UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación (TIC)
Autor/a:
Tacuri Japa Andrés Fernando
Tutor/a:
Mg. Toasa Guachi Renato Mauricio PhD. Urdaneta Herrera Maryory

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador.

Elaborado por: Andrés Fernando Tacuri Japa, de C.I: 0104521174, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador.

Elaborado por: Andrés Fernando Tacuri Japa, de C.I: 0104521174, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Andrés Fernando Tacuri Japa con C.I: 0104521174, autor/a del proyecto de titulación denominado: Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2024

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

En la actualidad en la era digital las instituciones financieras enfrentan una amplia gama de amenazas cibernéticas entre ellas la ingeniería social, con el objetivo de engañar para tener un beneficio económico.

Asobanca (2023) menciona que “la banca ecuatoriana ha sido uno de los sectores con mayores crecimientos en digitalización. Es así como cerca del 90% de los servicios bancarios están disponibles por canales digitales”.

Es aquí donde los ciberdelincuentes utilizan la ingeniería social mediante la técnica de phishing, siendo unos de los ataques más usados donde se hacen pasar por instituciones financieras, donde utilizan el correo electrónico, redes sociales entre otros medios, para llegar al cliente y robar datos confidenciales como usuarios y contraseñas.

En este contexto expuesto, la protección de marca es crucial por varias razones fundamentales para la estabilidad y el éxito a largo plazo de las instituciones financieras y empresas en general. Esta protección debe garantizar confianza y seguridad entre los clientes, garantizando que la institución maneja sus finanzas de manera segura y profesional.

La protección de marca es esencial para las “Cooperativas de Ahorro y Crédito del Ecuador”. Estas instituciones financieras desempeñan un papel fundamental en la economía nacional, ofreciendo servicios financieros a sectores que a menudo no están bien atendidos por los bancos. Es un tema prioritario debido a la creciente incidencia de ataques fraudulentos que pueden dañar la reputación y la estabilidad financiera de estas cooperativas, ya que los ataques fraudulentos pueden tener consecuencias devastadoras, desde pérdidas financieras significativas hasta daños irreparables a la reputación. La marca no solo representa la identidad visual de una cooperativa, sino también su reputación.

Problema de investigación

En el contexto digital moderno, las “Cooperativas de Ahorro y Crédito del Ecuador” están cada vez más expuestas a diversos tipos de amenazas cibernéticas. Estas amenazas incluyen ataques de phishing, clonación de sitios web y perfiles falsos en redes sociales, llamaremos perfiles falsos a las redes sociales en general ya que depende de la red social lo llaman de diferente manera, por ejemplo, en Facebook se refieren a las páginas, en la red X antes llamada Twitter se les conoce como cuentas personales y cuentas de marca o empresa. Los

ciberdelincuentes utilizan estas tácticas para engañar a los clientes, robar información sensible y llevar a cabo fraudes financieros.

El impacto de estos ataques no solo se traduce en pérdidas financieras directas, sino que también puede dañar gravemente la reputación de la institución. Una brecha de seguridad o un incidente de fraude puede hacer que los clientes pierdan la confianza en la cooperativa, lo que puede llevar a una disminución de la base de clientes y afectar la sostenibilidad a largo plazo de la institución. Además, los daños a la reputación pueden ser difíciles de reparar y pueden tener efectos duraderos en la percepción pública de la cooperativa.

Por estas razones, la protección de la marca se ha vuelto un componente esencial en la estrategia de seguridad de las “Cooperativas de Ahorro y Crédito del Ecuador”. Implementar medidas para proteger la integridad de la marca ayuda a mitigar los riesgos asociados con las amenazas cibernéticas y a preservar la confianza de los clientes o socios.

Actualmente, muchas “Cooperativas de Ahorro y Crédito del Ecuador” carecen de herramientas y procesos para enfrentar estos tipos de ataques o no han contratado un servicio de protección de marca que monitoree la suplantación de dominios, aplicaciones móviles fraudulentas, suplantación de cuentas, hallazgos en redes sociales y mala reputación. Esto es crucial para alertar y tomar las acciones necesarias para mitigar estos problemas.

Asimismo, algunas cooperativas que han contratado servicios de protección de marca se enfrentan a limitaciones cuando ocurren ataques, como la clonación de páginas transaccionales y la utilización indebida de su imagen en redes sociales (Facebook, Red X, WhatsApp). Estos servicios a menudo incluyen paquetes denominados "takedown" que se refiere a eliminar o dar de baja, son limitados y una vez agotados, las empresas cobran tarifas muy altas para dar de baja y/o eliminar las páginas web clonadas y los perfiles falsos en redes sociales.

Por lo tanto, esta investigación se centra en elaborar una guía para la protección de marca frente a ataques fraudulentos, enfocándose en la baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales (Facebook, Red X, WhatsApp) que utilicen la imagen de las “Cooperativas de Ahorro y Crédito del Ecuador”, con el objetivo del robar credenciales y ser estafados financieramente.

Objetivo general

Elaborar una guía para la protección de marca frente ataques fraudulentos para “Cooperativas de Ahorro y Crédito del Ecuador”.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre la protección de marca frente ataques fraudulentos.
- Diagnosticar como afecta a la marca los ataques fraudulentos a las cooperativas con el uso de páginas web clonadas y perfiles falsos en redes sociales.
- Elaborar una guía para la baja y/o eliminación las páginas web clonadas y perfiles falsos en redes sociales.
- Valorar la propuesta por medio del criterio de especialistas.

Vinculación con la sociedad y beneficiarios directos:

La guía para proteger la marca de las "Cooperativas de Ahorro y Crédito del Ecuador" contra ataques fraudulentos se enfoca en dar de baja, eliminar páginas web clonadas y perfiles falsos en redes sociales. Esta guía contribuye al noveno objetivo de Desarrollo Sostenible (ODS), que promueve la industria, innovación e infraestructuras, fomentando la adopción de nuevas tecnologías y el uso eficiente de recursos.

El principal beneficiario de esta guía son los profesionales del área seguridad informática o afines a las áreas de sistemas de las cooperativas, quienes serán los que aplicarán la guía para tomar acciones directas o indirectas contra sitios web y perfiles falsos, fortaleciendo la seguridad.

Asimismo, otro beneficiario serán los clientes o socios de las cooperativas quienes obtendrán mayor protección contra fraudes digitales, reduciendo el riesgo de ser víctimas de ataques, robo de credenciales y ser estafados financieramente. Esto aumentará la confianza en las cooperativas y creará un entorno financiero más seguro.

La implementación de esta guía no solo mejora la seguridad de las cooperativas, sino que también impulsa la innovación en ciberseguridad, alineándose con el objetivo noveno ODS y fortaleciendo el sector financiero de las cooperativas.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La protección de marca es fundamental para las “Cooperativas de Ahorro y Crédito del Ecuador”, especialmente en el contexto actual donde las amenazas cibernéticas son cada vez más sofisticadas buscando la manera de vulnerar las seguridades empleadas. La implementación de medidas de protección efectivas no solo ayuda a prevenir pérdidas financieras y daños a la reputación, sino que también garantiza la confianza de los clientes y la sostenibilidad a largo plazo de las instituciones financieras, evitando así que los clientes o socios sean víctimas de estafas y perdidas financieros.

1.1. Contextualización general del estado del arte

Hoy en día los ataques de los ciberdelincuentes van mejorando notablemente sus ataques, afectando a diversas industrias, incluidas las instituciones financieras como las cooperativas.

Para ello los ciberdelincuentes utilizan diversas técnicas para realizar una estafa con el propósito económico, entre ellas es la ingeniería social.

Según Benavides et al. (2020) “Ingeniería Social (IS) es el acto de obtener información de las personas de manera fraudulenta, con la finalidad de usar esta información, en contra de ellas mismas o de sus organizaciones” (p. 98).

Entre las técnicas de ingeniería social utilizadas son los ataques phishing y smishing, ataques comunes en la actualidad que se realizan a las cooperativas y demás instituciones financieras.

Según Hernández et al. (2022) describe que:

> El phishing es un delito cibernético que consiste en atraer al usuario para que proporcione información sensible y confidencial al atacante. Por lo regular los datos que quieren saber acerca del usuario son detalles de la tarjeta de crédito, nombre de usuario y contraseñas, datos bancarios, etc. Estos ataques de phishing ocurren a través de correos electrónicos maliciosos, mensajes de texto y llamadas telefónicas. (p. 103)

CISA et al. (2021) establece que de igual manera otro tipo de ataque es el smishing que se realiza a través de mensajes de texto (SMS). En esta modalidad de ataque, los ciberdelincuentes envían mensajes de texto que parecen provenir de fuentes legítimas, como instituciones financieras, con el objetivo de estafar a las personas y robar datos personales, como usuarios y contraseñas personales.

Las cooperativas en Ecuador desempeñan un papel esencial, ya que integran a grupos vulnerables que anteriormente estaban excluidos del sistema financiero y actúan como motores del desarrollo económico, generando un impacto social significativo (BCE et al., 2022).

De esa manera desempeñan un papel importante en la economía nacional, ofreciendo servicios financieros a sectores frecuentemente desatendidos por los bancos tradicionales. La creciente digitalización de los servicios financieros, impulsada por la necesidad de eficiencia y accesibilidad, ha expuesto a estas cooperativas a una variedad de amenazas realizadas por los ciberdelincuentes, que requieren medidas de protección de sus servicios y una de ellas es la protección de marca. En particular, nos enfocaremos en el problema de la clonación de páginas web y perfiles falsos en redes sociales como una medida necesaria para garantizar la eficiencia y accesibilidad de los servicios para evitar cualquier tipo de estafa financiera.

> Ecuador atraviesa una ola de ataques de phishing de los cuales no se tiene registros. Los atacantes están recurriendo a técnicas nunca antes vistas en el país para evitar ser detectados, dejando expuestas a una gran cantidad de personas a ataque de los cuales no habrían sido víctimas de no ser por esta nueva modalidad. (Observatorio de Derechos Digitales, 2023, p. 1)

Con la creciente digitalización de los servicios financieros ha traído una mayor exposición a ciberataques, no solo afectando la operatividad de estas cooperativas sino que también ponen en riesgo la información sensible de sus clientes lo cual puede tener conciencias devastadoras tanto para la reputación como para las finanzas de estas cooperativas, así mismo el aumento de ataques de phishing en el Ecuador y otras técnicas avanzadas para el engaño, como clonación de páginas web y creación de perfiles falsos en redes sociales, con el objetivo de robar credenciales y datos personales para cometer fraudes. Esta situación conlleva a la necesidad de fortalecer las medidas de ciberseguridad.

> A medida en que las instituciones financieras adopten sus operaciones digitales asumen mayores riesgos de ataques cibernéticos que tienen alta probabilidad de suceder, es así que, en los últimos diez años se ha incrementado la delincuencia cibernética, atacando a los negocios de los diferentes sectores de la economía, en este sentido, los directivos de los entes económicos deben optar por nuevas directrices que garanticen la seguridad de la información, mitigando los riesgos cibernéticos. (Ojeda et al., p. 194-195)

El aumento de ciberataques en Ecuador, especialmente los basados en ingeniería social, evidencia la creciente vulnerabilidad del país frente a estas amenazas. A pesar de ciertos avances en ciberseguridad, como la creación de un marco legal y medidas preventivas, persisten desafíos significativos, principalmente debido a la falta de cultura digital entre la población. Los ataques, que han afectado tanto al sector público como al privado, se han intensificado debido a la meticulosa investigación que realizan los delincuentes, subrayando la urgencia de fortalecer la educación en seguridad digital y de mejorar las defensas tanto a nivel estatal como individual (Garzón et al., 2024).

1.2. Proceso investigativo metodológico

El enfoque de la investigación es cuantitativo ya que se basa en la recopilación de datos, usualmente a través de encuestas. Los resultados numéricos son procesados rápidamente con software especializado, y presentados en gráficos claros para facilitar su interpretación, de esa manera recopilar y presentar datos sobre la protección de marca frente a taques fraudulentos en las Cooperativas de Ahorro y Crédito del Ecuador (Calizaya et al., 2020).

Dentro del proyecto se utilizó el tipo de investigación aplicada en un entorno financiero donde se busca resolver un problema cotidiano, dado que el objetivo es desarrollar una guía práctica y específica para solucionar problemas específicos como los ataques fraudulentos, enfocándose en la baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales (Duoc UC et al., 2024).

La encuesta realizada a los colaboradores de cooperativas, pertenecientes al área sistemas y otras areas diferentes dentro de las cooperativas, esta encuesta se presenta en el Anexo 1. Esta encuesta tiene como objetivo recopilar información sobre el nivel de conocimiento general en temas de ingeniería social, phishing, y si tienen conocimiento de cómo proceder para gestionar de manera más efectiva las páginas web clonadas y los perfiles falsos en redes sociales dentro de sus respectivas cooperativas.

1.3. Análisis de resultados

Para el análisis de resultados se realizó una encuesta utilizando una muestra no probabilística dirigida a un grupo específico de personas, principalmente en áreas de sistemas y otras áreas diferentes dentro de cooperativas. El objetivo de esta encuesta fue recopilar información relevante para analizar tres aspectos clave, conocimiento general, experiencias personales y medidas y prevención, los resultados obtenidos se indica en el Anexo 2. A continuación, se presenta un análisis detallado de los resultados en cada uno de estos grupos.

Conocimiento General

En este grupo se analizó el nivel de conocimiento general de cada uno de los encuestados sobre temas de ciberseguridad, incluyendo ingeniería social y phishing. Los resultados indican que la mayoría de los participantes tiene un conocimiento de nivel intermedio, aún existe un porcentaje significativo que no se siente completamente seguro en estos temas. Este hallazgo sugiere la necesidad de continuar reforzando la educación y capacitación en ciberseguridad, especialmente en las áreas de identificación y prevención de ataques comunes.

Experiencias Personales

En este grupo, la encuesta exploró las experiencias personales de los encuestados con intentos de phishing, el reconocimiento de paginas web clonadas y perfiles falsos en redes sociales. Los datos indican que una parte considerable de los encuestados ha tenido algún tipo de contacto con estos intentos de fraude, lo que resalta la existencia normal de estas amenazas. Sin embargo, también se observa que no todos los encuestados han sido capaces de identificar estos intentos a tiempo, lo que indica la importancia de mejorar las capacidades de detección y respuesta ante tales situaciones.

Medidas y Prevención

En este grupo la encuesta se centró en las medidas y estrategias de prevención implementadas en las cooperativas. Aunque algunos encuestados informan que sus cooperativas han establecido campañas para la prevención del phishing y la identificación de las mismas, tambien existe el desconocimiento de la exisitencia o si el area correpondiente tiene una guia o proceso para dar de baja y/o eliminar paginas web clonadas y perfiles falsos en redes sociales lo que podría comprometer la seguridad de la cooperativa.

El análisis de los resultados de la encuesta destaca la necesidad de continuar desarrollando y reforzando las iniciativas de capacitación en ciberseguridad dentro de las cooperativas. Es fundamental mejorar el conocimiento general, así como las capacidades de los empleados para identificar y reaccionar ante amenazas cibernéticas. Esta investigación es crucial para la creación de una guía práctica que permita eliminar estos intentos de fraude de manera rápida y eficiente, sin necesidad de depender exclusivamente de proveedores externos para gestionar estas situaciones. La capacidad de actuar de manera autónoma y proactiva en la eliminación de estos riesgos fortalecerá la seguridad general de las cooperativas y protegerá sus clientes o socios.

CAPÍTULO II: PROPUESTA

En este capítulo se realizará la guia propuesta, donde se explicará cómo dar baja y/o eliminación de páginas webs clonadas y perfiles falsos de las cooperativas.

1.1. Fundamentos teóricos aplicados

Cooperativa de Ahorro y Crédito

Las cooperativas de ahorro y crédito son instituciones financieras sin fines de lucro, estas cooperativas tienen como objetivo principal satisfacer las necesidades financieras de sus socios ofreciendo servicios como cuentas de ahorro, préstamos, y otros productos financieros a tasas más favorables que las de los bancos tradicionales.

Ciberseguridad

"Se ocupa de la protección de los activos digitales, incluyendo redes, hardware y software, así como la información que es procesada, almacenada en sistemas o transportada a través de entornos de información interconectados" (Ortega, 2024, p. 2).

Protección de Marca

La protección de marca es un conjunto de estrategias y acciones destinadas a detectar, prevenir y mitigar ataques y amenazas dirigidos hacia la reputación y la integridad de una institución. Estos ataques pueden manifestarse de diversas formas incluyendo, phishing, ciberataques, suplantación de identidad, fraudes en redes sociales, entre otros.

Ingeniería social

La ingeniería social es una técnica utilizada por ciberdelincuentes para manipular a las personas con el fin de obtener información confidencial, acceder a sistemas restringidos o lograr otros objetivos maliciosos. Esta práctica se basa en el aprovechamiento de la confianza de esa manera conseguir que revelen datos sensibles o realicen acciones que comprometan la seguridad (Kaspersky et al., s.f.).

Tipos de ingeniería social

La ingeniería social abarca una variedad de ataques que se basan en la manipulación psicológica de las personas para obtener información confidencial o acceso no autorizado como se presenta en la Tabla 1:

Tabla 1.
Tipos de ingeniería social

Tipo de ingeniería social	Descripción
Phishing	Es uno de los ataques de ingeniería social más utilizados a nivel mundial por los ciberdelincuentes para engañar a los usuarios y obtener información sensible, como usuarios, contraseña y personales. Este tipo de ataque se basa en la manipulación psicológica, creando correos electrónicos, mensajes y sitios web falsos que parecen legítimos para engañar a las víctimas (Mayo et al., 2022).
Spear phishing	Es un ataque más elaborado y focalizado a un grupo específico, como empleados de una empresa, clientes de un banco o miembros de una organización, se caracteriza por la personalización de los mensajes. Estos mensajes se ajustan utilizando información real de los destinatarios, como sus nombres, cargos o referencias específicas, con el fin de incrementar la credibilidad y efectividad del ataque (San Martín et at., 2024).
Smishing	El smishing generalmente implica enviar a las víctimas potenciales un mensaje de texto que parece provenir de un remitente legítimo, como su banco, un servicio de entrega de paquetes o un sitio de redes sociales. En realidad, por supuesto, es una trampa diseñada por atacantes para engañar a las personas para que proporcionen información confidencial respondiendo o haciendo clic en un enlace de phishing (Tresorit et al., 2023).

Página clonada

Es una copia exacta o muy similar de una página web legítima. El objetivo principal es engañar a los visitantes para que ingresen sus usuarios, contraseñas, datos de tarjetas de crédito, o cualquier otra información sensible (Baker et al., 2023).

Perfiles falsos

Los perfiles falsos en redes sociales son cuentas creadas por atacantes que imitan la identidad de empresas o instituciones legítimas. Utilizan logotipos, fotos y otra información oficial para hacerse pasar por estas organizaciones con el objetivo de engañar a los usuarios y ofrecer servicios financieros falsos o realizar otros fraudes. Estos perfiles buscan ganar la confianza de las víctimas para obtener información sensible o dinero a través de engaños (Rico et al., 2022).

Takedown

En el contexto de ciberseguridad se refiere al proceso de eliminar contenido ilegal, dañino, o no autorizado de internet. Esto puede incluir la eliminación de sitios web, perfiles falsos en redes sociales, archivos compartidos ilegalmente y otros tipos de contenido que violan políticas, derechos de autor o leyes (Furtado et al., 2020).

1.2. Descripción de la propuesta

Cuando se habla de protección de marca, nos referimos a un conjunto amplio de medidas orientadas a apoyar a empresas e instituciones financieras en el buen uso de su marca institucional en Internet, así como a anticipar y gestionar eventos que puedan afectar su reputación.

Existen empresas especializadas en brindar servicios profesionales, técnicos y especializados en este ámbito. Estos servicios incluyen la anticipación, detección y respuesta ante ciber amenazas de diversas naturalezas. Es importante destacar su capacidad para llevar a cabo la eliminación efectiva de páginas web clonadas y perfiles falsos en redes sociales. La Figura 1 muestra una representación de una empresa que está dedicada brindar este servicio.

Figura 1.

Protección de marca.

Nota. Creada por la IA.

La protección de marca abarca numerosos aspectos de monitoreo, entre los cuales se incluyen:

- Attack Surface Management (Gestión de Superficie de Ataque).
- Digital Risk Protection (Protección de riesgo digital).
- Dark Web Monitoring (Monitoreo de la Web Oscura).
- Cyber Threat Intelligence (Inteligencia de Amenazas Cibernéticas)
- Protección de Marca.
- Gestión de incidentes.
- Reportes.

Es así que estas empresas monitorean y alertan cualquier tipo de amenaza en contra de las instituciones, donde lo centralizan en el punto de gestión de incidentes y de igual manera lo pueden alertar por otros medios como el correo electrónico o por medio de un canal de comunicación directo que puede ser por un grupo creado en WhatsApp.

Como se indica anteriormente la protección de marca abarca una amplia gama de actividades destinadas a salvaguardar la integridad y reputación de una maraca. Sin embargo, el punto importante para esta investigación es que las empresas dentro de sus contratos incluyen paquetes denominados "Takedown". Estos paquetes son diseñados para dar de baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales, pero estos paquetes son limitados, una vez agotados las empresas cobran tarifas muy altas para continuar proporcionando el servicio de baja y/o eliminación del contenido fraudulento.

