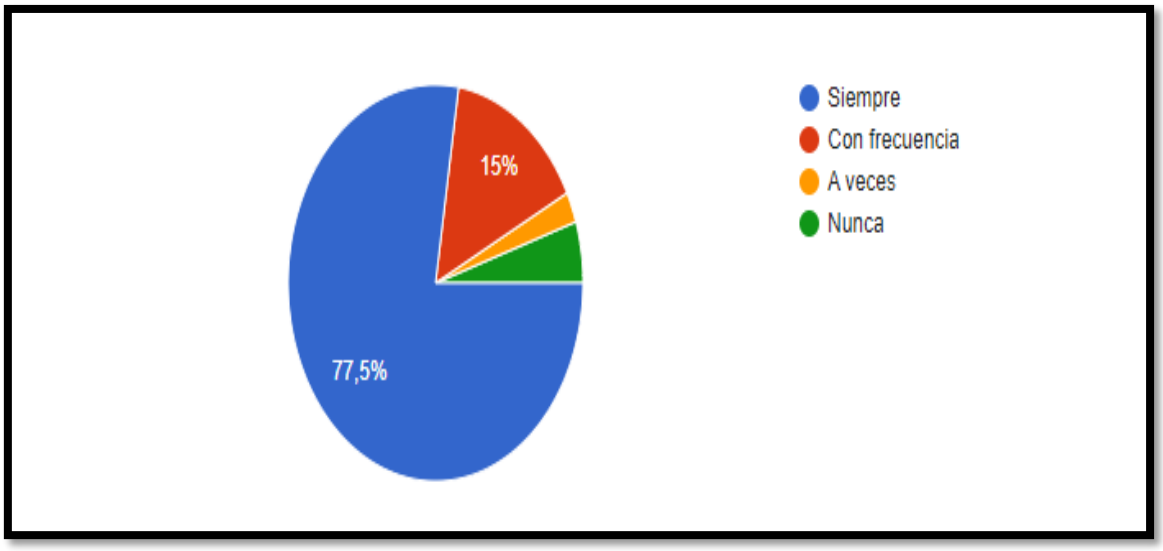
¿Conoce sobre Phishing?



Nota: El grafico por elaboración propia representa el 90% de usuarios que no conocen sobre los ataques de phishing.

Figura 2

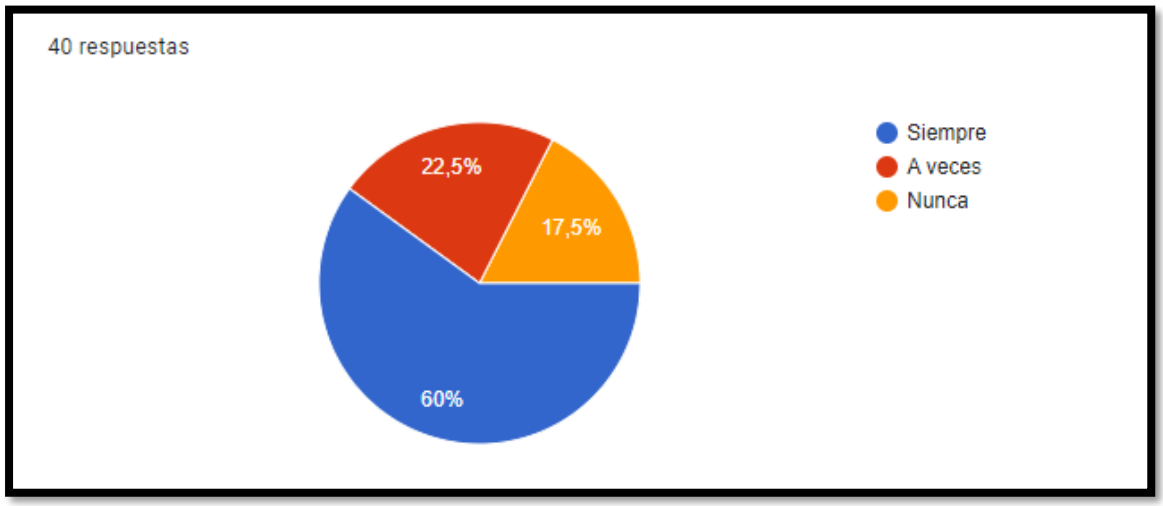
¿Al navegar en internet registra sus datos en páginas que no conoce?



Nota: El grafico por elaboración propia representa el 77.5% de usuarios que siempre registran sus datos en páginas desconocidas.