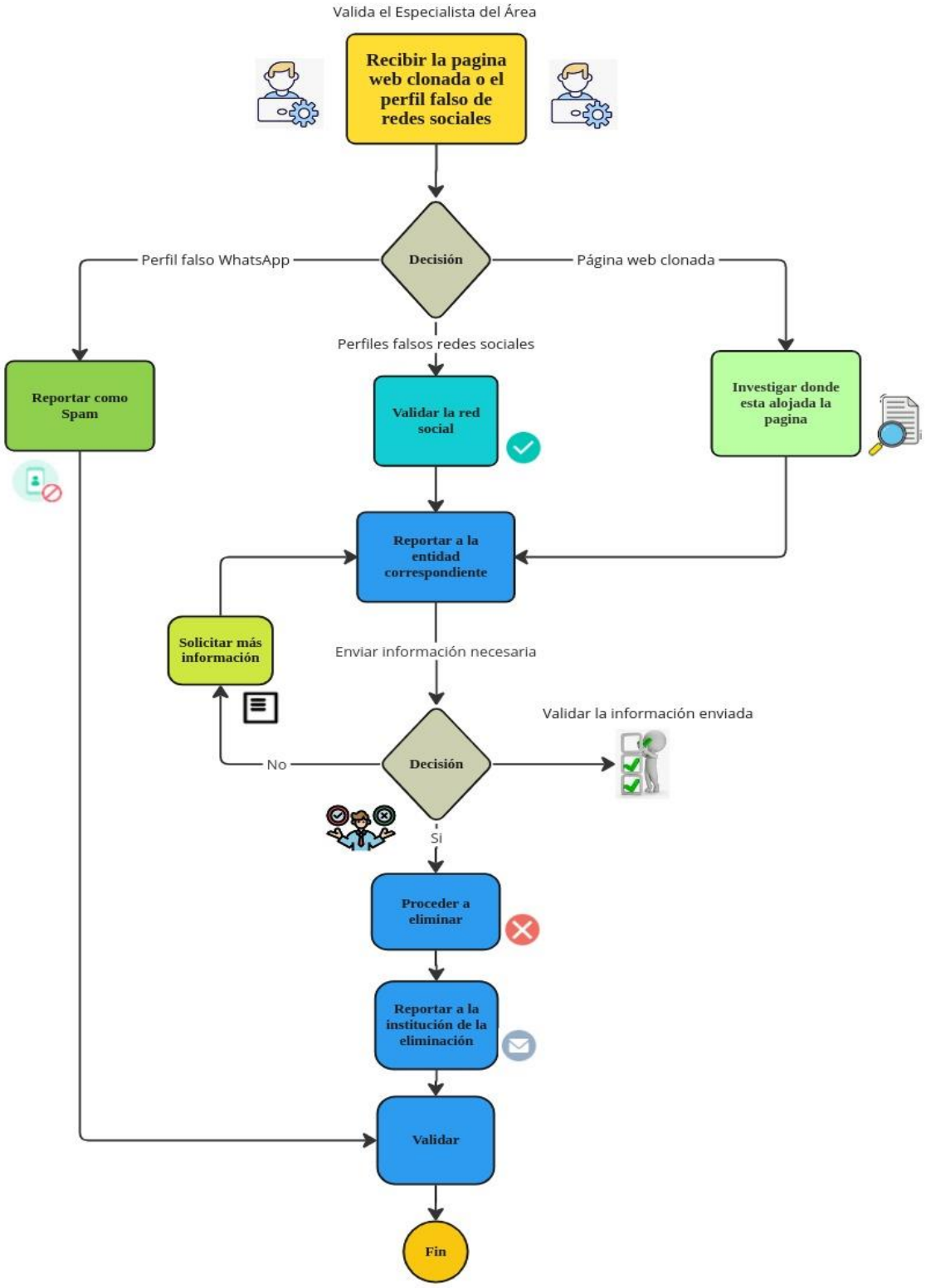
De esta manera la investigación tiene como objetivo elaborar una guía para proteger la marca de las “Cooperativas de Ahorro y Crédito del Ecuador” frente a ataques fraudulentos. Esta guía se centrará en la baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales que utilicen la imagen, el nombre o cualquier distintivo de estas instituciones. Se especificará detalladamente el proceso, a quién reportar, cómo reportar y los requisitos previos necesarios para que el reporte sea válido y efectivo.

a. Estructura general

Para diseñar la guía se tuvo que investigar cual sería el proceso a seguir, por lo cual en la figura 2 se ilustra de manera general la estructura de la propuesta para abordar la problemática de las páginas web clonadas y los perfiles falsos en redes sociales para las “Cooperativas de Ahorro y Crédito del Ecuador”, con el objetivo de crear un entorno digital más seguro y confiable.

Figura 2.

Estructura del procedimiento para la baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales.



Nota. Elaboración propia

b. Explicación del aporte

Esta guía aborda los diferentes pasos necesarios para la baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales, adaptándose a las circunstancias específicas de cada caso. Es crucial comprender desde el principio que cada situación puede requerir un enfoque diferente. A lo largo de la guía, se explicará cómo reportar estas amenazas a las instancias correspondientes.

Antes de detallar el procedimiento, es importante considerar que hay cooperativas que tienen contratado el servicio de protección de marca con empresas especializadas. Estas empresas son responsables de monitorear y detectar la presencia de páginas web clonadas en internet y perfiles falsos en redes sociales. Una vez identificadas estas amenazas, las empresas notifican a los especialistas de la cooperativa, de la existencia de estas amenazas, de esa manera indica si proceden a la eliminación de la misma. El especialista de la empresa al no tener el conocimiento de cómo proceder a realizar este proceso para eliminar estas amenazas indican a las empresas que procedan con la eliminación, aquí es cuando entra el contrato de los paquetes "Takedows" una vez que se terminen estos paquetes, las empresas comienzan a cobrar cantidades altas por cada Takedows que van realizando, siendo valores que van afectando financieramente a las cooperativas.

Es importante destacar que las alertas no solo son reportadas por las empresas especializada, sino también por los propios clientes o socios, quienes fueron o estuvieron a punto de ser víctimas de ingeniería social para ser estafados financieramente. Un ejemplo claro de esto es cuando los clientes ingresan a perfiles falsos en las redes sociales creyendo que están interactuando con la cooperativa para solicitar información sobre créditos, inversiones u otros servicios. Uno de los casos es cuando un cliente o socio solicitan en estos perfiles falsos un crédito, es aquí cuando los estafadores solicitan un depósito inicial en una cuenta bajo su control como requisito para desembolsar el crédito solicitado, lo que culmina con la estafa.

Por otro lado, algunas cooperativas no cuentan con contratos con empresas especializadas que monitoreen y eliminen estos tipos de ataques y tampoco disponen del conocimiento necesario para enfrentar estos desafíos.

La importancia de esta guia radica en proporcionar a los especialistas el proceso necesario para minimizar estas estafas, protegiendo así los intereses de los clientes o socios y salvaguardar el prestigio y la confianza de la cooperativa. Además, se busca evitarlos los altos costos asociados con los servicios de takedown.

Como punto inicial es tener la alerta de la existencia de una página web clonado o un perfil falso en las redes sociales, ya sea a través de la empresa contratada, los clientes o socios, los empleados de la cooperativa o los propios especialistas del área encargada de tomar acciones.

Una vez que se haya detectado la presencia de una página web clonada o un perfil falso en redes sociales, esta guía ayudara al especialista en el manejo de estas situaciones. Se detallará el procedimiento a seguir y los requisitos necesarios para que las denuncias sean válidas, permitiendo así que las instancias correspondientes procedan con la baja y/o eliminación de las páginas web clonadas o perfiles falsos en redes sociales.

En la Tabla 2 se presenta una explicación detallada de la Figura 2, considerando los tipos de ingeniería social descritos en la Tabla 1, de los cuales una persona puede ser víctima.

Tabla 2.

Explicación de la guía.

Guía	**Descripción**
Recibir la página web clonada o perfil falso en redes sociales	**Recibir la alerta:** Aceptar la notificación o reporte sobre la existencia de una página web clonada o un perfil falso en redes sociales. **Validación inicial:** Confirmar si el reporte recibido corresponde efectivamente a una página clonada o un perfil falso.
Perfiles falsos de redes sociales	**Identificar la red social**: Determinar en qué red social está alojado el perfil falso. **Análisis de contenido**: Revisar las publicaciones del perfil para identificar posibles fraudes. **Verificación de contactos:** Confirmar si el perfil está vinculado a algún medio de comunicación, como WhatsApp. **Recopilar evidencia:** Copiar URLs del perfil y las publicaciones. Realizar capturas de pantalla de fotos, logotipos, publicaciones y nombres relacionados a la cooperativa.
Perfiles en WhatsApp	**Reportar como spam:** Identificar y reportar repetidamente el número vinculado como spam.
Página web clonada	**Identificación del proveedor de hosting**: Investigar cuál es el proveedor de alojamiento de la página web clonada**.**

	Revisión de contenido: Analizar el contenido de la página para identificar actividades fraudulentas. **Verificación de enlaces**: Determinar si la página está vinculada a otros medios de comunicación, como WhatsApp. **Recolección de evidencia:** Recopilar toda la información relevante para el reporte, incluyendo capturas de pantalla de fotos, logotipos, publicaciones, y nombres relacionados con la cooperativa.
Reportar a la entidad correspondiente	**Acceso a formularios:** Acceder a los formularios específicos de las plataformas para realizar el reporte. **Completar el formulario:** Llenar todos los campos solicitados en el formulario con la información recolectada. **Envío del reporte:** Enviar el formulario completo a la entidad correspondiente.
Validar la información enviada	**Revisión por la entidad:** La entidad receptora validará la información proporcionada. **Solicitud de información adicional:** Si es necesario, la entidad solicitará más detalles a través del correo electrónico proporcionado. **Verificación de la validez:** Una vez que sea válida la información, procederá con la eliminación.
Proceder a eliminar	**Eliminación del contenido:** La entidad reportada procederá a eliminar la página web o perfil falso reportado.
Reportar a la institución de la eliminación	**Notificación a la cooperativa**: La entidad notificará que el contenido ha sido eliminado.
Validar	**Verificación de la eliminación**: El especialista o encargado validará que la página o perfil reportado haya sido efectivamente eliminado.
Cierre del proceso	Se da por concluido el proceso de la baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales.

c. Estrategias y/o técnicas

Antes de presentar la denuncia o reporte a las entidades correspondientes, es fundamental contar con la documentación requerida. Estos documentos serán solicitados según la entidad a la que se dirija el reporte, con el fin de validar su legitimidad.

En primer lugar, es necesario disponer del documento de registro de marca, el cual debe ser gestionado a través del Servicio Nacional de Derechos Intelectuales (SENADI). Este documento certifica la propiedad de la marca de la cooperativa y debe ser obtenido con anticipación por lo que el trámite dura entre unos 6 menes para su entrega. La gestión de este documento puede ser coordinada con el departamento legal de la cooperativa, asegurando que todos los aspectos legales estén cubiertos. Ver el Anexo 3.

En segundo lugar, es esencial obtener un certificado de autorización emitido por la cooperativa, en el cual se debe especificar el nombre de la persona que será responsable de realizar los trámites para reportar ante la red social correspondiente. Este certificado debe autorizar explícitamente a esta persona para gestionar la protección de los derechos de marca comercial en nombre de la cooperativa. Ver el Anexo 4.

Estos documentos son esenciales para que las plataformas de redes sociales puedan validar que la cooperativa es la legítima propietaria de la marca en cuestión. El documento de registro de marca y el certificado de autorización no solo certifican la propiedad de la marca, sino que también autorizan al representante designado para llevar a cabo los trámites necesarios. La presentación de estos documentos es crucial para que las plataformas consideren y actúen sobre las solicitudes de eliminación de cuentas falsas o contenido no autorizado.

Facebook, Red X, WhatsApp y páginas web clonadas fueron utilizadas en esta investigación debido a que son las plataformas más comunes y efectivas que los ciberdelincuentes emplean para cometer estafas. Estas redes sociales, ampliamente utilizadas en todo el mundo, ofrecen un acceso masivo a potenciales víctimas, lo que las convierte en canales ideales para la distribución de mensajes fraudulentos, enlaces maliciosos y comunicaciones engañosas.

Además, la creación de páginas web clonadas, que imitan a sitios legítimos, permite a los delincuentes engañar a los usuarios para que ingresen sus datos personales, como nombres de usuario y contraseñas, facilitando así el acceso no autorizado a sus cuentas. La elección de estas plataformas en la investigación responde a su alta frecuencia de uso en incidentes de fraude y su capacidad para facilitar la obtención de información personal sensible de manera rápida y efectiva.

Redes sociales

Los ciberdelincuentes han encontrado en las redes sociales una plataforma ideal para realizar fraudes, aprovechándose de la enorme popularidad de estas plataformas. Entre todas Facebook es la red social más utilizada y conocida a nivel mundial, lo que la convierte en un objetivo atractivo para estos estafadores. Los delincuentes crean páginas falsas utilizando el nombre, logotipo y fotografías de empresas, instituciones financieras y otras organizaciones legítimas. El objetivo de estas páginas es interactuar con usuarios desprevenidos, engañándolos para que caigan en diversas estafas. La Figura 3 muestra una representación de ciberdelincuentes que están al frente de las estafas en las redes sociales.

Figura 3.

Ciberdelincuentes en redes sociales

Nota: Creado por la IA.

Una de las estafas más comunes es la suplantación de cooperativas financieras. Los ciberdelincuentes atraen a las víctimas hacia estas páginas falsas, donde se promocionan ofertas de créditos con tasas de interés extremadamente bajas. Además, estas páginas fraudulentas suelen estar vinculadas a un número de WhatsApp, a través del cual los estafadores interactúan directamente con las víctimas. Una vez que la víctima muestra interés, los delincuentes ganan su confianza mediante la interacción en WhatsApp, logrando que les proporcionen la información necesaria para cometer el fraude. Un ejemplo típico es cuando la víctima solicita un crédito y se le indica que, para recibir el desembolso, primero debe realizar un depósito inicial

en una cuenta controlada por los estafadores, bajo la falsa promesa de que recibirá el crédito solicitado.

Estas actividades no solo causan un perjuicio económico a las víctimas, sino que también dañan la reputación de las organizaciones legítimas cuyas identidades son utilizadas de manera fraudulenta.

Cuando las víctimas descubren la estafa, ya sea antes o después de ser afectadas, suelen reportar la existencia de estas páginas y números vinculados a WhatsApp a las instituciones correspondientes. A continuación, se detallará el proceso para reportar estas páginas falsas y perfiles fraudulentos en WhatsApp, para que puedan ser eliminados por las entidades correspondientes. En el Anexo 5 se encuentra la guía con el procedimiento detallado para la eliminación de páginas web clonadas y perfiles falsos en redes sociales.

Facebook

Para realizar una denuncia de una página falsa a Facebook se seguirán los siguientes pasos:

- Tener el documento de registro de marca, documento que se adjunta como anexo.
- Ingresar a la siguiente URL: https://www.facebook.com/help/contact/1057530390957243
- Llenar el formulario, seleccionando la opción “Continuar con el reporte marca comercial” donde debemos llenar cada uno de los campos con información en relación de la cooperativa que se está denunciando, datos como:
    - Relación con el propietario de los derechos.
    - Información de contacto, aquí podríamos ingresar el nombre del propietario de los derechos, en este caso poner el nombre de la cooperativa.
    - Dirección postal.
    - Dirección de correo donde Facebook notificara el número de caso y la confirmación cuando se elimine la página.
    - Nombre del propietario de los derechos, aquí se ingresaría el nombre de la cooperativa.
    - Proporcionar el enlace oficial del propietario de los derechos, en este caso ingresar la url de la página oficial.
    - Ingresar el nombre de la marca comercial, aquí debemos ingresar el nombre registrado como está el en documento que otorga el SENADI.
    - Ingresar el país donde está registrada la marca.
    - Ingresar el número de registro que envió el SENADI y adjuntar el documento.

- Seleccionar el contenido de lo que se desea reportar, puede ser “Esta foto, video, publicación”.
- Proporcionar las URLs que lleven directamente al contenido especifico que se desea reportar.
- Ingresar el nombre de la página falsa y proporcionar un detalle del anuncio.
- Adjuntar las imágenes donde se encuentran los anuncios con sus respectivos detalles.
- Ingresar información que ayudara a entender lo que se está pretendiendo reportar.
- Por último, ingresar el nombre de la cooperativa como firma.

Respuesta de Facebook.

- Una vez enviado la denuncia, llegara una notificación de parte de Facebook al correo electrónico, indicando el número de caso para su revisión.
- Si Facebook considera solicitar más información se debe responder al correo recibido con la información que solicita.
- Una vez que se envió la información se debe esperar la respuesta de Facebook donde indiquen que fue eliminada la página denunciada, considerar que el tiempo de respuesta es demorado sin embargo la misma puede estar ya eliminada en Facebook.
- Por último, revisar que la página este fuera de servicio.

Perfiles en WhatsApp

Una estrategia efectiva para bloquear temporalmente o incluso suspender de manera permanente los números que se están haciendo pasar por la cooperativa, violando los términos de servicio de WhatsApp, es reportarlos masivamente como spam. En muchas cooperativas, existen grupos de WhatsApp que se utilizan para la comunicación interna; estos grupos podrían ser aprovechados para coordinar estos reportes.

Se informaría en estos grupos sobre el número que está utilizando de manera fraudulenta el nombre o logotipo de la cooperativa y solicitar a todos los miembros que lo reporten como spam. Este enfoque no solo aumenta la visibilidad del problema para WhatsApp, sino que también acelera la revisión y bloqueo del número infractor por parte de la plataforma.

Implementar este tipo de estrategia de respuesta rápida puede ayudar a mitigar los daños causados por estos delincuentes y proteger la reputación de la cooperativa de manera más efectiva.

Reportar como spam.

- Ingresar al número reportado, seleccionar en los tres puntos y seleccionar la opción Reportar.
- Reportar este contacto a WhatsApp, seleccionar Bloquear contacto y vaciar el chat.

Validar el número si fue bloqueado.

Para validar que ese número fue bloqueado se usará la siguiente herramienta:

- Instalar un Emulador, el mismo que simulara ser un dispositivo móvil.
- Instalar WhatsApp dentro del emulador.
- Tratar de registrar en WhatsApp el número reportado.
    - Seleccionar el país.
    - Ingresar el número de celular.
    - Verificar el número de teléfono seleccionando “Verificar de otra manera”.
    - Seleccionar “Enviar SMS”.
    - Si se llega al punto de verificación de tu número y donde se debe de ingresar el código de 6 dígitos, eso indica que el número no está bloqueado.
    - Si sale el mensaje “Esta cuenta no tiene permisos para usar WhatsApp debido a spam” eso indicaría que la cuenta ya se encuentra bloqueada.

Red social X (Twitter)

Asimismo, otra red social que utilizan los ciberdelincuentes es la red social X antes conocida como Twitter de igual manera para realizar una denuncia de seguirán los siguientes pasos:

- Tener el certificado emitido por la cooperativa donde se indica que se tiene la autorización para realizar dicha denuncia.
- Ingresar a la siguiente URL: https://help.twitter.com/es/forms/ipi/trademark/trademark-owner
- Llenar el formulario, seleccionando la opción “Problemas de propiedad intelectual”. Continuar con el reporte donde debemos llenar cada uno de los campos con información solicitada, datos como:

- Qué problema se tiene, seleccionar “Necesito denunciar una posible infracción de marca.
- Seleccionar la relación con el propietario de los derechos, en este caso seleccionar “Soy el propietario de la marca o trabajo directamente para el propietario de la marca”.
- Ingresar la información personal de quien está realizando la gestión de la denuncia y cargar la parte frontal de la cedula.
    - Nombre y Apellido
    - Cargo en la institución.
    - Dirección de correo electrónico el cual servirá como punto de comunicación para notificación o respuestas.
    - Numero de celular.
    - Imagen de la cedula de la parte frontal en .png
- Ingresar la información de la cuenta que se va a denunciar.
    - Seleccionar la plataforma donde se encuentra la cuenta, en este caso X.
    - Ingresar el nombre de usuario de la cuenta que se quiere denunciar.
    - Proporcionar detalles sobre el problema.
    - Seleccionar el uso del nombre de usuario en este caso “Nuestra empresa no quiere usar activamente este nombre de usuario en X”.
    - Ingresar el nombre del propietario de la marca.
    - Dirección del propietario de la marca.
    - País del propietario de la marca.
    - Sitio web del propietario de la marca.
    - Nombre de usuario de X del propietario de la marca.
    - Palabra o símbolo de marca registrada.
    - Numero de registro de marca.
    - Clase de bienes o servicios de marca registrada.
    - Nombre de registro en este caso “SENADI-Servicio Nacional de Derechos Intelectuales”.
    - Enlace directo al registro de marca en este caso ingresar “ http://servicios.propiedadintelectual.gob.ec/validador/index.xhtml#resultado”.
    - Confirmar las declaraciones para completar la denuncia y enviar.

Respuesta de la red X.

- Una vez enviado la denuncia, llegara una notificación de parte de la Red X confirmando la recepción de la denuncia.
- Si la Red X considera solicitar más información se debe responder al correo recibido con la información que solicita, por lo general aquí es cuando solicitan el Certificado de autorización de parte de la cooperativa.
- Una vez enviada la documentación requerida, la Red X emitirá un correo electrónico de respuesta, confirmando la eliminación de la cuenta denunciada.
- Por último, revisar que la cuenta este fuera de servicio.

Páginas webs clonadas.

Para dar de baja un dominio, ya sea gratuito o pagado, es fundamental realizar las denuncias correspondientes, ya sea directamente al proveedor de hosting o a Google. Los proveedores de hosting pueden ser GoDaddy, Host4Geeks, Bluehost, HostGator, SiteGround, Amazon Web Services (AWS), entre otros. Cualquiera de estas opciones puede ser efectiva para resolver la situación de una página web clonada. Este procedimiento es crucial para proteger la integridad de la marca y garantizar que los usuarios no sean engañados por sitios fraudulentos.

Antes de realizar la denuncia, es importante tener en cuenta los siguientes puntos y tenerlos listos:

- URL del dominio clonado.
- Capturas de pantalla que demuestren la suplantación de identidad.
- Descripción detallada del problema y cualquier evidencia adicional que respalde la denuncia.

Proveedor de hosting.

- Investigar donde esta alojada la página, para ello nos podríamos ayudar con la herramienta hostingchecker ingresando a la siguiente url: https://hostingchecker.com/ donde nos indicara la siguiente información:
    - Donde esta alojada.
    - Nombre de la organización.
    - Dirección Ip.

- Ciudad y país.

- Contactar al proveedor de Hosting.

  Acceder a la página oficial del proveedor del hosting y buscar la sección destinada a reclamos o soporte técnico. Dependiendo del proveedor, el reclamo puede realizarse a través de un correo electrónico o llenando un formulario en línea.

- En caso de reclamo por correo electrónico.

  Redactar un correo detallado explicando la situación. Asegurar de incluir la URL del dominio en cuestión, capturas de pantalla relevantes y cualquier otra evidencia que respalde el reclamo. Es fundamental adjuntar el documento de registro de marca otorgado por la SENADI, incluyendo el número de registro y un enlace a la URL de validación correspondiente. Para mayor claridad, se adjuntará un ejemplo de correo electrónico. Ver el Anexo 6.

- En caso de reclamo mediante formulario.

  Completar toda la información solicitada en el formulario del proveedor de hosting, asegurándose de proporcionar detalles como la URL del dominio, la descripción del problema y cualquier evidencia adicional requerida.

Respuesta del proveedor

De igual manera, el proveedor de hosting enviará cualquier respuesta a la dirección de correo electrónico proporcionada. En su respuesta, detallará si necesita información adicional para validar el reclamo o si ha decidido proceder con la eliminación del contenido por incumplimiento de sus políticas.

Denuncias a Google.

Para realizar una denuncia a Google se puede realizar de dos formas ingresando a las siguientes Urls:

https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en

https://search.google.com/search-console/report-spam?hl=es

Primera Url: Reporte de Phishing

En el primer enlace, se debe ingresar la URL de la página web clonada. En el reporte, es crucial proporcionar todos los detalles relevantes sobre la página, explicando que está siendo utilizada para robar información personal y cometer fraudes. Es importante destacar que este reporte debe enviarse varias veces para que Google lo considere como una prioridad y proceda a su validación.

Esta estrategia incrementa las posibilidades de que Google actúe con mayor rapidez, aumentando la visibilidad del problema y ayudando a proteger a otros usuarios de posibles estafas.

Segunda Url: Contenido fraudulento, engañoso o de baja calidad

Para reportar el contenido fraudulento en este enlace se debe ingresar la siguiente información:

- Url de la página web clonada.
- Seleccionar que problema hay con esta página, en este caso seleccionar “La página es engañosa.
- Seleccionar cual es el problema exactamente, en este caso seleccionar “Estafa y fraude y Funciones engañosas”.
- Ingresar información adicional.

Una vez enviado el reporte, se recibirá una notificación al correo personal de Gmail confirmando que se ha enviado un informe de usuario sobre la calidad de la Búsqueda.

Validación.

Una vez que se han completado los reportes indicados y se han recibido las respuestas correspondientes, es fundamental proceder con la validación de los resultados. Es importante tener en cuenta que no siempre se recibirá una notificación clara indicando que la página ha sido dada de baja o eliminada. Por lo tanto, es necesario estar atentos y verificar directamente la URL que fue reportada.

1.3. Validación de la propuesta

En este apartado, la propuesta fue validada por tres especialistas en el área, utilizando un instrumento diseñado específicamente para este propósito, cuyos detalles se presentan a continuación:

Primera validación

El Ing. Leandro Damian Quezada Ochoa evaluó esta guía de protección de marca para cooperativas y la calificó como "Muy adecuada" en todos los aspectos. Esta evaluación subraya la relevancia del tema debido al creciente riesgo de fraudes. Además, indica que la guía ofrece procedimientos prácticos para que las cooperativas protejan su marca, lo que disminuye la dependencia de proveedores externos y refuerza la confianza de socios y clientes. Además, resalta la necesidad de implementar programas de educación y concienciación para prevenir fraudes, lo que podría reducir significativamente el impacto de los ataques cibernéticos.

Segunda validación

El Ing. Byron Adrián Ortega, según la evaluación realizada, la guía fue considerada "Muy adecuada" en todos los aspectos evaluados. Las observaciones indican que el tema es relevante y aplicable en el contexto financiero cooperativo, dado que estos fraudes afectan a los clientes o socios. Como recomendación, se sugiere que se enfatice en próximas investigaciones la educación continua tanto para los socios como para los colaboradores de la institución para reducir los riesgos de fraude.

Tercera validación

El Ing. Paul Zhañay, según la evaluación realizada, la guía fue considerada "Muy adecuada" en todos los aspectos evaluados.

Las observaciones destacan que la protección de la marca es fundamental para las instituciones, ya que una gestión adecuada de los eventos de suplantación asegura que los servicios ofrecidos son auténticos. La guía evaluada es útil porque proporciona pasos organizados para proteger la marca en caso de suplantación.

Las recomendaciones sugieren que, aunque los pasos descritos en la guía son aplicables actualmente, es crucial mantenerse al día con los nuevos tipos de ataques de suplantación.

También se recomienda analizar las mejores maneras de mitigarlos, considerando las condiciones establecidas por los sitios de hosting y redes sociales para garantizar una respuesta oportuna y efectiva en la protección de la marca.

Las validaciones realizadas por los especialistas se encuentran detalladas en el Anexo 7.

1.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 3.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Investigación de temas de ciberseguridad.	Teoría de ciberseguridad.	Metodología bibliográfica.	Revisión en artículos, tesis y libros.	Aprovechar los beneficios de la investigación en ciberseguridad para fortalecer las defensas digitales.	Fuente bibliográfica.
Ataques fraudulentos en redes sociales y páginas web**.**	Teoría de seguridad informática.	Investigación de casos específicos de ataques fraudulentos en instituciones financieras	Programas de formación para educar a los usuarios en reconocer y evitar fraudes.	Tendencias observadas, nuevas tácticas y métodos empleados por los ciberdelincuentes.	Herramientas de detección, víctimas de fraude, casos reportados por ataques fraudulentos.
Encuestas a grupos en función de criterios específicos.	Proceso de investigación cuantitativa.	Encuestas, revisión documental.	Elaboración de encuestas.	Las encuestas revelan que la mayoría tiene un conocimiento básico-medio sobre ciberseguridad y desconocen la existencia de	Encuestas.

				una guía para eliminar páginas web y perfiles falsos.	
Eliminación de las páginas web clonadas.	Principios de ciberseguridad aplicados a la protección de la propiedad intelectual en línea.	Proceso para denunciar y solicitar la eliminación de páginas clonadas a proveedores de hosting y a Google.	Uso de herramientas que monitoricen la actividad en internet para identificar paginas clonadas. Uso de formularios para solicitar la eliminación de contenido clonado.	Incremento en la protección del sitio web contra futuras clonaciones. Impacto positivo en la percepción de seguridad y confianza por parte de los usuarios.	Formularios de proveedores de hosting y Google y otros documentos legales utilizados para la denuncia y eliminación.
Eliminación de perfiles falsos en redes sociales.	Conceptos teóricos sobre la seguridad y protección de datos en plataformas de redes sociales.	Proceso de validación y verificación un perfil en redes sociales antes de solicitar su eliminación.	Uso de herramientas que monitoreen la actividad en redes sociales para identificar cuentas falsas. Denuncias de socios o personal de la cooperativa. Uso de formularios para solicitar la eliminación de contenido que otorgan las plataformas.	Reducción del número de perfiles falsos. Mejora la confianza del cliente o socio. Eficiencia del proceso de denuncia y eliminación, con tiempos de respuesta mejorados por parte de las plataformas.	Formularios y registros de denuncias realizados ante las plataformas de redes sociales. Documentos legales para ser utilizados para la denuncia y eliminación.

CONCLUSIONES

Los fundamentos teóricos sobre la protección de marca en el contexto de las cooperativas de ahorro y crédito permitieron validar los conocimientos sobre ciberseguridad y la gestión de la identidad digital. La protección de la marca frente a ataques fraudulentos, como la creación de páginas web clonadas y perfiles falsos en redes sociales, es crucial para mantener la confianza de sus clientes o socios y preservar la integridad de la cooperativa. Teorías sobre la ciberseguridad, ingeniería social y el marco legal en torno a los derechos de propiedad intelectual y derechos de autor son fundamentales para establecer un enfoque robusto para proteger las marcas de las cooperativas en el entorno digital.

Los ataques fraudulentos, como las páginas web clonadas y los perfiles falsos en redes sociales, afectan significativamente la marca de las cooperativas. Estos ataques deterioran la confianza de los socios y clientes, lo que puede conducir a una disminución en la reputación y credibilidad de la cooperativa. La propagación de sitios clonados y perfiles falsos puede también resultar en pérdidas financieras, fraudes a los usuarios y un aumento en los costos operativos debido a la necesidad de implementar medidas correctivas. En última instancia, estos ataques no solo amenazan la integridad financiera de la cooperativa, sino que también debilitan la relación de confianza con sus socios y el público en general.

Como resultado de la investigación, se ha desarrollado una guía práctica para la eliminación de páginas web clonadas y perfiles falsos en redes sociales. Esta guía abarca todo el proceso, desde la investigación y denuncia hasta la eliminación de contenido fraudulento y detalla la importancia de contar con el documento de registro de marca y el certificado de la cooperativa que autorice a la persona encargada de gestionar la baja o eliminación de estas páginas y perfiles. Además, la guía incluye una herramienta para verificar el hosting de las páginas web y proporciona accesos directos a los formularios de denuncia en las plataformas digitales. Un aspecto clave es que, gracias a esta guía, las cooperativas pueden reducir su dependencia de proveedores externos para realizar este trabajo, ya que promueve la capacitación continua de los responsables, preparándolos para enfrentar otros tipos de ataques y dotándolos de las herramientas necesarias para responder eficazmente a nuevas amenazas. Esto refuerza significativamente la seguridad digital de las cooperativas.

RECOMENDACIONES

Se recomienda que futuras investigaciones se enfoquen en desarrollar programas de capacitación dirigidos a socios y empleados de las cooperativas de ahorro y crédito, para que adquieran conocimientos sólidos sobre los diferentes tipos de ataques cibernéticos, como la clonación de páginas web y la creación de perfiles falsos en redes sociales. Además, es fundamental que estas investigaciones promuevan la importancia del registro de la marca para aquellas cooperativas que aún no lo hayan realizado, ya que esto es un paso crucial en la protección de su identidad digital.

Asimismo, se sugiere profundizar en la aplicación de técnicas avanzadas de seguridad para proteger las páginas web de posibles clonaciones. Estas técnicas incluyen el uso de firmas digitales, controles de seguridad robustos en los servidores y la educación continua de los usuarios para reconocer y evitar sitios clonados. También es esencial que las cooperativas gestionen sus redes sociales para que cuenten con cuentas verificadas, lo que contribuirá a la autenticidad y confianza de su presencia en línea.

A partir de los problemas diagnosticados durante este proyecto, se recomienda que las cooperativas realicen evaluaciones periódicas de la efectividad de sus estrategias de protección de marca, adaptándolas según la evolución de las amenazas cibernéticas. Además, se debe explorar la creación de alianzas con otras cooperativas y entidades financieras para desarrollar un sistema de alerta temprana ante la detección de páginas web clonadas y perfiles falsos, lo que contribuirá a mitigar el impacto de estos ataques.

Se recomienda para una próxima investigación que la guía desarrollada sea socializada entre todas las cooperativas, lo que puede incluir la organización de talleres y seminarios para capacitar a más personas en su aplicación. Además, se sugiere la creación de un repositorio digital accesible para compartir casos de éxito y lecciones aprendidas, fomentando una cultura de colaboración y mejora continua en la seguridad digital. También es importante investigar otros métodos efectivos para dar de baja o eliminar páginas web clonadas, así como explorar cómo gestionar la eliminación de perfiles falsos en otras redes sociales, asegurando la autenticidad y protección de la reputación de las cooperativas en todas las plataformas digitales.

BIBLIOGRAFÍA

Asobanca. (2023). *Asobanca y Mintel socializarán los avances y desafíos de la Ley.* https://asobanca.org.ec/wp-content/uploads/2023/10/2023-10-24-BP-Asobanca-Mintel-Evento-Proteccion-de-Datos-en-la-Era-Digital-1.pdf

Baker, K. (21 de Agosto de 2023). *WHAT IS CLONE PHISHING AND HOW DO I AVOID IT?* IDENTITYIQ: https://www.identityiq.com/scams-and-fraud/what-is-clone-phishing-and-how-do-i-avoid-it/

BCE. (08 de 2022). *Todo lo que no sabías sobre las cooperativas en Ecuador*. Banco Central del Ecuador: https://www.bce.fin.ec/educacion-financiera/articulos/todo-lo-que-no-sabias-sobre-las-cooperativas-en-ecuador#:~:text=El%20rol%20de%20las%20cooperativas,con%20un%20notable%20impacto%20social.

Benavides, E., Fuertes, W., Y Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia Y Tecnología*, 98. https://doi.org/https://doi.org/10.18779/cyt.v13i1.357

Calizaya, J., Bellido, R., Alemán, Y., Morales, P., Monzón, G., Y Ceballos, F. (2020). La investigación cuantitativa. AutanaBooks. https://doi.org/10.47460/uct.v24i107.418

CISA. (2021). *Cybersecurity and Infrastructure Security Agency*. Avoiding Social Engineering and Phishing Attacks: https://cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Duoc UC. (14 de Enero de 2024). *Investigación Aplicada, Innovación y Transferencia*. Duoc UC Bibliotecas: https://bibliotecas.duoc.cl/investigacion-aplicada/definicion-proposito-investigacion-aplicada

Furtado, F. (22 de Julio de 2020). *Takedown 101: cómo eliminar contenidos infractores de internet*. Axur: https://blog.axur.com/es/takedown-101-como-eliminar-contenidos-infractores-de-internet#:~:text=Existen%20varios%20nombres%20para%20denominar,opciones%20para%20todos%20los%20gustos.

Garzón, C., Navas, C., Illicachi, A., Espinoza, R., Y Estrella, G. (2024). ANÁLISIS DE LOS ATAQUES DE INGENIERÍA SOCIAL EN ECUADOR. *Ciencia Latina Revista Cientifica Multidisciplinar, 8*(1). https://doi.org/https://doi.org/10.37811/cl_rcm.v8i1.9777

Guevara, G., Verdesoto, A., & Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). 171. https://recimundo.com/index.php/es/article/view/860/1363

Hernández, W. O., Osuna, C. S., Jiménez, B. N., Y Vazquez, D. M. (2022). ANÁLISIS DEL CRECIMIENTO DE PHISHING EN LOS ÚLTIMOS AÑOS. *Revista Digital de Tecnologías Informáticas y Sistemas*, 103. https://www.redtis.org/index.php/Redtis/article/view/132/122

Kaspersky. (s.f.). *Qué es la ingeniería social*. Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Mayo, C. (2022). Análisis y técnicas de prevención, detección y ataques de phishing. (U. N. (España), Ed.) *UNED*, 27. https://apidspace.linhd.uned.es/server/api/core/bitstreams/0f93f8ec-b652-4bc9-b90f-f517011786c1/content

Observatorio de Derechos Digitales. (11 de 2023). *Nueva ola de ataques de phishing en Ecuador.* Orden Conflicto Violencia. https://ordenconflictoyviolencia.org/wp-content/uploads/2023/11/alerta_02_ddoec.pdf

Ojeda, F., Moreno, V., Y Torres, M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *Cienciamatriarevista*, 194-195. https://cienciamatriarevista.org.ve/index.php/cm/article/download/366/469?inline=1

Ortega, J. M. (2024). *CIBERSEGURIDAD MANUAL PRÁCTICO.* Bogotá: ECOE EDICIONES. https://books.google.es/books?hl=es&lr=&id=oWT7EAAAQBAJ&oi=fnd&pg=PA1&dq=qu%C3%A9+es+ciberseguridad&ots=Bb7hVBRDIf&sig=FKiRML4Dy7cxDxBt9FA4B99-_Cs#v=onepage&q=qu%C3%A9%20es%20ciberseguridad&f=false

Rico, R. (9 de mayo de 2022). *Perfiles Falsos en Redes Sociales*. Nordstern Technologies: https://www.nordsterntech.com/post/perfiles-falsos-en-redes-sociales

San Martín, R. I. (Abril de 2024). Evaluando la peligrosidad del Spear Phishing generado con soporte de IA generativa. 7. http://repositorio.udec.cl/bitstream/11594/12168/1/san_mart%C3%ADn_g_r_2024_ING.pdf

Tresorit, T. (11 de Sepriembre de 2023). *Clone phishing attacks, plus how to spot and avoid them, explained [2023]*. Tresorit: https://tresorit.com/blog/the-clone-wars-everything-you-need-to-know-about-clone-phishing-attacks-and-how-to-avoid-them/

UNIR. (03 de 01 de 2023). *La Universidad en Internet*. https://ecuador.unir.net/actualidad-unir/propiedad-intelectual/

ANEXOS

ANEXO 1: Formato de la encuesta

Encuesta

Estimado colaborador,

Gracias por participar en esta encuesta. Nuestro objetivo es comprender su conocimiento y experiencias relacionadas con la protección de la marca en Cooperativas de Ahorro y Crédito. En particular, nos enfocaremos en temas como ingeniería social, phishing, páginas web y perfiles falsos en las redes sociales.

La información recopilada nos ayudará a crear una guía para saber cómo proceder y reportar a las instancias respectivas, para dar de baja y/o eliminar dichas páginas y perfiles falsos. Sus respuestas serán confidenciales y se usarán únicamente con fines de investigación.

¡Gracias por su colaboración!

[redacted].com Cambiar de cuenta

No compartido

Conocimiento General

1. Cuál es su nivel de conocimiento sobre Ingeniería Social? *

	1	2	3	4	5	
Principiante	○	○	○	○	○	Experto

2. ¿Cuál es su nivel de conocimiento sobre que es phishing? *

	1	2	3	4	5	
Principiante	○	○	○	○	○	Experto

3. ¿Cuál es su nivel de conocimiento para identificar un intento de phishing? *

	1	2	3	4	5	
Principiante	○	○	○	○	○	Experto

4. ¿Cuál es su nivel de conocimiento para identificar una página web y perfiles falsos en el internet? *

	1	2	3	4	5	
Principiante	○	○	○	○	○	Experto

Experiencias Personales

1. ¿Ha recibido un correo electrónico que sospechó que era un intento de phishing? *

	1	2	3	4	5	
Nunca	○	○	○	○	○	Muy frecuentemente

2. ¿Alguna vez a sido víctima de un intento de phishing? *

- ○ No
- ○ Si
- ○ No estoy seguro

3. ¿Ha reconocido perfiles falsos en redes sociales de cooperativas? *

- ◯ No
- ◯ Si

4. ¿Ha visitado una página web falsa pensando que era la página legítima de la cooperativa? *

	1	2	3	4	5	
Nunca	◯	◯	◯	◯	◯	Muy frecuentemente

Medidas y Prevención

1. ¿La cooperativa ofrece campañas para identificar y evitar el phishing? *

	1	2	3	4	5	
Nunca	◯	◯	◯	◯	◯	Muy frecuentemente

2. ¿Alguna vez a reportado al área de Seguridad Informática o al área correspondiente de la existencia de páginas web y perfiles falsos? *

	1	2	3	4	5	
Nunca	◯	◯	◯	◯	◯	Muy frecuentemente

3. ¿Alguna vez a reportado páginas web y perfiles falsos a las entidades correspondientes directamente para que se dé de baja y/o eliminen? *

	1	2	3	4	5	
Nunca	○	○	○	○	○	Muy frecuentemente

4. ¿Conoce si el área de Seguridad Informática o el área correspondiente tiene una guía para reportar una página web y perfiles falsos que se dé de baja y/o eliminen? *

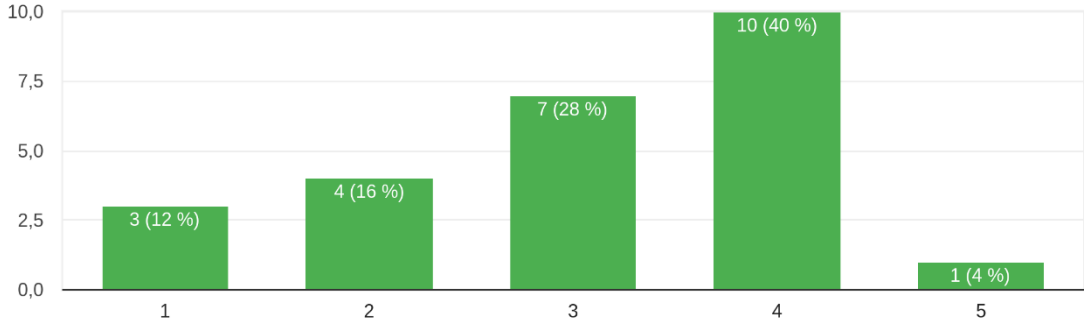
- ○ Sí
- ○ No

ANEXO 2: Resultados de la encuesta

Conocimiento General

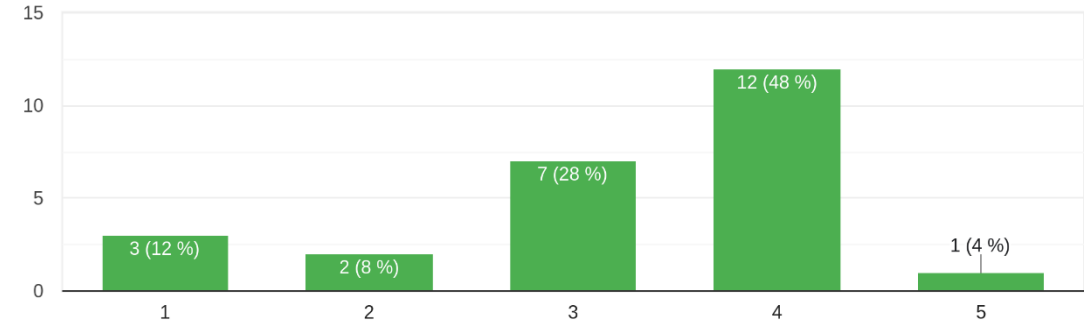
1. Cuál es su nivel de conocimiento sobre Ingeniería Social?