Figura 3

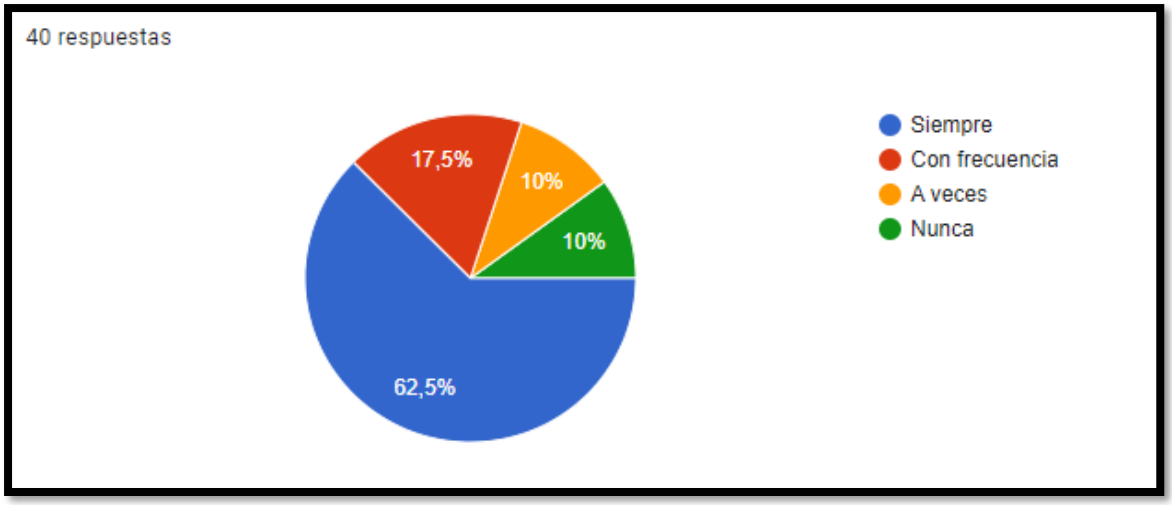
¿Confía en mensajes de su correo electrónico?



Nota: El grafico por elaboración propia representa el 60% de usuarios que siempre confían en el correo electrónico, en un porcentaje de 20.5% a veces confían en emails y un 17.5% nunca confía a los mensajes de correo electrónico.

Figura 4

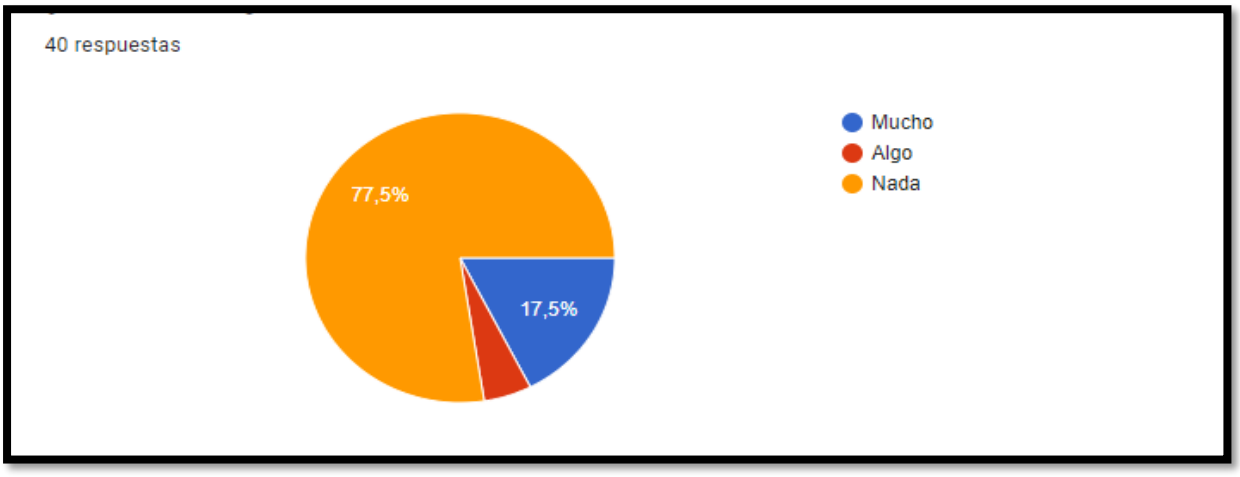
¿Ingresa a cualquier link que envían en su correo electrónico, sms, redes sociales?



Nota: El grafico por elaboración propia representa el 62.5% de usuarios que siempre ingresan a enlaces por medio de mensajería, en porcentaje 10% a veces ingresan a enlaces de mensajería, por lo que un porcentaje de 17.5% ingresa con frecuencia a mensajes, y un porcentaje de 10% nunca ingresa a link de mensajería.

Figura 5

¿Confía en la seguridad de internet?



Nota: El grafico por elaboración propia representa el 77.5% de usuarios que no confían nada en la seguridad de internet, en porcentaje de 17.5 % que confían mucho, además un porcentaje de 5% que confía algo en la seguridad de internet.

COOPERATIVA EN TAXIS

"SAN FERNANDO DE BABAHOYO"

R.U.C: 1290010760001

Fundada el 22 de noviembre de 1990

Mediante Acuerdo Ministerial No. 2983

Dirección: Cdla. Luz Marina 1ro Longitudinal y 1ro Transversal

Teléfono: 2023940

Email: cooperativasanfernando44@gmail.com

AUTORIZACIÓN

Yo, Pedro Manuel Bazán Castro, portador de la cedula Nº 120190827-2 en calidad de Gerente de la cooperativa de transporte de taxis "San Fernando de Babahoyo" autorizo:

Que la Srta. Lisbeth Dayana Baños Galeas, portadora de la cédula de identidad Nº 1251171847; estudiante de la Universidad Técnica de Babahoyo de la carrera Ingeniería en Sistemas de Información; realice su trabajo de titulación modalidad estudio de caso para la obtención del grado académico profesional universitario de tercer nivel como ingeniera en sistemas de información. El estudio de caso: Análisis y Simulación de un ataque de phishing con el uso del Framework Gophish para la cooperativa de transporte en taxis san Fernando de Babahoyo, año 2022.

Autorizo que extiendo en honor a la verdad para que la interesada haga uso legal que estime conveniente.

Babahoyo, 24 de Marzo del 2022.

Unidad, trabajo y Superación,

Atentamente

Lcdo. Pedro Bazán Castro

GERENTE-COOP.