25 respuestas



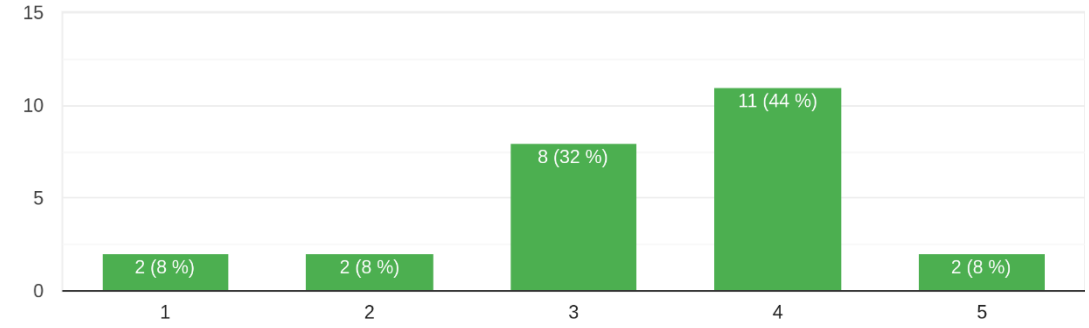
2. ¿Cuál es su nivel de conocimiento sobre que es phishing?

25 respuestas



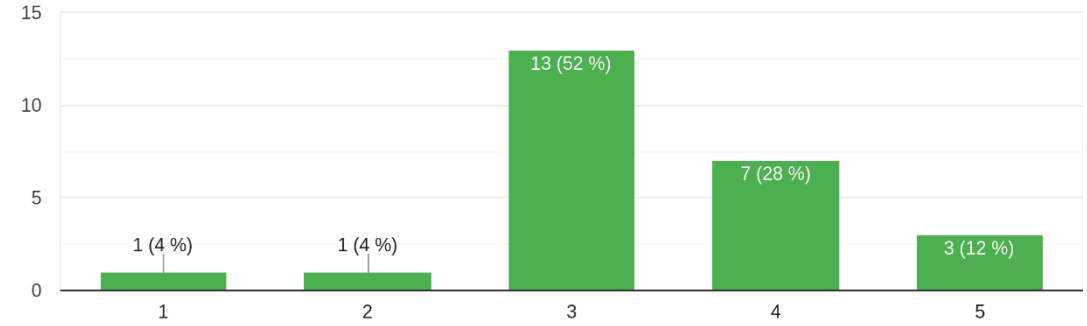
3. ¿Cuál es su nivel de conocimiento para identificar un intento de phishing?

25 respuestas



4. ¿Cuál es su nivel de conocimiento para identificar una página web y perfiles falsos en el internet?

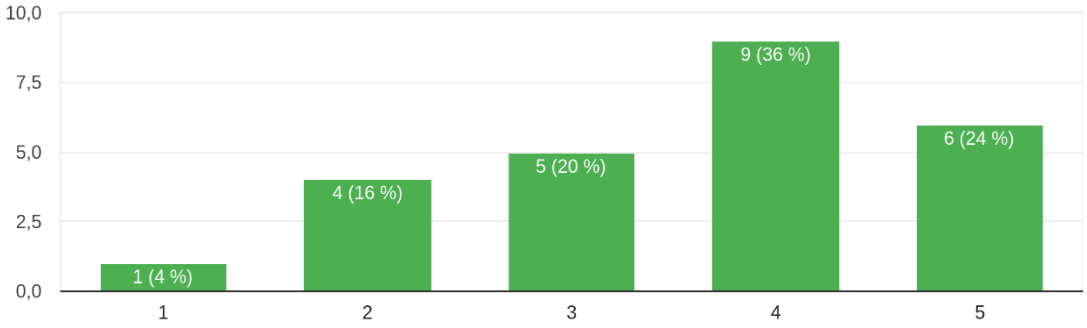
25 respuestas



Experiencias Personales

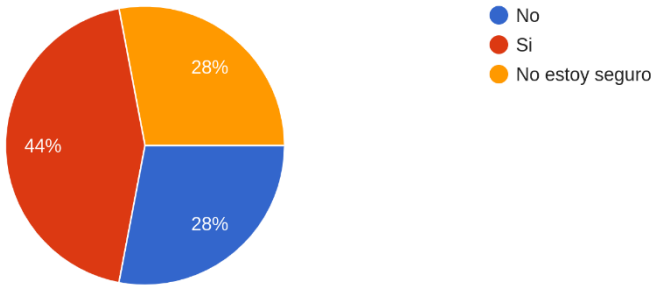
1. ¿Ha recibido un correo electrónico que sospechó que era un intento de phishing?

25 respuestas



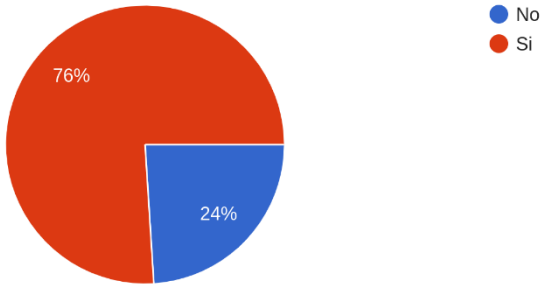
2. ¿Alguna vez a sido víctima de un intento de phishing?

25 respuestas



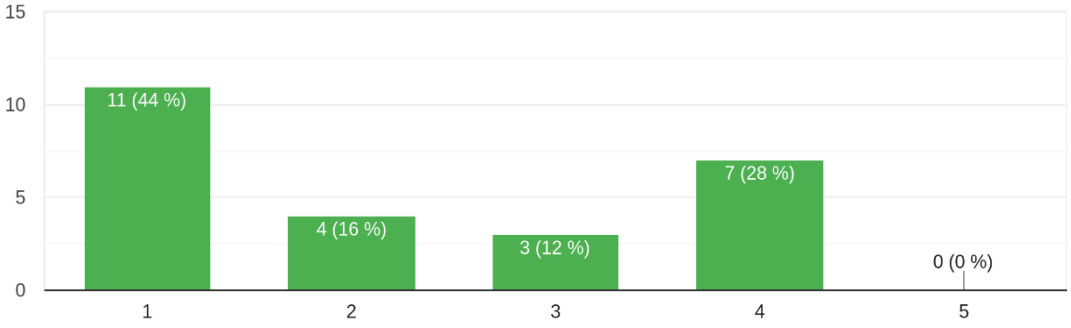
3. ¿Ha reconocido perfiles falsos en redes sociales de cooperativas?

25 respuestas



4. ¿Ha visitado una página web falsa pensando que era la página legítima de la cooperativa?

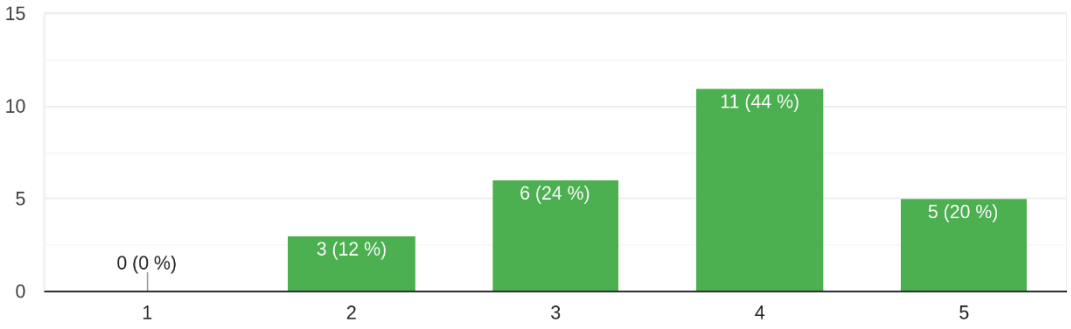
25 respuestas



Medidas y Prevención

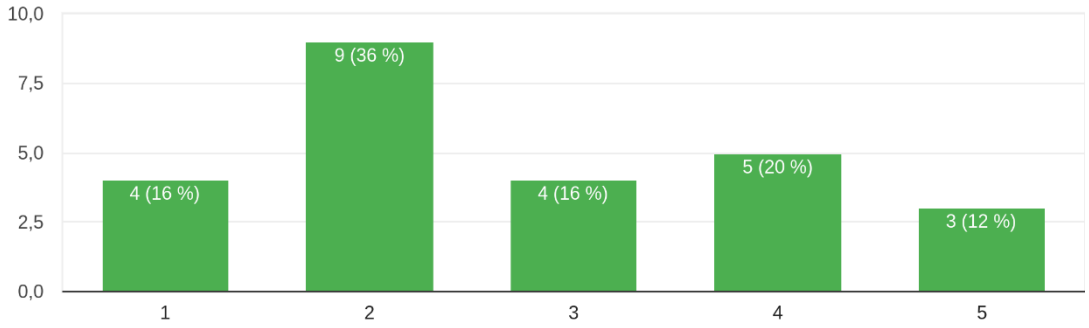
1. ¿La cooperativa ofrece campañas para identificar y evitar el phishing?

25 respuestas



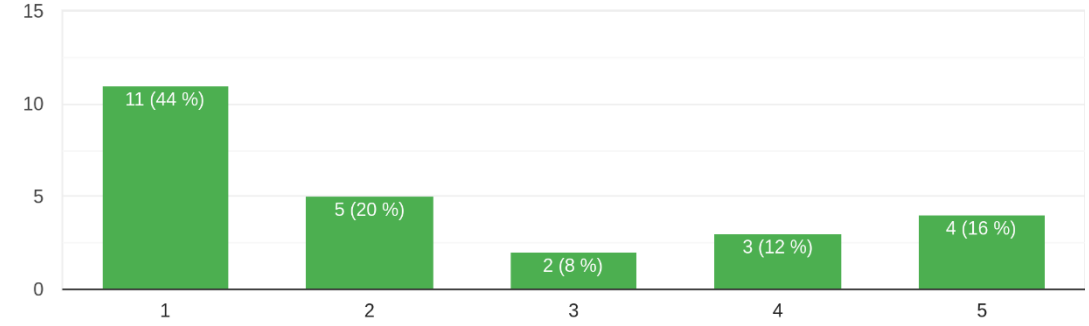
2. ¿Alguna vez a reportado al área de Seguridad Informática o al área correspondiente de la existencia de páginas web y perfiles falsos?

25 respuestas



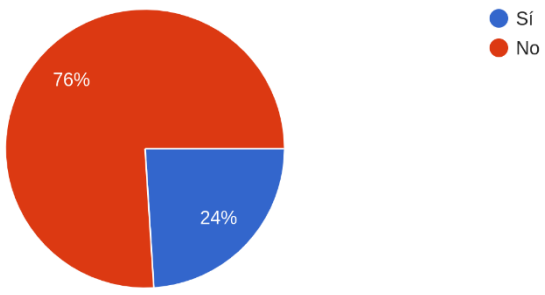
3. ¿Alguna vez a reportado páginas web y perfiles falsos a las entidades correspondientes directamente para que se dé de baja y/o eliminen?

25 respuestas



4. ¿Conoce si el área de Seguridad Informática o el área correspondiente tiene una guía para reportar una página web y perfiles falsos que se dé de baja y/o eliminen?

25 respuestas



ANEXO 3: Modelo de certificado de registro de marca

Servicio Nacional de Derechos Intelectuales

SENADI_2023

Direccion Nacional de Propiedad Industrial

En cumplimiento a lo dispuesto en la Resolución No. SENADI_2023_RS_12963 de 22 de agosto de 2023, se procede a OTORGAR el título que acredita el registro MARCA DE SERVICIOS, trámite número SENADI-2023- del 16 de febrero de 2023

DENOMINACIÓN: COOPERATIVA DE AHORRO Y C

PRODUCTOS O SERVICIOS QUE PROTEGE:

Préstamos con garantía, investigación financiera, servicios de pago po

Clase Internacional 36

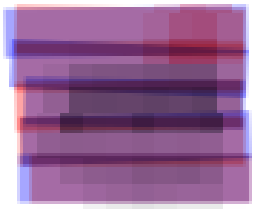
DESCRIPCIÓN: Igual a la etiqueta adjunta, con todas las reservas que sobre ella se hacen.

VENCIMIENTO: 22 de agosto de 2033

TITULAR: Cooperativa de Ahorro y C

DOMICILIO:

REPRESENTANTE:



Guayaquil, 26 de octubre de 2023

Documento firmado electrónicamente
Nathalie Rostan
DIRECTORA REGIONAL GUAYAQUIL

ANEXO 4: Modelo de certificado

Ciudad, X de agosto de 2024

CERTIFICADO

Yo, **Nombre del Gerente de la Cooperativa**, con cédula de ciudadanía **XXXXXXXXX**, en mi calidad de representante legal de la Cooperativa de Ahorro y Crédito **XXXXXXXXX**, declaro y autorizo a **Nombre de la persona que va a realizar las gestiones** con cedula de ciudadanía **XXXXXXXXXX** colaborador de la Cooperativa de Ahorro y Crédito **XXXXXXXXXXX**, para que realice los tramites o procesos correspondientes para gestionar la eliminación de páginas web clonadas y perfiles de redes sociales (Facebook, Red X, WhatsApp) y así proteger derechos de autor y marca comercial de la Cooperativa de Ahorro y Crédito **XXXXXXXXXXX**.

A continuación, detallo la página web y las redes sociales con las que cuenta la Cooperativa:

Página web: https://XXXXXXXXXXXXXXXXX

Facebook: https://www.facebook.com/XXXXXXXXXXX

Red X: https://twitter.com/XXXXXXXXXXX

El correo que utilizará el colaborador para los respectivos trámites es: sXXXXXXXXXX@XXXXXXXXXX.fin.ec

Atentamente

Gerente General

Cooperativa de Ahorro y Crédito XXXXXXXXX

ANEXO 5: Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador

GUÍA PARA LA PROTECCIÓN DE MARCA FRENTE ATAQUES FRAUDULENTOS PARA COOPERATIVAS DE AHORRO Y CRÉDITO DEL ECUADOR

Responsable: Andrés Tacuri **septiembre 2024**

INTRODUCCIÓN

Hoy en día, las redes sociales y los sitios web se han vuelto esenciales en la vida cotidiana de personas en todo el mundo. Debido a su amplia presencia, se han convertido en objetivos ideales para los ciberdelincuentes, quienes los utilizan para llevar a cabo estafas mediante la creación de sitios web clonados y cuentas falsas en redes sociales. Estos delincuentes se aprovechan de la confianza que los usuarios depositan en estas plataformas para engañarlos y estafarlos. Las consecuencias de estas actividades ilícitas pueden ser devastadoras tanto para los usuarios, quienes pueden enfrentar pérdidas financieras y el robo de información personal, como para las instituciones cuya identidad es falsificada, ya que pueden sufrir graves daños en su reputación y credibilidad en el mercado.

PROPÓSITO

El propósito de esta guía es ofrecer un procedimiento claro y detallado para dar de baja y/o eliminar páginas web clonadas y perfiles falsos en redes sociales que estén utilizando de manera fraudulenta el nombre, logotipo o identidad de alguna cooperativa. Esta guía está dirigida a los especialistas en sistemas y a los encargados de la seguridad y protección de la marca, quienes tienen la responsabilidad de gestionar estos temas y asegurar la eliminación de estos elementos fraudulentos en las plataformas digitales para mitigar cualquier estafa que se pueda dar con el uso de cualquiera de estos medios.

IMPORTANCIA DE LA GUÍA

La propagación de páginas web clonadas y perfiles falsos en redes sociales puede causar daños significativos a la reputación de las cooperativas. Estos ataques no solo confunden a los usuarios, sino que también se pierde la confianza depositada en la misma. Al eliminar estas amenazas, la cooperativa protege su integridad y asegura que su imagen no sea utilizada de manera indebida para actividades fraudulentas.

Dado que las redes sociales son una herramienta común en la vida diaria, es crucial que la cooperativa actúe de manera proactiva para proteger a sus miembros de potenciales estafas y fraudes. Al garantizar que estos elementos fraudulentos sean eliminados rápidamente, la cooperativa asegura que las interacciones con la institución sean seguras y confiables.

En general, esta guía no solo es una herramienta esencial para la protección de la marca, sino también un mecanismo importante para salvaguardar la seguridad de los clientes o socios frente a los crecientes ataques que se va dando en la vida diaria.

GLOSARIO DE TERMINOS

- **Marca:** Identidad comercial de una empresa que incluye su nombre, logotipo y otros elementos distintivos que la diferencian de otras entidades en el mercado.
- **Logotipo:** Símbolo gráfico que representa a una marca o empresa, y que es utilizado para identificarla y diferenciarla de otras.
- **Registro de Marca:** Proceso legal mediante el cual se obtiene la propiedad de una marca comercial a través de una entidad gubernamental, como la SENADI, que otorga derechos exclusivos sobre el uso de esa marca.
- **SENADI:** Servicio Nacional de Derechos Intelectuales, entidad gubernamental encargada del registro y protección de marcas, patentes, y otros derechos de propiedad intelectual.
- **Ciberdelincuentes:** Individuos o grupos que utilizan la tecnología y el internet para cometer delitos, como el fraude o el robo de información.
- **Eliminar:** Acto de suprimir o quitar algo, en este contexto se refiere a la eliminación de páginas web clonadas o perfiles falsos en redes sociales.
- **Genymotion:** Emulador de Android utilizado para simular dispositivos móviles en un entorno de escritorio, a menudo usado para probar aplicaciones o validar bloqueos en WhatsApp.
- **Dominio:** Nombre único que identifica a un sitio web en internet. Por ejemplo, "www.tuempresa.com" es un dominio.
- **URL:** Abreviatura de Uniform Resource Locator, es la dirección específica de una página web o recurso en Internet.
- **Hosting:** Servicio que proporciona espacio en un servidor para alojar sitios web, permitiendo que estos sean accesibles en Internet. Ejemplos de proveedores de hosting son GoDaddy, Bluehost y HostGator.
- **Google:** Motor de búsqueda y proveedor de servicios en línea que también ofrece herramientas para reportar y eliminar contenido fraudulento de la web.
- **HostingChecker**: Herramienta en línea utilizada para identificar el proveedor de hosting de un sitio web específico.
- **Facebook:** Red social global que permite a los usuarios conectarse, compartir contenido y comunicarse. A menudo es objeto de intentos de fraude mediante la creación de perfiles o páginas falsas.

- **WhatsApp:** Aplicación de mensajería instantánea que permite a los usuarios enviar mensajes de texto, voz, imágenes y realizar llamadas. También puede ser utilizada fraudulentamente para suplantar la identidad de empresas.
- **Formulario:** Documento o página web en la que se ingresan datos específicos para realizar una solicitud, denuncia o reporte, como parte del proceso de eliminación de contenido fraudulento.
- **Correo:** Medio de comunicación electrónica utilizado para enviar mensajes y archivos. En esta guía, se refiere al correo electrónico utilizado para contactar a proveedores de hosting o realizar denuncias.
- **Foxy Proxy:** Es una extensión de navegador que facilitara la gestión de servidores proxy, que actuara como intermediario entre el usuario y el servidor al que se desea acceder permitiendo que el tráfico de internet pase a través de este intermediario antes de llegar a su destino.
- **Burp Suite:** Es una plataforma integrada que se utiliza para realizar pruebas de seguridad en aplicaciones web, misma que ofrece un conjunto de herramientas que permiten realizar una variedad de pruebas de seguridad.

REQUISITOS PREVIOS

Para proceder con la baja y/o eliminación de páginas web clonadas y perfiles falsos en redes sociales, es esencial contar con ciertos documentos clave que respaldan la solicitud y garanticen la legitimidad del reclamo. Estos documentos son:

- **Documento de registro de marca otorgado por la SENADI:** Este documento certifica oficialmente que la cooperativa es la propietaria de la marca registrada ante el Servicio Nacional de Derechos Intelectuales (SENADI), este documento se lo debe de tramitar con anterioridad, se puede ayudar con el departamento legal para su respectivo tramite.
- **Número de registro de marca:** Este número identifica de manera única el registro de la marca y es necesario para demostrar la propiedad de la misma.
- **Link de validación del registro de marca de la SENADI:** Un enlace directo al registro de la marca en el portal de SENADI, que permite a las entidades verificar la autenticidad del registro y la propiedad de la marca.

  http://servicios.propiedadintelectual.gob.ec/validador/index.xhtml#resultado

- **Certificado de autorización otorgado por la cooperativa:** Este certificado debe indicar que una persona específica está autorizada para realizar trámites de eliminación de páginas web y perfiles falsos en nombre de la cooperativa. Es crucial que este certificado sea detallado y específico sobre los poderes otorgados, este certificado lo solicitan dependiente de la entidad que se reporte, no en todas solicitan.

ATAQUES FRAUDULENTOS FRECUENTES EN COOPERATIVAS

Facebook

PASOS PARA LA DENUNCIA DE PÁGINAS FALSAS A FACEBOOK

Para realizar una denuncia de una página falsa a Facebook se seguirán los siguientes pasos:

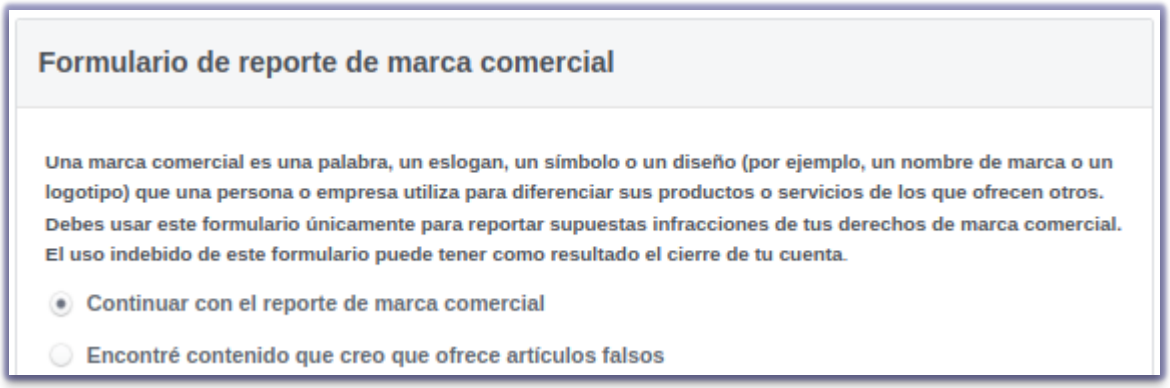
a. Url del Formulario.

Para realizar el reporte de marca comercial se debe ingresar a la siguiente URL:

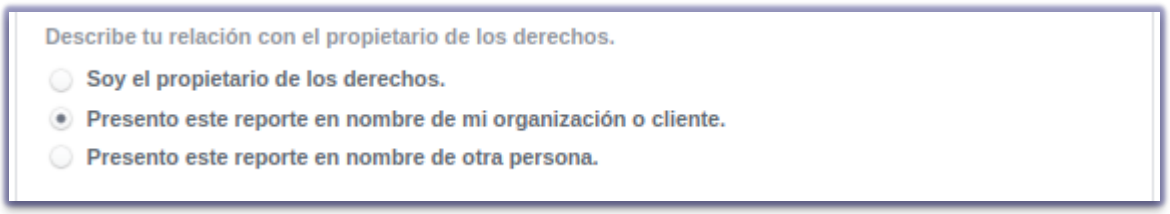
https://www.facebook.com/help/contact/1057530390957243

b. Llenado de Formulario.

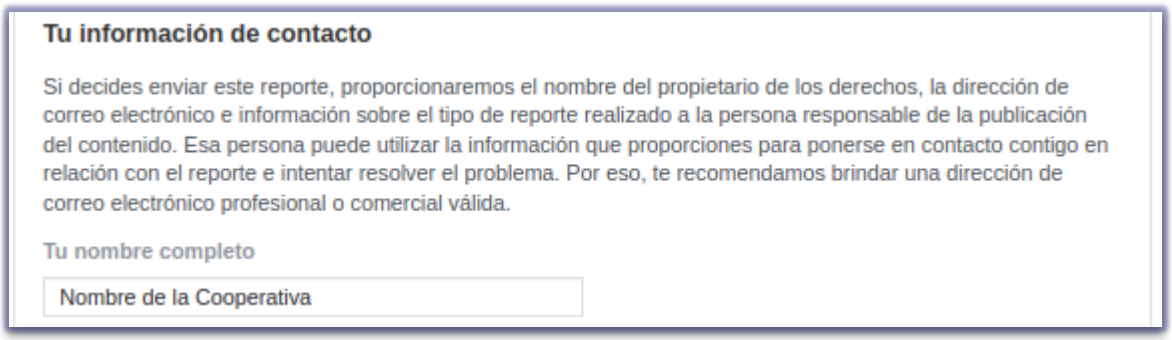
- Seleccionar la opción “Continuar con el reporte de marca comercial”.



- Describir la relación con el propietario de los derechos.



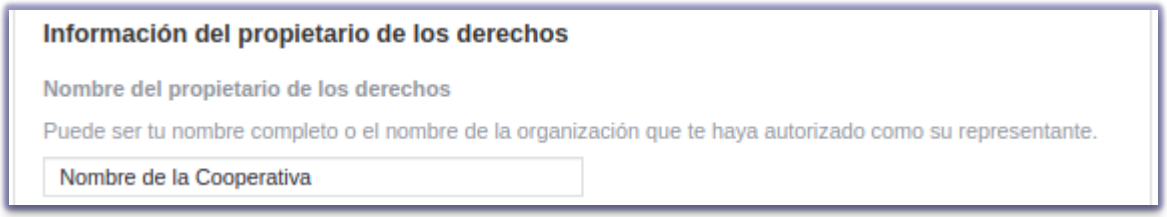
- Ingresar el nombre de contacto en este caso poner **Nombre de la Cooperativa**.



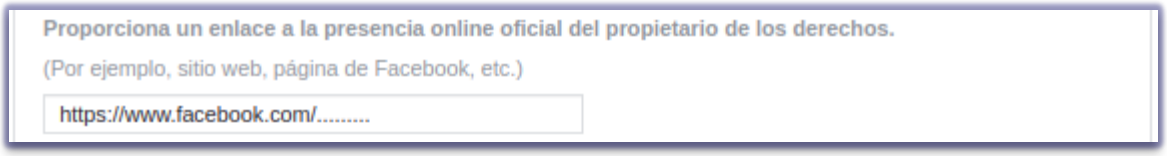
- Ingresar la dirección postal de la ciudad en la que se encuentra la Cooperativa.

- Ingresar una dirección de correo electrónico donde Facebook notificará el número de caso y la confirmación cuando se dé la baja la página, de preferencia un correo institucional.

- Ingresar el nombre del propietario de los derechos, en este caso igualmente ingresar el nombre de la cooperativa. “Cooperativa de Ahorro y Crédito **Nombre de la Cooperativa**”.

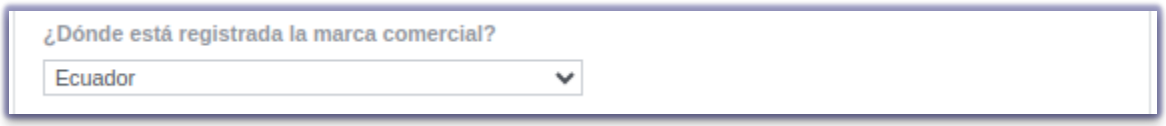


- Ingresar la url del propietario de los derechos, en este caso la url de la página de Facebook de la Cooperativa.

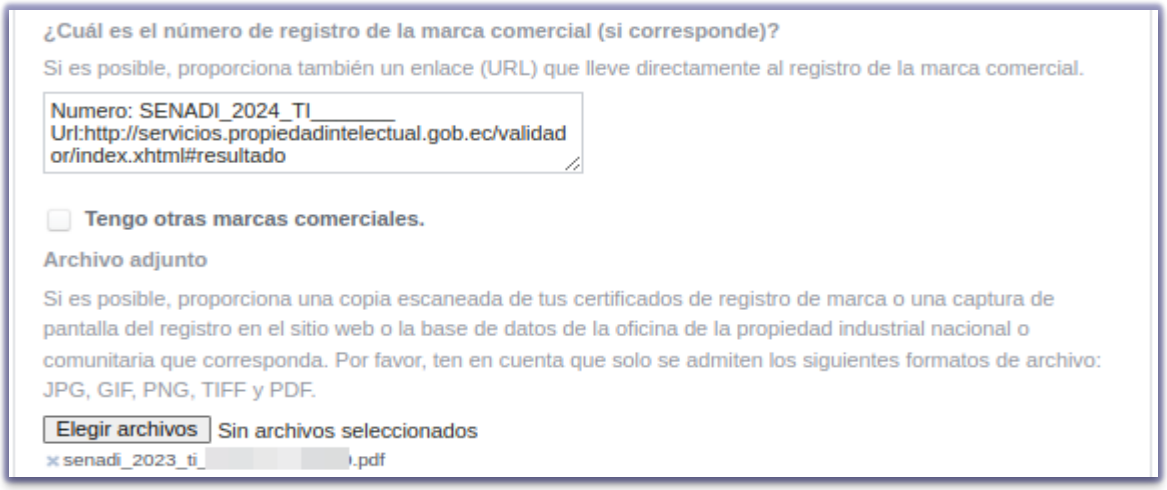


- Ingresar el nombre de la marca comercial como está en el certificado que otorga el **SENADI.**

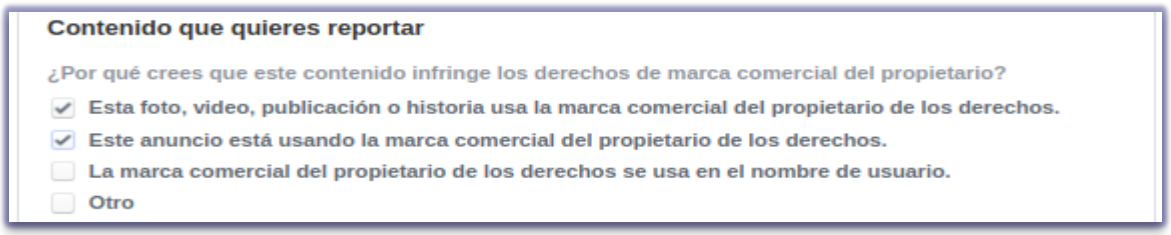
- Ingresar el país donde está registrada la marca, seleccionar Ecuador.



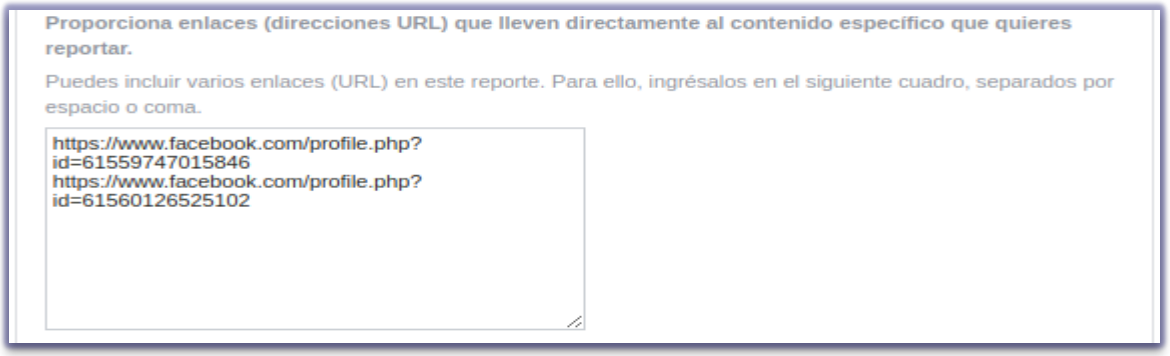
- Ingresar los siguientes datos:
    - Número de registro que envía el SENADI “SENADI_2023_TI_XXXXX”
    - URL para validar el documento: http://servicios.propiedadintelectual.gob.ec/validador/index.xhtml#resultado
    - Adjuntar el documento entregado por el SENADI.



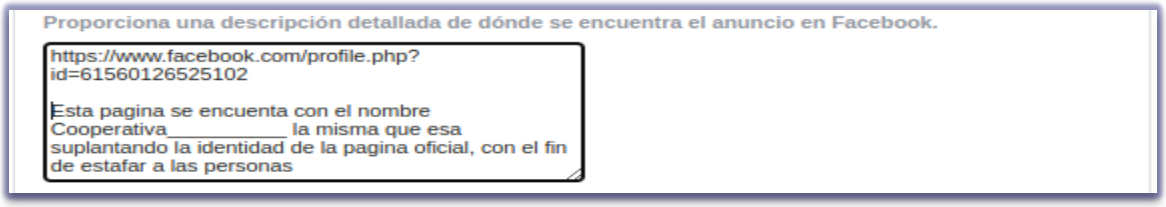
- Seleccionar el contenido de lo que se desea reportar, depende de lo que se está infringiendo.



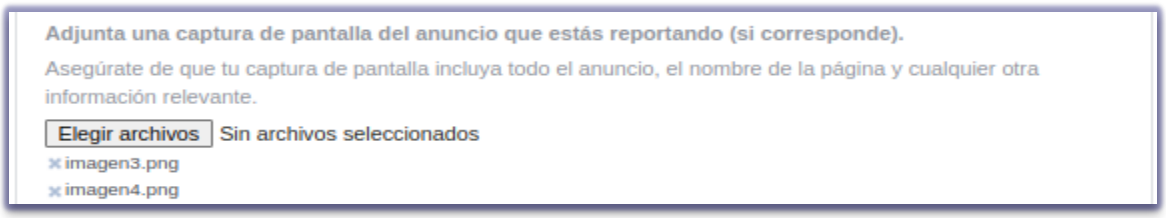
- Proporcionar los URLs que lleven directamente al contenido especifico que se desea reportar.



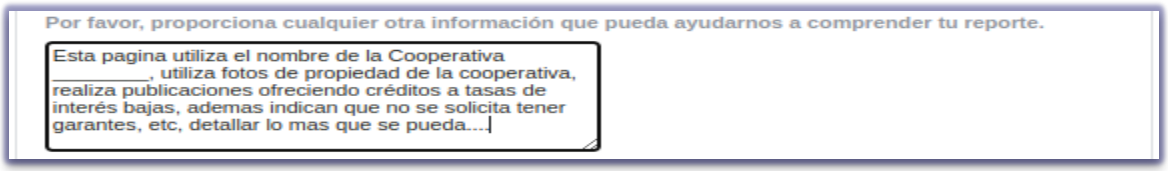
- Ingresar el nombre de la página falsa que se está denunciando y proporcionar un detalle del anuncio.



- Adjuntar las imágenes donde se encuentran los anuncios con sus respectivos detalles.

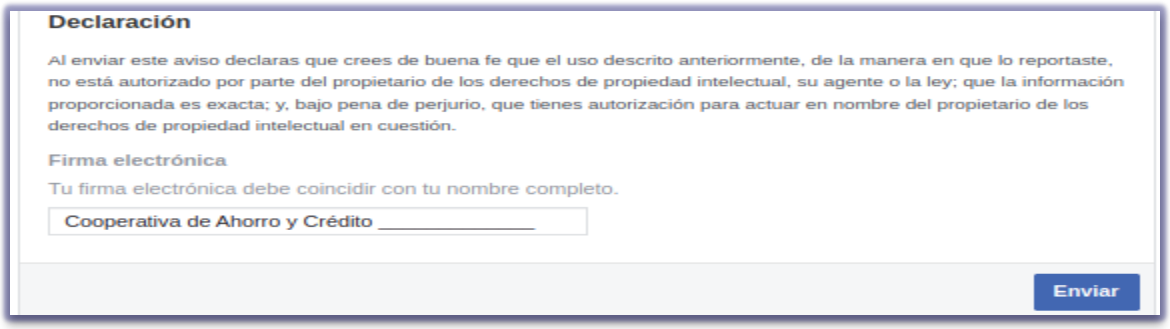


- Ingresar información que ayudará a entender lo que se está pretendiendo reportar.

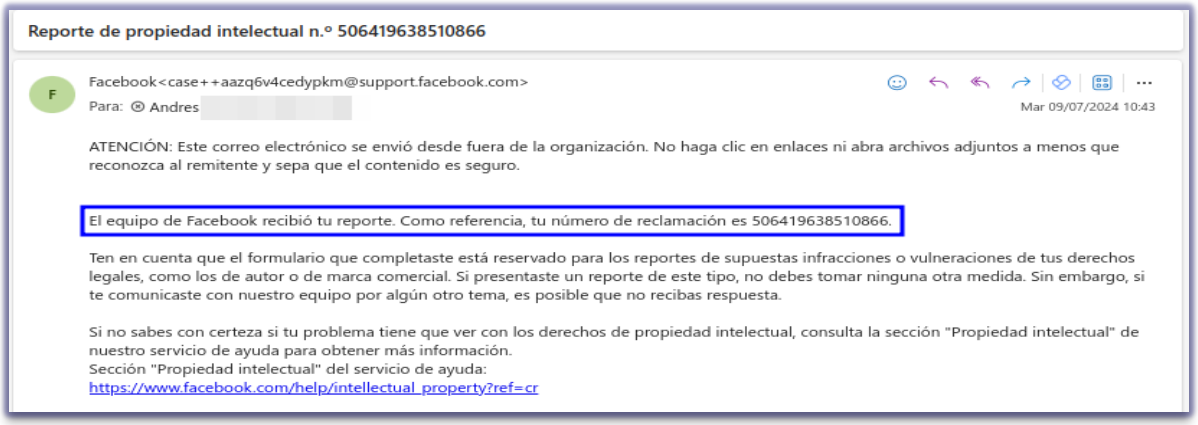


- Adjuntar imágenes con las evidencias indicadas.

- Ingresar el nombre de la cooperativa como firma y enviar el formulario.

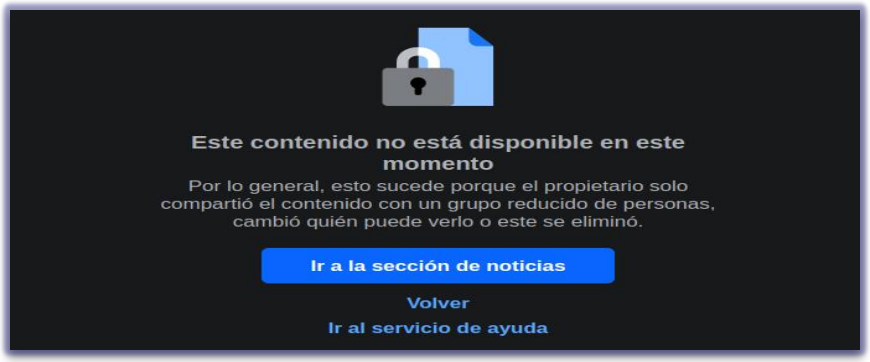


- Una vez enviado la denuncia, llegará una notificación de parte de Facebook al correo electrónico, indicando el número de caso para su revisión.



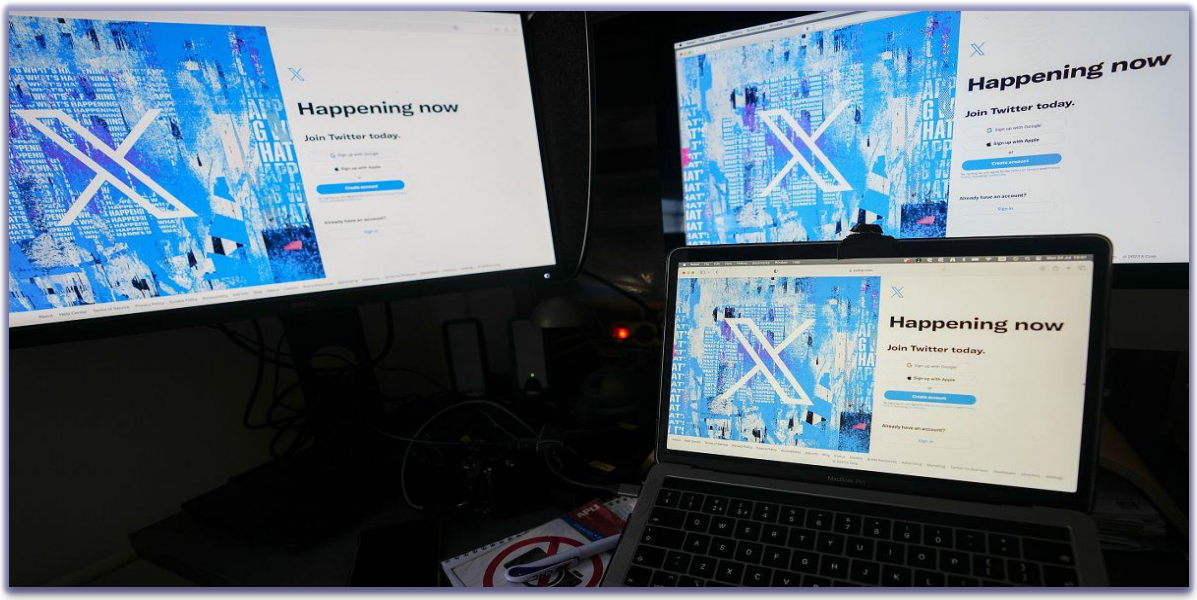
- Si Facebook considera solicitar más información se debe responder al correo recibido con la información que solicita.
- Una vez que se envié la información solicita por parte de Facebook de ser el caso, se debe esperar la respuesta de Facebook donde indiquen que fue eliminada la página denunciada, considerar que el tiempo de respuesta es demorado sin embargo la misma puede estar ya eliminada en Facebook.

- Validar que la página este fuera de servicio.



Red X

PASOS PARA LA DENUNCIA DE PÁGINAS FALSAS EN LA RED X (TWITTER)



Para realizar una denuncia de una página falsa en la Red X (Twitter) se debe seguir los siguientes pasos:

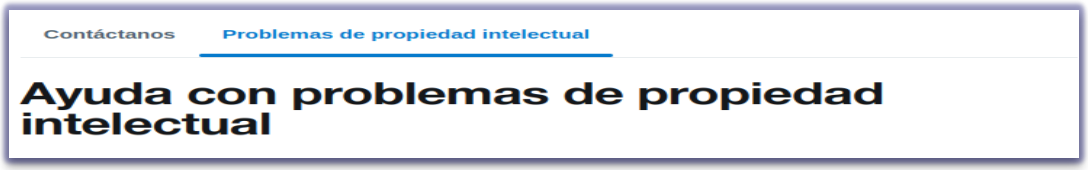
a. Url del Formulario.

Para realizar el reporte se debe ingresar al Centro de Ayuda de la Red X (Twitter) ingresando a la siguiente URL:

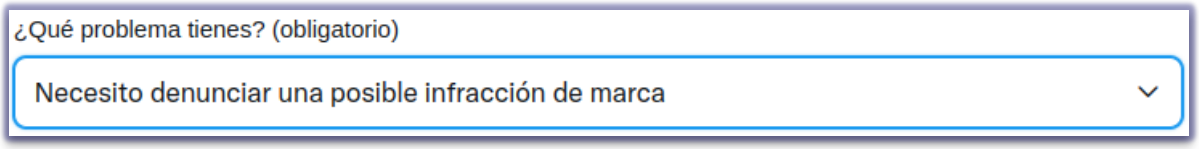
https://help.x.com/es/forms/ipi/trademark/trademark-owner

b. Llenado de Formulario.

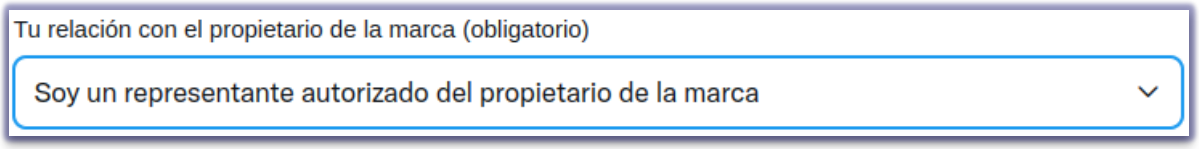
- Seleccionar el problema que se ha presentado, en este caso seleccionar “Problemas de propiedad intelectual”.



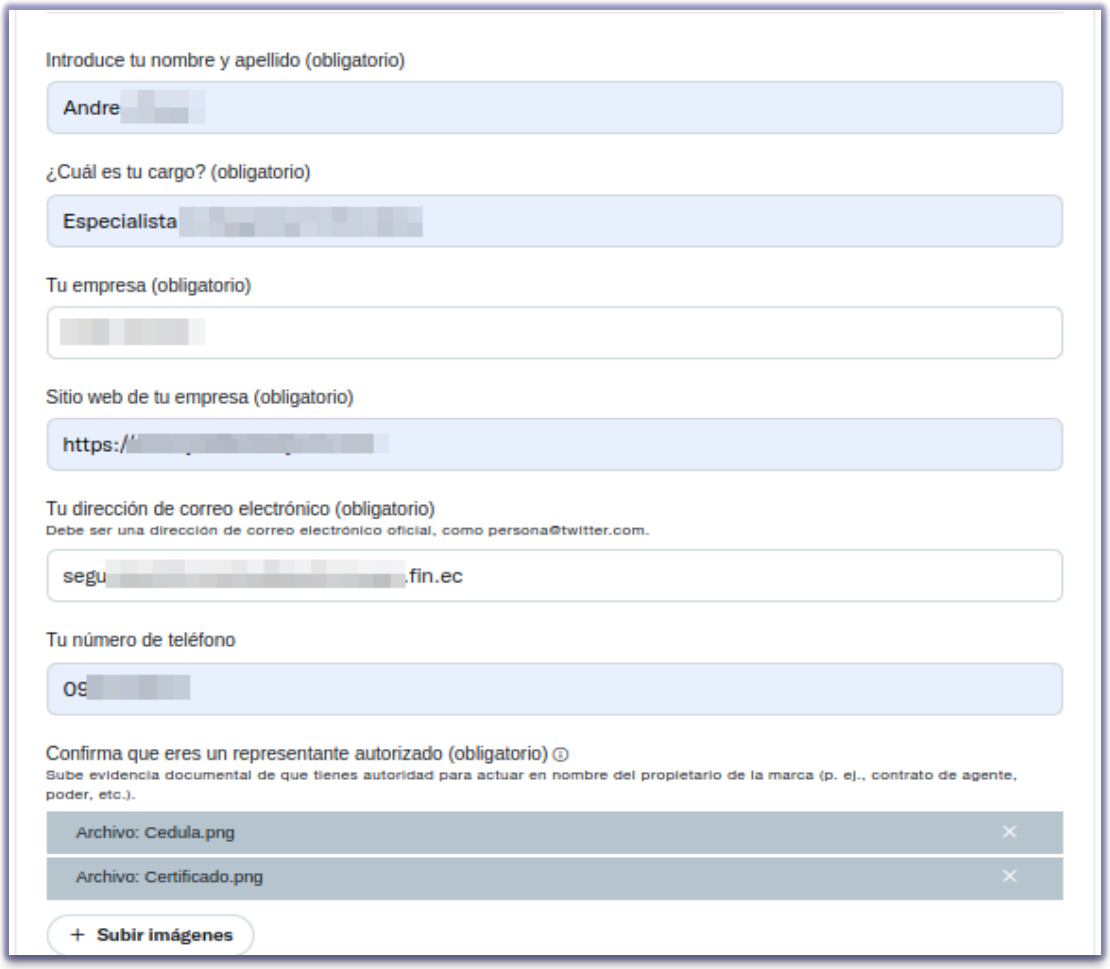
- Seleccionar el problema que se tiene “Necesito denunciar una posible infracción de marca”.



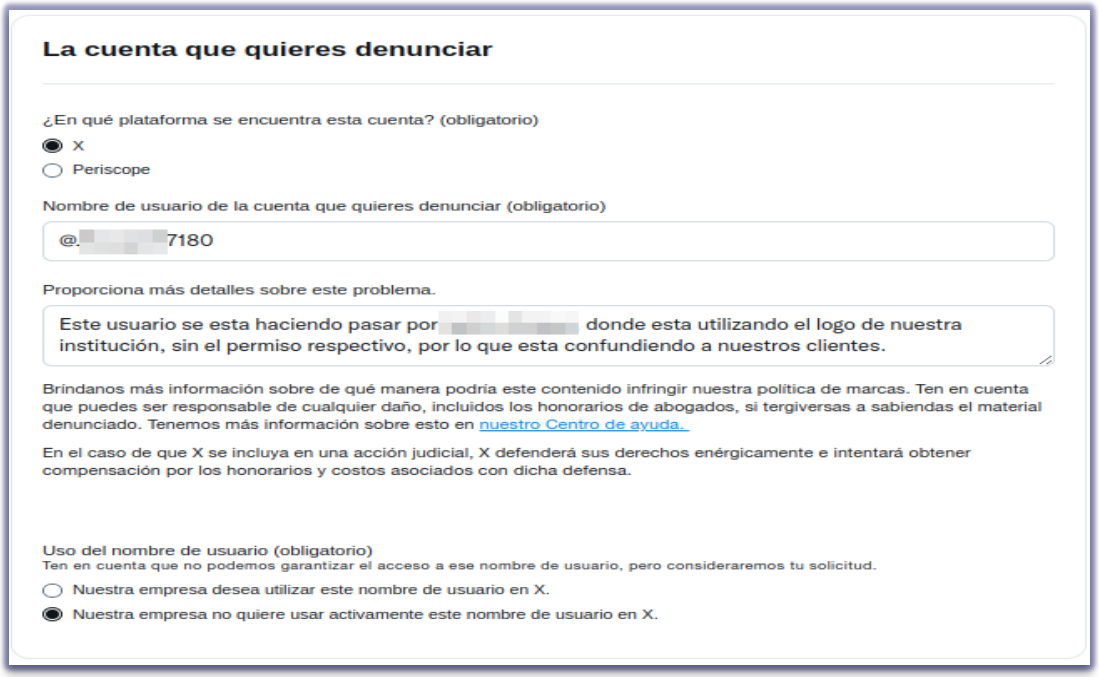
- Seleccionar la relación con el propietario de la marca “Soy un representante autorizado del propietario de la marca.



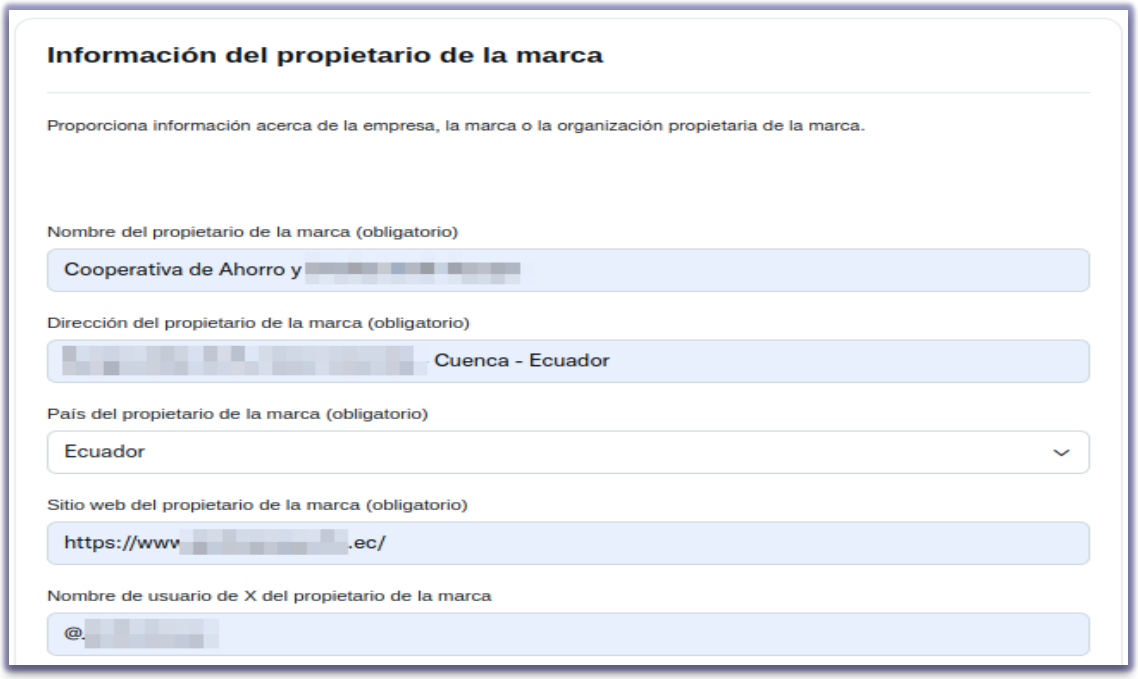
- Ingresar la información personal de la persona que está realizando la denuncia, adjuntar la cedula y certificado que emite la cooperativa donde indique que estas autorizado para realizar esta denuncia.



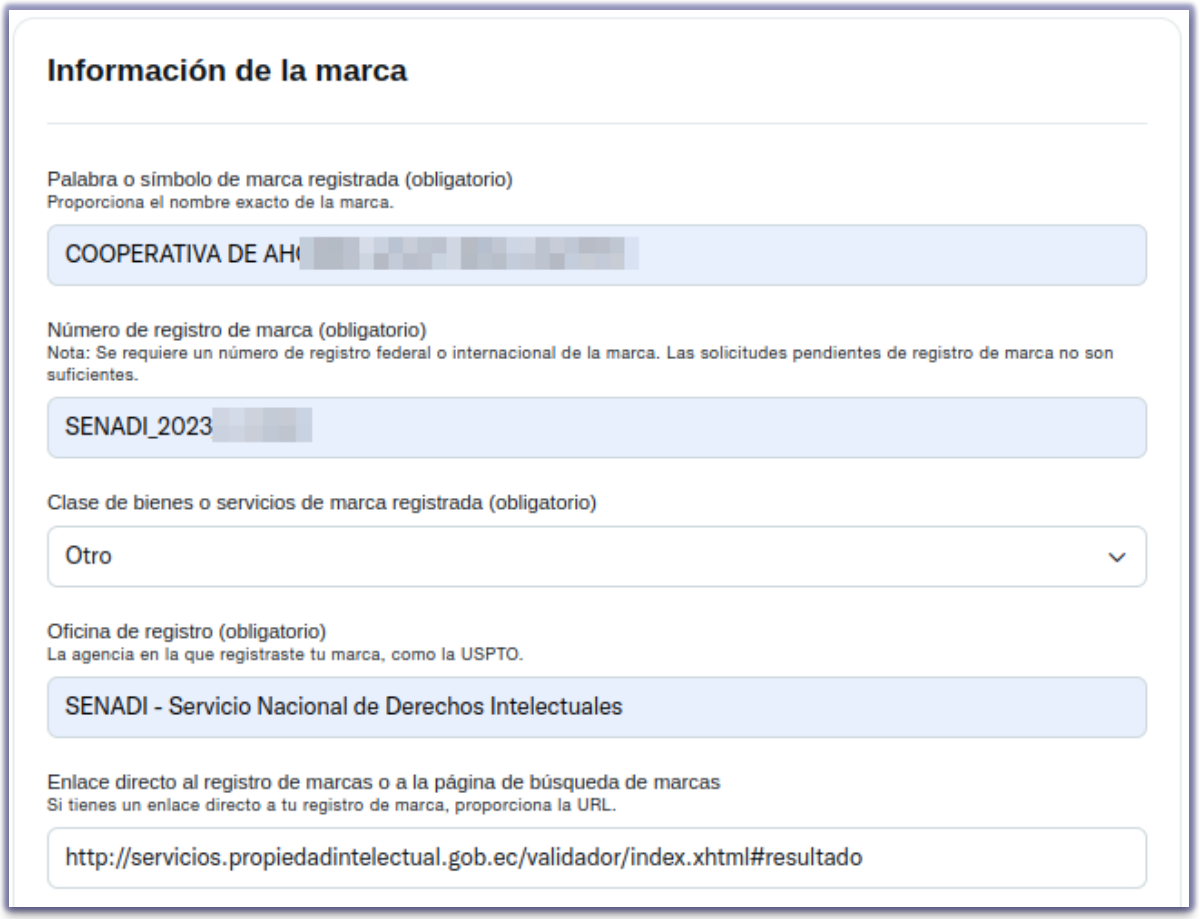
- Seleccionar la plataforma en la que se encuentra la cuenta, ingresar el usuario de la cuenta que se va a denunciar, proporcionar un detalle sobe el problema y marcar el uso del nombre de usuario.



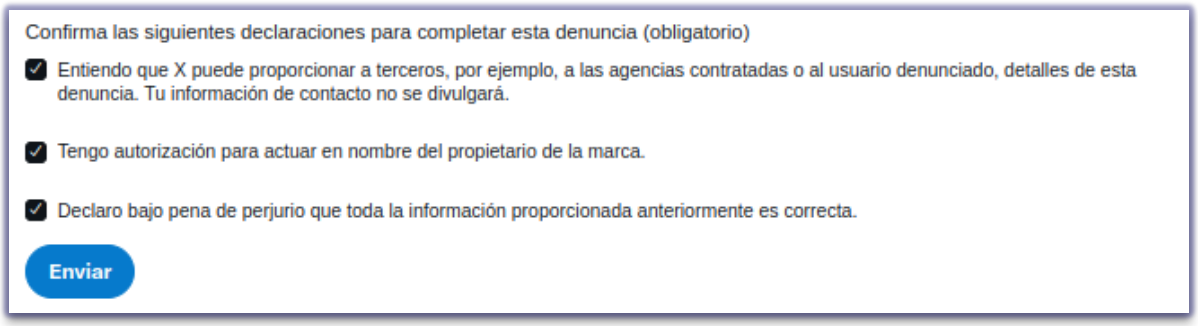
- Proporcionar información del propietario de la marca, como nombre del propietario, dirección, país, sitio web del propietario de la marca y nombre de usuario de la red X propietario de la marca.



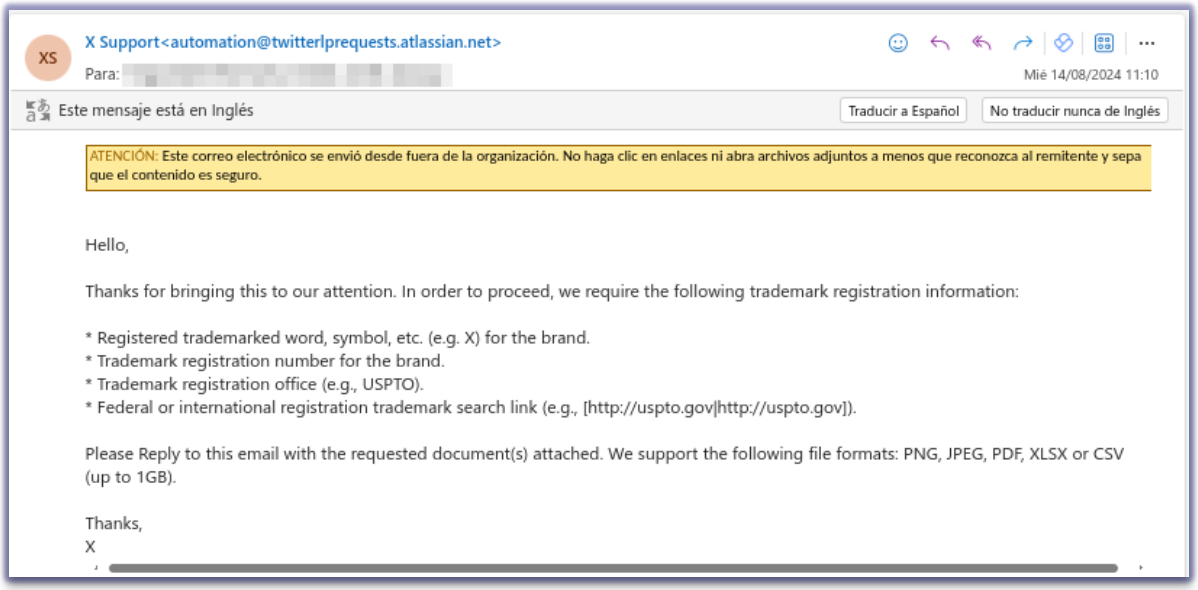
- Proporcionar información de la marca, como el nombre, número de registro de marca, el tipo de clase, oficina de registro y la url directa para la validación del registro de marca que proporciona la SENADI.



- Confirmar las declaraciones para completar la denuncia.



- Enviado el formulario de la denuncia, la red X responde con un correo electrónico indicando que para continuar se requiere más información del registro de marca, esta información trata de evidenciar que sé que se tiene autoridad sobre la marca antes indicada, por lo cual se debe de responder al mismo correo con la información solicitada.



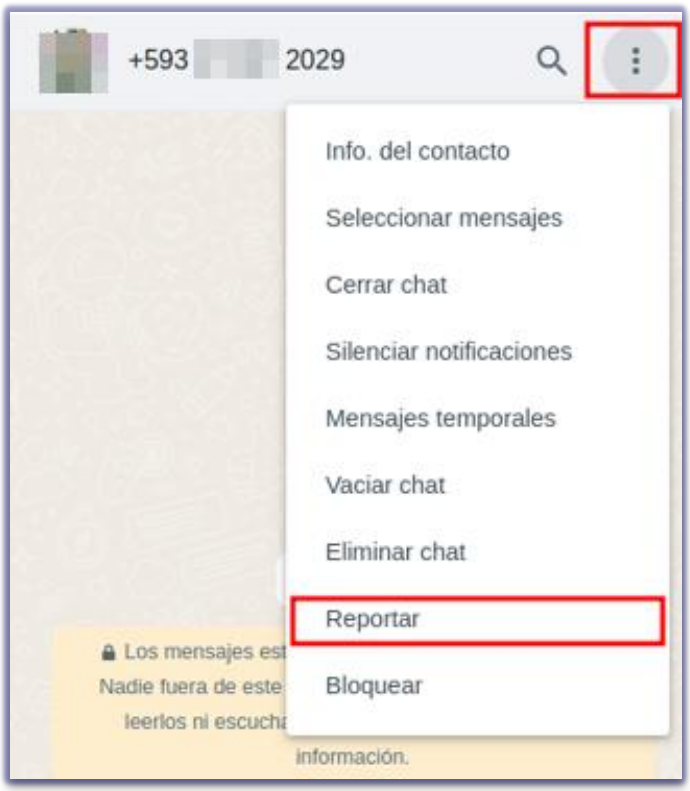
- Una vez enviada la documentación requerida, la Red X emitirá un correo electrónico de respuesta, confirmando la eliminación de la denuncia o solicitando información adicional, según corresponda.

WhatsApp

PASOS PARA LA DENUNCIA DE NÚMEROS DE CELULAR EN WHATSAPP

Una estrategia válida para bloquear o suspender números que se hacen pasar por la cooperativa en WhatsApp es reportarlos masivamente como spam. Las cooperativas pueden utilizar sus grupos internos de WhatsApp para coordinar estos reportes, informando a los miembros sobre el número fraudulento y solicitando que todos lo reporten. Este enfoque aumenta la visibilidad del problema para WhatsApp y acelera el proceso de revisión y bloqueo del número infractor. Implementar esta estrategia puede mitigar los daños y proteger la reputación de la cooperativa de manera más efectiva.

- Ingresar al chat del número reportado, seleccionar en los tres puntos y seleccionar la opción Reportar.



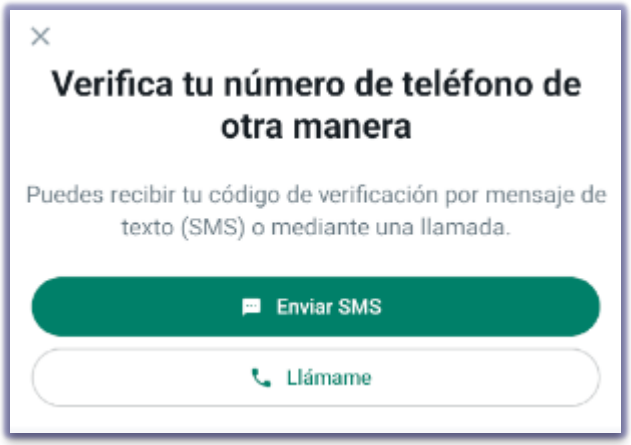
- Proceder a reportar ese contacto a WhatsApp, mientras más se reporte ese número, WhatsApp lo tomará como Spam.

- Para validar que el número ha sido bloqueado, se utilizará el emulador Genymotion, que simula un dispositivo móvil, adjunto el link de descarga:
  https://www.genymotion.com/product-desktop/download/
  En este emulador, se instalará la aplicación de WhatsApp. Una vez instalada, se intentará registrar la cuenta utilizando el número reportado. Para ello, se seleccionará el país correspondiente, se ingresará el número de celular y se hará clic en "Siguiente".

Este proceso permitirá verificar si el número ha sido efectivamente bloqueado por WhatsApp.

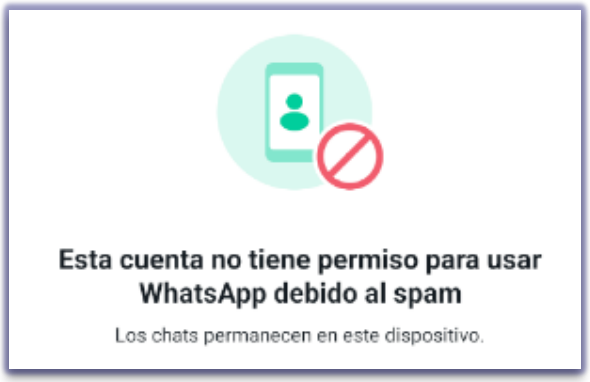
- Para realizar la verificación dar clic en la opción “Verificar de otra manera”.

- Una vez seleccionado “Verificar de otra manera”, escoger la opción “Enviar SMS”.

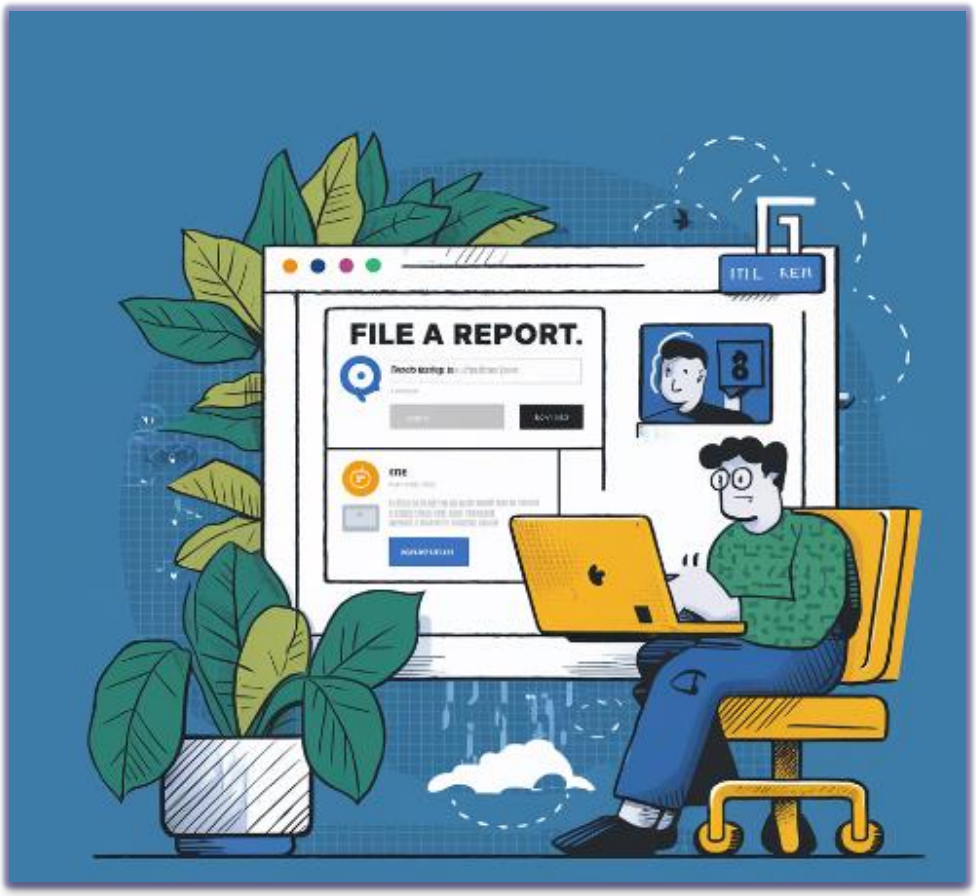


- Si se llega a este punto y solicita la verificación del número donde se debe ingresar el código de 6 dígitos, eso indica que el número no está bloqueado como se muestra en la imagen.

- El mensaje que debería salir, es que la cuenta no tiene permiso para usar WhatsApp debido al spam, como se muestra en la imagen.



PASOS PARA LA DENUNCIA DE PÁGINAS WEB FALSAS



Para dar de baja y/o eliminar un dominio, ya sea gratuito o pagado, es fundamental realizar manualmente utilizando herramientas de ciberseguridad o las denuncias correspondientes, al proveedor del hosting, o a Google. Cualquiera de estas opciones puede ser efectiva para resolver la situación de una página web clonada. Este procedimiento es crucial para proteger la integridad de la marca y garantizar que los usuarios no sean engañados por sitios fraudulentos. A continuación, se detallará el proceso a seguir para llevar a cabo estas denuncias y asegurar la eliminación de la página clonada.

- Reunir la información de la página clonada.
    - URL del dominio clonado.
    - Capturas de pantalla que demuestre la suplantación de identidad.
    - Descripción detallada del problema y cualquier evidencia que respalde la denuncia.

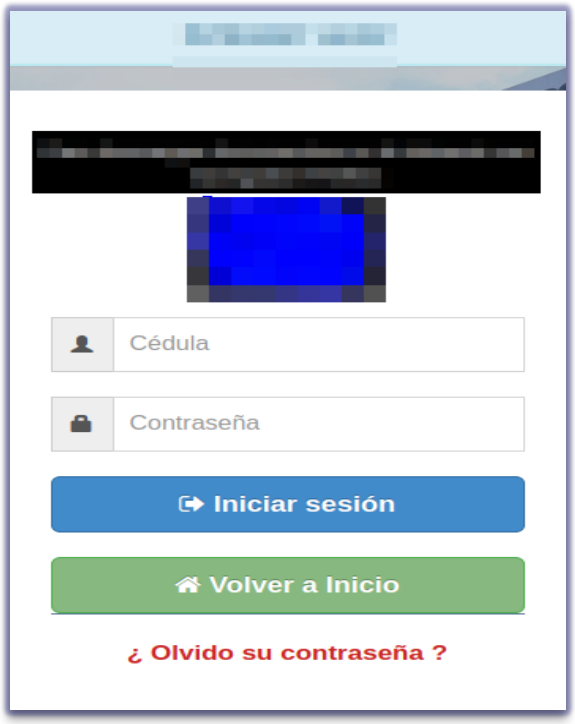
Herramientas de seguridad

En este caso se va a realizar un ataque de denegación de servicio (DoS) para que se vuelva inaccesible a la página web clonada, el objetivo principal es interrumpir el funcionamiento normal del servicio, causando una caída temporal o, en algunos casos, prolongada del mismo, para ello vamos a utilizar las siguientes herramientas:

- Navegador
- Foxy Proxy
- Burp Suite

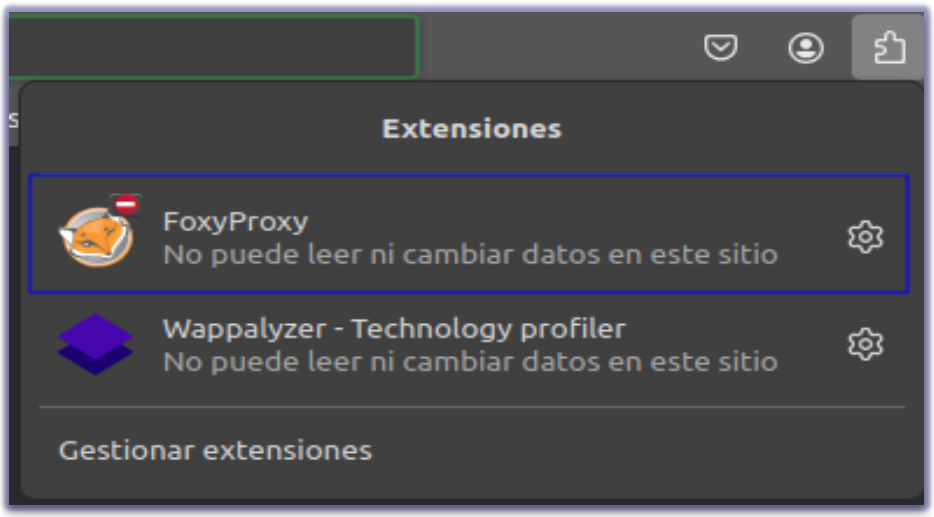
Estas herramientas se las puede instalar dentro de una maquina Linux Kali o algún otro sistema operativo Linux, dentro del mismo instalar un navegador como Firefox, Burp Suite Community Edition y el plugin Foxy Proxy.

Instaladas las herramientas debemos tener el objetivo, en este caso la página web clonada como se ve en la siguiente figura.



Foxy Proxy

Instalado el plugin Foxy Proxy en el navegador nos dirigimos a las extensiones que esta en la parte superior derecha del navegador Firefox para configurar nuestro proxy.



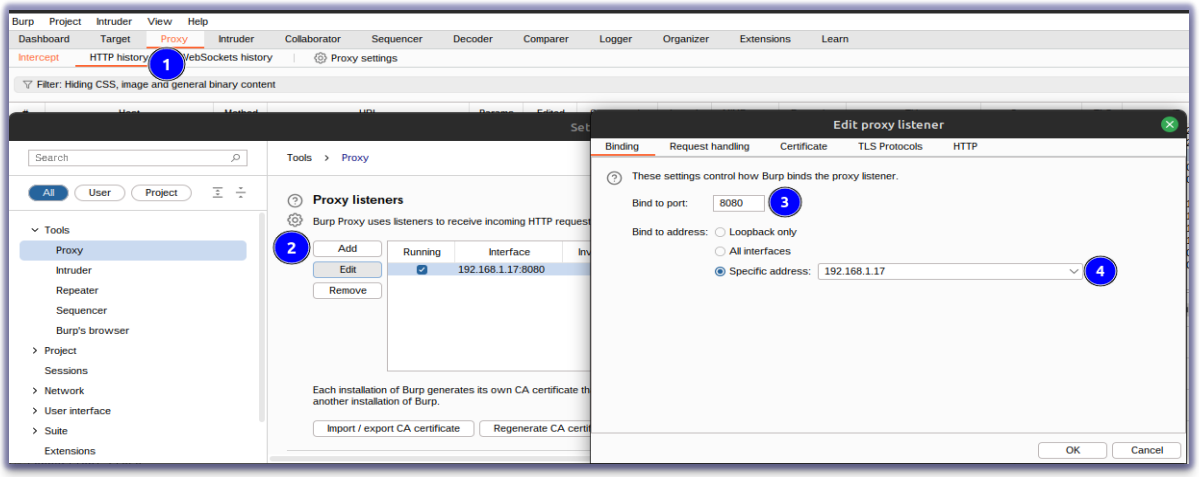
Dentro de la extensión dar clic en Opciones para configurar nuestro proxy con el que se va a trabajar para capturar el tráfico de la página web clonada.

Ingresamos en la pestaña Proxies, luego damos clic en el botón Añadir, ingresamos un nombre, ingresamos el hostname en este caso sería la ip de la maquina local con la que se va a trabajar, por último, ingresamos el puerto y guardamos la configuración.

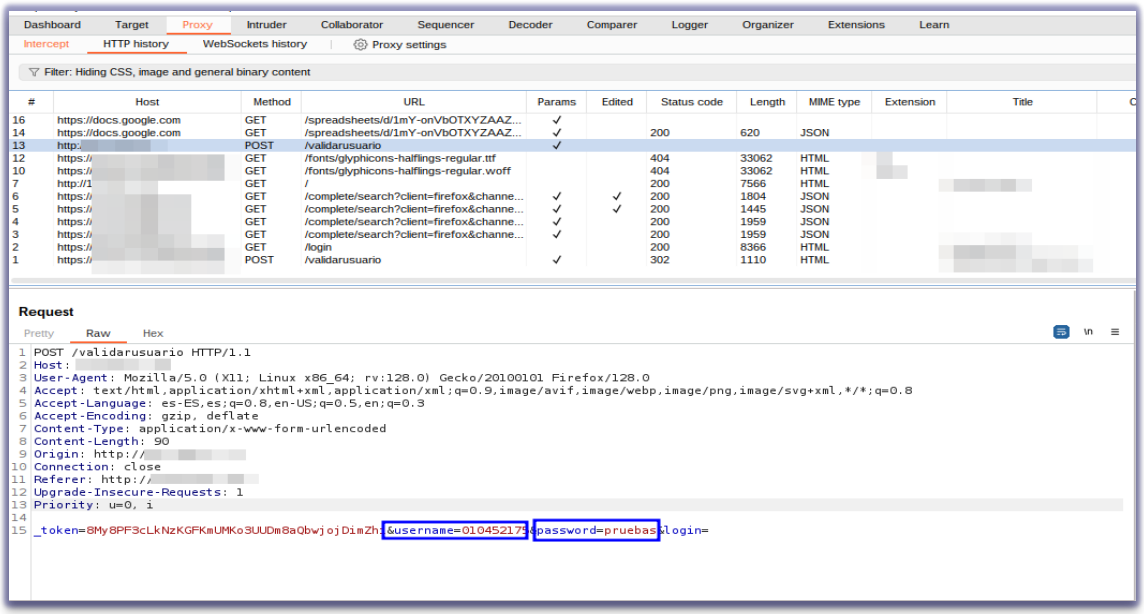
Una vez configurado nuestro proxy en el navegador, seleccionamos Equipo local.

Burp Suite

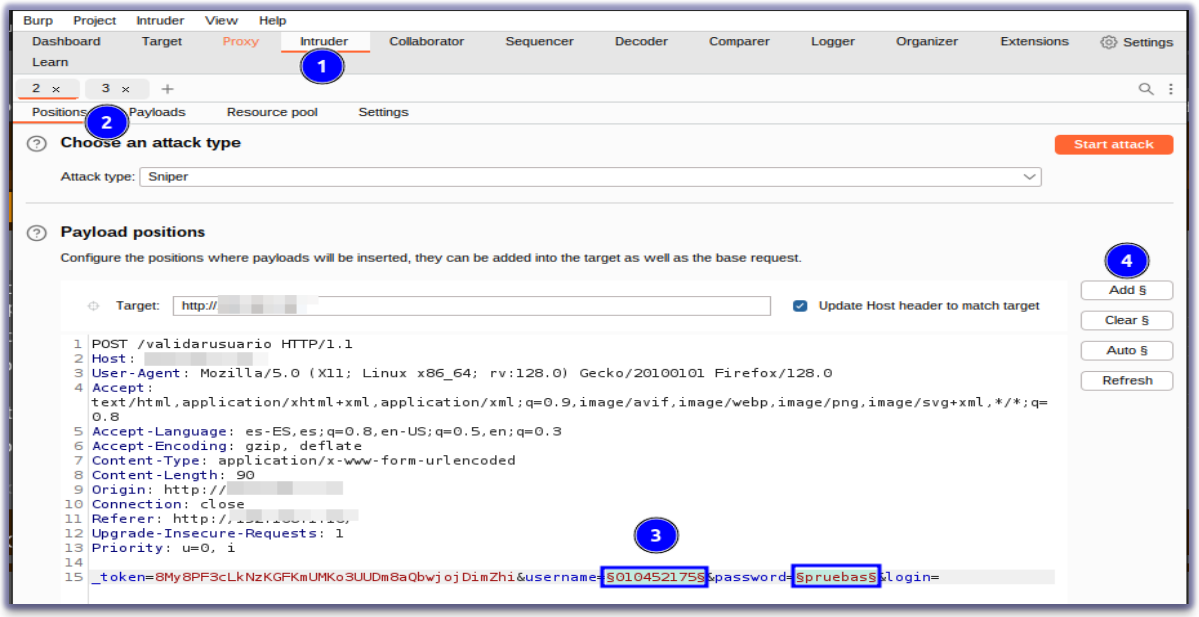
Dentro de la herramienta Burp Suite, es necesario configurar el proxy. Para ello, acceder a la pestaña "Proxy" y hacer clic en el botón "Add" para ingresar el puerto y la dirección IP de tu equipo, de manera similar cómo se realizó en la extensión FoxyProxy. Este proceso se muestra en la siguiente figura.



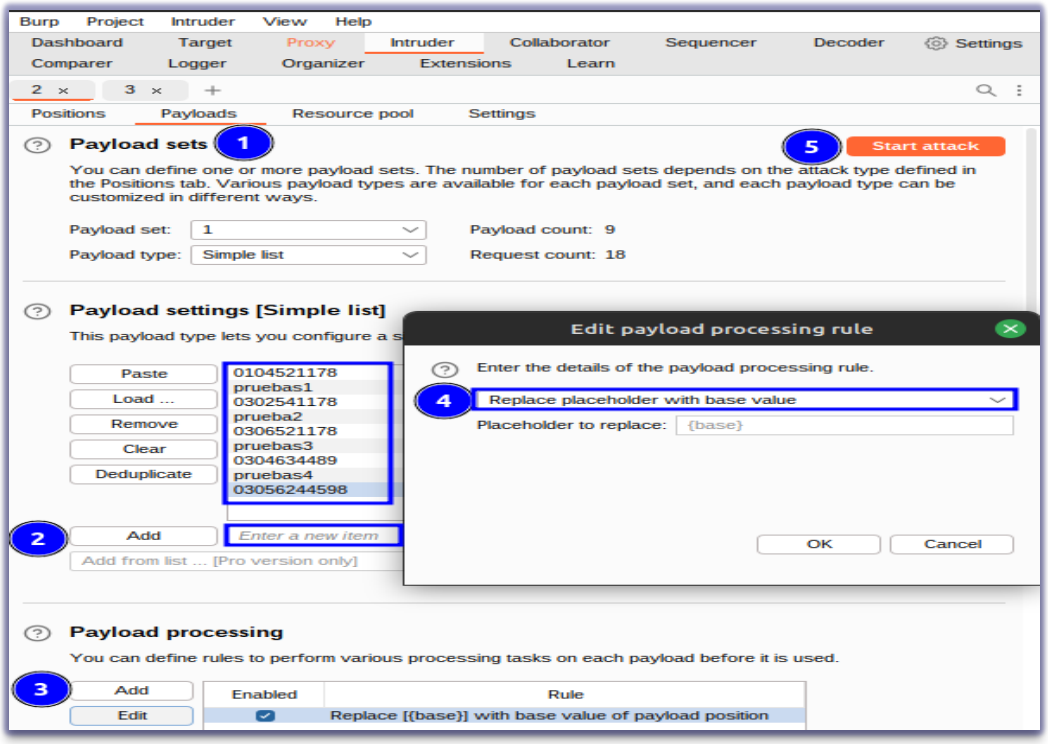
Configurado el proxy, es necesario capturar el tráfico. Esto implica interactuar con la página web clonada, ingresando datos como el nombre de usuario y la contraseña. De esta manera, se puede identificar el método en el que se capturan estos datos, tal como se muestra en la siguiente figura.



Una vez que se ha capturado el método que contiene los datos, hacer clic derecho y seleccionar la opción "Enviar a Intruder". Dentro de Intruder, dirigirse a la pestaña "Positions" para agregar un nuevo Payload. Para ello, primero seleccionar con el ratón el resultado del campo "username", que en este caso corresponde al número de cédula, y luego hacer clic en el botón "Add". A continuación, seleccionar de la misma manera el campo "password", que en este contexto corresponde a la contraseña utilizada “pruebas”. El proceso se muestra en la siguiente figura.

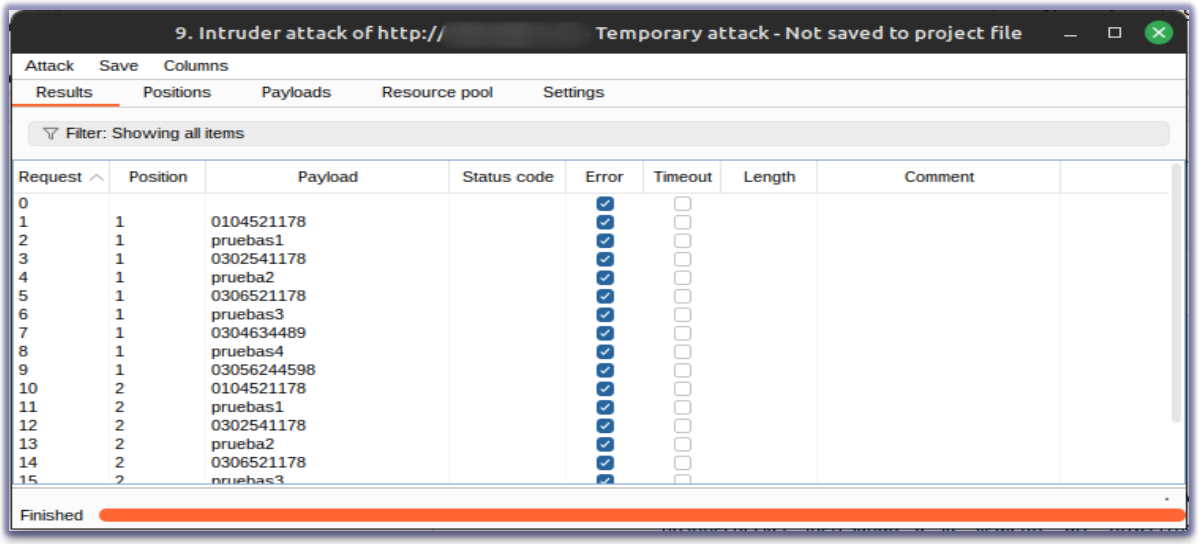


Ingresados los campos necesarios, acceder a la pestaña "Payloads" para ingresar los valores correspondientes, como el nombre de usuario y la contraseña, los cuales pueden ser configurados según se requiera. Ahora dirigirse a la sección "Payload Processing" para añadir la regla de procesamiento de la carga útil. Finalmente, proceder con el ataque haciendo clic en "Start Attack". Este proceso se muestra en la siguiente figura.



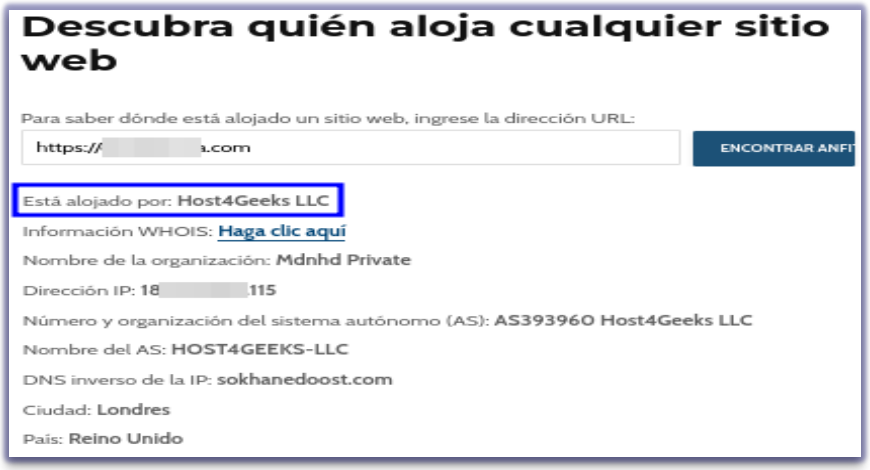
Finalmente, se visualizarán los resultados del ataque. Este proceso puede repetirse tantas veces como sea necesario o hasta que la herramienta lo permita, teniendo en cuenta que se

está utilizando la versión Community Edition. Este procedimiento puede ser un punto de partida eficaz para contrarrestar los ataques fraudulentos de los ciberdelincuentes. Al detectar el ataque, los atacantes podrían optar por desactivar el servicio, cambiar a otra página, o hacer que la página web clonada sea inaccesible. El objetivo principal es interrumpir el funcionamiento normal del servicio, lo que podría ayudar a prevenir que más personas caigan en sus estafas.



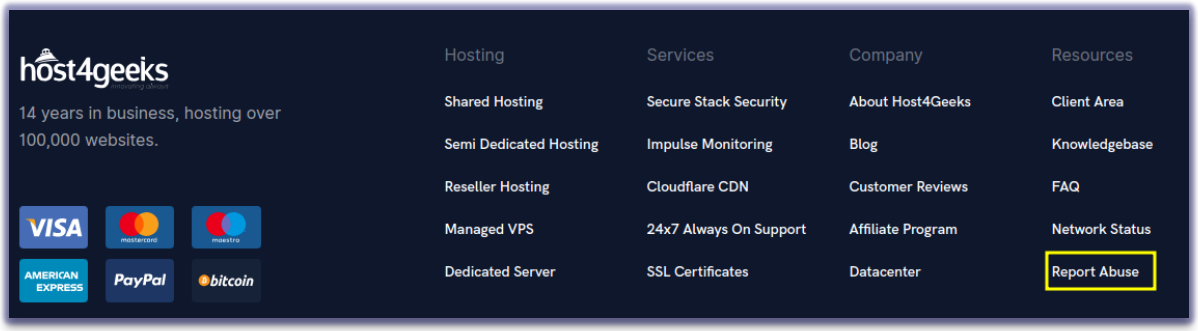
Proveedor de hosting

- Investigar donde esta alojada la página, para ello podríamos ayudarnos con la herramienta hostingchecker ingresando a la siguiente url: https://hostingchecker.com/, donde ingresaríamos el dominio que se está usando para clonar la página, para que nos dé el nombre donde esta alojada la página.

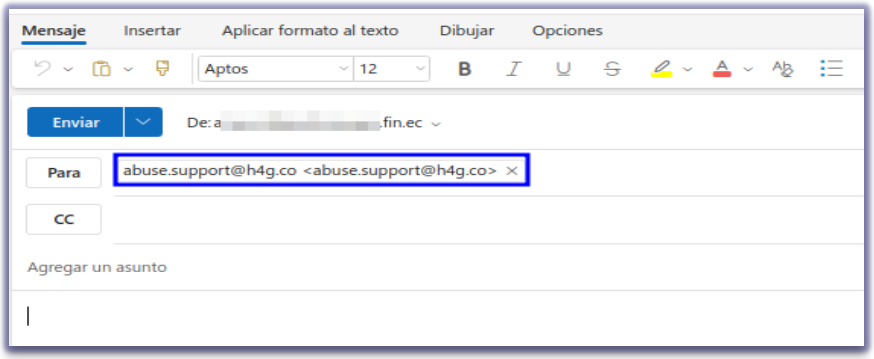


- Contactar al proveedor de Hosting.

Acceder a la página oficial del proveedor del hosting y buscar la sección destinada a reclamos o soporte técnico. Dependiendo del proveedor, el reclamo puede realizarse a través de un correo electrónico o llenando un formulario en línea.



- En caso de reclamo por correo electrónico.
    - Redactar un correo electrónico dirigido al proveedor, cuando se selecciona la opción "Report Abuse", al hacer clic, se redirige automáticamente a la dirección de correo de la empresa.



    - Incluir en el correo toda la información relevante:

      Asunto: Reporte de Suplantación de Identidad - [nombre del dominio].
      Cuerpo del correo: Describir detalladamente la situación, incluyendo la URL del dominio, capturas de pantalla y cualquier otra evidencia que se tenga.

- En caso de reclamo mediante formulario.
    - Completar toda la información solicitada en el formulario del proveedor de hosting, asegurándose de proporcionar detalles como la URL del dominio, la descripción del problema y cualquier evidencia adicional requerida.

- Respuesta del proveedor

  De igual manera, el proveedor de hosting enviará cualquier respuesta a la dirección de correo electrónico proporcionada. En su respuesta, detallará si necesita información adicional para validar el reclamo o si ha decidido proceder con la eliminación del contenido por incumplimiento de sus políticas.

Reporte a Google

a. Urls para reportar las páginas web clonadas.

Para realizar el reporte de las páginas web clonadas se debe ingresar en las siguientes URLs:

https://safebrowsing.google.com/safebrowsing/report_phish/?hl=en

https://search.google.com/search-console/report-spam?hl=es

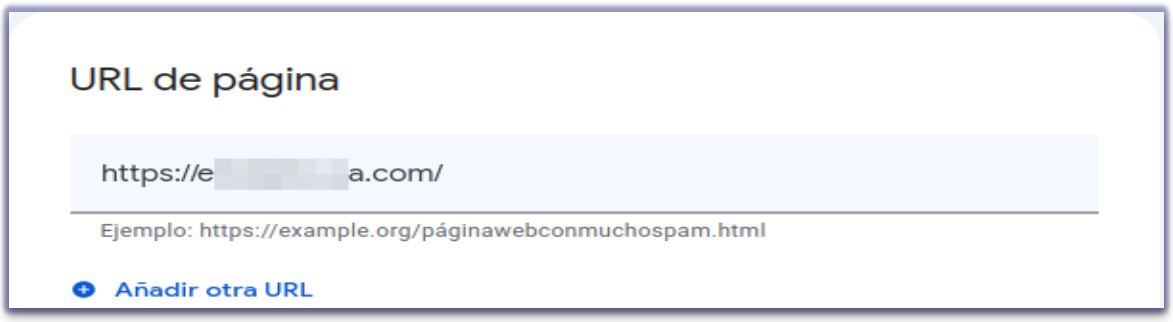
b. Primera Url: Reporte de Phishing

En el primer enlace, se debe ingresar la URL de la página web clonada. En el reporte, es crucial proporcionar todos los detalles relevantes sobre la página, explicando que está siendo utilizada para robar información personal y cometer fraudes. Es importante destacar que este reporte debe enviarse varias veces para que Google lo considere como una prioridad y proceda a su validación.

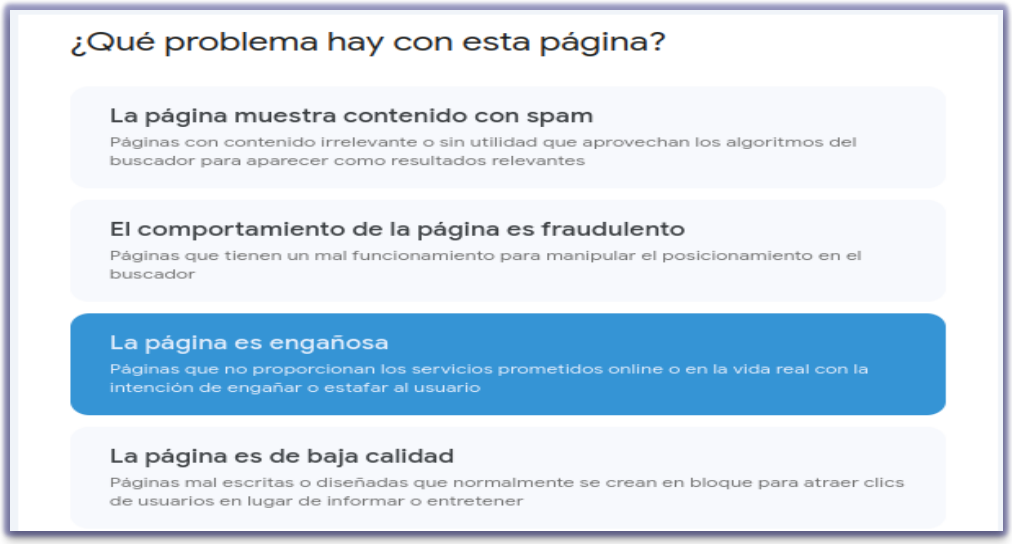
c. Segunda Url: Contenido fraudulento, engañoso o de baja calidad

Para reportar el contenido fraudulento en este enlace se debe ingresar la siguiente información:

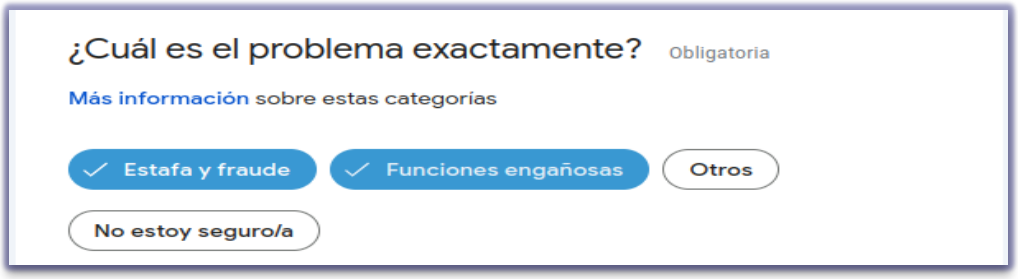
- Url de la página web clonada.



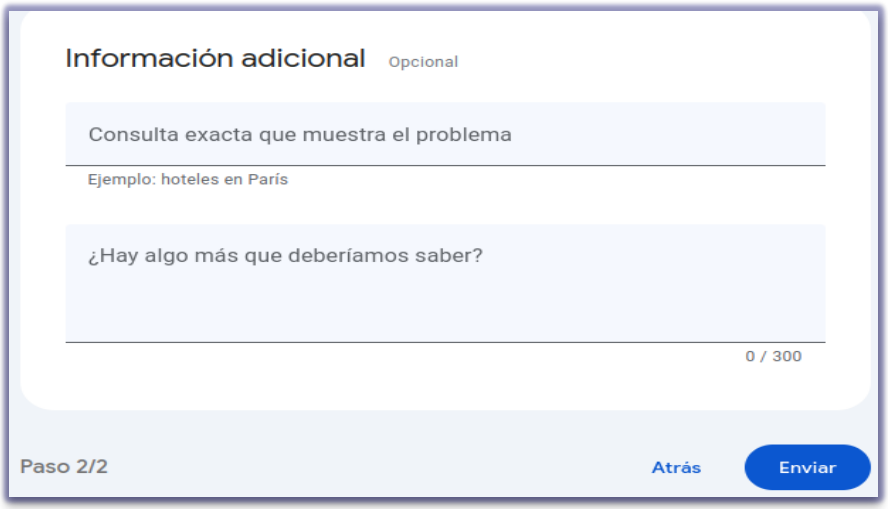
- Seleccionar que problema hay con esta página, en este caso seleccionar “La página es engañosa.



- Seleccionar cual es el problema exactamente, en este caso seleccionar “Estafa y fraude y Funciones engañosas”.



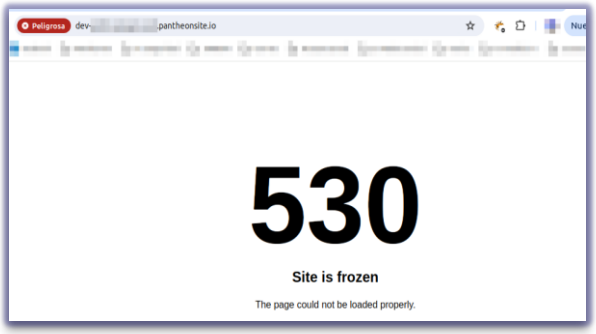
- Ingresar información adicional y enviar el formulario.

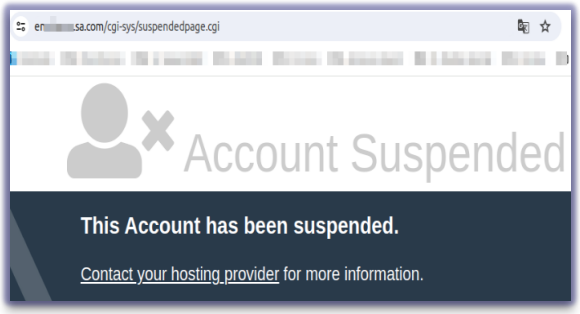


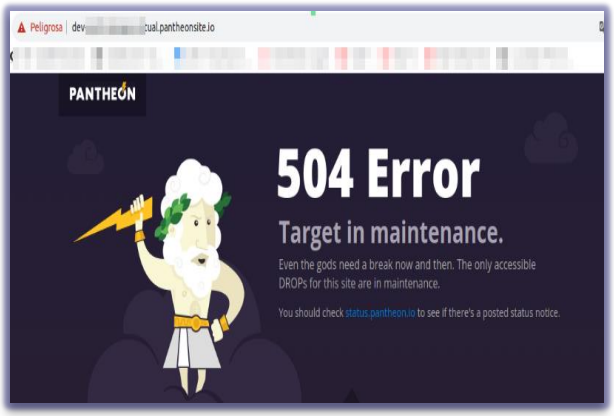
Una vez enviado el reporte, se recibirá una notificación al correo personal de Gmail confirmando que se ha enviado un informe de usuario sobre la calidad de la Búsqueda.

Validación de páginas web clonadas

Una vez que se han completado los reportes indicados y se han recibido las respuestas correspondientes, es fundamental proceder con la validación de los resultados. Es importante tener en cuenta que no siempre se recibirá una notificación clara indicando que la página ha sido dada de baja o eliminada. Por lo tanto, es necesario estar atentos y verificar directamente la URL que fue reportada, de esa manera se podría visualizar los siguientes mensajes:







ANEXO 6: Modelo de correo electrónico

Asunto: Reporte de Suplantación de Identidad "**nombre del dominio**"

Cuerpo del mensaje:

Estimado equipo de (**nombre de la empresa que tiene alojado el dominio**),

Me dirijo a ustedes para reportar que el dominio (**nombre del dominio**) alojado en sus servidores está suplantando la identidad de la institución a la que represento "**nombre de la cooperativa**".

Adjunto a este correo capturas de pantalla, registro de marca y una descripción detallada de la actividad fraudulenta.

Detalle de la actividad fraudulenta.

_____

_____

Agradecería que investiguen este asunto y tomen las medidas necesarias para suspender este dominio, ya que está causando daño a la reputación de la institución y confusión entre nuestros clientes y socios.

Quedo a su disposición para proporcionar cualquier información adicional que necesiten.

Atentamente,

(Nombre)

(Cargo)

(Nombre de la institución)

ANEXO 7: Validación de especialistas

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Leandro Damian Quezada Ochoa
Título obtenido: Magister en Seguridad Informática
C.I.: 0105073175
E-mail: l.quezadao@jardinazuayo.fin.ec
Institución de Trabajo: Jardín Azuayo
Cargo: Responsable de Seguridad Informática
Años de experiencia en el área: 4

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador.

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad	**X**				
Novedad	**X**				
Fundamentación pedagógica	**X**				
Fundamentación tecnológica	**X**				
Indicaciones para su uso	**X**				
TOTAL	**35**				

Observaciones: De acuerdo con lo expuesto, la investigación aborda un tema de gran relevancia en la actualidad, dado que los ataques fraudulentos son una amenaza constante. Esta guía proporciona un procedimiento para que las cooperativas puedan tomar acciones rápidas y efectivas para contrarrestar estos ataques, sin depender exclusivamente de proveedores externos. De esta manera, no solo se reducen costos adicionales, sino que también se fortalece la confianza de los socios y clientes en la seguridad de la cooperativa.

Recomendaciones: Tener en cuenta que un componente clave para la protección de marca es educar a los socios o clientes y empleados de las cooperativas sobre cómo identificar y reportar fraudes. La concienciación sobre las tácticas comunes utilizadas por los ciberdelincuentes puede reducir significativamente el impacto de estos ataques.

Lugar, fecha de validación: Cuenca, 22 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

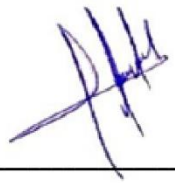
En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.



Firma del especialista
Ing. Leandro Damian Quezada Ochoa. MSc

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Byron Adrián Ortega Guillén
Título obtenido: Magister en Ciberseguridad NoReg: 1029-2022-2465496
C.I.: 002011960
E-mail: b.ortega@jardinazuayo.fin.ec
Institución de Trabajo: Jardín Azuayo
Cargo: Especialista en Administración de Aplicaciones
Años de experiencia en el área: 3

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador.

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad	**X**				
Novedad	**X**				
Fundamentación pedagógica	**X**				
Fundamentación tecnológica	**X**				
Indicaciones para su uso	**X**				
TOTAL	**35**				

Observaciones: De acuerdo con lo expuesto, la investigación aborda un tema de gran relevancia en la actualidad, dado que los ataques fraudulentos son una amenaza constante. Esta guía proporciona un procedimiento para que las cooperativas puedan tomar acciones rápidas y efectivas para contrarrestar estos ataques, sin depender exclusivamente de proveedores externos. De esta manera, no solo se reducen costos adicionales, sino que también se fortalece la confianza de los socios y clientes en la seguridad de la cooperativa.

Recomendaciones: Tener en cuenta que un componente clave para la protección de marca es educar a los socios o clientes y empleados de las cooperativas sobre cómo identificar y reportar fraudes. La concienciación sobre las tácticas comunes utilizadas por los ciberdelincuentes puede reducir significativamente el impacto de estos ataques.

Lugar, fecha de validación: Cuenca, 26 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

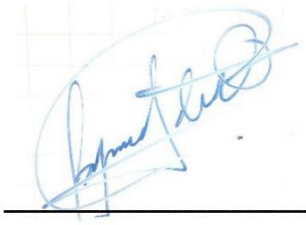
En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.



Firma del especialista
Ing. Byron Adrian Ortega Guillén Mg.

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Paúl Zhañay Ledesma
Título obtenido: Magister en Seguridad Informática
C.I.: 0102807807
E-mail: h.zhanay@jardinazuayo.fin.ec
Institución de Trabajo: Jardín Azuayo
Cargo: Responsable de Seguridad Informática
Años de experiencia en el área: 7

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.

- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Guía para la protección de marca frente ataques fraudulentos para Cooperativas de Ahorro y Crédito del Ecuador.

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad	**X**				
Novedad	**X**				
Fundamentación pedagógica	**X**				
Fundamentación tecnológica	**X**				
Indicaciones para su uso	**X**				
TOTAL	**35**				

Observaciones: La protección de marca es uno de los principales objetivos que debe implementarse en las instituciones ya que a través de una adecuada gestión de los eventos de suplantación se garantiza que los servicios ofrecidos a las personas son en verdad los que se promocionan. La guía es de mucha ayuda ya que establece los pasos que deben aplicarse para la protección de la marca de cualquier institución de una manera organizada ante alguno de los eventos que se describen en esta guía.

Recomendaciones: Los pasos descritos en la presente guía están establecidos con las situaciones que son factibles aplicar en la actualidad. Sin embargo, es importante mantenerse actualizado de los diferentes tipos de ataques en cuanto a suplantación se refiere y así mismo analizar las mejores maneras de proceder para mitigarlos con las condiciones también establecidas por los sitios hosting y de redes sociales con el objetivo de garantizar tanto el tiempo de respuesta como la protección.

Lugar, fecha de validación: Cuenca, 30 de agosto de 2024

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto protecciondatospersonales@uisrael.edu.ec es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo protecciondatospersonales@uisrael.edu.ec.

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: Política de Protección de Datos Personales | UISRAEL

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.

Firmado electrónicamente por:
HENRY PAUL ZHANAY LEDESMA

Firma del especialista
Ing. Paul Zhañay Ledesma. MSc